The SIM card as control point for Mobile Network Operators

A secure means for mobile authentication and identification services

Joan Sebastiaan Blok
Student number: 1510622
Faculty of Technology, Policy and Management
TU Delft

Keywords: Authentication, Identification, Control points, Value networks, SIM card

Graduation committee

Chair:	**Prof.dr. Y. Tan**
Officious chair:	**Prof.dr. W.A.G.A. Bouwman**
1st supervisor:	**Dr.ir. G.A. de Reuver**
2nd supervisor:	**Prof.dr. M.J.G. van Eeten**
Officious 2nd supervisor:	**Dr.ir. C. H. Ganan**
UL supervisor:	**T. Janssen MSc.**

Abstract

The SIM is able to function as a Secure Element (SE), which can securely store applications and credentials while providing a secure execution of the applications. This means that the SIM can provide secure authentication and identification for all kinds of online and offline services. However, there are alternatives in the market that offer similar functionalities as the SIM. The introduction of cloud-based solutions and embedded SEs has weakened the strategic position of the SIM in regard to providing mobile authentication and identification services.

This report aimed to identify markets where Mobile Network Operators (MNOs) could exploit the SIM as an authentication and identification means. As such, this study applies the concept of control points. The concept helps to identify possible profitable sources of revenue by mapping positions of economic power. Control points can be seen as functional areas where power can be exercised within value networks. Control points explain why and how members of the value network can extract value. Therefore, if the SIM would qualify as a control point, it should be able to generate revenue to MNOs. Based on this, the following research question was formulated:

> *Does the SIM card qualify as a control point, which can be exploited by MNOs beyond authentication and identification services?*

During this research three markets were identified where the SIM could possibly be of value by providing authentication and identification for online as well as offline services:

- Enterprise ID. Requires authentication and identification to allow employees access to company assets.
- Mobile payment. Requires authentication and identification of the user to authorize payment transactions.
- Government services. Requires authentication and identification of citizens.

To determine whether the SIM could qualify as a control point in these markets, semi-structured interviews have been conducted with industry experts related to mobile authentication and identification and the three application markets. The interviews were analysed to identify whether the SIM could meet the control point criteria in the three markets. The criteria are as follows. First, is that the value networks are viable, as control points exist within value networks. Next to that, the following criteria can be used to define and evaluate a control point:

- *Interchangeable or scarcity:* The ease by which alternative players can own a similar control point asset
- *Demand:* The extent to which a control point is accessed by players within a value network.
- *Value:* The amount of tangible and intangible value that a control point is able to capture.
- *Time*: Affecting the other parameters, as they are dynamic and may change over time.

Based on the interviews, it was concluded that the SIM would not qualify as a control point in the Enterprise ID market. It is not likely that there is a business case for SIM-based authentication and identification in this market. High investment costs and the inability to replace existing authentication and identification systems, as not all handsets are suitable to provide mobile authentication and identification services, are seen as barriers for a business case.

For mobile payments, it was concluded that there is business case for mobile authentication and identification services. The SIM scored well on the control point criteria, mainly due to the unique combination of three characteristics. The SIM is secure and standardized. Next to that, the SIM has reach among potential mobile payment users. However, the research showed that viability of the value network is not considered to be high. Most of the respondents did not find it likely that there is a role for MNOs in mobile payment, as they argued that for banks it is difficult to collaborate with

MNOs. The reason for this is that MNOs focus on control of the customer. Next to that cultural differences with banks play a role. Besides, banks are not dependent of the SIM technology, as there are alternatives in the market that could meet their needs. Banks do still consider the SIM as an option, but only if it is offered for the right price and if they are allowed to issue their own mobile wallet. One MNO seemed to comply with these requirements and therefore there is still a possibility that the value network would occur. This means that there is possibility that the SIM could qualify as control point.

Finally, the government market was assessed. This showed that there are no use-cases for storing driver's licenses or ID cards on the SIM in the next couple of years, as law changes are required. However, the development of the Dutch eID scheme was marked as a possible opportunity. This is a new standard for online identification that is being developed by the Dutch government in cooperation with the business sector. This standard allows users to login with authentication and identification means offered by private organizations. Based on the interviews, it showed that the SIM technology is able to comply with the needs of the eID scheme and therefore it scores well on the control point criteria. Similar to mobile payment, security, standardization and reach were marked as key drivers for demand and value in this market. However, a barrier for the SIM to qualify as control point is that MNOs have to upgrade their enrolment procedure to ensure that the SIM can verify a person's identity. This means that the SIM must be linked to a person during a physical meeting, in order to comply with the eID requirements. Furthermore, the eID scheme is still under development and therefore the revenue model is uncertain. This leads to hesitation among MNOs to join the scheme. Therefore the answer remains indefinite whether the SIM could qualify as control point. However, the SIM technology is suitable to provide authentication and identification in the eID scheme.

From a practical perspective, this research identifies possible opportunities for MNOs to provide mobile authentication and identification services. It shows that the SIM can be added value in the markets of mobile payment and in the eID scheme. However, there are a number of barriers that MNOs should overcome before they can exploit the SIM. Examples are lowering the costs for the SIM in mobile payment and upgrading the enrolment procedure for eID services.

The main theoretical contribution of this research comes from the application of the control point concept. Overall, this research shows that the concept of control points helps to explain the added value of the SIM for mobile authentication and identification services. However, this research showed that the emergence of a value network could be a barrier for the existence of a control point. Therefore this research proposes that for future studies first the viability of the value network is researched. If that is the case, then the control point's concept can be used to determine how much value an organization can extract from the value network. Based on these findings, this research proposes further research on how the viability of value networks can be assessed.

In relation to that, it was concluded that control points are not suitable to determine whether a resource can be exploited in value networks that are bound to uncertainties. However, the concept could possibly be applied to evaluate control points in existing value networks. It could help to identify positions of power in existing value networks. With this in mind, it is proposed that case studies are conducted in which the concept of control point is applied to existing value networks. This should lead to empirical data and help in the further development of the concept.

Table of Contents

List of figures

List of tables

1. Introduction

In this chapter the research problem is introduced. The research problem is defined by describing different aspects of the problem. First, the practical problem is explained which is followed by the scientific problem. Next, the research objective is discussed and this leads to the research questions. This followed by explaining the scientific and practical relevance of this research. The research approach is discussed in section 1.5. Finally, the outline of the thesis is introduced.

1.1 Practical problem

Mobile Network Operators (MNOs) are facing difficult times. Currently their revenues are declining, as the use of SMS and regular phone calls are being replaced by over-the-top (OTT) services such as Whatsapp and Viber. Forecasts show an expectation of a 1.5 per cent revenue decrease per year for mobile networks in Europe in the coming decade (ATKearney, 2013). These forecasts do not show a bright economic future for MNOs and therefore they are looking for new sources of revenue in the form of new services that they can offer to market.

An asset of MNOs is that they own the Subscriber Identity Module (SIM) card, which is used to identify and authenticate devices such as mobile handsets. The SIM card is a tamper resistant independent part of the mobile phone which can become a trusted entity guarding personal information and identifying each user (Mantoro & Milisic, 2010). The SIM card, in the form of a Universal Integrated Circuit Card (UICC) can take over functions of plastic smartcards since it is able to hold a number of applications (Jaemin, Kyoungtae, & Minjeong, 2008). This makes the SIM potentially valuable to the MNO since the SIM can be used for different services for which the technical infrastructure does not need to differ much. The SIM card can be used for services such as ID, bank card, bus ticket or even a security element that confirms a person's identity without the need to introduce new hardware elements in the mobile handset (Mantoro & Milisic, 2010). The SIM is a means that MNOs can manage and control freely (Jaemin et al., 2008), which "opens the door" for MNOs to exploit the SIM's authentication en identification qualities.

One service that MNOs have tried to develop is mobile payment, as it requires secure authentication and identification. Mobile payment can be defined as *"the use of a mobile device to conduct a payment transaction in which money or funds are transferred from payer to receiver via an intermediary, or directly, without an intermediary"* (Mallat, 2007, p. 3). For NFC-enabled mobile payments, a Secure Element (SE) is needed to ensure a safe transaction. A SE stores applications and credentials, while providing a secure execution of the applications (Smart Card Alliance, 2014b). The SE is a critical component since it ensures that transactions are protected from unauthorized data access (GSMA & Booz & Co, 2011). The SIM card, a cloud-based solution, an embedded element in the handset or a microSD are all technical solutions that can serve as SE. The benefit of the SIM card is that it is one of the safest and secure options (GSMA & Booz & Co, 2011; Madlmayr et al., 2007; Pannifer, Clark, & Birch, 2014). The SIM card is thus able to securely store an application and this implies that it can be of added value for authentication and identification services that require a high level of security.

The mobile payment initiatives, in which the SIM is used as a SE, show that there are opportunities for MNOs to use the SIM for security purposes. However, the results of the mobile payment initiatives by the MNOs are mixed. In South Korea and Japan mobile payment solutions have reached the market (Gaur & Ondrus, 2012), while in the Netherlands a collaboration between banks and MNOs was dissolved (De Reuver, Verschuur, Nikayin, Cerpa, & Bouwman, 2014). A possible reason for the mixed results could be the complexity of the market. The mobile payment ecosystem is complex since it consists of many stakeholders with different interests (Au & Kauffman, 2008; De Reuver et al., 2014). The limited success in mobile payments and the introduction of alternatives for SIM based security (i.e. cloud-based solutions and embedded SE) have weakened the position of

MNOs. Apple introduced Apple pay which uses an embedded SE, while the release of Android KitKat enabled Host Card Emulation (HCE) (Android Developers, 2014; Marwaha, 2014). HCE uses the cloud as secure environment rather than a physical SE. So, for both solutions the SIM is not needed. However, in a cloud-based solution the SIM could be used to authenticate to the cloud since the mobile device should be identified to ensure safe transactions. The high level of security that the SIM offers can be value adding in such a system. Even though a cloud-based solution is an alternative for the SIM, it could also prove to be an opportunity for the SIM as an authentication and identification means.

As the SIM is available in every phone, it could be a real asset to MNOs. However, the development of embedded SIMs threatens the existence of the SIM card in its current form. An embedded SIM can serve as an alternative for the original SIM card (ABI research, 2014; Wireless Watch, 2014). GSMA (2013a, p. 1) states that "the embedded SIM specification is designed to enable the remote provisioning and management of operator profiles within soldered and inaccessible SIMs to facilitate simple and scalable connection of an array of new mobile connected products." Although embedded SIMs allow MNOs to connect more devices (e.g. internet of things), the deployment can be a threat for SIM based security services (ABI research, 2014; Wireless Watch, 2014). Handset manufacturers are able to replace the original SIM with an embedded SIM, which means that MNOs will lose ownership of the SIM as hardware asset in the handset (Jaemin, Kiyoung, & Cheoloh, 2013). To prevent this replacement, MNOs can try to increase the dependency of other parties of the SIM by offering SIM based authentication and identification services. This increase in dependency could lead to a higher threshold for handset manufacturers to replace the SIM with an embedded SIM. Ensuring that the SIM will remain part of the handset could be a motivation for MNOs to offer SIM based security services to other businesses, as it increases the need for the SIM.

In summary, the practical problem is that the SIM card could prove to be a valuable asset for MNOs to provide authentication and identification for services that require a high level of security. However, the necessity for the SIMs presence is becoming less due to the introduction of different alternatives in the market (e.g. alternative SE or embedded SIM). Therefore the focus in this research is on how MNOs can exploit the SIMs authentication and identification qualities in such a way that the dependency of the SIM can be increased to increase the threshold for handset manufacturers to replace the SIM with an embedded SIM.

1.2 Scientific problem

In order for MNOs to exploit the SIM they must collaborate with other organizations, as Bouwman, De Vos, and Haaker (2008) argue that a service cannot be offered by a single company and that a number of companies have to work together to create and deliver a service. This can be seen in relation to Pfeffer and Salancik (1978), who introduced the Resource Dependence Theory (RDT). They explain that organizations cannot own all resources and capabilities needed for its business but they can have access to resources of other firms, which creates interdependency (Pfeffer & Salancik, 1978). This means that MNOs have to collaborate with other organizations when offering authentication and identification services and that, based on the RDT, the SIM could possibly be a reason for other firms to collaborate with MNOs.

According to Allee (2000), organizations involved in developing and offering mobile services work together in a value network. The concept of value networks has been widely discussed and applied in the scientific literature (Allee, 2000, 2008; Ballon, 2009a; De Reuver, 2009; Li & Whalley, 2002; Normann & Ramirez, 1993). Value networks help to analyse how actors exchange tangible and intangible assets to contribute to a product or service offering. According to De Reuver (2009, p. 12) value networks can be defined as *"a dynamic network of actors working together to generate customer value and network value by means of a specific service offering, in which tangible and intangible value is value exchanged between the actors involved".* Value networks can be derived

from Porter's (1985) concept of value chains, which explained that at every point along the chain, one should add value to the product or service. In value networks the value-adding role can be described as *"when a role receives a value input, ideally people playing that role would find ways to use that input to provide greater value in the form of products and services"* (Allee, 2008, p. 15). This quote shows that a value network is not a linear chain with consecutive in- and outputs but when participants receive an input they will try to add tangible and/or intangible value to the network. In this research, value networks can help to analyse how actors are involved with authentication and identification services.

The RDT shows that if MNOs want to exploit the SIM, it is key to determine if other parties in the value network require the SIM to conduct their business. MNOs can ask for financial compensation to allow firms access to the SIM as resource. This means that the SIM could be a source of economic power to the MNO. In this research the concept of control points is applied, as it can be used to determine positions of economic power for mobile services (Eaton, Elaluf-Calderwood, & Sorensen, 2010a). Control points can be defined to examine where and how members of the value network extract value. If the SIM would qualify as control point, it would be able to function as revenue source to MNOs. Eaton, Elaluf-Calderwood, and Sorensen (2010b) define control points as functional areas where power can be exercised within value networks. According to Ballon (2009a) and Kartseva, Hulstijn, Tan, and Gordijn (2006), power is manifested through control and can be operationalised through different patterns such as authorisation, confirmation and compensation. Based on Ouchi (1979), control can be defined as the design and improvement of mechanisms through which an organization can be managed, so that it moves towards its objectives. In a control point control is exerted through business, regulatory and/or technical means (Eaton et al., 2010a).

Control points are first discussed in a white paper of the Value Chain Dynamics Working Group, which is part of the MIT Communications Futures Program. They describe control points as a functional element within a business model where management can be applied (Trossen & Fine, 2005). An organization that can 'manage' a control point can decide who is allowed access and under what conditions. The strength of a control point, which can change over time, depends on its level of uniqueness, demand and value. Alternatives affect the power position of a control point owner, as the necessity for the control point decreases. An example of a value network with control points is when buying apps in Apple's app store. The end user has a control point because they are the source of revenue. Apple owns the App store, which is a control point because they have decision rights over what is allowed in the store (Eaton et al., 2010a). Another aspect that Trossen and Fine (2005) take into account is triggers. Triggers help to explain changes to the business model and its sustainability. Triggers are external factors that cause a transition from one set of control points to another (Trossen & Fine, 2005).

In order to identify where and how the SIM could qualify as control point, two steps can be used (Eaton et al., 2010b):

- The various actors and the analysis of interplay of their revenue models within the value network should be mapped.
- The control points should be analysed to identify where and how members of the value network can extract value.

According to Eaton et al. (2010a), the use of control points and triggers in value networks, is a promising way of analysing business models for mobile services because the concept helps to determine positions of economic power. Therefore this research applies the concept of control points to determine whether the SIM could be exploited as an authentication and identification means.

Based on findings in the discussed literature, a number of knowledge gaps are identified. Since cloud-based solutions have been recently introduced to the market, there is limited to no literature about this technical solution. Furthermore, there is lack of empirical data on the concept of control points and there is need to apply it to mobile services (Eaton et al., 2010a). There have been studies on value networks and the role of MNOs and the SIM card (De Reuver, de Koning, Bouwman, & Lemstra, 2009; M'Chirgui, 2009; Madlmayr et al., 2007; Markendahl, Smith, & Andersson, 2010). These studies discuss the power position of MNOs in different value networks and their relationship with involved actors. In these studies a central role for MNOs within value networks is discussed on the basis of the services that the MNO can provide. None of the studies focus on the SIM as resource that gives the MNO the ability to participate in the value networks. The amount of control and economic power that the SIM offers to MNOs within value networks has not been studied. A study on the SIM as control point can help in analysing the control and economic power that it offers to MNOs. There have been studies on control points for MNOs but none of these include an important role for the SIM nor do they focus on authentication and identification services (Cimiotti & Schonowski, 2010; Eaton et al., 2010b).

1.3 Research objective & questions

Based on the practical problem and scientific problem, the following research objective is formulated:

> *The objective of this research is to provide insight in whether MNOs can exploit the SIM for mobile authentication and identification services by applying the concept of control points*.

In order for MNOs to exploit the SIM it must qualify as control point, as this ensures that the SIM can capture value for the MNOs. As control points occur within value networks, a requirement for the SIM as control point is that the value network is viable. This means that the involved actors must be willing to cooperate to deliver the authentication and identification service to the end-user. Furthermore, the SIM must be of added value to other actors in the value network to serve as control point. Therefore the capabilities and the control parts of the SIM card are studied. This leads to insight on the value-adding role that the SIM can have for authentication and identification services. Next to that, alternatives for the SIM are researched. If adequate alternatives exist for the functions that the SIM could perform, it will have effect on the strength of the SIM as control point because it can be replaced. In order for the SIM to qualify as a control point it must provide economic power to the MNO and therefore be able to extract value from the value network. Based on this, the following research question is formulated:

> ***Does the SIM card qualify as a control point, which can be exploited by MNOs beyond authentication* and identification *services?***

To structure the research the main research question is decomposed in three sub questions. These sub questions should help in forming a comprehensive answer to the main research question.

1. *What are core concepts and theories related to control points?*
   In order to assess whether the SIM qualifies as control point, a comprehensive understanding of control points and related concepts and theories is needed. This provides insight where and under what conditions control points exist. Furthermore, criteria can identified that help to evaluate and define a control point.

2. *What are the capabilities and characteristics of the SIM and what are technical alternatives?*
   This question aims to map the technical capabilities of the SIM and how these could be of use for authentication and identification services. Answering this question will provide insight in the

functionalities that the SIM offers. Furthermore, alternatives for the SIM as authentication and identification means are discussed.

3. *What are application markets where the SIM could be of value as an authentication and identification means?*
   After answering sub question 2, an overview of the SIMs capabilities is acquired. By answering this question, the aim is to identify markets where the capabilities of the SIM could possibly be of value. These markets could be opportunities for MNOs to exploit the SIM.

4. *What is the viability of the SIM as control point for mobile authentication and identification services?*
   The markets identified by answering sub question 3, could be opportunities for MNOs to exploit the SIM. By answering this question insight is gained whether the SIM could qualify as a control point in these market and therefore be exploited by MNOs. Therefore knowledge and perspectives from practitioners are sought on whether they view the SIM as a viable option for mobile authentication and identification in these markets.

The research questions are answered using two research methods: literature review and interviews.

1.4 Societal and scientific relevance

The relevance of this research is twofold. From a societal point of view the research can give industry players insight in ways to exploit the strengths of the SIM card in regard to authentication and identification services. Furthermore, the research can help MNOs in forming new strategies. Different architecture designs in which the SIM plays a role are discussed on their business potential. It can help to identify what type of service is worthwhile to develop and set in the market by MNOs.

On a scientific level this research contributes to the further development of the concept of control points, as it is applied to a specific case (Eaton et al., 2010a). This research provides empirical data through interviews with industry experts. Next to that, this research focuses on the control and economic power that the SIM offers to MNOs within value networks and aims to determine whether the SIM gives MNOs the ability to participate in a value network.

1.5 Research approach

The first phase of the research consists of a literature review. During the literature review the core concepts related to control points are identified. This leads to criteria and conditions, which can help to assess whether the SIM qualifies as control point. With an obtained theoretical background, the control parts of the SIM (i.e. capabilities and characteristics) can be analysed to determine in which markets these could be of value. In order to provide scientific and practical value to this research academic literature and grey literature (e.g. white papers) is used.

Based on the literature review, existing value networks related to mobile authentication and identification are conceptualized to determine opportunities for the SIM and MNOs. These value networks help to identify possible applications for the SIM as authentication and identification means. The conceptualisation is used as input to design multiple value network architectures in which the SIM is defined as control point. These value networks are designed for different application markets where the SIM could possibly be of value.

All this serves as the foundation for interviews, where the designs are validated. Industry experts are interviewed to determine the viability of the value networks and the SIM as control point. Interviews will complement the literature review with real-world knowledge and perspectives from industry experts. The interviews shall follow a semi-structured approach in order to maintain an open view towards new insights and theories. The interviews shall be transcribed and analysed by making use

of coding. In total 15 - 20 interview candidates with backgrounds in mobile authentication and identification as well as the application markets will be consulted. A more extensive description of the interview methodology will follow in chapter 6. Figure 1-1 provides an overview of the research approach.

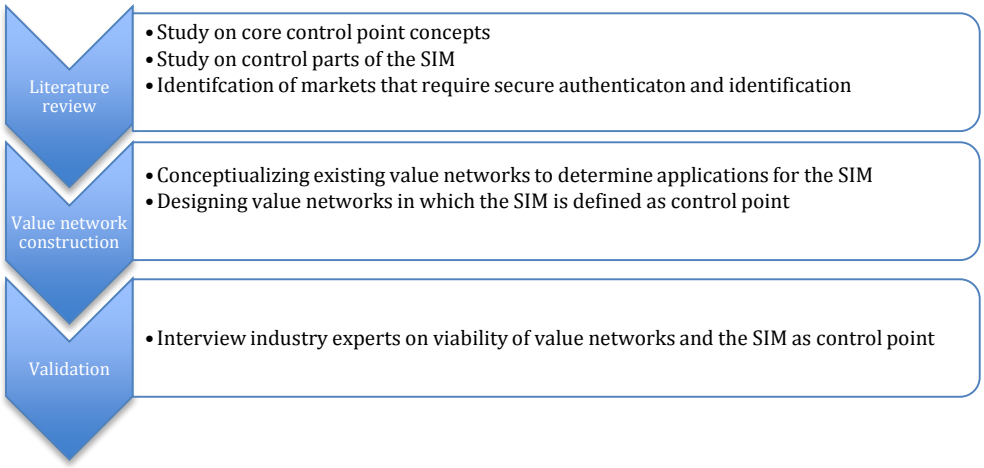


Figure 1-1: Research approach

1.6 Report structure

Based on the different research questions, the structure of this thesis is composed in a logical sequence as can be seen in Figure 1-2. The findings of each chapter will serve as input for the rest of the research, as is discussed below.

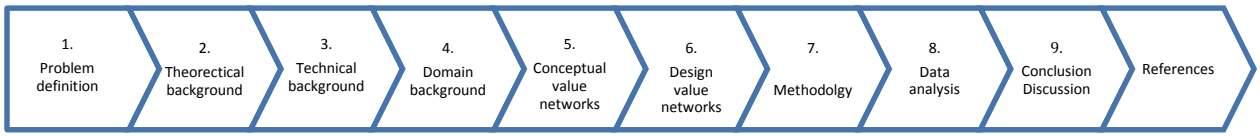


Figure 1-2: Report structure

Chapter 1: Problem definition
In chapter 1 the purpose and objective of this research is explained. This is followed by the main research question and the sub questions. Furthermore, the research approach and report structure are defined.

Chapter 2: Theoretical background
Chapter 2 discusses core concepts and theories related to control points.

Chapter 3: Technical background
Desk research and company expertise should lead to information on the technical background, which is discussed in chapter 3. This leads to an overview of the SIM's capabilities and its alternatives.

Chapter 4: Domain background
Desk research and company expertise should lead to information on the domain background. In this chapter different markets are discussed where the SIM could possibly be of value as an authentication and identification means.

Chapter 5: Conceptualization of value networks

Based on the findings in chapter 2 and 3, existing value networks related to mobile authentication and identification are conceptualized. This chapter identifies applications for the SIM as authentication and identification means.

Chapter 6: Design value networks
The conceptualized value networks will serve as input for the designs. The designs include the applications markets that have been identified in chapter 3.

Chapter 7: Methodology
In this chapter the proposed interview methodology is discussed. The interview questions will based on the insights gained on control points.

Chapter 8: Data analysis
In chapter 8 the data collected from the industry expert interviews is analysed and discussed.

Chapter 9: Conclusion and discussion
Chapter 9 discusses the conclusions, limitations of this research and presents recommendations for follow-up research.

2. Theoretical background

This chapter discusses the theoretical concepts related to value networks and control points. These concepts are relevant for this research as they can help in structuring the relations and power of involved actors. Value networks help in mapping the added value of the actors and the relations among them. By expanding value networks with the concept of control points the power that actors hold over each other are explored, which shows how they generate value. First, value networks are discussed. Second, control points are introduced and what they entail within value networks. Third, theories and concepts related to control points are discussed. Finally, a conclusion on the discussed concepts is given.

2.1 Value networks

As discussed in chapter 1, Pfeffer and Salancik (1978) argue that an organization cannot own all resources and capabilities needed for its business. Therefore organizations are dependent of other firm's resources, which means that they have to cooperate to create and deliver a service. Allee (2000) explains that organizations working together in the mobile service industry can be viewed as a value network, where goods, services, revenues, knowledge and intangible benefits are exchanged. Therefore this paragraph discusses the origin of value networks and explains why it is a useful concept for this research.

2.1.1 From value chain to value network

Value networks derive from Porter's (1985) concept of value chains. According to Kaplinsky and Morris (2001, p. 4) *" the value chain describes the full range of activities, which are required to bring a product or service from conception, through the different phases of production (involving a combination of physical transformation and the input of various producer services), delivery to final consumers, and final disposal after use*". Each link in the chain is supposed to add value to the product. Value chain analysis was developed to identify and build upon areas of competitive advantage by analysing value-adding activities across and within an organization (Porter, 1985). Kaplinsky and Morris (2001) extended value chain analysis to include across firms analysis to identify positions of economic power within an industry. A value chain is thus a linear set of static links that should add value to a product or service in each phase of the production.

Many modern industries can, however, not be seen as a linear chain of organizations (Hearn, Roodhouse, & Blakey, 2006). For instance, Li and Whalley (2002) argue that the telecommunication industry is more a series of intertwined value chains with nodes that are involved in multiple value chains. They explain that telecommunications is a competitive market where companies not only compete in a conventional way (linear chain) but also compete with companies from other industries that operate under different value propositions and economics. Another point of criticism is that to generate revenue the focus within value chains is on the exchange of tangible assets and that the flow of intangible assets is not considered (Allee, 2000, 2008). Intangible assets are becoming more important in today's economy and should therefore be included when describing and analysing networks (Allee, 2002). Examples of intangible assets are customer loyalty and strategic alliances. The criticism shows that the value chain concept cannot be applied to all industries and especially not to the telecommunications industry. Therefore the industry is viewed as a value network rather than a value chain. In this research the definition of De Reuver (2009, p. 12) on value networks is used, who describes value networks *as "a dynamic network of actors working together to generate customer value and network value by means of a specific service offering, in which tangible and intangible value is exchanged between the actors involved"*. This definition deals with the criticism on value chains as it includes as well tangible as intangible value and does not assume a linear chain of organizations.

2.1.2 Value network analysis

A value network can be seen as an economic mechanism that converts one form of value to another with the goal to deliver a specific service or product (Allee, 2008). By making use of various value constellations, actors have the ability to focus on their core competence to contribute to the value creation process rather than providing maximum value to customers on their own (Stabell & Fjeldstad, 1998). In a value network the value is the highest at the end point, where the consumer receives the final product (Basole & Rouse, 2008; Peppard & Rylander, 2006). Within the scientific literature different definitions of economic value are used (Allee, 2000; Eaton et al., 2010a; Peppard & Rylander, 2006; Porter, 1985; Woodard, 2008). Therefore there does not seem to be consensus on the definition. In this research the definition of Allee (2000) is used as it is concrete and helps to understand the relations among stakeholders. Allee (2000) defines the following value exchanges:

- Goods, services and revenue
- Knowledge
- Intangible benefits

This definition further specifies tangible and intangible value as it is used in definition of De Reuver (2009). An example of a value exchange is the purchase of a product. Goods are exchanged for money. Another example is a company take-over. In this case a fee is paid to acquire the knowledge and customer-base of a company. This example includes an exchange of all three classes of value. The examples show how value is converted, which is also the case within value networks.

Allee (2008) states that *"value network analysis offers a way to model, analyse, evaluate, and improve the capability of a business to convert both tangible and intangible assets into forms of negotiable value, and to realize greater value for itself".* Value networks describe the dynamics of work groups within a network and the role that each actor plays in the value creation process. A value network is ultimately defined by the customer and all parties within the network have to co-operate in order to deliver the needed value to the end customer (De Reuver, 2009; Peppard & Rylander, 2006). Hence, Basole and Rouse (2008) express that to use a network approach, one must understand whom the actors are but also understand the types and the extent of the relationships they have within the network. Bouwman, Faber, Haaker, Kijl, and De Reuver (2008) identify three types of participants within ICT value networks:

- *Structural or tier-1 partners*. These participants provide essential and non-substitutable tangible and/or tangible assets to the value network on an equity or non-equity basis. They play a direct and core role in determining the intended customer value and in creating the business model.
- *Contributing or tier-2 partners*. These participants provide goods and/or services to meet requirements that are specific to the value network. They do not play a direct role in determining the intended customer value and in creating the business model. The business model and intended customer value could remain intact if these assets are substituted.
- *Support or tier-3 partners.* These participants provide generic goods and services to the value network and are key for the viability of the value network. However, these goods and services could be used in connection with a wide variety of intended customer value and business models.

According to Bouwman, Faber, et al. (2008), structural partners are the core of the network, while contributing and support partners are loosely connected to the value network. This relates to Basole and Rouse (2008), who argue that the more central a firm is positioned within a value network, the more dependent other parties are and this leads to more control of a central firm.

In order to analyse the role of an actor and his value-adding contribution to the end service the value network must be mapped along with all the value in- and outflows (Allee, 2000). It essential that all

network aspects that can influence the value creation of the firm are included within the overview of the value network (Peppard & Rylander, 2006). However, value networks that offer new services are could prove difficult to depict as "*developing and offering an innovative service increasingly requires organizations to work together in complex organizational networks" (De Reuver & Bouwman, 2012, p. 1)*. In relation to that, Halinen and Törnroos (2005) argue that due to the interconnected nature of inter-organizational networks the boundaries of the system are arbitrary and therefore networks can be extended without limits through connected relationships. Nevertheless, mapping the relations among organizations helps to gain insight in the following (Peppard & Rylander, 2006, p. 133):

- Where value lies in the network and how a service or product is co-created
- How the firm's activities will affect the network
- How other members are likely to respond

Network analysis is thus a tool to determine how a networked business model should be improved or developed. Peppard and Rylander (2006) define five steps in order to conduct a value network analysis. The steps and a brief explanation are shown in Table 2-1. For this research the value types of Allee (2000) are integrated within the steps Peppard and Rylander (2006). An important remark is that mapping a value network per definition gives a static view of the situation, plus it depicts a mental map of what we "see" connected in reality (Peppard & Rylander, 2006).

Table 2-1: Value network analysis (Peppard & Rylander, 2006)

	Value network analysis steps
1	***Define the network***
	The first step is to define the boundaries of analysis. Key in this is to take the focal organizations (tier-1) as a starting point. The focal organization is the organization whose business model relies on the considered network.
2	***Identify and define network participants***
	Identify all actors (tier-2/3) that have influence on the value that the focal organization delivers to its end-consumers.
3	***Define the value each actor perceives from being member of the network***
	During step three, the value that actors perceive must be defined. The perceived value can differ per actor and therefore this step involves investigating why members are part of the network. This step identifies the underlying motivation of an actor for participating in the network. The perceived value is a key driver of behavior, which in turn is a key force of network development. Three types of value exchanges are distinguished: • Goods, services and revenue • Knowledge • Intangible benefits
4	***Identify and map network influences***
	The nature of the relations between members is determined during this step. These relations are defined as network influences. Only the influences that have effect on the value of the network are taken into account. The amount of influences is important because it is indicator of how much attention must be given to that actor.
5	***Analyze and shape***
	The final step is to analyze the constructed value network. Key in this is to have a thorough understanding of the value dimensions of the different actors and how other participants influence them.

2.1.3 VIP framework

In this research, value network analysis is extended with the VIP framework of Solaimani (2014). This helps to gain insight in the network on strategic and operational level. Solaimani (2014) proposes a multi-layer analysis to bring the business model and business operations closer together. In networked-enterprise environments three layers of exchange can be defined that help to understand the network (Solaimani, 2014):

- Value
- Information
- Process

The value-layer aims at analysing the actors, goals, value activities and the value dependencies within the network. The value-layer is the top layer of the network and aims to answers the questions what

is offered and what is expected in return from one actor to another. In the second layer information is mapped that is needed to execute the different processes in the network. This layer aims to identify actors, their interactions and dependencies (Solaimani & Bouwman, 2012). In the third layer the operational structure of the network is discussed as business processes describe how activities are carried out and how they are related to each other (Solaimani, 2014). Figure 2-1 shows the layers of the VIP framework with its related components. The layers are interactive components, which means that they are sub-elements that all contribute to the business model (Solaimani & Bouwman, 2012). The framework divides the complex interactions of actors into a set of generic domains as can be seen in Figure 2-1.

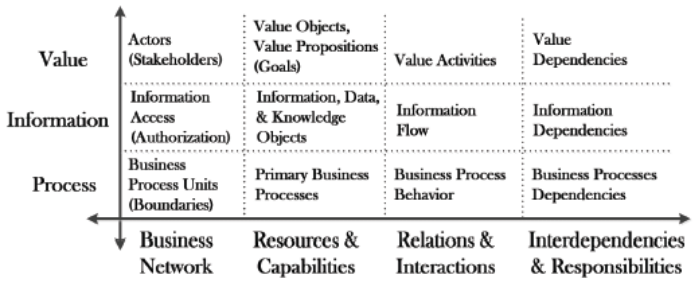


Figure 2-1: VIP framework (Solaimani, 2014)

The layers in the VIP framework have overlap with the value exchanges defined by Allee (2000) as she defines three types of value: tangible, intangible and knowledge. The value layer and information layer of Solaimani (2014) could be grouped under these values, even though Allee (2000) focuses on a more strategic level. However, Solaimani (2014) shows that to get a comprehensive understanding of how value is generated the underlying operational processes should be mapped as well. By analysing the network on different levels a comprehensive understanding of the relations among the actors can be gained. Therefore in this research the value network approach of Peppard and Rylander (2006) is extended by mapping the network process flows.

2.1.4 Ecosystems

Another much used concept that focuses on inter-organizational networks is business ecosystems. The concept of ecosystems is borrowed from the biological world and applied to a business setting in the study of Moore (1993). Ecosystems can be defined as *"an organization group crossing many industries working cooperatively and competitively in production, customer service and innovation"* (Peltoniemi, Vuori, & Laihonen, 2005, p. 2). De Reuver (2009) identifies two major distinctions between value networks and ecosystems. First is that, within value networks actors collaborate to enable a service offering, while in an ecosystem the relationship between actors can also be competitive. Therefore it can be argued that ecosystems consist of one or more value networks, as these can also compete. A second distinction is that the boundaries of a value network are determined by a specific service offering and the boundaries of an ecosystem are rather determined by the intensity of the relationships. In this research the focus is on whether the SIM card can have a value-adding role when offering authentication and identification services. As value networks help in analysing the value exchanges and the value-adding role of actors for a specific service offering, this concept seems more useful for this research than the concept of business ecosystems.

2.2 Control points

According to Tiwana, Konsynski, and Bush (2010), control is a major factor within platforms in trying to understand the interactions between stakeholders. Hawkins and Ballon (2007) explain that for a business model the main design consideration is to maintain control over the overall technical and business architecture. Ouchi (1979, p. 833) views organizational control through two questions: "*What are the mechanisms through which an organization can be managed so that it moves towards*

it objectives? How can the design of these mechanisms be improved, and what are the limits of each basic design?" Based on Ouchi (1979), control is defined as the design and improvement through which an organization can be managed, so that it moves towards its objectives. This research uses the concept of control points to identify positions of economic power and control within value networks.

The origin of control points lies within the Value Chain Dynamics Working Group (VCDWG), which is part of the Communications Futures Program (CFP) of MIT. The task of the group was to develop a methodology that could be used to detect the positions of economic power for services within the telecommunications industry and to understand the sustainability through business model scenarios (Trossen & Fine, 2005). This led to control points as method of analysis, which can be used to understand the relationships between stakeholders and the roles and value they bring to the network as well as the long and short term effects of those relationships (Elaluf-Calderwood, Eaton, Herzhoff, & Sorensen, 2011). This fits in with Ballon (2009a), who argues that creating revenues at the level of the overall value network do not automatically lead to incentives for all firms to participate and therefore the inherent hierarchies, value capture and control by individual firms must be analyzed.

Control points have been used in several contexts, Trossen and Fine (2005) use the concept to characterize the generation of value while Woodard (2008) uses it to characterize architectural design decisions. Woodard (2008, p. 5) defines architectural control points as "*a system component whose decision rights confer architectural control over other components".* In this definition a control point is used to influence the design of other components in the system. Trossen and Fine (2005) define control points as functional elements within a business model where management can be applied and where any encapsulated functional element can be a control point. In a control point control is exerted through business, regulatory and/or technical means (Eaton et al., 2010a). However, these definitions are not very concrete and therefore this research uses the comprehensive definition of Elaluf-Calderwood et al. (2011). They define a control point as a socio-technical mechanism that expresses the boundaries of areas of economic control in the value network and enables the controller to exercise power over other actors in a socio-technical system. Control points can be framed as socio-technical objects, which are driven by the need to share resources and content over networks (Elaluf-Calderwood et al., 2011). According to Herzhoff, Elaluf-Calderwood, and Sørensen (2010) control points emerge within socio-technical systems and are legal, social, economic or technical related. Overall, it can be concluded that a control point is of strategic value, as it offers a stakeholder economic power within a value network.

Ballon (2009a) argues that not all positions within a value network carry the same 'weight' and therefore the positions must be analysed to fully take into account power relations and structural asymmetries. As discussed, Bouwman, Faber, et al. (2008) divide players within a value network in tier 1,2 and 3 players. To categorize value network members insight is needed in the strength of the control points. Eaton et al. (2010b, p. 462) define four key characteristics by which control points are defined and evaluated:

- *Interchangeable or scarcity:* The ease by which alternative players can own a similar control point asset
- *Demand:* The extent to which a control point is accessed by players within a value network.
- *Value:* The amount of tangible and intangible value that a control point is able to capture.
- *Time*: Affecting the other parameters, as they are dynamic and may change over time.

Interchangeable or scarcity reflects to whether other players in the market can offer the same services or products. This relates to whether the control point owner is tier 1,2 or 3 player. The demand expresses the market share that the control point is able to capture and can be measured in

subscribers, sales units or other similar information. According to Eaton et al. (2010a), the value a control point can capture is hard to determine, as it can be tangible as well as intangible. Besides the amount value that a control point can capture is related to the interchangeability and demand parameters. This means that the parameter value aims to determine how much value can be extracted rather than whether it can create value for the value network. However, whether a control point creates value can be seen as a prerequisite for demand, as other firms will only need a control point when it is of added value for their business. Time is the final parameter since the interchangeability, demand and value of a control point can change over time. These parameters help to assess the strength of a control point and thus the power position of its owner.

Besides control points the VCDWG identifies trigger points. These components focus on the interaction of different systems which relates to Luhmann's Theory of Social Systems (1984): *"Systems are operationally closed but structurally open"* (Herzhoff et al., 2010, p. 419). Triggers are defined as external factors that cause a transition from one constellation of control points to another (Trossen & Fine, 2005). Triggers can directly influence an existing business model or indirectly by affecting a chain of other triggers that directly affect a control point. Regulatory, technical, social acceptance (e.g. consumer behaviour) and business (e.g. competitor behaviour) change factors are the main external factors that contribute to a trigger (Eaton et al., 2010a). Identifying triggers helps to understand how control points change over time and it allows for an evaluation of the business sustainability. However, the literature does not address how to identify triggers and therefore it remains unclear how to apply triggers in this research.

The concept of control points, as it is introduced by the VCDWG, can help to assess business models in the mobile industry as it is straightforward and focuses on factors that contribute to changing the dynamics of business models. Furthermore, it has been applied in the context of the telecommunications industry (Eaton et al., 2010a). However, there is different literature that criticizes the VCDWG on a number of aspects (Eaton et al., 2010a; Elaluf-Calderwood et al., 2011). First point of critique is that the VCDWG focuses on value chains rather than value networks. As explained, Li and Whalley (2002) argue that the mobile industry is more network structured and should therefore not be viewed as a linear value chain. Another point of critique is that the focus within the analysis is on one focal company instead of on the industry. Eaton et al. (2010a) address these points of critique in their research and therefore include value networks as a method of analysis. Furthermore, the authors incorporate Lessig's modalities of regulation as origin of factors that influence triggers and control points. The modalities of regulation consist of law, social norms, markets and architecture (Lessig, 2006). Eaton et al. (2010b) propose two steps to identify where and how constituent members can extract value:

- Use value networks in order to map the various constituent actors within the industry and their relations
- Define control points to examine where and how members of the value network can extract value.

The steps defined by Eaton are applied in this research to help determine if the SIM qualifies as a control point for mobile authentication and identification services.

2.3 Related concepts

In the scientific literature the concept of control points to extract economic value from a network is not unique. There are similar concepts that discuss power positions and resources that can be used to capture value. Examples are bottlenecks, leverage points, gatekeeper roles and boundary resources. As some confusion might arise between the concepts a brief explanation is given on the differences and similarities with control points.

In the scientific literature bottlenecks have been discussed in a wide range of studies (Baldwin & Clark, 2006; Ballon, 2009b; Jacobides, Knudsen, & Augier, 2006). Bottlenecks have been researched in fields varying from transaction cost, supply chain management, economics, anti-trust law, platform theory to design science and are thus well documented (Ballon, 2009a). Jacobides et al. (2006, p. 1209) define a bottleneck as *"a segment in a system where mobility (both in terms of switching costs and potential entry) is limited and competition is softened"*. Bottlenecks can constrain the overall system's performance at the expense of the service quality but the identification, nurturing and retention of a bottleneck may also lead to sustainable economic advantage (Baldwin & Clark, 2006; Porter, 1985). When owning and controlling a bottleneck the owner is provided with bargaining and economic power as bottlenecks are critical resources that are limited in supply and high in demand (Ballon, 2009a; Boudreau, 2010). Therefore a bottleneck can be viewed as a strong control point, which is owned by tier-1 players. According to Jacobides et al. (2006) bottlenecks can change over time due to exogenous and endogenous factors and therefore new bottlenecks arise. Overall, it seems that bottlenecks have similar characteristics as control points. Even triggers are accounted for in the form of exogenous and endogenous factors. This corresponds with the findings of Eaton et al. (2010a), who state that control points resemble bottlenecks. However, a difference is that not every control point is limited in supply and high in demand. Eaton et al. (2010a) shows that every actor in the value network has at least one control point and not all of them are limited in supply and high in demand. For example, they mark the distribution of mobile handsets as a control point but it can be argued that there are many webshops, stores and mobile network operators that can facilitate this service and therefore it is not limited in supply. It does, however, explain how an actor can extract value from the value network. Therefore this research views bottlenecks as strong control points that are owned and controlled by tier-1 players.

Another concept that is closely related to control points and bottlenecks is that of the gatekeeper function. It is a concept that is often used in media and communication studies to describe persons and organizations selecting and processing ideas and information (Ballon & Van Heesvelde, 2010). A gatekeeper controls the access in a modular system to the resource or platform and can function as a bottleneck that adds value as it is able to qualitatively alter information (Ballon, 2009b). The owner of a gatekeeper can adopt a dominant position within the value network as he is able to open up information resources and thereby attract a large number of customers while controlling it (Ballon, 2009b). The gatekeeper decides who and what is granted access to the resource. A gatekeeper function can therefore be seen as a specific type of control point as value is extracted by allowing access. A platform such as the app store is a control point that fulfils the function of gatekeeper as it allows app makers access to iPhone users. An example of a control point that is not a gatekeeper function is the creation of a mobile handset, as it not related to providing access.

Next, the concept of leverage points is discussed. Leverage points are places within a complex system (e.g. a corporation or an ecosystem) where a small shift in one thing can produce big changes in everything as they are points of power (Meadows, 1999). It is popular concept within system dynamics as leverage points are opportunities for making critical changes at relatively low effort (Hjorth & Bagheri, 2006; Klein & Wolf, 1998). Meadows (1999) points out that is hard for physical components to be leverage points as they are not simple or quick to change. A leverage point is the starting point for insight and imaginative problem solving (Klein & Wolf, 1998). Understanding what the bottlenecks and limitations of system are gives leverage (Meadows, 1999). A leverage point can be seen as place where intervention can lead to big impact and could prove to be a real opportunity. This concept clearly differs from the control point concept as a strong control point is scarce, not easy to substitute and high in demand. Leverage points focus on small shifts that can have a huge impact. A strong control point should not be a leverage point, as this would affect its sustainability. Leverage points exist temporarily while a successful control point should exist for a longer period. If a leverage point can affect or change a control point it is a trigger as triggers can influence the dynamics of a business model.

The final concept that is discussed is the concept of boundary resources. Boundary resources "*constrain and enable interactions among heterogeneous actors including third-party developers, hardware manufacturers, content creators and consumers*" (Eaton, Elaluf-Calderwood, Sorensen, & Yoo, 2015, p. 2). Boundary resources can function as the interface that allows access to the platform (Ghazawneh & Henfridsson, 2012). It allows the owner to determine the "rules of the game" that exist within the platform and within the rules of the game other parties are free to do what they want. Therefore a boundary resource can provide governance and control on what is permissible within the system. An example of a boundary resource is provided by Ghazawneh and Henfridsson (2012), who state that API's can function as a boundary resource. API's extend the platform by allowing access to third-party developers. The design of a boundary resource provides a delicate tension between maintaining control of the platform and at the same time stimulate third-party developers to develop applications (Ghazawneh & Henfridsson, 2012). Boundary resources show a lot of resemblance with the gatekeeper function, as both focus on who is allowed access and to what extent.

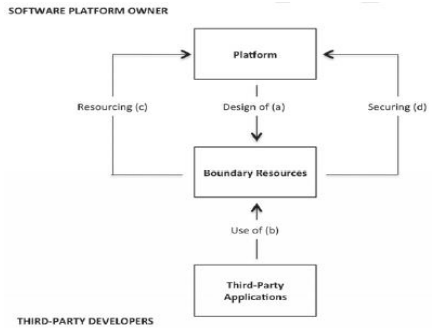


Figure 2-2: Boundary resource model (Ghazawneh & Henfridsson, 2012).

All these concepts (i.e. control points, boundary resources, bottlenecks, etc.) focus on points or elements that lead to control. It shows that a lot of studies have been done on how control in value networks can lead to economic value. Leverage points focus on areas where a small change can have significant impact. This means that the SIM should not be a leverage point. It should function as a revenue source and therefore it must not be easy to replace the SIM. Boundary resources and gatekeeper functions are a specific type of control point as they deal with access to a platform or resource. Both concepts can be seen as an interface and are less relevant for this research as they focus on very specific functions. In this research a broader approach is taken to identify new service applications for the SIM and therefore the concept of control points seems more useful. Control points can perform similar roles as boundary resources and gatekeeper functions but the concept is not limited to these functions alone. This means that other uses of the SIM, besides providing access to a platform are also within scope. Furthermore, the SIM is not a boundary resource as it is able to function as a platform of its own. The concepts of control points and bottlenecks seem relevant for this research as the SIM can possibly offer control by securely storing credentials and applications. The capabilities of the SIM seem able to match the demands of a control point or a bottleneck. However, bottlenecks represent critical components of a system and not all actors involved own a bottleneck. Actors are thus able to extract value from a network without owning a bottleneck. So, in order for the SIM to function as a revenue source it does not need to be a bottleneck. The SIM must, however, be able to function as a control point as this allows an actor to extract value from the network. Overall, the concept of control points seems to be a useful concept to determine whether and how MNOs can exploit the SIM for authentication and identification services.

2.4 Conclusion

In this chapter the concepts of value networks and control points have been discussed, as they seem relevant for this research. Value networks help in addressing the relationships between actors and the value-adding role they fulfil within the network to produce a certain product or service. Value networks are used rather than value chains because many modern industries cannot be seen as a linear chain in which tasks are completed consecutively. Value networks can be described as "*a dynamic network of actors working together to generate customer value and network value by means of a specific service offering, in which tangible and intangible value is exchanged between the actors involved"*. A value network can be seen as an economic mechanism that turns one type of value in another, in which the following value exchanges can be distinguished:

- Goods, services and revenue
- Intangible benefits
- Knowledge

The focus within a value network is on core competence and competence complementarity rather than one actor providing maximum value to a customer on their own. However, not all actors are 'equally' positioned within the value network. Structural partner are the core of the network, while contributing and support partners are loosely connected to the value network:

- *Structural or tier-1 partners*. These participants provide essential and non-substitutable tangible and/or tangible assets to the value network on an equity or non-equity basis. They play a direct and core role in determining the intended customer value and in creating the business model.
- *Contributing or tier-2 partners*. These participants provide goods and/or services to meet requirements that are specific to the value network. They do not play a direct role in determining the intended customer value and in creating the business model. The business model and intended customer value could remain intact if these assets are substituted.
- *Support or tier-3 partners.* These participants provide generic goods and services to the value network and are key for the viability of the value network. However, these goods and services could be used in connection with a wide variety of intended customer value and business models.

The application of the value network concept can be a useful means to analyse the relations among actors. By mapping a value network an overview is created of the relationships, positions and the value-adding role of actors in the network. It helps to understand where value lies in the network, how value is co-created, how the firm's activities will affect the network and how other members are likely to respond to changes. In chapter 4 the steps defined by Peppard and Rylander (2006) are used as a guideline to conceptualize existing value networks related to mobile authentication and identification. Within these steps the mentioned value exchanges are integrated. As the steps of Peppard and Rylander (2006) focus more on a strategic level, the analysis for this research is expanded by mapping the value network on a technical and process level. Mapping the network on multiple levels helps the in-depth analysis of this research.

To examine where and how members of the value network can extract value, the concept of control point is used. A control point represents a socio-technical mechanism that expresses the boundaries of areas of economic control in the value network and enables the controller to exercise power over other actors in a socio-technical system. Control points lead to control and economic power of actors, which ensures that will be part of the business model. Control points can be legal, social, economic or technical related and the strength of a control point depends on four crucial parameters:

- *Interchangeable or scarcity:* The ease by which alternative players can own a similar control point asset
- *Demand:* The extent to which a control point is accessed by players within a value network.
- *Value:* The amount of tangible and intangible value that a control point is able to capture.
- *Time*: Affecting the other parameters, as they are dynamic and may change over time.

A strong control point is scarce and cannot be replaced easily. This relates to whether the control point owner is tier 1,2 or 3 player. The demand reflects how much market share the control point is able to capture. The third parameter aims to map the amount of value that a control point can extract from the value network, which can be tangible (e.g. revenue) as well as intangible (e.g. customer information). The fourth parameter relates to the fact that control points change over time. Changes to control points can be caused by triggers, which are external factors that influence the business model. These external factors can be of regulatory, technical, social acceptance or business nature.

Although, related concepts to value networks and control points can be found in the literature (e.g. ecosystems, bottlenecks and boundary resources), these two concepts seem useful for this research to determine whether MNOs can exploit the SIM for authentication and identification services. The concepts help in analysing the current situation to define opportunities for the SIM as a control point. Based on the literature discussed in this chapter, it can be concluded that for the SIM to qualify as a control point a number of conditions must be met. First, is that the value network must be viable because control points exist within value networks. Second, is that the SIM must score on the parameters scarcity, demand, value and time. Otherwise it will not qualify as a control point. Therefore the following criteria will form the basis of the interview protocol:

- Viability of value network
- Control point criteria
    - Scarcity/uniqueness
    - Demand
    - Value
    - Time and triggers

A more detailed description of the interview protocol and an overview of the questions related to the concepts of value networks and control points is given in chapter 6.

3. Technical background

This chapter provides an overview of the technical background. In this chapter the SIM card characteristics are discussed to gain insight to what kind of services the SIM card can contribute. Next to that several alternatives for the SIM are discussed. Finally, a conclusion is presented.

3.1 SIM card characteristics

The subscriber identity module, also known as SIM card stores data of mobile phone subscribers. The SIM is used for user identification, authentication and message encryption in cellular networks (Tsai & Chang, 2006). However, the SIM can do much more, as it is a mass-market smart card. This means that it can be used for all kinds of security applications, which reach far beyond the mobile world (M'Chirgui, 2009; MPFI, 2008). In this research security is defined as the degree of resistance to or protection of a possible attack. Smart cards help to reduce the risk of a successful attack in a financial viable way and can be seen as secure for different reasons (Abbott, 2002; MPFI, 2008):

1. The cards have been designed from the inside out to be secure and tamper resistant. For smart cards security has been the main requirement for the design. This demand is incorporated from the physical design, to the circuit logic and to the encryption schemes.
2. The added encryption capabilities on the smart cards provide a means of securely storing private keys that do not need to leave the card while providing the ability to digitally sign and encrypt messages.
3. The smart card industry has a significant incentive to address vulnerabilities and is constant looking to improve the existing security. The cards are primarily designed as a secure device and often need to meet strict standards such as government documents or credit cards.
4. PIN and PUK codes with limited attempts are other factors that increase security.

Smart cards are capable of securely storing secret cryptographic materials and executing undetected executions of cryptographic algorithms (Boudriga, 2009). The smart card is a module that can safely store data in the sense that is highly protected against all unauthorized or unforeseen access. Typically, smart cards are used in application-specific ways of which the SIM is such an application (Boudriga, 2009). The SIM is thus a tamper resistant module in the form of a smart card. The SIM is able to perform the following functions (MPFI, 2008; Reveilhac & Pasquet, 2009):

1. Identification of a subscriber
2. Authentication of a subscriber
3. Storage
4. Run and store applications

Besides connecting to the network, these functions can be used to bring all kinds of plastic smart cards to the mobile phone without the need to introduce new hardware elements (Mantoro & Milisic, 2010). The SIM security could be of added value to the mobile phone, as handsets provide a user interface and possess powerful data processing and communication capabilities but have a poor record when it comes to security (Mayes & Evans, 2008). Bringing new applications of plastic cards to the mobile phone merely extends the functions of the mobile phone, which fits in the trend of today's society on the growing importance of the mobile phone (Bae, Banerjee, Loozen, Murdoch, & Saksena, 2014).

3.1.1 SIM authentication and identification

The SIM is able to identify and authenticate a mobile handset. Identification is the process of presenting an identity to a system or person. Authentication aims to verify a person's identity. Therefore identification is the first step in an authentication process. Authentication deals with the problem who should be provided access. It tries to ensure that an individual is really who he claims

to be. When authenticating someone or something the chances of assuming another person's identity must be kept to a minimum (Mantoro & Milisic, 2010). In general there are three ways for a human to authenticate himself to a machine (Stamp, 2006):

- Something you know (e.g. password)
- Something you have (e.g. smart card)
- Something you are (e.g. biometrics)

By combining the methods, the authentication security is increased (Mantoro & Milisic, 2010). Many authentication systems are based on two-factor authentication, in which two of the methods are combined (Abbott, 2002; Stamp, 2006). For example, a payment card uses two-factor authentication, as users need to present the card (something you have) and need to enter a PIN (something you know). By entering the PIN number the user can verify himself to the card, after which the card will respond by using its private key to digitally sign the payment data (Abbott, 2002). On the SIM private keys are stored to authenticate the user to the network. As the SIM is able to host multiple applications, it is able to store multiple private keys in a secure environment. The authentication and identification qualities of the SIM can thus be used for other applications as well. In fact, the SIM card is able to provide authentication in any wireless network (Noll, Calvet, & Myksvoll, 2006).

3.1.2 Universal Integrated Circuit Card

According to Alimi and Pasquet (2009), the Universal Integrated Circuit Card (UICC), which is the next generation SIM cards, can host multiple applications either from the issuer or from other authorized parties each defining and controlling its own applications. The UICC is compliant with all smartcard standards and can thus host non-telecom applications (Reveilhac & Pasquet, 2009). On the UICC there are separate security domains for each application, which are based on the use of secret administrative keys and administered by the application issuer. The operating system on the card prevents the applications from accessing or sharing data between them (Alimi & Pasquet, 2009). The UICC can thus be safely used for other applications besides providing access to the mobile network. For the remainder of this research, a referral to the SIM card is a SIM in the form of a UICC unless mentioned otherwise. The SIM is secure, in the subscribers hand and manageable (Mayes & Evans, 2008). Manageable meaning that the SIM is a remotely managed platform and that means for application and data management are available (Madlmayr et al., 2007). The SIM can be remotely managed by making use of Over-The-Air (OTA) technology. This is a technology that enables updates and changes on the smart card without having to reissue the cards (Alimi & Pasquet, 2009). The SIM has proven itself as a standardized and controllable platform, which has provided value added services across a wide range of legacy handsets (Mayes & Evans, 2008). A more detailed overview of the SIM card architecture can be found in Appendix B.

3.1.3 SIM as Secure Element

As discussed, the SIM is can host multiple applications and provide secure authentication and identification. When the SIM is used in such fashion, it is often called a Secure Element (SE). This means that the SIM is used to store applications and credentials while providing a secure execution of the applications (Smart Card Alliance, 2014b). For NFC transactions the SE is a critical component since it ensures that transactions are protected from unauthorized data access (GSMA & Booz & Co, 2011).

A SE is a combination of hardware, software, interfaces and protocols embedded in a mobile handset, which enable secure storage (Reveilhac & Pasquet, 2009). It is generally used for payment applications but it can be used for all kinds of applications, which involve authentication and require security mechanisms (e.g. mobile ID or bus ticket) (Mantoro & Milisic, 2010; Reveilhac & Pasquet, 2009). A SE must be manageable and have the following functions: secure memory, cryptographic

functions and a secure environment for execution (Madlmayr et al., 2007). When multiple applications are stored on the SE, they must be protected from each other and the applications should only be managed by authorized parties (Madlmayr et al., 2007; UL TS, 2014b). As the SIM is able to comply with these requirements, it can be seen as a SE already integrated within the handset.

When the SIM is used as SE, application data and secure assets are stored on the SIM. Although the application data can be stored anywhere in the mobile handset, the SIM offers storage with a high level of security (Noll et al., 2006). The SIM provides strong cryptographic calculation power and offers security while being managed via the MNO telecommunication network (Chen, Mayes, Lien, & Chiu, 2011). The SIM can be used to emulate physical smart cards and these cards can be accessed by making use of a mobile wallet (Steffens, Nennker, Zhiyun, Ming, & Schneider, 2009). This means that by making use of a SE the mobile handset is able to take over the functions of a traditional proximity smart card. The mobile wallet is merely the user interface on the handset that allows a user to select and use a card. So, in the case that the SIM functions as a SE, it can be used for secure authentication, identification and data storage.

3.1.4 Secure Element applications

The SIM SE is a PIN-protected platform on which different applications can be stored that require a high level of security. Examples of such applications have been mentioned in the form of mobile payment or public transport. These applications can be stored and executed on the SE. Especially, for mobile payment this was a preferred solution (Au & Kauffman, 2008), which means that all related payment data is stored on the SIM.

Another form of a SE application that requires a high level of security is a Mobile Public Key Infrastructure (MPKI). The MPKI is also stored on the SE and it can provide the authentication service for an OS application. This application is executed on the OS but the keys are stored on the SE. In this case only the user credentials and secret keys are stored on the SIM application while the OS application contains all other data. According to Mayes and Evans (2008) a good marriage of capabilities is to put most of the application on the handset but to exploit the security of the SIM card, as is the case with a MPKI solution. The public key technology can provide a strong mobile authentication method and integrated on the SIM it can perform cryptographic operations without exposing the secret keys (Rongyu et al., 2009). In principal you can authenticate to anything with the SIM (Mayes & Evans, 2008) and storing a MPKI on the SE-SIM is a secure way to do so.

3.2 SIM alternatives

The SIM has clear qualities when it comes to providing security in the mobile handset. It is, however, not the only option that can provide mobile authentication and identification services. Other options that are available in the market are an embedded SE, cloud or micro SD. These options can all store applications and credentials while providing a secure execution of the applications. In this paragraph a comprehensive explanation is given on the alternatives.

3.2.1 Embedded SE

The embedded SE is a module that is soldered onto the mobile handset and offers the same level of security as the SIM (Reveilhac & Pasquet, 2009). As with the SIM, the whole application is stored on the element. The chip is embedded within device during the manufacturing phase and must be personalized after the device is delivered to the user (EMVCo, 2007). As the SE is soldered onto the handset in cannot be used in a different handset. This means that the user must personalize his handset every time he purchases a new one. The iPhone 6 is an example of a mobile handset with an embedded SE.

3.2.2 Cloud-based solution

Another option that can take over the role of SE is a cloud-based solution. Google recently introduced Host Card Emulation (HCE) for the Android OS in which a cloud-based solution can be used rather than a physical SE in the mobile handset. In this case the application is held within the operating system of the mobile phone which is called the "host"(Pannifer et al., 2014). With a cloud solution the credentials to exchange with the contact point can be stored in the cloud owned by the SP. The handset must connect to the cloud by making use of the Internet, after which the handset will receive keys that allow to use the application at a contact point. These keys are provided via an internet connection and to ensure security they are often provided in a limited amount with a limited validity period (Smart Card Alliance, 2014a).

3.2.3 Micro SD

Another alternative that can serve as SE is a micro SD card. Over the years the relevance of this solution has decreased and therefore during the rest of the research the micro SD is not considered as a realistic alternative. Nowadays, many handsets do not even have a slot for the micro SD. However, the micro SD card can be a Secure Memory Card, which means that it is a combination of a smartcard and a memory card (Reveilhac & Pasquet, 2009). This means that a SD card is able to function as a SE.

3.3 Conclusion

The SIM card is a mass-market smart card that can be used for more applications besides providing access to the mobile network. It is a tamper-resistant module within the mobile handset and is as secure as any other smart card due to its cryptographic qualities. The SIM card is well standardized as it is transferable between most mobile handsets, which means that the user's data is not tied to a specific device. So, without the need to introduce new hardware plastic smart cards can be introduced to the mobile handset. Next to these features, the SIM can be remotely managed by the MNO due to the OTA technology. The characteristics of the SIM show that it is a proven technology that can securely store all kinds of authentication applications in the mobile handset by using it as a SE. Two types of applications have been discussed in the form that the whole application is stored and executed on the SIM or a MPKI solution is stored on the SIM and the rest of the application is stored on the OS. These solutions show that it possible to use the SIM for all kinds of authentication and identification services.

However, there alternatives in the market that offer similar functionalities as the SIM. This chapter discusses three alternatives: embedded SE, Micro SD and cloud-based solutions. Many handsets today, do not have a slot for Micro SD and therefore this is not considered to be a relevant alternative. The embedded SE shows a lot of similarities with the SIM but is soldered onto the handset and cannot be removed. A cloud-based solution does not make use of a physical element to store credentials but stores the credentials in the cloud of the service provider. These credential can be downloaded onto the phone before transaction is conducted. An overview of the characteristics that been discussed in this chapter is provided in table 3-1.

Table 3-1: SE overview (UL TS, 2015b)

Features	SIM	Embedded SE	Cloud
Removable	Yes	No	N/A
Standardization	Yes	No	N/A
Lifetime of credentials	Years	Years	Seconds to days, and/or limited number of transactions
Security	Hardware	Hardware	Software
Remote control	OTA/OTI	OTI	OTI

4. Domain background

Based on the characteristics of the SIM discussed in the previous chapter, different markets are identified where the SIM could possibly function as an authentication and identification means. This chapter discusses the markets that have been picked for this research. In appendix C other markets are discussed where the SIM could possibly be of value. The remainder of this chapter discusses the markets of enterprise ID, Government and mobile payment. Finally, a conclusion is presented.

4.1 Application markets

As discussed, the SIM is able to provide secure authentication and identification for online as well as offline applications. This means that markets that require a high level of security could prove to be an opportunity for MNOs. In Appendix C multiple application markets, where the SIM could be of value, are discussed. However, due to time constraints this research focuses on three application markets:

- Enterprise ID
- Government
- Mobile payment

These application markets have been chosen for this research, as they require a high level of security and currently make use of two-factor authentication. Furthermore, the end-services in these markets differ substantially and therefore different insights might be gained. Mobile payment focuses on payment transactions, while Enterprise ID focuses on access and government services focus more on identification means for the user.

For the market of mobile enterprise ID and government services limited literature is available while for mobile payment a lot of studies have been conducted, as it is a more mature market regarding mobile authentication and identification. Within these studies a lot of themes are discussed. Some focus on the technical infrastructure that is needed to facilitate mobile payment (Madlmayr et al., 2007; Pannifer et al., 2014; Steffens et al., 2009). Other studies focus more on the collaborations between different stakeholders and the struggles they face (De Reuver et al., 2014; Markendahl et al., 2010). Furthermore, the entrance of tech giants such as Google and Apple has been discussed (Ondrus & Lyytinen, 2011) as well as different business models for the industry (Au & Kauffman, 2008; Wiedemann, Palka, & Pousttchi, 2009). All these studies show that there is a lot of knowledge on the mobile payment market and the struggles they face. Literature on mobile authentication and identification services for the government and enterprises is less available. Nevertheless, a brief explanation of the markets is presented next.

4.1.1 Enterprise ID

The market of enterprise ID consists of organizations, which want to identify and authenticate users of their networked systems (Smart Card Alliance, 2015). These systems vary from physical access to authentication for the intranet. As companies have resources and information that should only be accessed by authorized persons, security is required. Nowadays, smart cards and passwords are often used to authenticate users at enterprises (Smart Card Alliance, 2015). This means that this market could be an opportunity for MNOs to target with SIM-based authentication and identification.

Over the years the enterprise security market has only been increasing and is expected to grow to $86 billion in 2018 (Canalys, 2011). Security is thus becoming more important to companies. As companies have to protect their resources, it is key that the right persons are allowed access. Mobile authentication and identification services can contribute to this need. In this research the focus is on large security companies that manage the access of employees to company access. The core product

of these companies is to deliver security solutions to enterprises. By collaborating with security companies MNOs can profit from their expertise and existing customer base. The security companies will serve as service provider, while MNOs would provide the SE as authentication and identification means. Overall, the solution must be cost efficient, secure and convenient in order to compete with traditional measures such as smart cards and one-time passwords.

4.1.2 Government

Several studies showed that mobile services can be of value for government services (Hung, Chang, & Kuo, 2013). Governments supply their citizens with passports, driver licenses, ID cards but also DigiD (online authentication in the Netherlands for government services). The mobile phone and the SIM have the capability to securely bring these services to the handset. For example, the SIM can be used to store an ID card. Furthermore, the SIM could be used to authenticate a person online. Kushchu and Kuscu (2003) argue that mobile government can lead to benefits for the citizens, industry and governments as it can provide cost reduction, efficiency, more convenience and flexibility.

The development of the eID scheme by the Dutch government is a concrete opportunity for MNOs, as it is currently in a pilot phase (Nu.nl, 2015). The eID scheme is an initiative by the government and the business sector to develop a standard for secure access to online services (Rijksoverheid, 2015b). The eID aims to provide authentication for government websites as well as private websites such as webshops , banks and insurance companies (Figure 4-1). The eID can be seen as the successor of the less secure DigiD and is open to multiple authentication means (Rijksoverheid, 2015c). This means that the system offers the possibility for a user to login with an ID card or even a bankcard, as long as the authentication and identification means complies with the standards of the eID scheme. According to the government, this makes the system flexible and less vulnerable for malfunctions (Rijksoverheid, 2015c). Users have the ability to choose their login method, which should make the system more convenient. As the Dutch government wants private companies to connect to eID and provide authentication and identification, it could prove to be an opportunity for the SIM and MNO.

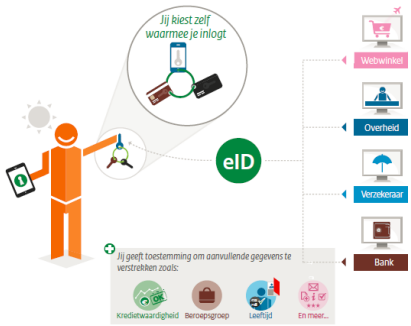


Figure 4-1 eID applications (Rijksoverheid, 2015b)

Furthermore, this research aims to determine whether the SIM can be used to store offline government documents such as a driver's license or ID card. All these service require a high security because the user must be authentic. In this market the government will function as service provider and the MNO could possibly offer authentication and identification.

4.1.3 Mobile payment

The mobile payment market is included in this research because it is potentially a large market. The expectation is that globally over 700 billion dollars of transactions will take place by 2017 (Statista, 2012). However, the competition in this market is fierce and different initiatives of MNOs have failed (Au & Kauffman, 2008; De Reuver et al., 2014). This research should help to determine whether there is still a role for MNOs in the mobile payment market, as it is still a potential cash cow. Initially mobile payments will be a complement to credit and debit cards but at the same time it has the

potential to overtake these traditional methods (Au & Kauffman, 2008). The payment market can be described by making use of the four-corner model, which is depicted in Figure 4-2.

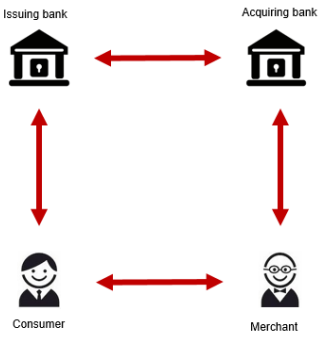


Figure 4-2: Four-corner model (UL TS, 2014a)

The four-corner model describes the market infrastructure for payments. The model is composed by the consumer or cardholder, the issuing bank, the acquiring bank and the merchant. These are the main parties that are involved with the facilitation of the transaction. When the consumer wants to conduct a payment at the merchant he can use his payment card. The payment card is issued to the consumer by the issuing bank. A payment scheme between the issuing bank and acquiring bank facilitates the transaction after receiving authentication and authorization from the cardholder. Finally, the transaction is processed and received by the merchant. The acquiring bank has a contract with the merchant. It is possible that the issuing and acquiring bank are the same but then the consumer and the merchant must both have a contract with the same bank. Currently, the four-corner model is an example of how card payments are processed but this model can also be used for mobile payments except rather than a card the mobile phone is used.

The prospect is that mobile payments would increase the amount of electronic cash, which means that banks would have less costs for handling cash (Gaur & Ondrus, 2012). Eventually, mobile payments can even replace physical cards and this would lower the operational costs due to the ability of remote provisioning. Au and Kauffman (2008) state that mobile payments must be convenient, generalizable, cost efficient plus trustworthy to the consumer. Convenient relates to the fact that the solution must be user friendly. Generalizable means that the solution must be able to serve a large market and furthermore the costs for implementing and operating mobile payments must not be too high for the service provider.

Furthermore, the SIM could be used to provide authentication for online payments such as iDeal in the Netherlands. Currently, random readers are used to generate one-time passwords. The SIM could possibly increase the user experience. Therefore this research includes online and offline mobile payments.

4.2 Conclusion

In this paragraph three markets have been discussed where the SIM could possibly be used to provide online and offline authentication and identification services. First, the market of enterprise ID has been discussed. This market requires authentication and identification services in order to allow employees access to company assets. Another opportunity for the SIM could be to provide authentication and identification for government services. The development of the eID scheme in the Netherlands seems as a concrete opportunity as it allows private organizations to offer authentication and identification. Besides, the SIM can be used to store government identification documents such as driver's licenses or ID cards. Finally, the mobile payments market was identified as an opportunity for the SIM. This market requires authentication and identification in order to

authorize transactions. In chapter 5, value networks are designed for mobile authentication and identification services for the three markets. Table 3-2 provides an overview of the discussed markets and examples of the services to which the SIM can contribute as authentication and identification means.

Table 4-1: Overview application markets

Market	Online services (e.g.)	Offline services (e.g)
Mobile payment	iDeal	NFC payments
Government services	DigiD	Mobile driver's license
Enterprise ID	Intranet	Physical access

5. Conceptualization of value networks

This chapter conceptualizes value networks and control points related to the different SEs discussed in chapter 3. These value networks can deliver similar services but involve different actors and resources. As discussed in chapter 2, value networks help to map the actors and the value exchanges involved with a service delivery. After conducting a literature study and consulting the opinion of industry experts, the conclusion is that there are three types of SEs that are currently being deployed in the market: SIM, cloud and embedded. Therefore three value networks are constructed to provide insight in the power position of MNOs and possible opportunities for the SIM as authentication and identification means. The constructed value networks aim to give a generic overview of the infrastructure that can be used for different online as well as offline authentication and identification services. The application markets are therefore not discussed in this chapter.

The SE is a platform that can securely store application data and has access to the consumer. Therefore it is marked as a critical resource in the value network. As the owner or issuer of a SE can decide who is allowed access to this critical resource, they are marked as tier-1 players. Based on this, the value networks are constructed around the SE issuer. In this chapter the following value networks are constructed:

- Value network SIM SE
- Value network embedded SE
- Value network cloud-based solution

In these value networks the technical infrastructure differs due to the used resources and therefore the actors involved are different. In order to get a comprehensive overview the value networks are explained on a technical, process and organizational level. The technical infrastructure helps to define the resources involved with mobile authentication and identification services. Mapping the processes will show what the role of the resources is. The processes are depicted in Appendix D, as it overlaps with the discussion on the technical infrastructure. As discussed, the value networks are mapped around the SE issuer. Based on the technical infrastructure other actors are identified and categorized as tier 1, 2 or 3 players. This means that all actors within the value network control at least one control point that contributes to the service delivery.

An important remark is that the discussed value networks are mostly being deployed to facilitate mobile payment, while the other application services have rarely been introduced to the market. However, the technical infrastructure does not need to differ much for the different markets. Therefore value networks related to the technical infrastructure are mapped. The remainder of this chapter is as follows. First, an overview of the different roles involved within the value network is provided. Next, the SIM SE value network is discussed, which is followed by the embedded SE value network. The final discussed value network focuses on cloud-based solution. Finally, a conclusion is provided in which the opportunities for the SIM and MNO are discussed.

5.1 Roles of involved actors

Based on information of industry experts and the literature study on the processes and technical infrastructures (Pannifer et al., 2014; Steffens et al., 2009; UL TS, 2015b) different roles within the value networks are identified. The discussed roles all control resources needed to provision the service applications on the handset. The roles have been mapped in Table 5-1 along with a tier 1, 2 or 3 classification.

Table 5-1 Role within value network

Role	Type of participant
SE Issuer	Tier 1
Service provider (SP)	Tier 1
User	Tier 1/2
Handset manufacturer	Tier 2
SIM vendor	Tier 3

In total six role have been identified and categorized. As discussed, the SE issuer is marked as a tier 1 participant as it provides a critical resource with the SE. It can allow other parties to store applications in the secure environment of the SE. The SP is also a tier 1 player because they offer the end service to the customer. Both the SE issuer and SP have access to the customer and are therefore marked as tier 1 players because as explained in chapter 2, the value is the highest at the customer. The user is categorized as a tier 1/2 player because as a collective they have a lot of power. Although, individually a user is still a revenue source, their position is not that strong. Nevertheless, they are crucial players that determine the success of a service. The handset manufacturers are contributors, as they deliver the handset and determine what operating system is used. Furthermore, the SIM vendors are marked as tier 3 players as they have a more supportive role and are not directly involved with the service offering. The discussed roles can be identified in the three value networks. However, not all actors are involved in all value networks because different infrastructures require different resources.

5.2 Value network SIM SE

In a SIM SE value network the MNO is a tier 1 player as they issue the SIM to the customer. Before the value network can be depicted an understanding of the technical infrastructure is needed. This shows how the system works and what resources are involved to enable authentication and identification services. Next, the value network is mapped with mutual relations of the actors. Finally, the control points are identified.

Technical infrastructure

In this paragraph a graphical overview is given in which the SIM is used as a SE. In this case an application is safely stored in the controlled environment of the SE. The technical infrastructure is split into two figures. Figure 5-1 shows an overview of the technical infrastructure needed for the provisioning of the service application, while Figure 5-2 focuses on the infrastructure needed for the use of the service.

Figure 5-1 shows that the service application is stored in the secure environment of the SIM SE. The mobile wallet application on the device manages the interactions between the user and the application (Kemp, 2013). The mobile wallet application can be provided by different parties in which a central role for the SE issuer, SP or a combination of both is most common (Dahlberg, Mallat, Ondrus, & Zmijewska, 2008). The trusted service manager (TSM) mediates the interaction between SPs and the SE issuer in this case the MNO. Its core function is to mediate in issuing and managing a secure service on a mobile device, so that the user's secure credentials can get onto the SE (GSMA, 2013b). The TSM of the MNO provisions the application on the SE. The SP TSM personalizes the application on the SE via the network of the MNO. Due to the SIM card the TSMs are able to make use of the OTA technology. This means that the MNO is able to offer new services or to modify content of smart cards in a rapid and cost-effective way (Alimi & Pasquet, 2009). OTA is able to provide life-cycle management in the form of application downloads, software updates, security updates as well as dynamically delete data in real-time and pre-empt the unauthorized use of the handset (GSMA & Booz & Co, 2011). This ability of life-cycle management can enhance the security of the SIM.

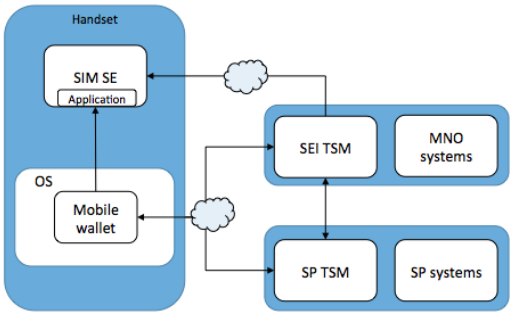


Figure 5-1: Technical infrastructure provisioning SIM SE

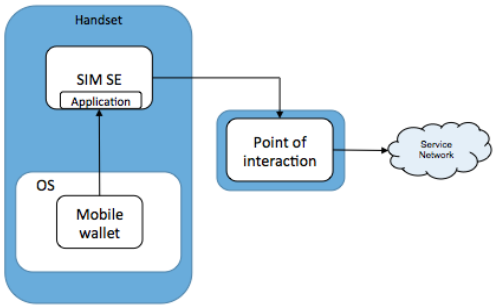


Figure 5-2: Technical infrastructure use of service SIM SE

The technical infrastructure for the use of service is shown in Figure 5-2. The application has been stored on the SE during the provisioning and is ready for use. The mobile wallet allows the user to select the application after which in can be used for a transaction. This transaction takes place at the point of interaction, which can be pay desk, a ticket scanner, webpage or even an app on the mobile phone. The communication channel between the handset and the point of interaction differs per solution. For proximity services a NFC controller needs to be present in the handset while for a webpage an Internet connection is used. The point of interaction communicates with the back-end systems of the service network and this differs per service. The discussed technical infrastructure shows a generic overview of the system in which the SIM is used as SE and can thus be used for all kinds of purposes. In Appendix D an overview is provided of processes related to the provisioning of the application and the use of service.

Value network

The technical infrastructure and service processes provide an overview of the resources needed when the service application is stored on SIM SE. Based on the technical infrastructure, the identified actors, service processes and input of industry experts value networks have been constructed. The value networks are graphically mapped in order to provide an understanding of the positions and relations of the actors involved with the technical infrastructure. Figure 5-3 shows a value network in which the MNO takes on a focal role as SE issuer. The SP and MNO are tier 1 players as they have access to the consumer, who uses the service in return for monetary benefits. The MNO supplies the SIM to the customer while it allows the SP to store a service application on the SIM, all in return for monetary benefits. This allows the SP to facilitate a service to the user. The SIM vendor plays a supportive role by facilitating the SIM to the MNO. The scenario in this research is that the handset manufacturer delivers the handset to the user in return for monetary benefits.

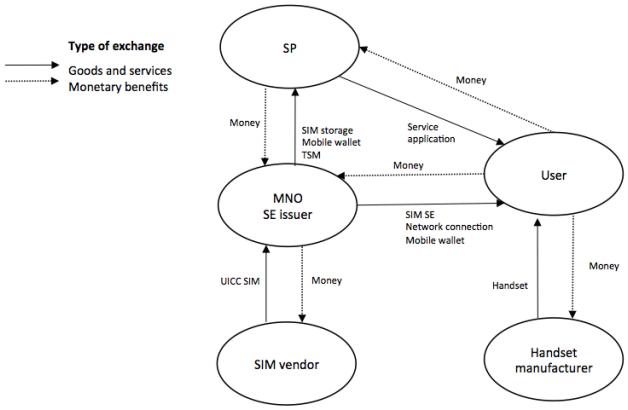


Figure 5-3: Value network MNO SE

Control points

Within the value network control points can be defined that explain how an actor can extract value. The control points are shown in Table 5-2 with the actor that owns/controls it. The value network and control points show that in this technical solution the MNO can be marked as a tier 1 player. The SIM is used as SE, which enables the MNO to extract value from the network. Another actor that plays a key role within this value network is the SP, as they offer the end service to the user. In this value network the MNO and the SP are crucial players that have to work together to deliver a service to the consumer. All other players are identified as contributing or supporting players.

Table 5-2: Control points MNO value network

Actor	Control point
MNO (tier 1)	SIM SE Mobile network
User (tier 1/2)	Source of information Source of revenue
Handset manufacturer (tier 2)	Device creation Device OS distribution
SIM vendor (tier 3)	SIM creation
SP (tier 1)	Service development Service network

5.3 Value network embedded SE

The embedded SE value network is based on the Apple pay infrastructure as this is a solution that has currently been implemented in the US market. In this value network Apple plays a focal role as it provides the SE. The embedded SE is soldered onto the mobile handset and is thus non-removable. It is owned and offered by the handset manufacturer and therefore the value network differs from the MNO value network. To mark the difference of the two technical solutions the technical infrastructure value networks are discussed. An overview of the related processes can be found in Appendix D.

Other embedded SE solutions would show similarities with the Apple infrastructure. However, Apple is a very dominant player and has the ability to play a very central role in the value network. Whether this would be the case for other embedded SE solutions is questionable but since these solutions have not widely been applied in the market the focus is on Apple as SE issuer.

Technical infrastructure

In this paragraph a graphical overview is given in which an embedded SE is used. Similar as with the SIM, the application is safely stored in the controlled environment of the embedded SE. The technical infrastructure is divided into two figures. Figure 5-5 shows an overview of the technical infrastructure needed for the provisioning of the service application while Figure 5-4 focuses on the infrastructure needed for the use of the service.

Figure 5-5 shows the infrastructure that is needed for the provisioning of the service. It is similar to the infrastructure where the SIM is used as SE. Only, in this case the service application is stored in the secure environment of the embedded SE. Apple passbook performs the role of mobile wallet as it provides access to the application on the SE. To enable the provisioning there are two TSMs that are used. As SE issuer Apple has its own TSM that is able to communicate with the service provider's TSM. In order to simplify the infrastructure Apple has only allowed a minimum of payment TSMs in the value network therefore SPs must connect to an existing TSM rather than creating its own. The TSM connection with the SE goes Over The Internet (OTI) as the embedded SE cannot connect to TSM over the mobile network.

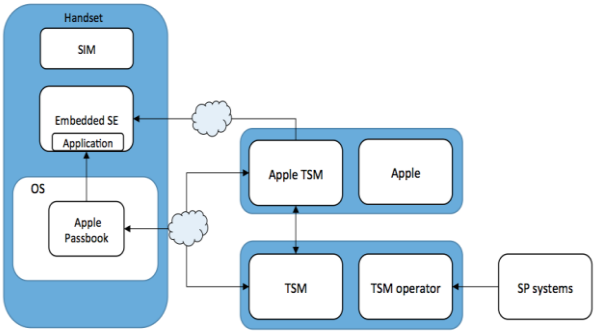


Figure 5-5: Technical infrastructure provisioning Apple (UL TS, 2015a)

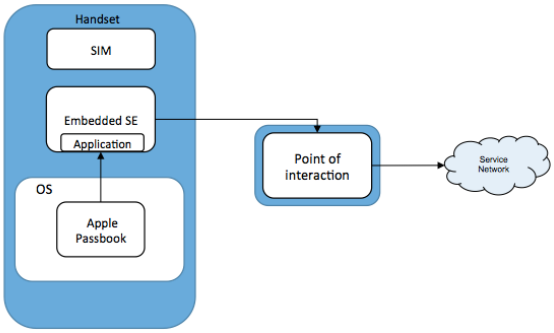


Figure 5-4: Technical infrastructure Use of service Apple (UL TS, 2015a)

The technical infrastructure for the use of service is shown in Figure 5-4. The application has been stored on the SE during the provisioning and is ready for use. With passbook the user can select the service application and use it for a transaction. The transaction is conducted at the point of interaction. As mentioned, this can be anything from a pay desk to a webpage and depending on the point of the communication channel differs. The point of interaction communicates with the back-end systems of the service network and this differs per service. The discussed technical infrastructure shows a generic overview of the system in which an embedded SE is used. This system is based on the existing Apple pay infrastructure and currently no other services have been offered within this system. It remains unclear if Apple would implement a similar TSM infrastructure for other services. In Appendix D an overview is provided of the resource ownership and the processes related to the provisioning and use of the service.

Value network

The Apple value network based on the embedded SE is composed based on the defined resources, actors and processes. In this value network Apple takes on a focal role, as it is the SE issuer. Apple offers secure storage to the SP and the mobile wallet in exchange for monetary benefits. The user pays Apple for the handset and the SP for the service application. The SP can use the TSM of the TSM operator to perform lifecycle management of the application in return for monetary benefits. The value exchange between Apple and TSM operator is that they both offer a TSM that can connect the handset with SPs.

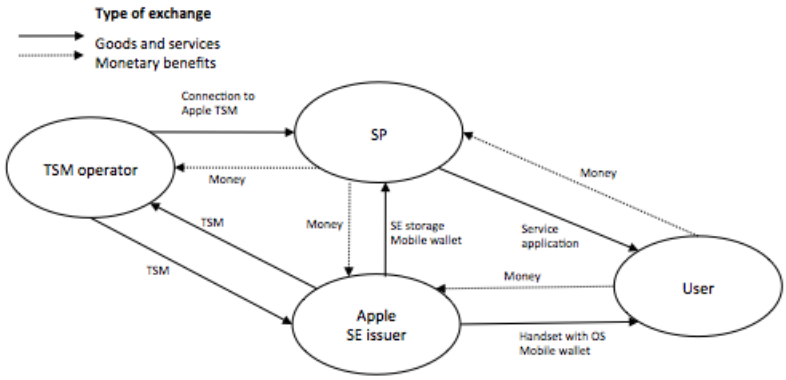


Figure 5-6: Value network embedded SE

Control points

Based on the resources and processes the control points in the embedded SE value network have been identified. Table 5-3 shows an overview of the control points related to the actors in the value network. The overview shows that Apple has different control points within this value network and can therefore extract a lot of value of the network. Therefore Apple is marked as a tier 1 player. The SP can also be seen as a tier 1 player because they offer the service to the user. The TSM operator is a tier 2 player because they contribute to service by allowing life cycle management. However, they are not directly involved. Based on the discussed value network and related control points, it does not seem likely that there will be a role for MNOs, as the SE issuer is able to offer similar services as the MNO.

Table 5-3: Control points embedded SE value network

Actor	Control point
User (tier 1/2)	Source of information Source of revenue
Apple (tier 1)	Embedded SE Mobile wallet/passbook Device OS distribution Device creation
SP (tier 1)	Service development/application
TSM operator (tier 2)	Working connection with Apple system

5.4 Value network Cloud-based solution

The third technical solution that has been discussed is a cloud-based solution, where the sensitive data is stored in the cloud rather than on a physical SE. As the cloud can be operated by the SP this cloud-based value network differs substantially from the other value networks. In the remainder of this paragraph the technical infrastructure is discussed, followed by the value network and control points. The processes related to this technical infrastructure can be found in Appendix D.

Technical infrastructure

Figure 5-8 shows the technical infrastructure of solution where the credentials are stored in the cloud rather than on a physical SE. This technical infrastructure can be used for all kinds of end services without having to make large adjustments to the technical infrastructure. In this infrastructure the application is stored on the OS of the mobile handset instead of on the SE. The application can be accessed and registered by making use of the mobile wallet. The cloud takes over the secure function of the SE, which means that the sensitive data and credentials are stored there rather than on a physical SE. The cloud is either hosted by the mobile wallet provider or a SP (Smart Card Alliance, 2014a).

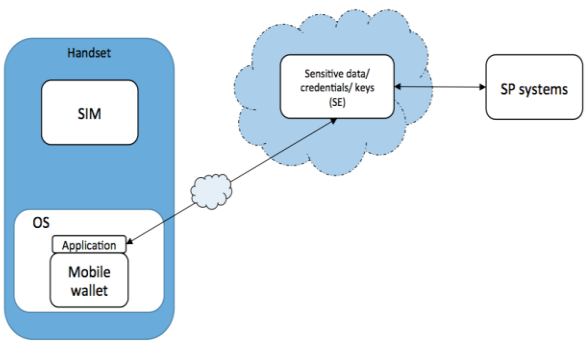


Figure 5-8: Technical infrastructure provisioning cloud-based solution

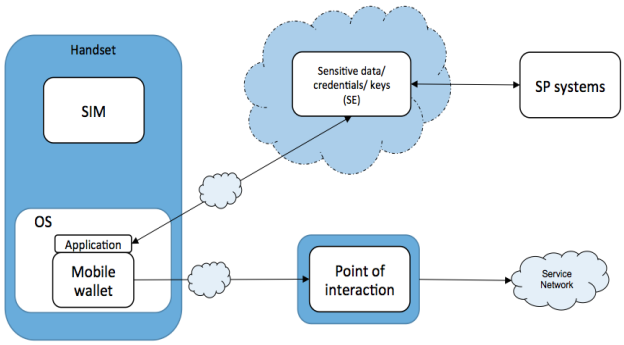


Figure 5-7: Technical infrastructure use of service cloud-based solution

Figure 5-7 is graphical overview of the technical infrastrucutre for the use of service. To use the service at the point of interaction a connection with the cloud is needed. The connection with the cloud provides keys or tokens necessary to conduct a transaction at the point of interaction. The keys are issued via the internet in a limited amount with a limited validity to ensure the safety of the transactions (Smart Card Alliance, 2014a). By making use of tokenization unique identification keys are created that replace sensitive data to enhance security. The connection with the cloud can be in real-time or at given intervals, although real-time would probably not be optimal for the user experience due to network latency (Smart Card Alliance, 2014a). Therefore the keys are often downloaded in advance and multiple transactions are possible. When the keys have been retrieved from the cloud the handset can make a transaction at the point of interaction, which has a connection with the underlying service network. An overview of the resource ownership and the related processes to the provisioning and use of service can be found in Appendix D.

Value network

The value network for a cloud solution is shown Figure 5-9. This value networks is based on the discussed technical infrastructure and the process, which are depicted in Appendix D. For this value network the assumption is made that the SP is also the wallet provider. The handset manufacturer provides the mobile device on which Android is used as OS. The SP assumes a central role in this value network as it offers a service to the user. The SP owns and manages the cloud that securely stores the credentials. The token provider is able to offer the SP a tokenization service that increases

the security as the sensitive data is replaced with unique keys. The value network shows that the complexity to offer a service is reduced for a SP with this solution, as less actors are involved. The SP is the focal organization in this network and is not dependent on a SE issuer. This solution seems to be a real threat for MNOs as it takes away a lot of complexity and that there is no role defined for the MNO. However, this solution is software based instead of hardware and this might prove to be an opportunity in regard to needed security.

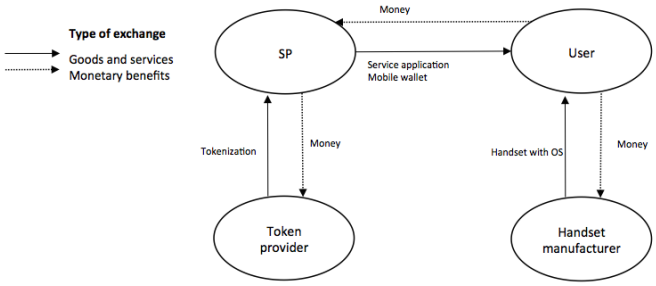


Figure 5-9: Value network cloud-based solution

Control points

In the value network of the cloud solution the control points related to the four actors are presented in Table 5-4. It shows that the SP has a number of control points and therefore they have a dominant position. The value network shows that a SP is less dependent of other actors in a cloud-based solution than with a SIM SE or embedded SE. This means that a cloud-based solution is an attractive option for SPs, as it allows them to maintain control over the value network. However, as discussed in chapter 3 the security of a software-based solution is lower, which is thus a trade-off to be made.

Table 5-4: Control points cloud-based value network

Actor	Control point
User (tier 2)	Source of information Source of revenue
SP (tier 1)	Cloud storage Service application Mobile wallet
Token provider (tier 3)	Tokenization system
Handset manufacturer (tier 2)	Device creation OS distribution

5.5 Conclusion: Opportunities for SIM

The three discussed value networks provide an overview of mobile authentication and identification solutions that are used in today's market. The first discussed value network defines a central role for the SIM and MNO, as the whole application is stored on the SIM. When MNOs are able to introduce this value network to the market the SIM will function as a critical resource.

The second value network that was discussed is the embedded SE value network. In this value network there is no role for MNOs or the SIM, as the handset manufacturer issues the SE. The embedded SE value network was based on the infrastructure of Apple pay. As Apple exploits the embedded SE, it is not likely that Apple will allow a role for the SIM card within the value network. Apple is a global player that enjoys a lot of power within their value network and therefore they have strict demands for all SPs that want to make use of their infrastructure. Overall it is safe to say that an embedded SE (even if Apple is not the issuer) does not allow a role for the SIM, as an embedded SE has similar capabilities as the SIM.

The third value network that was discussed was related to a cloud-based solution. In this a solution the SP plays a central role. A cloud-based solution stores the sensitive data in the cloud rather than on a physical SE. The application itself is stored in the OS of the handset. This means that the SIM is not needed to store the application. However, there is an opportunity for the SIM within this value network. A cloud-based solution is a software-based solution and, as discussed in chapter 3, software is seen as less secure than a physical SE. In a cloud-based solution the handset needs to provide authentication to the cloud, where the credentials are stored, to download keys that enable transactions. As the cloud has access to the private credentials, it is essential that the authentication is legitimated and secure. If the SIM is used as an authentication means to the cloud, it can enhance the security of a cloud-based solution. This would mean that MNOs would play a less central role and that they are not directly involved with the service offering to customer. Nevertheless, it could prove to be an opportunity for MNOs to exploit the SIM.

In two of the value networks the SIM could have a value-adding role. However, different initiatives of MNOs in the mobile payment market show that the struggles within a value network are not on a technical level but more on a business level. Collaborations between MNOs and banks have not led to great success, even though there was an understanding in the market that they should work together due to resources they owned (Dahlberg et al., 2008). De Reuver et al. (2014) show how a consortium in the Netherlands between the major banks and telecom companies was dissolved due to differences in strategic objectives and interests, conflicts, lack of dependencies and governance issues. This shows that it could be quite difficult for MNOs to collaborate with SPs such as banks. It is, however, essential for MNOs to team up with a financial institution in order to bring a mobile payment solution to the market (Ondrus, Lyytinen, & Pigneur, 2009). So, technically there is an opportunity for the SIM in a cloud-based and SIM SE value network but whether it can be realized depends on the collaborations between actors within the value network. Therefore in the next chapter, value network designs are constructed that relate to the application markets that have been discussed in chapter 4. These value networks should help to determine who the key actors are and how value is created in the markets of enterprise ID, government services and mobile payment. The value networks will serve as input for the interviews and help to determine whether the SIM qualifies as control point.

6. Design of value networks

In this chapter two value networks, which focus on different technical solutions, are designed for the application markets of enterprise ID, government services and mobile payment. These markets have been discussed in chapter 3 and have been marked as a possible opportunity for MNOs to target with mobile authentication and identification services. In chapter 4, it was concluded that the opportunity for the SIM is twofold. First, the SIM could act as a SE on which the whole application is stored. Second, the SIM can be used as an authentication means to the cloud in a cloud-based solution to enhance security. Based on these findings six value networks are designed in which the SIM function as control point, two for each application market. These value networks are used to identify actors, who can influence whether the SIM qualifies as control point. The value networks will therefore serve as input for the interviews with industry experts. The remainder of this chapter is as follows. First, value networks are designed related to the SIM SE. Second, the SIM-cloud designs are discussed. Finally, a conclusion is presented.

6.1 SIM SE designs

In chapter 5, a conceptualization of SIM SE value network was constructed. This showed that a SIM SE solution is a way for MNOs to offer mobile authentication and identification services. Therefore this paragraph discusses three value network designs in which the SIM SE functions as control point. As, mentioned, the designs relate to three different markets: enterprise ID, government services and mobile payment. The value networks are designed around tier 1 players: the MNO and SP. These parties offer critical resources needed for mobile authentication and identification services and will therefore form the core of the value network. Figure 6-1 shows the technical infrastructure of a SIM SE solution. Based on the added value that a resource or element has to another actor, control points are defined. Next, the value network related to enterprise ID is presented. Followed by the value network for government services. Finally, the mobile payment value network is depicted.

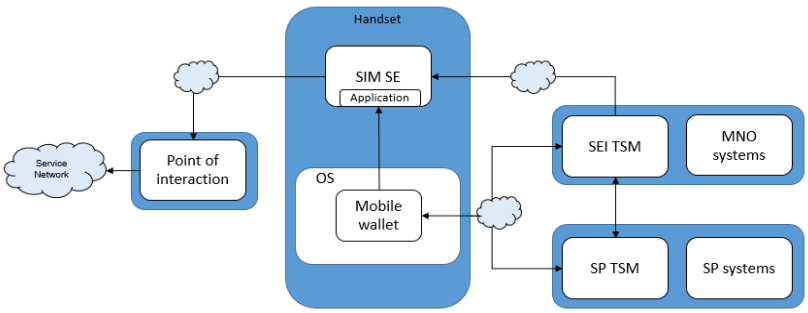


Figure 6-1: Technical infrastructure SIM SE

6.1.1 Enterprise ID

The value network for SIM SE - Enterprise ID is shown in Figure 6-2. This value network is constructed by combining the SIM SE value network with actors involved with the enterprise ID market. All actors own one or more control points that explain why they are part of the value network. In this value network three tier 1 actors are identified, the MNO, security company and employer. The MNO supplies the SIM. The security company can store an application on the SIM that can authenticate the user. The employer is the source of revenue, as they pay a security company for authentication and identification. The SIM vendor and handset manufacturer have a more supportive role, as they are not directly involved with the service offering but supply goods needed for the end service. At the end of the value network the user will use his handset to gain access to company assets. An overview of the value exchanges is provided Figure 6-2 and the related control points are presented in Table 6-1.

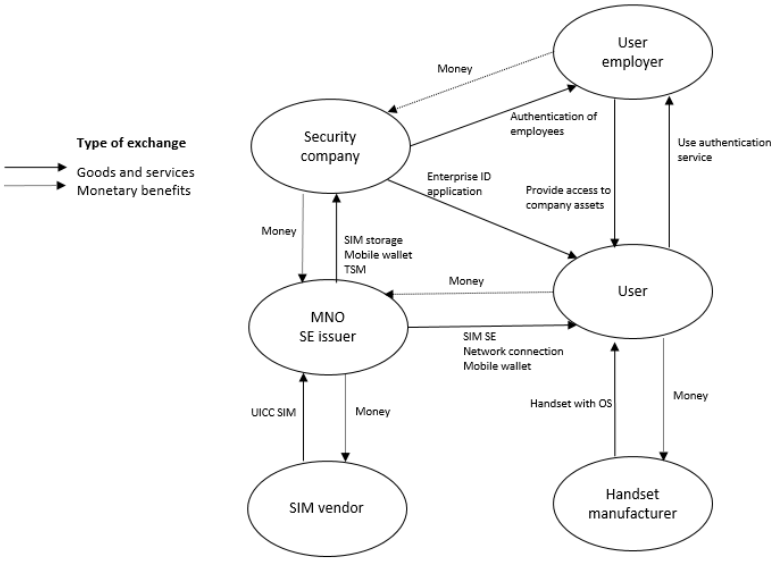


Figure 6-2: Value network SIM SE Enterprise ID

Table 6-1: Control points SIM SE - Enterprise ID

Actor	Control point
MNO (tier 1)	SIM SE Mobile network
User (tier 2)	Source of information Use of service
Handset manufacturer (tier 2)	Device creation Device OS distribution
SIM vendor (tier 3)	SIM creation
Security company (tier 1)	Supply of authentication service Customer base
Employer (tier 1)	Source of revenue Company assets

6.1.2 Government services

The value network related to government services is depicted in Figure 6-3. In this value network the government functions as SP. The government will provide its citizens with the ability to authenticate or identify themselves with their mobile handset. In return, the user will pay the government directly (fee) or indirectly (taxes) and use the service. The MNO provides the SIM on which the government can store its authentication application in return for monetary benefits. In this value network the MNO and government are marked as tier 1 players. The MNO is the SE issuer, while the government functions as SP. Both provide critical resources (SIM and m-government service) and therefore have a key role in the provisioning of the service to the customer. The user is marked as a tier 1/2 player because as a group they are a critical source of revenue. However, individually they have less power and can be replaced. So, overall three crucial control points can be determined in this value network. The actors and related control points that explain why and how they extract value from the network are shown in Table 6-2.

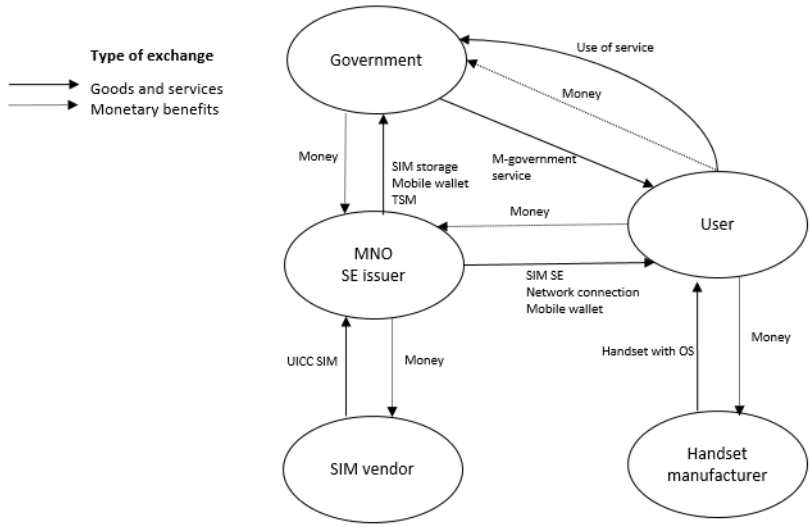


Figure 6-3: Value network SIM SE- Government

Table 6-2: Control points SIM SE - Government

Actor	Control point
MNO (tier 1)	SIM SE Mobile network
User (tier 1/2)	Source of information Source of revenue
Handset manufacturer (tier 2)	Device creation Device OS distribution
SIM vendor (tier 3)	SIM creation
Government (tier 1)	Creation of authentication service Legislative power

6.1.3 Mobile payment

Mobile payment is the third service market for which a value network is designed. The value network is presented in Figure 6-4. In this value network the issuing bank functions as SP. The SIM SE value network is extended by integrating the four-corner model. The issuing bank supplies the user with the payment service, which the user can use at the merchant. The acquiring bank processes the transaction on behalf of the merchant and the issuing bank on behalf of the user. The SP stores the application on the SIM in return for monetary benefits. In this value network the SE issuer and SP or issuing bank are seen as tier 1 players because they facilitate key resources (SIM and bank account) needed for mobile payment to the customer. The MNO supplies the SIM while the issuing bank offers the possibility to store a mobile payment application on the SIM. The user is the end point of the value network, as they will use the service. The other parties play a more supportive role and do not directly influence the service. For example, the role of the acquirer and merchant does not change if a mobile payment is conducted rather than a smart card payment. The control points related to each actor are defined in Table 6-3.

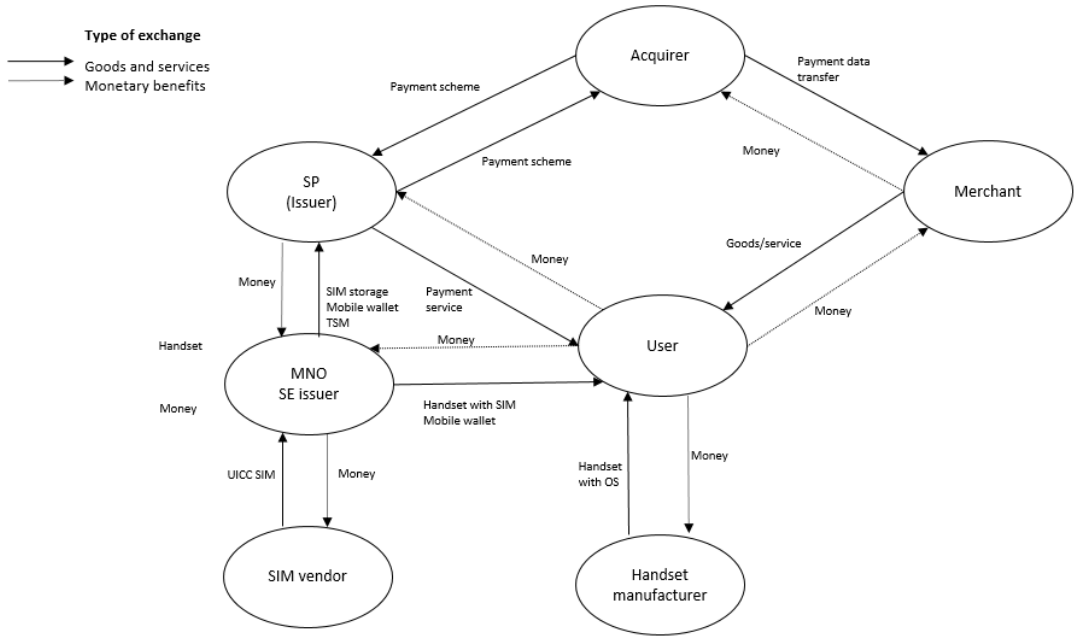


Figure 6-4: Value network SIM SE - Mobile payment

Table 6-3: Control points SIM SE – mobile payment

Actor	Control point
MNO (tier 1)	SIM SE Mobile network
User (tier 1/2)	Source of information Source of revenue
Handset manufacturer (tier 2)	Device creation Device OS distribution
SIM vendor (tier 3)	SIM creation
Issuer (tier 1)	Mobile payment service Customer bank account Access to payment network
Acquirer (tier 3)	Bank account merchant Access to payment network
Merchant (tier 3)	Goods/service facilitation

6.2 Cloud - SIM designs

Chapter 5 concluded that the SIM could be used as authentication means to the cloud to enhance security. With this solution the application is stored in the OS of the handset while the credentials are stored in the cloud of the SP. Before the service can be used tokens need to be downloaded from the cloud that can enable the transaction. To download the tokens the handset must be authenticated to the cloud. The SIM could prove to be a secure means to do so. The technical infrastructure related to this solution has been depicted in Figure 6-5. The related value networks are constructed around the SPs, as they are marked as the structural players of the value networks. They facilitate the service to the customer and own the cloud. The value network is constructed extending the cloud-based value network that has been discussed in chapter 4. The MNO is included as authenticator. Furthermore, the value networks are adjusted to the specific service markets of enterprise ID, government services and mobile payment.

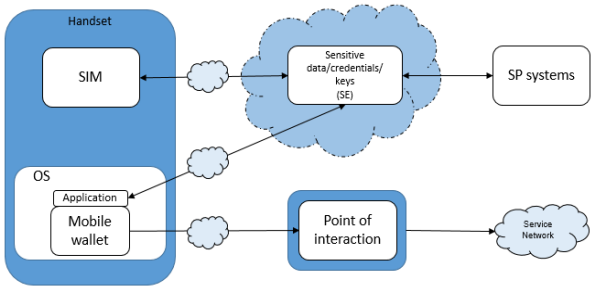


Figure 6-5: Technical infrastructure Cloud-SIM

6.2.1 Enterprise ID

Figure 6-6 shows a SIM-Cloud value network and related value exchanges designed for the enterprise ID market. In this value network the security company and employer are marked as tier 1 players. The security company is offers the authentication service to the employer, who can then allow its employees to authenticate themselves. In this value network, the security company owns the cloud in which the tokens and credentials are stored. The employer is the source of revenue and therefore a crucial player in this value network. The user is the end point of the value network, as he will use the service to gain access to the company's assets. The value network shows that a SIM-Cloud solution assumes a less central role for the MNO. The SIM is only used to authenticate the handset to the cloud of the SP and therefore the MNO plays a contributing role rather than a structural role. Other actors that play a supportive role are the handset manufacture and token provider, as they are not directly involved with the service offering but supply resources that contribute to the development of the service. An overview of the control points that contribute to the value creation of the service can be found in Table 6-4.

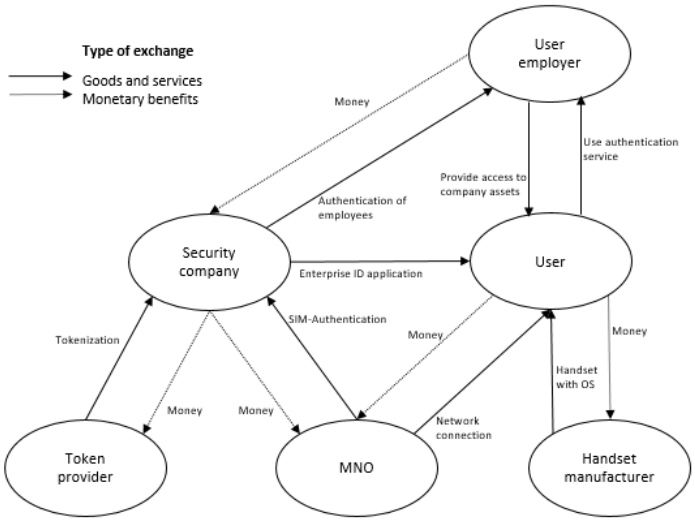


Figure 6-6: Value network Cloud - SIM Enterprise ID

Table 6-4: Control points Cloud – SIM - Enterprise ID

Actor	Control point
MNO (tier 2)	SIM authentication Mobile network
User (tier 2)	Source of information Use of service
Handset manufacturer (tier 2)	Device creation Device OS distribution
Security company (tier 1)	Creation of authentication service Cloud Customer base
Employer (tier 1)	Source of revenue Company assets
Token provider (tier 3)	Token creation

6.2.2 Government services

The SIM-Cloud value network for government services shows a key role for the government as supplier of the authentication service to its citizens. The government can be viewed as a tier 1 player, as it holds crucial control points such as the cloud and the creation of the authentication service. The government can oblige its citizens to use the service. For instance, DigiD is needed for taxes. The citizens will therefore be the end users of the service. In this value network the SIM and MNO have a contributing role, as they can authenticate and identify the user's handset but are not directly involved with the offering the service to the customer. The token provider and SIM vendor both offer resources that provide a supportive role in the value network. An overview of the value network members and related control points can be found in Table 6-5.

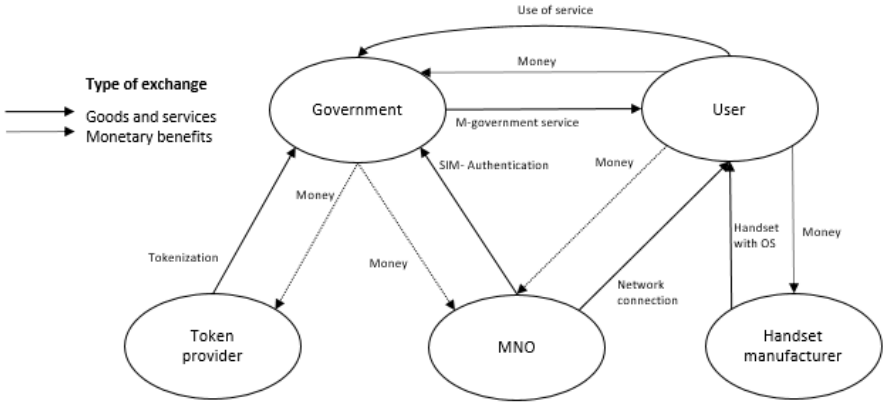


Figure 6-7: Value network Cloud - SIM Government

Table 6-5: Control points Cloud - SIM Government services

Actor	Control point
MNO (tier 2)	SIM authentication Mobile network
User (tier 1/2)	Source of information Use of service
Handset manufacturer (tier 2)	Device creation Device OS distribution
Government (tier 1)	Creation of authentication service Cloud Legislative power
Token provider (tier 3)	Token creation

6.2.3 Mobile payment

The SIM-Cloud solution for mobile payments shows a focal role for the issuing bank. This bank supplies its customers with a mobile application and controls the service, the cloud and the consumer's bank account. Therefore the issuing bank is a tier 1 player. The value network is depicted in Figure 6-8. The SIM-Cloud solution is integrated with the four-corner model. It shows that the merchant and acquirer have a supportive role in facilitating the mobile payment. However, their role will not change if a handset is used rather than a smart card. They are therefore marked as supportive players in this value network. The MNO, who authenticates the handset, can be seen as a contributing player, as they increase the security of the solution. The handset manufacturer creates the handset and decides on the OS that is distributed is marked as a supporting player because they are not directly involved with the service offering. An overview of the control points that each actor has in the value network is given in Table 6-6.

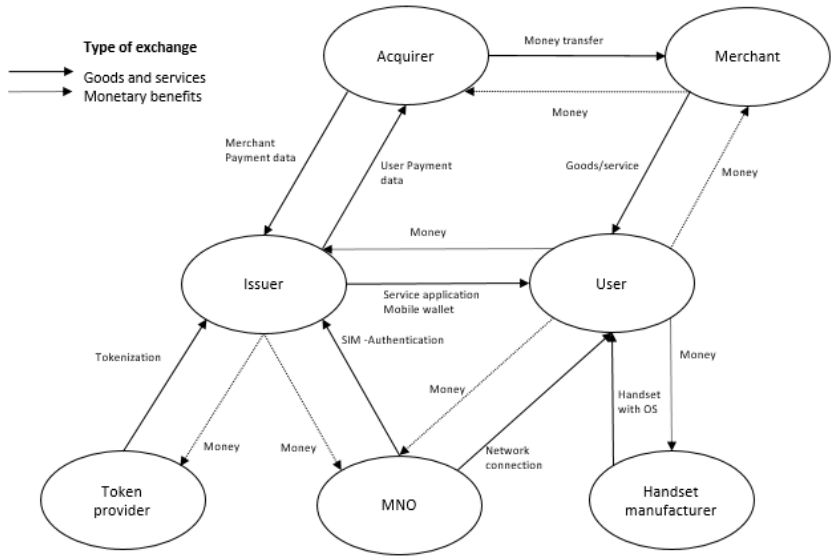


Figure 6-8: Value network Cloud-SIM Mobile payments

Table 6-6: Control points Cloud - SIM mobile payments

Actor	Control point
MNO (tier 2)	SIM authentication Mobile network
User (tier 1)	Source of information Source of revenue
Handset manufacturer (tier 2)	Device creation Device OS distribution
Issuer (tier 1)	Mobile payment service Customer bank account Cloud Access to payment network
Token provider (tier 3)	Token creation
Acquirer (tier 3)	Customer base Access to payment network
Merchant (tier 3)	Distribution of services/goods Point of sale

6.3 Conclusion

In total six value network with the related control points have been constructed. These networks consist of two technical designs for three application markets. The first technical solution focuses on a SIM SE solution, where the whole application is stored in the secure environment of the SIM. The second technical solution is a Cloud-SIM solution. In this solution the application is stored in the OS of the handset and the credentials of the application are stored in the cloud. In this solution the SIM is used to authenticate the handset to the cloud. These technical solutions can be used for all kinds markets that require secure authentication and identification measures as well online as offline. For this research three markets are researched in the form of Enterprise ID, Government services and mobile payment. Therefore the following value networks have been designed:

- SIM SE
    - Enterprise ID
    - Government services
    - Mobile payment
- Cloud-SIM
    - Enterprise ID
    - Government services
    - Mobile payment

Per technical solution the technical infrastructure is quite similar, however the involved actors differ per service application as the SP and related service network differ per application market. Value networks can map the value exchanges between actors and control points help to explain how these actors can extract value from these networks. In the designed value networks the SIM is incorporated as a control point for MNOs.

A major difference between the SIM SE value networks and SIM-Cloud value networks is that in a SIM SE value network the MNO and SP are marked as tier-1 players, while in a SIM-Cloud value network the SP is seen as a tier 1 player and the MNO as a tier-2 player. The SIM SE allows for a more dominant role for the MNO. However, both value networks show that the SIM can contribute to create a secure authentication and identification service. In order to determine whether these value networks are viable, they will be discussed with industry experts. The experts are consulted on whether they find a role for the SIM and MNOs viable within the three application markets.

7. Methodology

In the previous chapter six value networks have been designed in which the SIM qualifies as a control point. In this chapter an interview setup is discussed that should help to validate the designs. As this research has an explorative nature limited data is available. Interviews are therefore a suitable method as it allows for a more in depth discussion on the value networks and the role of MNOs and the SIM, when offering mobile authentication and identification services. The six value networks are conceptual designs and therefore interviews with industry experts should provide insight in whether the SIM could indeed qualify as control point. Industry experts have experience with real-world solutions and their tacit knowledge and perspectives could be of a value for this research, as they could provide insights beyond the scientific literature. The remainder of this chapter discusses the selection of respondents, the interview protocol and the data analysis approach.

7.1 Selection of respondents

For this research a broad diversity of respondents was sought to gain a comprehensive overview of the industry thoughts on the SIM as a means for authentication and identification. Aside from a diverse group, the aim was to include respondents that are affiliated with the tier 1 organizations in the value networks, which are the SPs and MNOs. These parties play a key role in the service delivery. As the focus within this research is on the opportunities for the SIM, only actors that are directly involved with the facilitation of the mobile service were marked as relevant to interview. Actors related to the underlying service network are less relevant as their role will not change when implementing a mobile service. Besides actors involved with the value networks, independent experts have been interviewed that have knowledge and experience with mobile authentication and identification services. This could lead to new insights on relations and struggles among the actors involved. Independent parties can speak more freely as they are not directly involved with the value network. Besides being affiliated with the mentioned parties, respondents were sought that had knowledge on a technical or/and business level, as the value networks have been constructed on an organizational level and on a technical level. By interviewing respondents with different technical expertise a comparison between the SIM and technical alternatives can be made. The respondents that are involved on a business level can provide insight in the added value of the MNO in the network and whether this role is feasible.

The interviews candidates were acquired in a number of ways. First, the client network of UL Transaction Security was consulted. Second, the network of academics from the Delft University of Technology was contacted. Third, the researcher's personal network was used to make contact with industry experts. Finally, interviewees were asked if they knew experts that could be of value for the research. This approach led to a diverse group of respondents that fall within the defined type of experts. In total 16 candidates have been interviewed. The number of respondents has been the result of the saturation principle that has been applied in this research. Table 7-1 provides an overview of the type of respondents that have been interviewed. The respondents have been made anonymous, as some of the respondents shared confidential information. All the experts have been interviewed on their field of expertise in relation to their organization. This means that a MNO has been asked to give their view on the all three application markets while banks have only been interviewed on the topic of mobile payments. Per application market 9 to 11 industry experts were consulted.

Table 7-1 Overview of respondents, functions and expertise

Code	Role	Function	Expertise	Technical expertise	Business expertise
MNO1	MNO	Manager mCommerce	mCommerce	✓	✓
MNO2	MNO	Manager mCommerce	mCommerce	✓	✓
BA1	Bank	Sr. Product manager	mCommerce	+/-	✓
BA2	Bank	Cards and online payments professional	mCommerce	+/-	✓
BA3	Bank	Sr. Product manager	mCommerce	✓	✓
GOV	Government	Chief Security Officer	Government services	✓	✓
IE1	Independent expert	Managing consultant	Authentication	✕	✓
IE2	Independent expert	Consultant	mCommerce	✓	✓
IE3	Independent expert	Consultant	Government services	+/-	✓
IE4	Independent expert	Card scheme manager	mCommerce	✓	✕
IE5	Independent expert	Business developer	mCommerce	✓	✓
IE6	Independent expert	Managing partner	Authentication	✓	✕
IE7	Independent expert	Associate professor	mCommerce	✕	✓
IE8	Independent expert	Program Director	mCommerce	✕	✓
IE9	Independent expert	Senior consultant	ICT Government	✕	✓

The goal was to interview multiple technical and business experts with a minimum of three per role. In practice this turned out to be rather difficult, which means that not all the expert roles have been covered during the interviews. Unfortunately, we were unable to interview SPs that offer enterprise ID services. These service providers are traditionally located outside of the Netherlands and their products are often sold through an integrator. Although efforts have been made to schedule an interview through these integrators the results turned out to be negative. Next to that, efforts have been made to schedule interviews with experts from the four major MNOs in the Netherlands. As MNOs stand at the centre of this research it would be very useful to have their view on mobile authentication services. Two out of four MNOs responded positively for an interview. The other MNOs responded that an interview would not be of use, as they do not undertake any efforts on mobile authentication and identification services. However, for this research it would have been relevant to know why these parties are not developing any mobile authentication services but unfortunately this was not possible. Furthermore, only one government organization has been interviewed, as we were unable to schedule interviews with other organizations. In general, it turned out to be hard to interview actors that are directly involved with the value networks. Interviewing multiple independent industry experts that were closely related to the specific SPs and had sufficient knowledge on the topic covered this gap. Next, to that it was undesirable to schedule multiple interviews with the same company due to existing business relations of the publishing company. Therefore it was not possible to schedule interviews with a technical and business expert of the same company. However, most of the interviewees turned out to be well grounded on technical as well as on a business level. One of the interviews turned out to be less relevant for the research and therefore this interview was not further used.

7.2 Interview structure

The interviews have been conducted by using a semi-structured approach. The semi-structured approach gives the respondent the ability to share his view on the industry by addressing aspects that he finds important while ensuring that information on the SIM as control point can still be gathered. The interview protocol has been designed to evaluate the control point criteria that have been identified in chapter 2. These criteria have been converted into interview questions. Next to that, interview questions have been formulated to evaluate the role of the MNO in the different application markets. Table 7-2 provides an overview of the interview protocol. The interviews lasted between 40 and 60 minutes and in two select cases the interviews were reduced to 30 minutes due

to the agenda of the respondent. In advance of the interview, the respondent was sent a letter that contained a brief introduction of the research. At the start of the interview the goal of the research was further explained.

Table 7-2 Interview protocol

Concepts	Question
Introduction	• Is audio recording allowed? • Explain the research and the research objective • Explain structure of the conversation
SIM	• What is your opinion on the function of the SIM in regard to mobile authentication and identification services?

Application markets	• What do you find interesting markets to target with mobile authentication and identification services and why?
	• Are the following service markets options for your company to offer mobile authentication and identification services considering the market size, potential revenue and needed security:
	  ○ Enterprise ID (e.g. Physical access, intranet)
	  ○ Government services (e.g. online identity, mobile passport)
	  ○ Mobile payment (e.g. online, proximity)
	• What do you see as requirements when offering mobile authentication and identification services to the specific markets?

Value network	• What is your opinion of the value networks and do you see a role for your company?
	• What role is the most likely role for the MNO in the different service markets:
	  ○ As cloud authentication provider?
	  ○ As SE provider?
	  ○ Or no role at all?

Control point criteria	
Uniqueness/scarcity	• What added value can the SIM provide to your company in regard to mobile authentication and identification services? • What technical alternatives would you consider when offering authentication services and why? • What technical solution would have you preference and why? • Why not another solution?
Demand	• For what service would the SIM be of added value and in what technical form? • What market share would the MNO be able to capture with the SIM for this service? • What are limitations of the SIM when offering authentication and identification services on a business and organizational level?
Value	• What influence does the SIM give the MNO in the value networks? • Can the SIM function as a revenue source to the MNO? • What would be a revenue sharing model that is likely to be supported by the service providers?
Time	• Do you see the SIM as a long-term solution for mobile authentication and identification services?
Triggers	• What are external (technical, organizational, business, social acceptance) factors that may influence the SIM as control point? • How do you estimate the chances of these factors indeed influencing the SIM as control point?
Concluding	• Do you have additional remarks or thoughts that you want to share?

7.3 Data analysis

In order to answer the research question the interviews must be processed and analysed. First, the interviews have been transcribed by making use of notes and audio recordings. The data was structured by coding the transcripts by making us of the Atlas.ti software. Coding helps to build a theory to answer the research question. Coding takes place in three rounds: open coding, axial coding and selective coding. In the first round of coding key elements related to authentication

services are highlighted. In the second round of coding the interview transcripts are analysed and the focus is on finding communalities and differences related to the SIM and the MNO in regard to the concepts of control points and value networks. Finally, selective coding was done where the findings of the interviews are coupled to the control point criteria.

Based on the coded answers of the respondents, an assessment is done whether the SIM qualifies as control point in the three application markets. The assessment consists of three steps. The first step is to determine whether industry experts believe there is a business case for mobile authentication and identification services in the application markets. If the industry experts do not see the application market as an opportunity for mobile authentication and identification services, it is not likely that MNOs will target that market and therefore the designed value network will not be viable. During the second step, the SIM is evaluated on the control point criteria, which are shown in Figure 7-1. This allows for an assessment of the potential strength of the SIM as control point. Finally, the value network and the role of MNO are analysed. The value network can only be viable if the MNO and the SP are open for collaboration. Based on these three steps of analysis it can be determined whether the SIM could qualify as control point in the three application markets.

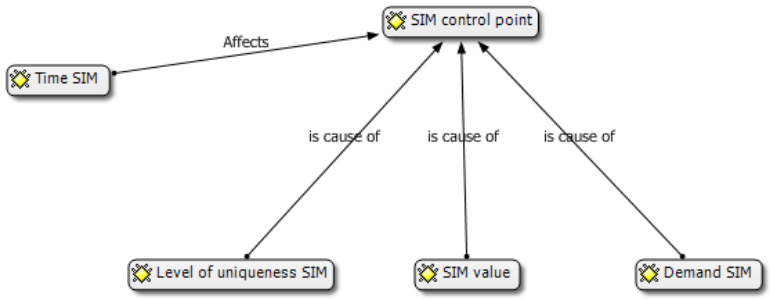


Figure 7-1: Control point parameters

8. Results

In this chapter the main findings of the interviews are discussed. The interview results focus on the question: *What is the viability of the SIM as control point for mobile authentication and identification services?*

The answer to this question was obtained during fifteen interviews using the designed value networks from chapter 5 and the interview protocol from chapter 6. The answers of the respondents are linked to codes that are presented in Table 7-1. The interviews focused on three application markets for mobile authentication and identification services: enterprise ID, government services and mobile payment. The results are discussed in three categories. First, the business case for the application markets is defined. Second, per application market it is discussed how the SIM scores on the control point criteria. Third, the results on the viability of the value networks are presented. Finally, a conclusion is presented.

8.1 Business case application markets

During the interviews the respondents were asked to give their view on the business case for the markets of enterprise ID, mobile payment and government services in regard to mobile authentication and identification services. This is the first step of the analysis, as MNOs will only target markets that can generate business to them. A condition for a control point is that the value network must be viable and this is not the case if the application market has limited business for MNOs. When the application market proves to be an opportunity for authentication and identification services, then the next step is to assess whether there is a role for the SIM and MNO. The remainder of this paragraph first discusses the results for the enterprise ID market. Second, the results on the business case for mobile payments are presented. Finally, the results on the government services are discussed.

8.1.1 Business case enterprise ID

The enterprise ID market was discussed with the two MNO and seven independent experts. According to one of the MNOs "*an Enterprise ID service would be a nice to have service but it has no priority. Currently, our focus is on the consumer market, as we focus on services that are used on a daily basis and can be used by everyone"* [MNO2]. Both MNOs recognize that the SIM could be used to facilitate these services but that they focus on other markets first. The strategy of the MNOs is currently aimed at solutions that can be implemented on a short-term and therefore they find the markets of mobile payment and public transport more interesting [MNO1, MNO2]. Next to that, [IE5] explained that his company had examined the possibility to offer enterprise ID services, as there is a high penetration of NFC technology. However, he stressed that "*a mobile authentication system leads to high investment costs and that it will have to co-exist with the current authentication system, as not every handset is suitable for mobile authentication."* This means that when an enterprise requires authentication, it has to invest in a system that cannot be used by all employees and visitors. Therefore the mobile authentication system should co-exist with another system that is able to serve all users. For this reason it is not likely that a mobile authentication system would be able to replace an existing authentication system that makes use of smartcards. A number of experts [IE2, IE5, IE6, IE8] share this view and stated that although mobile authentication is technically possible for enterprise ID services, it is not likely to replace systems that are currently being used for authentication. The two main reasons for this are the related investment costs for the customer (enterprise using and implementing the authentication service) and that there is no need to replace existing authentication systems that make use of smartcards, as it still suffices. One expert [IE4] did see a potential market for Enterprise ID services: "*Implementing a nationwide system such as mobile payment is very complex and will take a long time to realize. Therefore MNOs should focus on more specific markets such as enterprise ID. There it is much easier to implement a new authentication system, as it involves fewer parties and is therefore less complex. The user experience is often not*

great in these markets, which means that a lot of improvement is possible for the authentication procedures at large cooperation's. So, I believe there is a business opportunity in market where the authentication and identification procedure can be improved". The related investment costs that were addressed by the other respondents were not discussed during this interview. The respondent did state that he believed that companies would be willing to join a MNO authentication system if it was offered for the right price [IE4].

As most of the respondents stated that they currently do not believe there is a business case in the enterprise ID market, there was no use to further discuss how and if the SIM could function as control point in this market. Based on the interviews, it seems unlikely that MNOs will target this market in the near future, which means that the constructed value network is not realistic. So, according to the interview results, the SIM will not qualify as a control point for authentication services in the enterprise ID market.

8.1.2 Business case mobile payments

The second market that was addressed during the interviews is mobile payments. This market was discussed with two MNOs, three financial institutions and eight independent experts. Banks will serve as SP and will have to pay the MNO if they decide to use the SIM. Therefore their view on the mobile payments market can provide useful insights in the business case. One of the banks [BA3] explained that they introduced a mobile payment application that was only available on two handsets and that it led to a lot of disappointment among their customers. "*We see that customers are waiting for mobile payments and that there is a lot of demand for the product. Mobile payment is one of the few products that we introduced without advertising and still we see a lot of use and downloads of the application".* This quote relates to the views of most respondents that there is a market drive for mobile payment [BA1, BA2, BA3, MNO1, MNO2, IE5, IE6]. Many consumers are eager to use their mobile for payments. Next to that, all major banks in the Netherlands are working on solutions to introduce mobile payments to the market [BA2]. As banks feel the need to push mobile payment to the market [IE1], they could be biased in their view on the demand. This has, however, no major impact on the opportunity for the SIM. If the banks feel the need to introduce a mobile payment application, it means that they will have to use a technology to do so. So, the market drive shows that there is a demand for mobile payment on a business level. An important side note is that [BA3] mentioned that "*introducing a mobile payments solution will only increase our costs, as for the coming ten years it will co-exist with the regular payment card. Banks have a limited budget for mobile payments".* However, in contrast to this view another bank [BA1] said that: "*because Rabobank already introduced a payment solution to the market it is easier to raise budget for developing mobile payments, as we are lagging behind our competitors.* Overall, the statements show that the banks are eager to facilitate mobile payments to their customers. However, the banks stress that the costs for mobile payments must be reasonable because they have limited budget available [BA1, BA2, BA3].

The MNOs see the mobile payment market as a new opportunity to offer extra services to their customers. Payments are conducted on a daily basis and can be used by everyone. They see it as a big market that enables a lot of other services [MNO1, MNO2]. One of the MNOs said "*mobile payments is an enabler of the customer journey for all kinds of other services. For instance when buying tickets for a concert, then mobile payments is an enabler for the purchase of the ticket"* [MNO1]. This shows that the MNO wants to provide its customers additional services that they can use on a daily basis. The MNOs have the long-term ambition to offer all kinds of mCommerce services to their customers and see mobile payment as the start to do so, as it has many use cases [MNO1, MNO2]. Overall, MNOs find it important to offer mCommerce as an extra service to their customers to create customer retention.

There were two respondents that did not see business case in mobile payments for different reasons. One expert [IE2] said that the payment system in the Netherlands is so stable and efficient that there limited revenue to be made. Besides, he mentioned that mobile payments improve the ease of use with a minimum. The expert raised the question: "*How much easier is it to grab your mobile phone and use it for a payment than to grab your payment card?"* He does not consider it likely that consumers will adapt mobile payments in the near future, as it is not a real improvement of the current system [IE2]. The other respondent [IE8] did not think that there was a use case for mobile payment, as there is no organization that has sufficient reach to implement a solution that can serve the whole market. Standardization and reach are needed for success and currently the market is too fragmented to provide a solution [IE8, BA2]. Only collaboration between parties that have the ability to facilitate payments with parties that have reach over all handsets could solve this problem. However, such collaboration (SIXPACK) has failed in the past and it is not likely that a new one will be started [IE8]. These findings relate to the discussed literature on mobile payments.

Based on the interviews the mobile payment market scored well as eleven out of thirteen respondents think that there is a business case for mobile payment. The respondents see sufficient market size as many consumers are willing to use their mobile handset for payments. Next, to that banks show willingness to introduce mobile payments to the market. The Rabobank has already introduced a mobile payment solution that is available for two handsets. It shows that the industry is working on the introduction of mobile payment solutions. Besides, the banks and the interviewed MNOs feel the need to introduce mobile payments to the market as an extra service for their customers. This means that the interviewed banks and MNOs want to facilitate mobile payments. Overall, the majority of the respondents think that there is a market for mobile payments. Therefore the designed value networks for mobile payments can occur, especially since the key players (MNO and banks) are open to provide such a service. Whether the designed value network is indeed viable and whether the SIM qualifies as control point in the mobile payment market is discussed in paragraph 8.2.

8.1.3 Business case government service

The third application market that was discussed with the respondents is that of government services. This market was discussed with one government organization, two MNOs and nine independent experts. Six of the respondents pointed out the current development of the eID scheme in the Netherlands as a real opportunity for mobile authentication and identification [MNO1, GOV, IE1, IE3, IE6, IE9]. The eID scheme is new standard for online identification that is being developed by the Dutch government in co-operation with the business sector. It can be seen as the successor of the old and less secure DigiD. The government wants to allow a user to login with secure and trusted means and allows the possibility for businesses to connect to the eID scheme. One of the experts pointed out that "*the government can oblige their citizens to use a certain authentication means and therefore it can be successful. DigiD in the Netherlands is an example of an authentication service that has many users, as it is needed to do your taxes"*[IE1]. So, if a company can provide an authentication means for government services, it will have sufficient market size. However, this would also lead to dependency upon of the government.

The RDW is a governmental organization that is actively involved with discussions on the development of the eID scheme in the Netherlands. "This is because as a governmental organization t*he RDW hopes to become a supplier as well as a customer of the eID scheme"* [GOV]. The RDW supplies citizens with a driver's license that contains a chip, which could be used to store an eID. Furthermore, the RDW will be a user of the eID scheme, as they require secure authentication for when citizens want to register a vehicle [GOV]. Two experts [GOV, IE3] pointed out that the government wants a robust system and therefore want different companies that can provide secure authentication and have reach to connect to the eID scheme. If multiple authentication means (e.g.

bankcard, SIM or ID card) could be used the system would be more robust, as it offers the user alternatives to log in. So, if the chip on the bankcard is damaged then the user can still connect to the eID scheme, as he can make use of his ID card or SIM.

All the respondents stress that government services are privacy-sensitive and that there is a need for security. Two independent experts stressed that because of these privacy issues it is unlikely that in the coming years a persons identity is placed on the mobile handset [IE5, IE7]. "*From a societal perspective it is currently is not desirable to store an identity on the mobile handset. Scandals such as the Snowden affair have led to lack of trust among citizens and therefore due to privacy issues they are not willing to store their identity on a handset".* Due to a lack of trust and strict regulations related to privacy the two experts did not find it likely that there is a business case for mobile authentication and identification for government services [IE5, IE7]. One of the MNOs did not think that there is currenlty a business case in government services, as these are not used on a daily basis. The MNO focuses on consumer applications that can be used on a daily basis with large scale and which can be implemented short-term. Furthermore, the MNO stated that: "*The eID is still under development and has an uncertain outcome and is therefore currently not of interest to us. It is something for the long-term"* [MNO2]. This relates to the strategy of the MNO, which focuses on solutions that can be used now. Therefore their focus is more on mobile payment and public transport. These are all use cases that can be implemented now. Although, the other MNO acknowledges that their main focus is on mobile payment, they do see an opportunity for the SIM to be an identity carrier and therefore they are actively evaluating their options [MNO1, IE3]. What the reason is for this difference of opinion is unfortunately unclear and has not been discussed during the interviews. A possible explanation could be that MNO1 has a more local character and focus, while MNO2 offers its SIM based solution in multiple countries.

Furthermore, during the interviews the respondents were asked if the SIM SE could be used for offline services such as storing government documents (e.g. driver's license on the handset). Technically the SIM would be capable of securely storing a driver's licence on the handset [GOV, IE7]. However, the RDW, who is the issuer of the driver's license, said that it would require a change of European law and this could take years. Therefore it is not likely that the storing the driver's license or other government documents (ID card or passport) on the SIM would be a use-case anytime soon. This was in line with the answer of different experts [MNO2, IE4, IE5, IE7], who did not think that it would be a use-case. The interviews show that using the SIM for offline government services is not likely on a short-term and therefore it has not been further discussed. Therefore the focus for government services is on the SIM as an authentication means to the cloud. Based on the interviews the conclusion is that most of the respondents see an opportunity for mobile authentication for online services [MNO1, GOV, IE1, IE2, IE3, IE4, IE6, IE9]. The eID scheme relates to this opportunity, as it is a new identification standard that is being developed by the Dutch government in co-operation with the business sector. MNOs have the possibility to connect to this system and therefore the SIM could possibly qualify as control point in this market. The strength of the SIM and feasibility of the value network related to government services is discussed in paragraph 6.3.

8.1.4 Conclusion

The respondents were asked to give their view on the business potential for mobile authentication and identification services in the markets of enterprise ID, government services and mobile payment. Based on the interviews, it is concluded that the respondents do not find it likely that there is a demand and thus a business case for mobile authentication and identification services in the enterprise ID market. Therefore it is not probable that MNOs will target this market. This means that the designed value network is not viable and that the SIM does not qualify as a control point for the enterprise ID market. The respondents did think that there is a business case for providing authentication and identification for online government services. The development of the eID

scheme was marked as a real opportunity and therefore this is further discussed in the next paragraph. For offline services such as storing a driver's license on the SIM, the respondents did not think that would be a business case in the near future, as it would require a change of law. Besides government services, most of the respondents saw a market drive for mobile payments. The banks and MNOs are willing to facilitate mobile payment, which shows that there is a possible business case in this market. Mobile payments are therefore further analysed in the next paragraph.

An overview of the results on the business case per application market is presented in Table 8-1. It shows the number respondents per role that have a positive or negative view towards the business case in the markets of enterprise ID, mobile payment and government services. In total the interviews of fifteen respondents have been analysed. Not every respondent had knowledge of each application market, which explains the difference in the number of respondents per market. For instance the interviews with banks were only used for mobile payments, while the MNOs were asked about all three markets.

Table 8-1: Overview respondents on business case per application market

Application market	Role respondent	Positive view	Negative view
Enterprise ID	MNO	0	2
	Independent experts	1	6
	Total	**1**	**8**
Mobile payment	MNO	2	0
	Banks	3	0
	Independent experts	6	2
	Total	**11**	**2**
Government services	MNO	1	1
	Government	1	
	Independent experts	6	3
	Total	**8**	**4**

8.2 Results mobile payment

As paragraph 8.1 shows, most of the experts believe there is a business case for mobile payments. Therefore this paragraph discusses whether the SIM can meet the control point criteria. The findings of the interviews are linked to the control point criteria. Next to that, this paragraph discusses the viability of the mobile payment value network by discussing whether the banks and MNOs are open for collaboration.

8.2.1 Control point analysis

In the interviews multiple industry experts on mobile payment and authentication have been asked to give their view on the capabilities and the value of the SIM in comparison with other technical solutions. As explained in chapter 3, alternatives for the SIM exist in the form of an embedded secure element and a cloud-based solution. The strength of a control point depends on four parameters: value, demand, uniqueness and time. The parameter value represents the amount of value that the control point is able to extract from the value network, which can be tangible as well as intangible. The demand relates to the market share that the SIM is able to capture. Furthermore, a control point

is scarce and cannot be replaced easily. The final parameter relates to the fact that the value of the parameters changes over time.

During the analysis of the interviews it showed that the parameters overlap. The level of uniqueness has a direct effect on the strength of a control point but also indirect. The level of uniqueness has effect on the parameters demand and value because if there are alternatives for the SIM then this will likely lead to less market share. Next to that, if the level of uniqueness that the control point offers is low, then the value that the control point represents will be less, as there are other options that can take over its functions. The parameter demand also influences the value of the control point, as the scarcity principle shows that more demand leads to higher pricing. An overview of this overlap is depicted in Figure 8-1. Since these parameters have overlap, a number underlying factors influence multiple parameters. These factors have been derived from the interviews and are discussed next in relation to the SIM as possible control point.

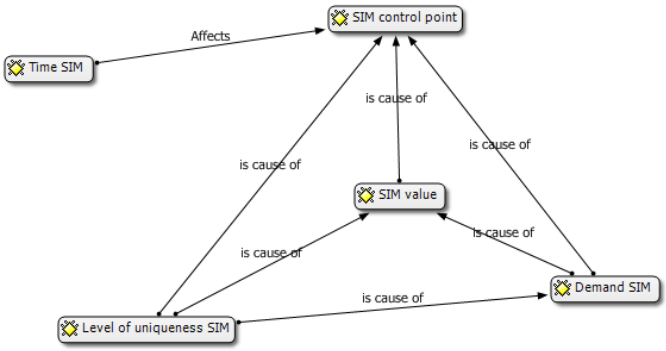


Figure 8-1: Control point parameters

Level of uniqueness SIM

The level of uniqueness of the SIM is determined by making a comparison with other solutions. The respondents were asked to compare the SIM with an embedded SE and a cloud-based solution. One of the MNOs said that "*a clear benefit of the SIM is that it is issued to all their customers and therefore it can take away the fragmentation among handsets*" [MNO2]. An industry expert added that "*the SIM is the only standardized element within the handset*" [IE6]. Due to the fragmentation of handsets and lack of standardization there is a fragmentation of embedded SEs [MNO1, MNO2, BA2, BA3, IE1, IE4, IE6]. A bank said that *"the embedded SE differs per supplier and per handset. The embedded SE can even differ per version, for instance not all Samsung Galaxy S6 handsets have similar embedded elements. This means that adjustments to the payment application have to be made per device. As the SIM is standardized, we see it as an easier solution for mobile payments"* [BA3]. This relates to a statement that was done by one of the MNOs: "*Fragmentation leads to a decrease of value and is something that is unwanted by a service provider, as they want to reach as much customers as possible with one solution"* [MNO1]. In total five respondents emphasized that the standardization of the SIM is an important characteristic, as it requires a minimum of changes to facilitate a payment application on different handsets [MNO1, MNO2, BA3, IE4, IE6]. However, it should be noted that MNOs might have a biased view towards the SIM, as they control it.

Another feature of the SIM is that it has reach. The SIM can be found in every handset and has a high coverage all over the world. Reach is seen as key for the success of an authentication and identification service because it means that a SP is able to reach all its customers with a minimum of resources [MNO1, BA1, BA2, BA3, IE1, IE4, IE6, IE7]. So, the reason why reach is important is similar to why standardization is important. In fact, one expert argued that standardization contributes to

reach [IE1]. Credit cards are an example of why reach and standardization are important. It is a successful payment method as it has reach all over the world and it has reach because it is standardized [IE1]. Therefore it is of real value that the SIM is in every handset. It means that if a service provider uses the SIM, he is able to reach most of his customers with a standardized platform. Facilitating a payment solution on the SIM would mean that the application has reach and that a minimum of changes is required to offer it over different handsets.

The SIM is, however, not the only mobile payment solution with reach. As cloud-based solutions can be offered on handsets that use an Android OS, this solution also has reach [BA1, BA2, BA3, MNO1, IE4]. Because of that Banks are actively exploring the options that the HCE functionality offers [BA1, BA2, BA3]. *"Cloud-based is a very promising solution for us, as it allows us to reach most of our customers. We cannot afford a solution that is available to 100.000 customers, when we have a total of 5 million customers. "* [BA1]. In addition to that [BA3] said that they received responses of disappointed customers, as the mobile payment application was only available on two handsets and therefore they are looking for solutions with more reach. However, one of the MNOs pointed out that cloud-based only works from Android 4.4 and higher, which means that its current reach is limited. This will, however, improve in the future, as more handsets will have the newest OS [MNO1]. The embedded SE offers limited reach due to the fragmentation of handsets [BA1, BA3, IE1, IE2]. If a service provider wants to reach all his customers they must collaborate with multiple handset manufacturers (e.g. HTC, Apple, Samsung, Huawei, etc.). However, one of the banks pointed out that 90% of their customers owns an iPhone or a Samsung phone. These figures affect their choice of technology. If they could use the embedded SE of these handsets, they would be able to reach most of their customers [BA3]. This means that the distribution of handsets among a SP's customers affect the reach of an embedded SE.

A third characteristic that contributes to the SIMs level of uniqueness is that it is seen as secure. The SIM is a hardware component. In general hardware is seen as more secure than software, as it is cannot be altered easily and software is easier to infect with malware [BA2, BA3, IE4]. The SIM is able to function as a SE and due to its cryptographic properties it offers the possibility to provide secure authentication services [IE5]. Security is valued by SPs as it minimizes the chance of fraud. In total nine respondents expressed that they view the SIM as a secure means for authentication and identification [MNO1, MNO2, BA1, BA2, BA3, IE4, IE5, IE6, IE7].

A fourth characteristic that was addressed during the interviews is that the SIM is able to provide connectivity. The SIM is able to connect the handset to the network of the mobile operator [MNO1, MNO2, IE7]. It can provide a secure communication channel, which means that the payment application is not dependent of a less secure Internet connection [MNO2]. However, this characteristic was only addressed by the two MNOs and one independent expert, which questions its relevance

Based on the interviews, it can be concluded that there are three main factors that make the SIM in comparison with the embedded SE and a cloud-based solution. The SIM is the only standardized element and it has reach. Furthermore, the SIM is secure. The combination of these three characteristics makes the SIM unique, as the alternatives do not have all three characteristics. An embedded SE provides similar security as the SIM but has less reach. A cloud-based solution does have reach but is seen as less secure. An overview of the characteristics of the different solutions that have been discussed during the interviews is provided in Table 8-1. Based on this over the SIMs level of uniqueness has been mapped in Figure 8-2. A more extensive overview can be found in Appendix E.

Characteristics	SIM	Embedded SE	Cloud-based
Reach	Yes	Limited	Yes
Secure	Yes	Yes	Limited
Standardized	Yes	No	N/A
Connectivity	Yes	No	No

Table 8-1: Characteristics solutions

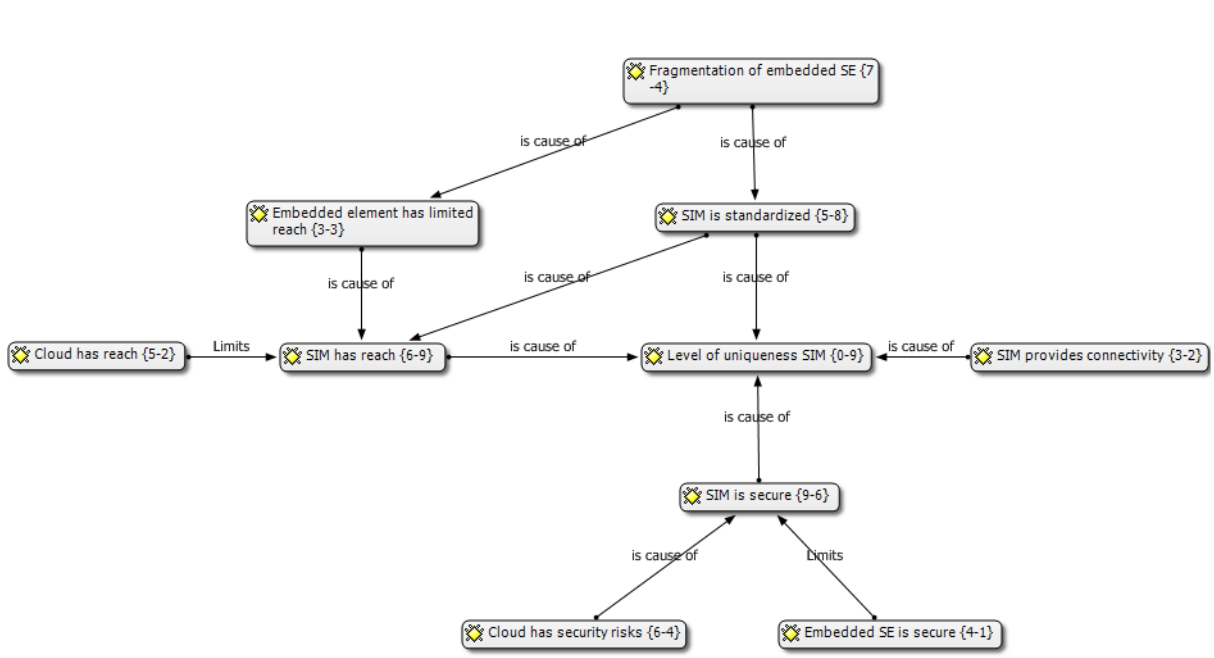


Figure 8-2: SIM level of uniqueness mobile payment

The figure shows an overview of the factors that make the SIM unique. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. Not all codes are shown in this figure. A more extensive overview can be found in the Appendix. The relations have been drawn by the researcher and are based on analysis of the interviews and a comparison of the authentication and identification means. The figure shows that the combination of characteristics makes the SIM unique. Similar characteristics of other solutions limit the uniqueness. As the level of uniqueness represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that influence the uniqueness of the SIM.

Demand SIM

As explained, the analysis of the interviews showed that the demand for the SIM partially depends on its level of uniqueness. There is demand for the SIM because of its capability to function as a secure authentication and identification means that is standardized and has reach. Reach is important because service providers want to serve all their customers. Standardization is valued because this means that a minimum of adjustments is needed to facilitate a payment application over different handsets. Furthermore, security is cause of demand as it minimizes the amount of potential fraud. A more comprehensive illustration of these features can be found in the paragraph on the level of uniqueness of the SIM.

The interviews showed that the unique characteristics of the SIM have a positive effect on the demand. However, based on the same interviews, a number of factors have been identified that limit the demand for the SIM. In the Netherlands there is a fragmentation of MNOs, which limits the reach of a payment solution [MNO1, MNO2, BA1, BA2, BA3, IE6, IE7]. As explained, fragmentation is

unwanted by a bank or a service provider because they want to serve as much customers as possible with a minimum of resources. The SIM itself has reach. However, to serve most of the market in the Netherlands cooperation with three MNOs is needed [BA1, IE6, IE7]. This means that banks have to make three different deals. A MNO stated that "*there is no party in the industry that can offer sufficient market share and therefore there is no technology that is successful yet"* [MNO2]. In fact, the whole smartphone market is fragmented and this makes solution hard [MNO2, BA2, IE1, IE6]. The fragmentation of MNOs has thus a negative influence on the demand for the SIM.

A second limiting factor for the demand of the SIM is the related costs. High costs have a negative impact on demand as banks acknowledge that they see the SIM as an option to facilitate mobile payments but only for a reasonable price [BA1, BA3]. The price for the SIM must at least be competitive with other solutions. An aspect that could lead to high costs is that a SIM swap is needed to facilitate authentication and identification services [MNO1, MNO2, IE7]. Most of the SIMs that are currently deployed in the market cannot meet the requirements needed to facilitate mobile payments. A SIM swap is an extensive process that leads to high costs. One MNO explained that this is a real barrier, as it hard to let consumers swap their SIM. Market research shows that most consumers will not to come to the shop for a new SIM [MNO1]. So, if most of the SIMs are not suitable for mobile payments then the reach is also small. The needed SIM swap thus affects the costs of the SIM but also the reach.

Another factor that limits the demand for the SIM is that banks are not dependent on the SIM to facilitate mobile payment. There are technical alternatives in the market: cloud-based and an embedded SE. As explained these alternative are seen as less secure or have limited reach. However, two respondents mentioned that although there is a market for mobile payments the need for security is limited [IE5, IE6]. Mobile payments will only consist of micro-payments. *"Consumers will only use mobile payments for micro-payments and this reduces the need for security"* [IE5]. Micropayments require less security than large payments because the related risk is a lot lower. Although, it can never be secure enough for mobile payment solutions there is a trade-off between needed security and costs [BA1, IE5, IE6]. So, if a cloud-based solution is much cheaper than the SIM the SP will make a security trade-off. In fact, a number of respondents agreed that the SIM is more secure than a cloud-based solution. However, they argued that a cloud-based solution has controllable security risks and is therefore secure enough [BA1, IE2, IE5]. This means that both technologies can be seen as realistic alternatives for the SIM and this can lead to a reduction of demand.

An overview of the factors that influence the demand for the SIM can be found in Figure 8-3. A more extensive overview on the factors that influence the demand of the SIM can be found in Appendix E. It shows that the unique characteristics of the SIM are a cause of demand. However, a number of factors have been identified that limit the demand for the SIM. The first factor is the fragmentation of MNOs, as it requires banks to collaborate with three MNOs. The costs are another limiting factor for demand. The banks require a competitive price if they want to consider the SIM for mobile payments. The third limiting factor that has been discussed is that the embedded SE and cloud-based solution are alternatives for the SIM and therefore the bank is not dependent on the SIM to facilitate mobile payment.

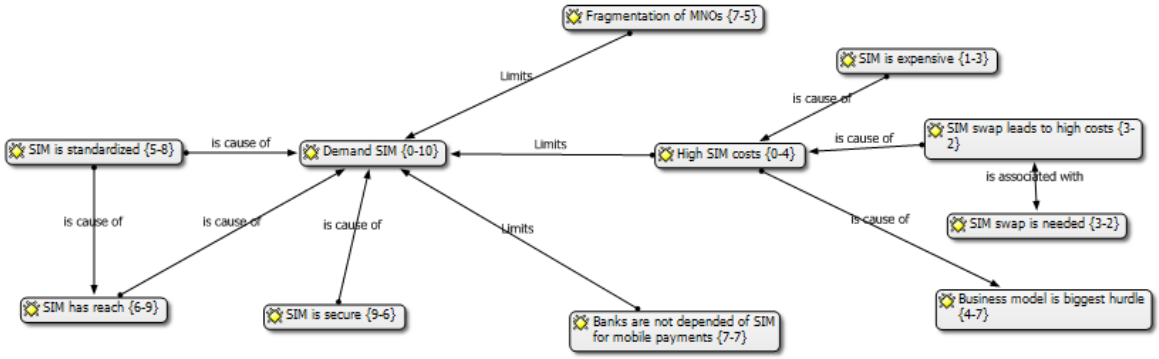


Figure 8-3: SIM demand mobile payment

The figure shows an overview of the factors and relations that cause and limit the demand for the SIM. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. Not all codes are shown in this figure. A more extensive overview can be found in the Appendix. The relations have been drawn by the researcher and are based on analysis of the interviews. As demand represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that influence the demand of the SIM.

Value SIM

The value of the SIM is the third control point parameter that is discussed. As explained in the introduction of this paragraph, the value that the SIM represents is related to the uniqueness of the SIM and the demand that it has. Therefore the value of the SIM is caused by the same factors, as discussed in the paragraphs on the SIMs level of uniqueness and demand. However, the parameter demand aims to illustrate the amount of value that the SIM can extract from the value network. During the interviews a number of relevant points were raised in regard to the value that the SIM represents.

The characteristics of the SIM make it a suitable means for authentication services and therefore it clearly has value. The question remains how much value does it represent? According to different respondents the MNOs have overestimated the value of the SIM. They wanted their own mobile wallet and a fee per payment transaction [BA1, BA3, IE8]. For banks it is essential that they can have their own mobile wallet because they want to exploit value-added services such as loyalty cards [BA1, BA3]. Furthermore, the price for the SIM must be reasonable, as the banks have a limited budget available [BA1, BA2 BA3, IE6]. Therefore the price of the SIM must be competitive with other solutions. Otherwise banks will choose a cheaper solution, even though this could lead to a security trade-off. One of the MNOs seemed to agree that the SIM price should be competitive with other solutions, as they indicated to have lowered the price of the SIM to a competitive level [MNO1]. The MNO also explained that banks are allowed to issue their own mobile wallet, which was not the case in the past. Therefore it seems that the MNO and the banks are on the same page in regard of the value that the SIM represents. Furthermore, the MNOs expressed that the SIM is extremely valuable to them because it is the only element in the handset that is owned by them [MNO1, MNO2].

Figure 8-4 provides an overview of the factors that influence the value of the SIM. As the parameter is dependent of the parameters uniqueness and demand, the factors show overlap with the other networks. This paragraph explained that if banks would consider the SIM for mobile payments, it should at least be offered for a competitive price. Furthermore, banks should be allowed to have their own mobile wallet, would they consider the SIM as an option. At least one of the MNOs is willing to comply with these demands and therefore they seem to attach similar value to the SIM the banks.

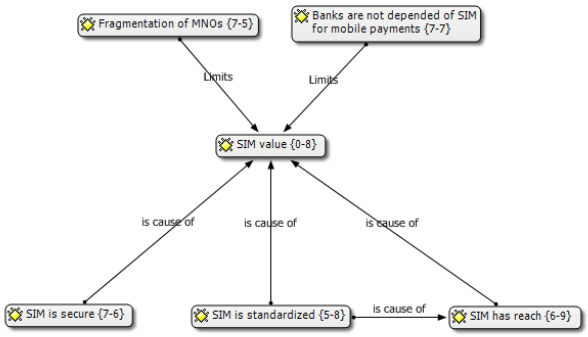


Figure 8-4 Value SIM mobile payment

The figure shows the factors and relations that cause and limit the value of the SIM. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews. As value represents a control point parameter, it has not been assigned codes in the transcripts but is linked to codes that influence the value of the SIM.

Time SIM

The fourth parameter is time, as over time the strength of a control point can change. Although it is not possible to predict the future and to sketch all the factors that have impact on the SIM as control point, some of the respondents named factors that possibly affect the sustainability of the SIM as control point in the next couple years. One of the experts said that there is a mismatch between the life cycle of the handset and an authentication means [IE5]. Authentication means are used over a longer period than a handset or a phone subscription. Due to this mismatch it is unlikely that the SIM is a long-term solution. For example, a credit card has a validity of a number of years while most phone subscriptions are only valid for one or two years. Related to that, a number of respondents emphasized that all future developments are going to cloud-based solutions [BA2, IE2, IE4, IE5]. Cloud-based solutions will lead to more control for the consumer and the lock-in will be limited. With cloud-based solutions a consumer can change more easily from handset or phone subscription without the need to go through a difficult provisioning process. Next, to that a cloud-based solution will offer the possibility to facilitate a payment application over multiple machines [IE2], which could be relevant if, for instance, smart watches would be used for payments. Furthermore, the world of mobile payments is subjected to change, which means that a solution that is implemented now must be seen as short-term (1-2 years), as new technologies are constantly introduced to the market [BA1, BA3]. The introduction of HCE is a prime example of this.

The final factor that was addressed by some respondents is the development of the Soft-SIM. This software based technology that can take over the SIM's capabilities, which means that the hardware SIM is no longer needed [MNO1, IE2]. However, two respondents stress that this development is currently not a threat to the SIM, as it will still take years before it will be introduced to the market [MNO2, IE6]. All the discussed factors could limit the sustainability of the SIM and affect its strength as control point over time. However the future is uncertain and impossible to predict which means that it is not said that these factors are relevant. Besides it is possible that other factors that have not been addressed by the respondents could affect the strength of the control point over time. Therefore the discussed factors only help to identify possible scenarios of change.

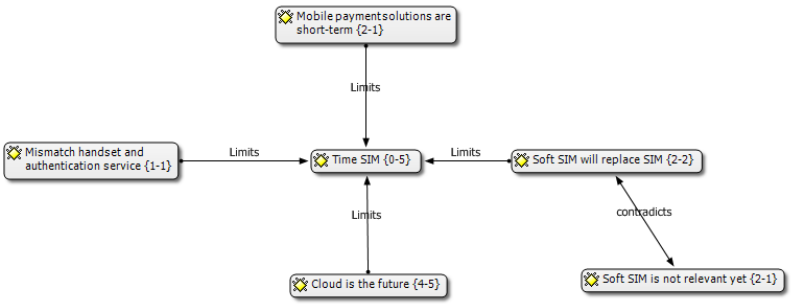


Figure 8-5: Time SIM mobile payment

The figure shows factors and relations that could possibly affect the strength of the SIM as control point over time. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews. As time represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that could influence the SIM over time.

8.2.2 Viability value network

In order for the SIM to qualify as control point the constructed value network must be viable. Therefore the bank and MNOs must be open to collaboration. If banks are unwilling to collaborate with MNOs the value networks will not be viable. The respondents were asked to give their view whether they see a role for MNOs in mobile payment and whether they could collaborate with banks.

Banks are no longer dependent of the SIM technology to offer a mobile payment solution, as other solutions that are scalable have been introduced to the market [BA1, BA2, BA3, IE2, IE5, IE6, IE7]. This means that MNO are not essential to facilitate mobile payments. In relation to that, two banks questioned the actual added value of a MNO for mobile payments [BA1, BA2]. They feel that other solutions would suffice and that there is no need to cooperate with MNOs. One the respondents stressed that "*banks want to stay in control and want limited dependence of other parties, especially if they come from a different sector"* [BA2]. So, even when the SIM would be offered for a reasonable price, it makes you dependent of the MNO. This is not something that is wanted by a bank because the MNO can then shut down the entire mobile payment system of the bank [BA2]. Another bank did not see this is as problem because they argued that this problem could be solved with contracts. Besides, he stated that the payment industry is an example of collaborations with different parties and he stressed that there will always be interdependencies [BA3]. It shows that the organizations in the payment industry have different views and this could be an explanation for the fact that banks are focusing on different technologies for mobile payment.

Another aspect that affects the role of MNOs in mobile payment is that they are marked as hard to collaborate with [BA1, BA2, BA3, IE2, IE6, IE7, IE8]. One of the banks stressed that the cultural differences between banks and MNOs makes it difficult to collaborate. This answer is in line with the conducted literature study. Banks focus more on customer retention while MNOs are more sales driven organisations [BA1]. One expert [IE7] said that "*There are many examples of failed attempts of MNOs to extend their business. MNOs believe in control to create value and this mindset is a barrier when entering a new market."* In payments the banks have control over the consumer's bank account and therefore the MNOs rely on the banks to facilitate mobile payment. This means that they can exert limited control, as they are more dependent of the bank than the bank is of a MNO. The difficulty of collaboration relates to another hurdle, which is the revenue model. As discussed, banks are not willing to spend too much on mobile payment because it will be a redundant solution next to the regular payment card [BA1, BA3]. The revenue model must be realistic and the SIM price must thus be competitive with other solutions [BA1, BA2, BA3, MNO1, IE6]. Next, to a reasonable

SIM price, banks want to have their own mobile wallet, as this allows them to exploit value added services such as loyalty [BA1, BA3]. Besides the conditions that the banks lay down, collaboration with three MNOs is needed to service the whole market [BA1, IE4, IE7]. Therefore banks need to make multiple deals before they would be able to reach all their customers. Due to these reasons, seven of the respondents said that they do not find it likely that there is a role for MNOs in mobile payment [BA1, BA2, IE2, IE5, IE6, IE7, IE8]. "*MNOs have overplayed their hand in the past, as they wanted maximum profit at the expense of the bank's business model"* [BA1, IE2, IE6].

Although, most respondents argue that it is not likely for MNOs to play a role in mobile payments, there still seems to be a small opportunity for MNOs. The banks still see the SIM as a suitable technology for mobile payments. However, the MNOs must meet the conditions of the banks for them to consider the SIM technology, otherwise they will choose for an alternative solution. Two banks said that they are still open to collaboration with MNOs, as long as it under right conditions (own mobile wallet, competitive price, need for hardware security) [BA1, BA2, BA3]. One of the MNOs said that they are willing to meet these conditions, as they have lowered the SIM price to a competitive level and that banks are allowed to exploit their own mobile wallet [MNO1, BA3]. The MNO said that "*We started a new trend as we have lowered the price of the SIM. We don't want that our customers base their decision on costs and therefore we want to offer the SIM for the same price as the costs for a HCE solution. Next, to that banks will be allowed to issue their own mobile wallet. Banks should really look at what they find the best technology and we are confident that the SIM scores well"* [MNO1]. It seems that the MNO realizes that other solutions are competitors for the SIM and that their dominant position has changed over the years. As these conditions of the banks were not known during the interview with the other MNO, it is unknown what their view is and if they are willing to meet these conditions.

With the barriers out of the way (e.g. revenue model and mobile wallet), it is time for banks to make their choice on what technology has the most potential [MNO1, BA3]. This choice of technology will consist of the choice between embedded SE, cloud-based and a SIM solution. The MNOs find the SIM technology better than its competitors [MNO1, MNO2], which seems logic because they own the SIM. It does, however, explain why they are still putting effort in mobile payment. The banks mentioned that they see no real difference between the viability of a SIM SE solution and a SIM-Cloud solution, as both solutions make them dependent of the MNO [BA1, BA2, BA3]. Therefore they did not have a specific preference for one of the two technical solutions. The MNOs had a similar view, as they stressed that they have no preference for a specific technical solution as long as the SIM is used [MNO1, MNO2]. Three of the independent experts see more potential in a SIM-cloud solution, as a SIM-cloud solution allows for better life-cycle management [IE4, IE5, IE6].

Based on the interviews, it can be concluded that there is a small opportunity for MNOs in mobile payments. Their position has changed, as banks are no longer dependent of the SIM. If MNOs want to play a role, they have to meet the conditions of the banks. Even then, it is not said that banks will choose for the SIM. This means that the viability of the designed value networks is low. Figure 8-6 provides a schematic overview of the interview findings regarding the role of the MNO in mobile payments.

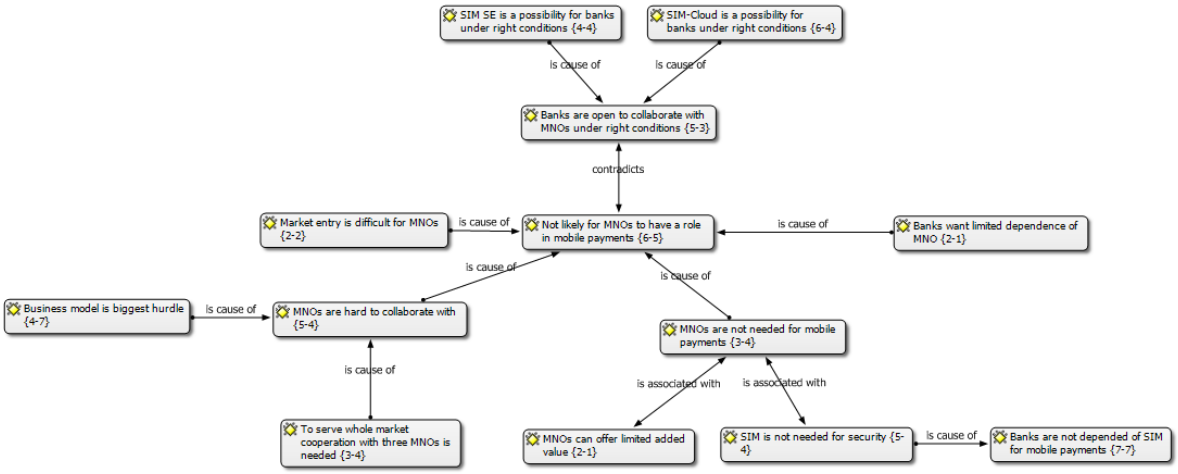


Figure 8-6: Role MNO in mobile payments

The figure provides an overview of the interview findings regarding the viability of the value network and the role of MNOs in mobile payments. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews.

8.3 Government services

As discussed in the first paragraph of this chapter, nine respondents believe that there is a potential business case to offer authentication and identification services for the Dutch eID scheme. There is currently no use case for offline services such as storing the driver's license on the SIM. Therefore this chapter aims to identify whether the SIM could qualify as a control point in the eID scheme. This paragraph discusses the potential strength of the SIM as control point by making use of the four parameters: level of uniqueness, demand, value and time. Next, the viability of the value network is assessed.

8.3.1 Control point analysis

In total 12 industry experts have been interviewed and asked whether they think that the SIM can be used to provide authentication and identification services for the government. All these interviews have been analysed and based on these interviews an assessment is done whether the SIM could qualify as control point for government services.

As was the case with mobile payment, during the analysis of the interviews it showed that the control point parameters overlap. The level of uniqueness is a cause of demand and value. Next, to that demand is also a cause of value. Since these parameters have overlap, a number underlying factors influence multiple parameters. These factors have been derived from the interviews and are discussed next in relation to the SIM as possible control point.

Level of uniqueness SIM

The level of uniqueness that the SIM represents is based on the differences with competitors. During the interviews it became apparent that the competitors for the SIM and MNO are different for government services than for mobile payment. In mobile payment an embedded SE and cloud-based solution form the alternatives for the SIM. This is different for government services. For eID authentication the handset is not necessarily needed. Therefore the SIM and MNOs have other competitors.

Based on the interviews the government and banks were marked as the main competitors for MNOs. The banks acknowledged that they are working on a 'BankID' that can be used for online authentication and identification [BA1, BA2, BA3]. In total eight respondents marked the banks as competitors for the provisioning of an electronic identity [BA1, BA2, BA3, GOV, IE1, IE4, IE6, IE9]. The banks are developing a standard that can help to identify a person online but currently they are not collaborating with the government on the eID scheme. Unfortunately, the reason for this has not been discussed during the interviews, as the focus was on MNOs. The banks are developing their own standard, which could possibly connect to the eID scheme in a later phase [GOV]. The banks were merely asked about their own initiatives and therefore their view on the MNO for eID services is not taken into account during the rest of the analysis.

Another competitor for providing eID authentication is the government, as they have the ability to provision secure authentication and identification means such as an ID card or a driver's license [GOV, IE1, IE2, IE9]. The new driver's licence in the Netherlands contains a chip that could be used to store an eID. However, the government wants to create a system, which offers the possibility to log in with multiple authentication means and these means can also be offered by businesses. This will create a more robust system because different means can be used to log in [GOV, IE3]. If one of the authentication means does not work, another can be used. Therefore the government can be seen as a competitor for the MNO, as they would supply their own authentication means, but also as a customer, as they want businesses to connect to the system to create robustness. This means that the eID scheme offers the option for multiple authentication means in the systems. Banks could offer

the bankcard as an authentication means, the government could offer ID cards and MNOs could offer the SIM.

Handset manufacturers are not seen as competitors [GOV, IE1, IE3, IE9]. The government has a preference for local players due to privacy issues (e.g. patriot act). Next to that, the fragmentation of handsets weakens the position handset manufacturers because the government wants a standardized solution. They do not want to differentiate per authentication means, as this leads to limited reach and high costs. Furthermore, a cloud-based solution is currently not seen as a competing technology for the SIM [GOV, IE3]. Although, the two respondents did point out that the Digidentity solution is secure enough for eID but then the government would need to embrace this technical solution to generate enough reach [GOV, IE3]. Therefore the banks and the government are seen as the main competitors for the MNO in the eID scheme. These are parties that already have authentication and identification means deployed in the market. The provisioning of these means is a costly process and this makes market entry for new parties hard [GOV].

The main distinction of the SIM with a bankcard and an ID card is that it is present in every handset. Of these three authentication means, the SIM is the only one that is able to offer authentication and identification through the handset. According to two respondents, this is valuable as people are more attached to their phone than bankcard [MNO2, IE9]. The MNO logically values his own product above others and as only one other expert mentioned this, one could doubt the value of this view. Another characteristic is that the SIM has reach, as many consumers own a SIM. Reach is a key requirement for authentication services, as SPs want to serve all their customers [MNO1, MNO2, GOV, IE1, IE2, IE3, IE4, IE6, IE7, IE9]. This also accounts for the government, who needs to provide a solution that is available for all citizens.

Another key feature of the SIM is that it is a secure means for authentication and identification [MNO1, MNO2, IE3, IE4, IE5, IE6, IE7]. The government must be able to trust that a person is really who he says he is and therefore a secure authentication is needed. To determine the level of assurance of the authentication means the government uses the STORK framework [MNO1, GOV, IE1, IE6, IE7]. This is a framework developed by the EU, which is used to determine the quality of assurance that an authentication means offers. For the eID scheme the government requires that a person's identity has been confirmed, which complies with STORK level 3 and 4. The SIM technology is able to meet the STORK requirements, as it securely stores secrets and could be linked to a person [MNO1, GOV, IE6, IE7]. The final feature that makes the SIM unique is that it is able to provide connectivity [MNO1, MNO2, IE6]. This connectivity can increase the security of the authentication and identification process, as the SIM provides a separate communication channel and therefore a man in the middle attack is less likely [GOV, MNO2]. All the discussed characteristics contribute to the level of uniqueness of the SIM. It is the combination of characteristics that makes the SIM unique compared to other solutions such as a bankcard or ID card. An overview of these characteristics is provided in Figure 8-7.

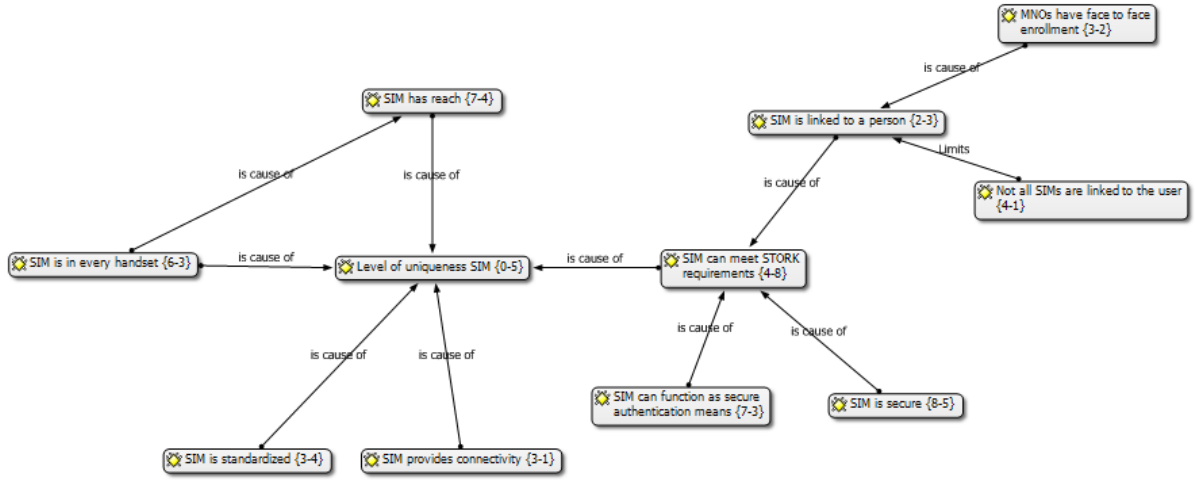


Figure 8-7: Level of uniqueness SIM government services

The figure shows an overview of the factors that make the SIM unique. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. Not all codes are shown in this figure. A more extensive overview can be found in the Appendix. The relations have been drawn by the researcher and are based on analysis of the interviews and a comparison of the authentication and identification means. The figure shows that the combination of characteristics makes the SIM unique. As the level of uniqueness represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that influence the uniqueness of the SIM.

Demand SIM

According to the respondents, there are a number of factors that are essential for authentication and identification. As discussed in the paragraph on the level of uniqueness, an authentication means must have reach because the government needs to reach all its citizens [GOV, MNO1, MNO2, IE1, IE2, IE3, IE7, IE9]. Next to that, the technology must be secure because the government requires a STORK level 3 or 4 security [GOV, MNO1, IE6, IE7]. Another requirement is that the authentication and identification means complies with the standards of the eID scheme, as the government does not want to differentiate per solution [GOV, IE6, IE9]. The characteristics discussed in relation to the SIMs level of uniqueness (e.g. reach, standardized and secure) show that the SIM is able to meet these requirements. Therefore it can be concluded that uniqueness of the SIM is a cause for demand.

However, based on the interviews a number of limiting factors have been identified. The first limiting factor has been addressed in the previous paragraph, as the SIM is not the only means that can offer authentication for the eID scheme. The development of a “BankID” can be a competitor because banks can meet the requirements for the eID scheme [BA1, BA2, BA3, GOV, IE1, IE4, IE6, IE9]. Furthermore, the government already supplies means that can offer secure authentication such as the driver’s license.

Furthermore, the costs related to the authentication and identification could limit the demand for the SIM. As explained in the mobile payments chapter, a SIM swap is needed as most of the deployed SIMs are technically not suitable to offer authentication and identification services [MNO1, MNO2, IE7]. A SIM swap is an extensive process that leads to high costs. A MNO explained that this is a real barrier as it hard to let consumers swap their SIM. Market research shows that most consumers will not to come to the shop for a new SIM [MNO1]. If most of the SIMs are not suitable for to offer authentication for the eID scheme, then the reach is also small and this is unwanted by the government. The needed SIM swap thus affects the costs of the SIM but also the reach of the solution.

Another limiting factor is the fragmentation of MNOs in the Netherlands. Although the SIM is standardized and has reach, cooperation with three MNOs is needed to serve most of the market in the Netherlands [MNO2, IE2, IE6 IE7]. The government does not want a fragmentation of solutions because it limits reach and requires adjustments per authentication means. Therefore the service must be standardized [GOV, MNO1, IE1, IE2, IE9]. As one of the respondents said: *"The operators must offer the same level of service because if they don't then their reach becomes really small"* [IE1]. Therefore a number of the respondents argued that the MNOs must collaborate together to create an independent authentication standard that could connect to the eID scheme [IE1, IE2, IE4, IE7]. Then the MNOs would be able to offer the same level of service and the government would not have to differentiate per MNO. Two respondents [IE1, IE4] said that the development of mobile connect is a promising authentication standard for MNOs. Mobile connect is being developed by the GSMA, an overarching body of MNOs worldwide. This is an authentication standard that can be adopted by all MNOs all over the world and therefore it has reach [IE1]. MNOs could use this authentication standard to connect to the eID scheme [IE1, IE4].

However, the RDW said that it is not essential for MNOs to create a standard, as MNOs could individually connect to the eID scheme [GOV]. This would mean that the eID requirements would lead to standardization. If a party is able to meet these requirements they could join the eID scheme. The RDW estimated that MNOs would be able to serve over a third of the eID market due to their reach and presence in the handset. However, the government wants the MNOs to join the eID scheme and therefore this estimation could possibly be too positive. Overall, it shows that most of the respondents think that there can be demand for the SIM in the eID scheme. An overview of the factors that influence the demand for the SIM is given in Figure 8-8. As discussed, the factors that make the SIM unique are a cause of demand. However, a number of factors that limit demand have also been discussed and are included in the figure.

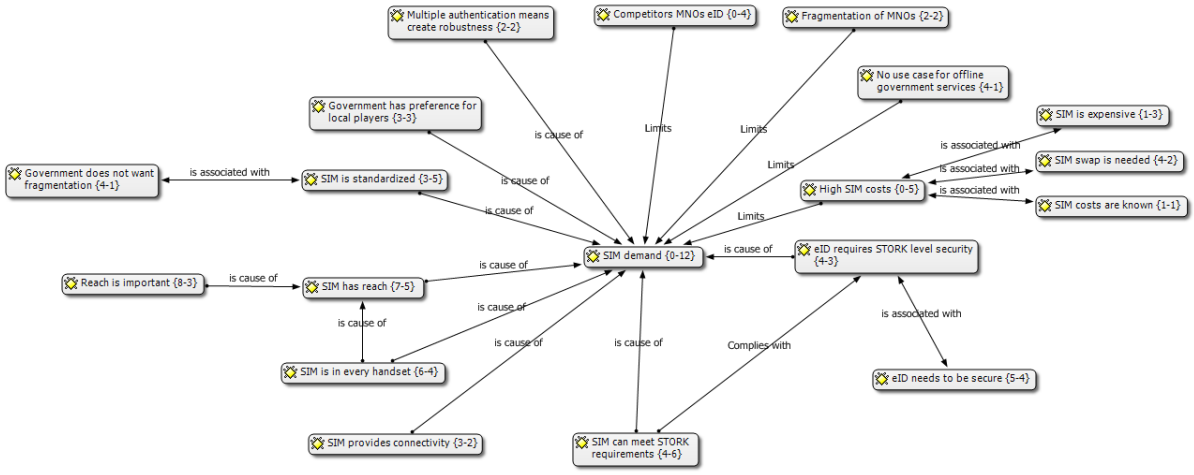


Figure 8-8: Demand SIM government services

The figure shows the factors and relations that cause and limit the demand for the SIM. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews. As demand represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that influence the demand of the SIM.

Value SIM

The parameter value is influenced by the already discussed parameters of uniqueness and demand. Therefore the same factors that impact the demand affect the value of the SIM. It is because of qualities that the SIM has that it creates demand and it is because of these qualities that it represents value. Furthermore, if there is more demand for the SIM then it becomes more valuable. This shows that both parameters influence the value of the SIM.

For MNOs it is key that the SIM will lead to revenue [MNO1, MNO2]. This means that a revenue model is needed. "*The idea is that authenticators will earn money by the provisioning of attributes and that the party asking for the authentication will pay"* [GOV, IE3, IE6]. For example, an online liquor store will have to verify whether its customer is 18 years of age. Based on a user's eID, the liquor store can receive a "yes" or "no" without actually receiving a customer's date of birth. In return, the liquor store will have to pay a fee to the authenticator. However, the revenue model of the eID scheme is uncertain, as the eID scheme it is still under development [GOV, MNO2, IE1, IE2, IE4, IE6, IE9]. It is uncertain what the system should look like and for what services it can be used, as it is currently in a pilot phase. This means that the infrastructure of the eID scheme is subjected to change. There is public-private partnership that is working on a standard for the eID scheme but for what end-services (e.g. online liquor store) the eID will be used is still unclear [GOV, MNO2, IE3]. This means that the business model is uncertain and therefore the value that SIM could extract within the eID scheme cannot be determined. Figure 8-9 provides an overview of the factors that influence the value of the SIM.

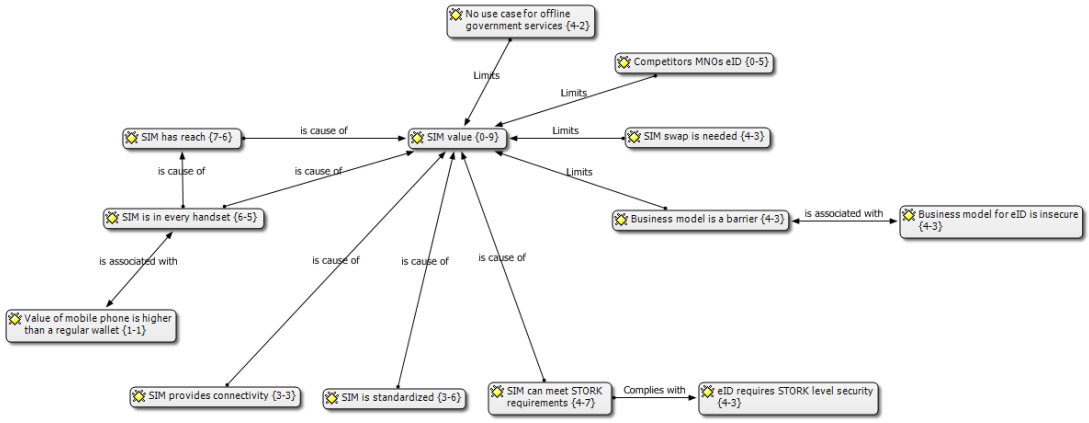


Figure 8-9: Value SIM government services

The figure shows the factors and relations that cause and limit the value of the SIM. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews. As value represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that influence the value of the SIM.

Time SIM

The fourth control parameter is time, as the strength of a control point can change over time. During the interviews, a number of aspects have been discussed that could influence the strength of the SIM as control point over the next couple years. As the future is uncertain, it is not said that these factors will indeed be of influence. A number of these factors have already been discussed for mobile payments and are therefore briefly repeated.

One of the experts said that there is a mismatch between the life cycle of the handset and an authentication means [IE5]. Authentication means are used over a longer period than a handset or a phone subscription. Due to this mismatch it is unlikely that the SIM is a long-term solution. An

identity card is valid for several years while most phone subscriptions are only valid for one or two years. Related to that, a number of respondents emphasized that all future developments are going to cloud-based solutions [IE2, IE4, IE5]. Cloud-based solutions will lead to more control for the consumer and therefore the lock-in will be limited. With cloud-based solutions a consumer can change more easily from handset or phone subscription without the need to go through a difficult provisioning process [IE5]. Some of the respondents mentioned the development of the Soft-SIM as a threat to the SIM. This is a software-based technology that can take over the SIM's capabilities, which means that the hardware SIM is no longer needed [MNO1, IE2]. However, two respondents stress that this development is currently not a threat to the SIM, as it will still take years before it will be introduced to the market [MNO2, IE6]. Furthermore, a number of respondents marked the SIM as an old technology and therefore the ease of use is not ideal. It is not capable of running large applications that require more processing power [IE4, IE6]. This relates to the fact that technology is subjected to change. Therefore new and better alternatives for the SIM might be introduced to the market, which of course affects its sustainability [IE4, IE6, IE9]. The final factor that could influence the strength of the control point is that the eID is still under development [GOV, MNO2, IE3]. This means that the outcome is uncertain and that the need for a secure authentication means such as the SIM might not be required. An overview of the different factors that could be of influence in the future is given in Figure 8-10. It could be that these factors would not play a role at all in the future but these factors could lead to changes of the SIM as control point.

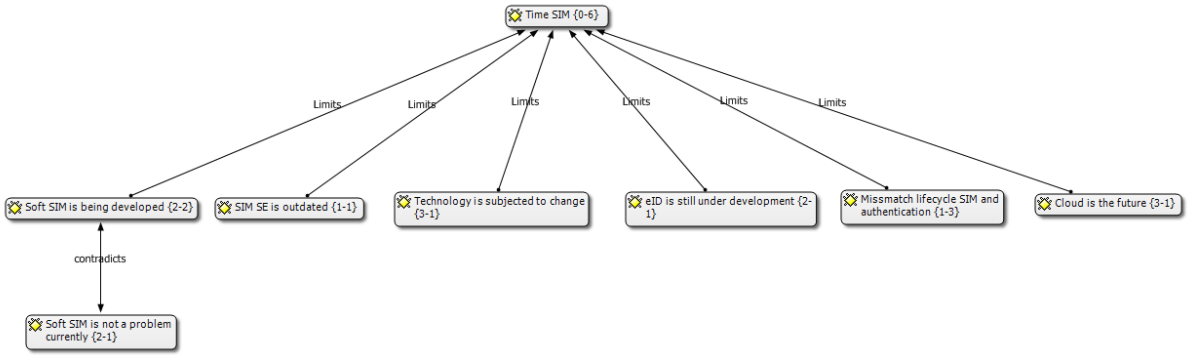


Figure 8-10: Time SIM government services

The figure shows factors and relations that could possibly affect the strength of the SIM as control point over time. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on an analysis of the interviews. As time represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that could possibly influence the SIM over time.

8.3.2 Viability value network

The respondents were asked to give their view on the role that MNOs could have within the eID scheme and whether they can collaborate with the government. This helps to assess the viability of the value network.

A key condition is that MNOs must comply with STORK level 3 or 4, as the eID scheme is build around this standard [MNO1, GOV, IE1, IE4]. As discussed, the security of the SIM can be STORK compliant. However, to reach STORK level 4 a physical meeting is needed, where the identity of the consumer is confirmed. In the Netherlands, MNOs require consumers to physically identify themselves when purchasing a phone subscription. However, in order for the SIM and MNOs to comply with STORK, the SIM must be linked to a person. One of the experts stated "*For a solid authentication there are two things that are key. First is the enrolment of a person. The person must be linked to an authentication means and his identity must be verified because garbage in is garbage out. Second, the authentication procedure has to be accurate and secure"* [IE1]. The statement shows that the issuing process of an authentication means is essential for the security. So, if the enrolment

procedure is not accurate then the entire authentication and identification procedure is weak. MNOs have a secure means with the SIM but they need to have an accurate enrolment procedure as well.

According to the respondents the MNOs have an issuing process that can meet the STORK requirements, as they have face-to-face enrolment [MNO1, GOV, IE1, IE4]. However, a number of respondents pointed out that not every SIM is linked to a person [MNO1, IE4, IE6, IE7]. The purchase of a pre-paid subscription does not require the user to physical identification. Furthermore, phone subscriptions can be passed on to other users (e.g. father pays subscription for daughter or company for employee). So, although MNOs have face-to-face enrolment, the SIM is not necessarily linked to a person. To meet the STORK requirements MNOs must upgrade their issuance process in such a way that the SIM is indeed linked to a person. This face-to-face moment can, however, be seen as another control point of the MNO. Experts explained that face-to-face enrolment is a very costly process because a consumer has to come to the shop where his identity needs to be verified by an employee [GOV, MNO1, IE3]. The RDW said that when parties have the ability to offer a secure authentication means with reach, market entry is difficult due the needed face-to-face enrolment [GOV]. However, another expert said that, according to the STORK framework, it is possible to rely on the enrolment of another party as long as somewhere in the network there is a face-to-face enrolment [IE3]. For example, if a party such as Google wanted to provide authentication and identification, it could rely on the enrolment procedure of a bank, as long as the bank has face-to-face enrolment. Nevertheless, it could still be barrier for market entry, as new players would be dependent of other company's enrolment procedure over which they have no control. This shows that MNOs have an advantage over other parties that do not have face-to-face enrolment.

Another factor that could influence the role of the MNO is that they need to become a trusted service provider [IE1, IE2, IE4, IE6, IE9]. "*Trust is essential for authentication because the company that requires authentication has to trust that the company, which facilitates the authentication, can verify the user. For instance, a web shop has to trust that they will receive a payment when the consumer purchases something. They have to trust the authentication and identification mechanism of the bank*" [IE1]. If the authentication procedure is not accurate then it cannot be checked if a user is who he says he is. So, a company that requires authentication wants to know that a user is indeed who says he is and has to trust another company that they can verify that. From a consumer perspective trust is important as well because they want their information handled carefully and securely. Most respondents thought that the MNOs were able to gain the trust of their customers as they are known brands and are seen as technically capable [MNO1, MNO2, IE2, IE4, IE9]. The view of the MNOs could be biased, as they have a clear interest to present themselves as credible companies. However, three independent experts share this view and even said that banks have more trust issues due bonus scandals. One expert warned that the MNOs must not overprice their product as they did with SMS because this will affect the trust of the consumer [IE6].

Based on the interviews, three other factors have been identified that have impact on whether the MNO could function as authenticator. These factors have already been discussed in the previous paragraphs and therefore a brief overview is given. The first factor is that there are competitors for providing an eID. Banks and the government have the ability to provide STORK level authentication means and this limits the need for the MNO as authenticator [BA1, BA2, BA3, GOV, IE1, IE4, IE6, IE9]. Another limiting factor could be the fragmentation of MNOs in the Netherlands and therefore a number of respondents [IE1, IE2, IE4, IE7] stressed that MNOs have to collaborate to create a standard for an authentication service, as they need to offer the same level of service. The third factor is the uncertain revenue model. The eID is still under development and therefore the outcome is uncertain [GOV, MNO2, IE1, IE2, IE4, IE6, IE9]. This means that it is not clear how the MNOs will earn money with the SIM and this could affect the viability of the MNO as authenticator. MNOs pursue profit and therefore they want a return of investment. In the current form the eID scheme requires an investment while the business model is uncertain. For this reason one of the MNOs is

currently pursuing this market [MNO2]. However, one expert mentioned that the window of opportunity is small for MNOs, as design decisions are currently being made. "*If MNOs are not already involved with discussions then they could miss the boat*" [IE9]. This could be a possible explanation for why the other MNO is actively exploring their options.

Based on the interviews, it seems that the MNO in the role of authenticator can be of value in the eID scheme. With some adjustments to the enrolment procedure, MNOs are able to offer STORK level 4 authentication. However, a barrier is that the revenue model for the eID scheme is still unknown and this leads to hesitation among MNOs to join the project. Nevertheless, one of the MNOs is actively pursuing the eID scheme and therefore the designed value network seems viable. Figure 8-11 provides an overview of discussed results.

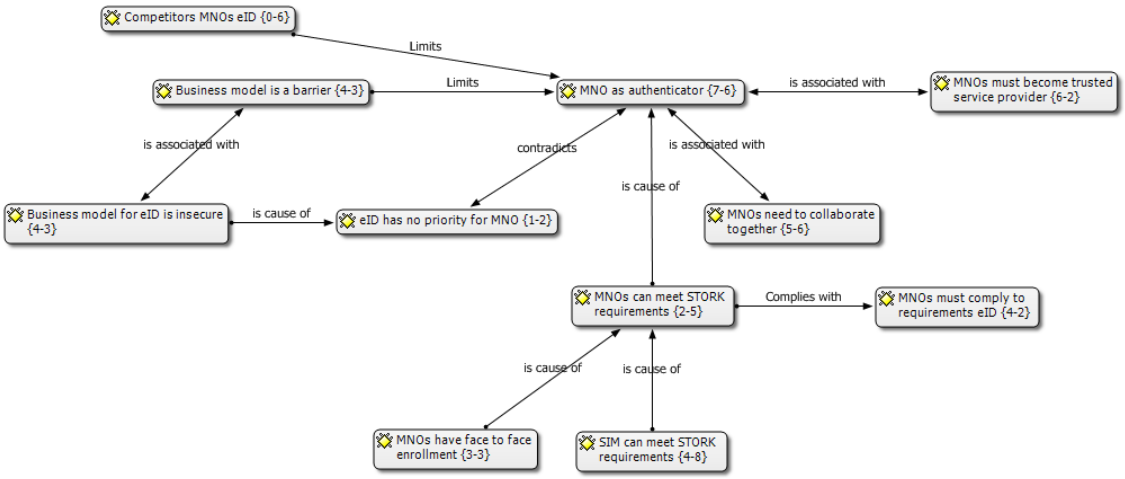


Figure 8-11: Role MNO government services

The figure provides an overview of the interview findings regarding the viability of the value network and the role of the MNO as authenticator. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. Not all codes are shown in this figure. A more extensive overview can be found in the Appendix. The relations have been drawn by the researcher and are based on analysis of the interviews.

8.4 Conclusion

In this chapter the potential strength of the SIM as control point has been assessed by analysing interviews with industry experts. In total three markets have been assessed: enterprise ID, mobile payment and government services. The results showed that the experts do not think that there is a business case for the enterprise ID market. High investment costs and the inability to replace existing authentication and identification systems, as not all handsets are suitable to provide mobile authentication and identification services, are seen as barriers for a business case. Therefore it is not likely that MNOs will target this market. This means that the designed value network is not viable and that the SIM does not qualify as control point for enterprise ID services.

The interviews showed that most of the respondents believed that there was a business case for mobile payments. Therefore the interviews were further analysed to determine whether the SIM qualifies as control point. Overall the SIM scored well on the control point parameters. The SIM is seen as a suitable technology to provide mobile authentication and identification for mobile payments, as it is secure, standardized and has reach. But in order for the SIM to qualify as control point, the value network must be viable. Most of the respondents said that it is not likely that MNOs will play a role in mobile payments because MNOs are hard to collaborate with. Besides banks are not dependent of the SIM as other technologies could meet their needs. However, all three banks

acknowledged that they are still open to the SIM as a solution as long as it is offered under the right conditions (e.g. own mobile wallet and competitive costs). The respondents pointed out that they did not see a real difference between a SIM-cloud solution and a SIM SE, as both solutions require cooperation with the MNO. Overall, based on the interviews, there seems to be a small possibility the constructed value network would emerge and that the SIM could qualify as a control point.

The third market that was addressed during the interviews focused on government services. Offline services (e.g. ID card) are not likely to be offered on the handset in the near future due to needed law changes. For online services, the respondents pointed out the development of the eID scheme as an opportunity for MNOs. However, the respondents pointed out the development of the eID scheme as an opportunity for the MNOs. Therefore, based on the interviews, an assessment was done whether the SIM qualifies as control point in the eID scheme. The interviews showed that the bankcards and government documents are the main competitors for the SIM, rather than an embedded SE or a cloud-based solution. Overall, the SIM scored well on the control point criteria, as it is able to comply with STORK level 3 or 4 security and has reach. Therefore the SIM has all the characteristics needed for a control point. Furthermore, the viability of the value network was assessed. The government wants private companies to provide authentication means for the eID scheme to create a robust system. The respondents marked the MNOs as a player that could facilitate one of these means. However, a barrier is the unknown revenue model of the eID scheme. The eID scheme is still under development and therefore the outcome is uncertain. Nevertheless, most respondents did see a role for MNOs in the eID scheme. Therefore the value network seems viable and this means that the SIM could qualify as control point in the eID scheme.

9. Conclusions and discussion

The aim of this thesis is to provide insight in whether MNOs can exploit the SIM for mobile authentication and identification by applying the concept of control points. This objective was formulated because the SIM is able to function as a Secure Element (SE) that can offer secure mobile authentication and identification. Therefore this research tried to define opportunities for the SIM as a secure authentication and identification means and therefore aimed to answer the following research question:

> *Does the SIM card qualify as a control point, which can be exploited by MNOs beyond authentication* and identification *services?*

In the chapter an answer to this question is formulated by combining the answers of different sub-questions. After drawing the conclusions, the limitations of the research are explained. Next, recommendations for follow-up research are discussed for practitioners and academics.

9.1 Main findings

Based on a literature study, it was concluded that control points exist within value networks. Therefore a requirement for a control point is that the value network is viable. Furthermore, control points are defined and evaluated by four parameters:

- *Interchangeable or level of uniqueness:* The ease by which alternative players can own a similar control point asset.
- *Demand:* The extent to which players within a value network access a control point.
- *Value:* The amount of tangible and intangible value that a control point is able to capture.
- *Time*: Affects the other parameters, as they are dynamic and may change over time.

These requirements were used to assess whether the SIM qualifies as control point for mobile authentication and identification services.

The findings of the domain chapter show that the SIM card is a mass-market smart card present in the handset and therefore it can be used to provide authentication and identification for online and offline services. However, it was also concluded that embedded SEs and cloud-based solutions are alternatives for the SIM. Given these findings, three markets were identified where the SIM could possibly be exploited for authentication and identification services:

- Enterprise ID
- Mobile payment
- Government services

The enterprise ID market needs authentication to allow employees access to company assets. Mobile payments requires authentication to conduct transactions and the government market focuses on authentication and identification of citizens.

By conceptualizing existing mobile authentication and identification value networks, it was concluded that the SIM could be used for two technical solutions. First, the SIM could function as a SE to securely store an application. This would assume a key role for the MNO in the value network, as the SIM is a critical resource for providing the service. Second, the SIM can be used as an authentication means to the cloud in a cloud-based solution to enhance security. This solution would assume a less central role for the MNO, as they play a contributing role in the service delivery. However, based on the interviews, it was concluded that the experts did not see a real difference between a SIM-cloud and a SIM SE solution, as both require collaboration with the MNO. Next, it is

discussed whether the SIM could qualify as control point in the three application markets and in what form.

Enterprise ID

Based on interviews with industry experts, it was concluded that for the enterprise ID market it is not likely that there is a business case for MNOs. This means that the value network is not viable and therefore the SIM does not qualify as control point for enterprise ID services. The added value of a mobile authentication and identification system is minimal. It would have to co-exist with a smart card system because not all handsets are suitable to provide mobile authentication and identification services. Furthermore, the related investment costs for such a system are high. Based on these reasons it does not seem likely that a company would invest in SIM based mobile authentication and identification services.

Mobile payment

It was concluded that in the mobile payment market there seems to be a business case for mobile authentication and identification services. Furthermore, the SIM is able to meet the control point criteria. The SIM is unique because it is secure, standardized and has reach. An embedded SE is equally secure but has less reach and is not standardized. A cloud-based solution has reach but is seen as less secure. The mobile payment market requires security, as it limits the amount of fraud. Next, to that reach is needed because a SP wants to serve as much customers as possible with a minimum of resources. Finally, standardization is wanted, as it leads to a minimum of needed adjustments, when issuing the payment application over multiple handsets. The requirements for mobile payment show that the unique characteristics of the SIM are a cause for demand and therefore lead to value of the SIM. Related to the parameter time, the research was unable to identify widely supported factors that could influence the SIM as control point in the next couple of years. Overall, it is concluded that the SIM scores well on the control point criteria.

However, the viability of the value network is not considered to be high. The research showed, that consulted industry experts did not find it likely that there is a role for MNOs in mobile payment. It proved to be difficult to collaborate with MNOs, as they focus on control of the customer and have cultural differences with banks. Besides, banks are not dependent of the SIM technology, as there are alternatives in the market that could meet their needs. Banks do still consider the SIM as an option, but only if it is offered for the right price and if they are allowed to issue their own mobile wallet. At least one MNO seemed to comply with these requirements and therefore there is still a possibility that the value network would occur. This would mean that the SIM would qualify as control point.

These findings correspond with existing mobile payment literature. This research shows that the SIM technology is suitable means to provide mobile payments, which relates to the findings of Dahlberg et al. (2008) that cooperation among MNOs and banks was a preferred option for mobile payments. However, this research shows that cooperation between MNOs and banks is difficult and this corresponds with De Reuver et al. (2014). He identified that differing strategic objectives and interests make collaboration among MNOs and banks difficult. Furthermore, Ondrus et al. (2009) state that the success of mobile payments greatly depends on the alignment of the business model with the environment in which operates, which also shows overlap with this research.

Government services

This research concludes that for government services there is a possible business case for online government services and in specific the development of the Dutch eID scheme. Offline government services are not likely to lead to use-cases in the next couple of years due to required law changes. Based on these findings, the SIM could possibly qualify as control point in the eID scheme solution.

The SIM scores well on the control point criteria. For this market, it showed that the alternatives for the SIM are not embedded SEs and cloud-based solutions but government issued identification means (e.g. ID card) and bankcards. Compared to these means the SIM is unique because it can provide authentication and identification by making use of the handset. Furthermore, all three means are seen as secure and have reach. The eID scheme requires authentication and identification means with reach, as the government wants to serve all its citizens. Furthermore, the eID scheme requires that the authentication means are STORK level 3 or 4 compliant. The SIM technology is able to meet the requirements of the eID scheme. Next to that, the government wants private companies to offer authentication and identification means for the eID scheme to create a robust system. Therefore if one of the means does not work, another can be used. Based on these findings, there seems to be demand for the SIM and therefore it should be able to extract value from the eID scheme. Overall, the SIM scores well on the control point criteria.

However, a threat to the viability of the value network is the uncertain revenue model. This leads to hesitation among MNOs to join the project because they want a return of investment. Furthermore, the MNOs must upgrade their enrolment procedure to comply with STORK level 4. Currently, they have face-to-face enrolment but they do not link a SIM to a person. Nevertheless, the research showed that MNOs and the SIM are suitable candidates to provide authentication and identification in the eID scheme. Therefore it is concluded that the SIM could qualify as control point in the eID scheme.

Based on the obtained results, it is concluded that the SIM has all characteristics needed for a control point. It can be of added value for facilitating eID services as well as mobile payments. However, the answer to whether the SIM indeed qualifies as control point remains indefinite. The research shows that the main complexity for these services lies in the viability of the value network. On the one hand collaborations with key players are difficult to realize, while on the other hand an unknown revenue model leads to uncertainties regarding the viability of the value network.

9.2 Contributions to theory

The biggest contribution of this research comes from the application of the control point concept. The concept was used to identify new business opportunities for MNOs. It helped to identify unique characteristics of the SIM that could be of value for offering mobile authentication and identification services. Control points help to identify critical resources and elements within a value network that contribute to a service creation. Therefore they help to explain why an organization is included in the value network. However, control points only answer part of the question whether the SIM could be exploited. Several conditions, beyond the concept of control points, have been identified that also determine whether the SIM could be exploited. First, is that the strategies and goals of an organization must be aligned with the purpose of the value network. Otherwise an organization will not join the value network, even though there might be demand for their resources/capabilities. Second, organizations must be able and willing to cooperate. The research showed that although the SIM could meet the needs of a SP that there was a preference for other options, as MNOs seemed difficult to collaborate with. Third, is that an uncertain business and revenue model could lead to hesitation among actors to join a value network. Even though, their resources/capabilities can be of added value for the service delivery.

Overall, this research shows that the concept of control points helps to explain the added value of the SIM for mobile authentication and identification services. However, whether it would it indeed qualify as control point depends on the viability of the value network. Control point and value networks are interrelated, as the control point is reason to include a party within a value network. This research showed that the emergence of a value network could be a barrier for the existence of a control point. Therefore this research proposes that for future studies first the viability of the value

network is researched. If that is the case, then the control point's concept can be used to determine how much value an organization can extract from the value network.

Furthermore, this research identifies a complexity related to the evaluation of control points. According to the literature, a control point is identified and evaluated by four parameters: level of uniqueness, demand, value and time. This research shows that these parameters are interrelated. It is because a control point is unique that it causes demand and is valuable. Next to that, a control point is only valuable if it has demand. Therefore underlying factors (e.g. a unique characteristic) can influence multiple control point parameters. However, each parameter adds a new dimension to the control point and therefore a control point should be evaluated on all three parameters. For example, a unique control point might not be able to extract value or have demand. Furthermore, a control point with demand is not necessary able to extract value. Therefore all parameters should be incorporated when evaluating a control point. However, for the ease of the analysis the parameters should be assessed consecutively:

1. Level of uniqueness/scarcity
2. Demand
3. Value
4. Time

Finally, this research identified three key characteristics that influence the strength of a control point in markets that require secure authentication and identification services: standardization, reach among intended users and security. These are underlying factors that influence multiple control point parameters in different markets. This leads to the conclusion that these characteristics possibly qualify as criteria that can help determine whether an authentication and identification means can be exploited in markets that require secure authentication and identification.

Furthermore, this research identified standardization, reach and security as key criteria for authentication and identification services. The researcher proposes a follow-up study to validate these findings. Therefore it is proposed that these criteria are applied to authentication and identification markets beyond mobile payment and the eID scheme.

9.3 Implication for practitioners

This research aimed to identify markets where MNOs could exploit the SIM for mobile authentication and identification services. Three markets have been studied. This showed that SIM based mobile authentication and identification services are not likely to succeed in the enterprise ID market. However, mobile payments and the Dutch eID scheme were marked as possible opportunities for SIM base authentication and identification services. In general, if MNOs want to offer authentication and identification services they must conduct a SIM swap. Most of the SIMs that are currently in use are not suitable to provide authentication and identification services. Therefore MNOs should provide consumers with SIMs that have the right capabilities for these services.

Based on the research findings, the revenue model of the eID scheme was marked as uncertain. Nevertheless, the SIM seems to be a suitable means for authentication and identification in the eID scheme. Therefore the researcher would like to recommend MNOs to actively contribute to the development of the eID scheme, as it could help to overcome the uncertainty related to the revenue model. However, in order for MNOs to provide authentication and identification for the eID scheme, they have to make their enrolment procedure STORK compliant. Currently, MNOs have face-to-face enrolment and therefore they know who is billed for a subscription. However, if MNOs want to provide eID services they must link the SIM to a person during a physical meeting.

In mobile payments a role for MNOs seems less likely. However, if MNOs do want to pursue mobile payments they should offer the SIM for a competitive price. The costs related to a SIM solution

should be similar to an embedded SE or a cloud-based solution. Next to that, MNOs should allow banks to issue their own wallet. These are key conditions for banks should they consider the SIM as an option for mobile payments.

9.4 Limitations

This research has a number of limitations. When looking at the research objective the goal was to determine markets where the SIM can be used as an authentication and identification means. However, due to time constraints only three markets were addressed. Therefore the SIM could potentially be exploited in other markets as well.

In addition, focusing on three markets rather than on one market comes at the expense of the research depth. If only market was researched, a more in-depth study could have been conducted. The different characteristics and requirements of the markets could have been studied in more detail. Due to the fact that the SIM was taken as starting point for this research, a lot of information was mobile payment related. Therefore embedded SEs and cloud-based solutions were marked as competitive alternatives. However, during the research it became apparent that the technical alternatives differ per application market. This could have possibly been identified in advance, if a more extensive market analysis was done. Next to that, the technical infrastructures and value networks were constructed on generic level and therefore simplified, so that they could be applied to multiple markets. If one market was studied a more detailed design could have been delivered. Furthermore, if the interviews would focus on one market, more market specific industry experts could have been consulted. This could provide more insight in the viability of the designed value networks, as they could have been discussed in more detail. In conclusion, this study identified two markets where the SIM could possibly be of value. However, there are a lot of uncertainties related to the viability of the value networks. It is likely that a study on one specific market would lead to more insights on under what conditions the SIM could qualify as control point.

Next to that, constructed value networks and technical infrastructures proved to be of limited added value to answer the research question. The value networks were constructed based on the technical infrastructure to identify the relations among actors involved with a service offering. However, during the research it showed that MNOs are dependent of service providers and their willingness to use the SIM. This means that to identify whether the SIM could be exploited, insight in the value exchanges among the other actors were not essential. Furthermore, the research showed that the complexity does not lie within the technical infrastructure but rather in the collaboration of service providers and MNOs. Therefore there should have been more focus on these bilateral relations rather than on the design of value networks and technical infrastructures.

Another limitation related to value networks is that the value exchanges have been mapped based on the technical infrastructure. The researcher did not have insight in the actual agreements and value exchanges among all actors. Therefore some of the mapped value exchanges in the value networks could differ in reality. The researcher tried to cover this gap by validating the designs with an independent industry expert.

Regarding the interviews a number of limitations are identified. First, due to practical reasons all the interviews were conducted with Dutch industry experts, with one exception. Therefore this research can only give an indication the Dutch market and cannot be generalized to a global perspective. Based on the interview with the non-Dutch respondent, it was concluded that he had sufficient knowledge of the Dutch market to include his view in this research.

Second, for this research it would have been valuable to interview more directly involved stakeholders. Unfortunately, it was only possible to interview two MNOs. Two other MNOs were contacted. However, they are currently not working on mCommerce solutions and therefore they

were not willing to contribute. However, for the research it would have been valuable to know why these parties are not undertaking any actions. Now, there is a risk that there is biased view on the added value of the SIM because only two MNOs have been interviewed that have a positive attitude towards mCommerce services. In relation to this, it was only possible to interview the RDW, as government organization. For the research it would have been useful to conduct interview multiple government organizations. Especially, an interview with the ministry of Binnenlandse Zaken would seem valuable, as they are the initiator of the eID scheme. However, this research tried to cover this gap by interviewing multiple independent experts.

Third, the degree of useful information regarding the added value of the SIM and markets where it can be exploited varied strongly across the interviews. During the coding, some of the interviews were assigned numerous codes and complex causal mappings, while others only contained a few codes. The main reason for this is that some experts were consulted about all three markets while other have only asked about one market. For example, interviewing a government organization about mobile payments would not help the research. Next to that, the technical and business knowledge varied per respondent. Finally, the independent experts had no direct interest in the value networks and could therefore speak more freely than involved stakeholders.

Next to that, the number of interviews can also be seen as a limitation to this study. Although the principle of saturation was taken into account, only one respondent per organization has been interviewed. This could lead to a bias per organization, as one employee cannot speak on behalf of the entire organization. Therefore it would have been preferred to speak to multiple employees with different expertise (i.e. business vs. technical). However, as only managers have been interviewed that had decision power this effect is probably limited.

Another limitation is that the interviewed respondents all have a history in the industry and therefore most of the respondents know each other as they conducted business together. Past business relation could therefore lead to a bias of the respondents towards other organizations. This effect seems especially relevant for the mobile payment market, as collaboration between MNOs and banks has failed in the past. Furthermore, it is worthwhile to expand on the tendency of respondents to provide positive biased answers regarding their own role in the value network.

Finally, the analysis of the interviews has its limitations. Atlas was used as a tool to analyse the interviews in a structured way. However, it was up to the researcher to connect causal relations related to control points because explanations are sometimes not explicit and hidden between the lines. Furthermore, the coding was dependent on the researcher, which could cause a bias. By conducting semi-structured interviews, respondents were allowed to bring in new concepts to the research. This showed that for authentication and identification services reach, standardization and security are key criteria. Therefore these factors have been linked to the control point criteria.

9.5 Recommendations for future research

It was concluded that the emergence of the value network is a barrier for the SIM to qualify as control point. Therefore this research proposes that for future studies first the viability of value networks is researched before control points are assessed. This would require insight in how to analyse the viability of a value network. During this research several issues were raised that influence the viability of value networks (e.g. collaboration among actors, business case). However, it is not clear whether these issues give a complete view of the value network's viability. Therefore this research proposes further research on how the viability of value networks can be assessed. These findings could then be applied to the three application markets discussed in this study.

In relation to that, this research showed that it proved to be difficult to apply the concept of control points to the three application markets. It was concluded that control points are not suitable to

determine whether a resource can be exploited in value networks that are bound to uncertainties. However, the concept could possibly be applied to evaluate control points in existing value networks. It could help to identify positions of power in existing value networks. With this in mind, it is proposed that case studies in which the concept of control point is applied to existing value networks. This should lead to empirical data and help in the further development of the concept.

Based on the findings, the researcher would propose a more in-depth study on the eID scheme. It was concluded that banks, MNOs and the government are key players that could facilitate authentication and identification in the eID scheme. However, during this research it showed that there is hesitation among MNOs to participate because the business model and related revenue model are uncertain. As this research focused on the MNO and the SIM, it is unclear whether other parties have similar doubts. Therefore the researcher proposes to study the strategic feasibility of the eID scheme in the Netherlands, in which the STOF model of Bouwman, De Vos, et al. (2008) al could be used as a guideline.

References

Abbott, J. (2002). Smart Cards: How secure are they?

ABI research. (2014). Embedded SIMs not the end for MNOs competing against Apple and Google for customer ownership. Retrieved December, 2014, from https://www.abiresearch.com/press/embedded-sims-not-the-end-for-mnos-competing-again

Alimi, V., & Pasquet, M. (2009, 16-19 March 2009). *Post-Distribution Provisioning and Personalization of a Payment Application on a UICC-Based Secure Element.* Paper presented at the International Conference on Availability, Reliability and Security, 2009. ARES '09.

Allee, V. (2000). Reconfiguring the value network. *Journal of Business Strategy, 21*(4), 36-39. doi: doi:10.1108/eb040103

Allee, V. (2002). *A value network approach for modeling and measuring intangibles*. Paper presented at the Transparent Enterprise, Madrid.

Allee, V. (2008). Value network analysis and value conversion of tangible and intangible assets. *Journal of Intellectual Capital, 9*(1), 5-24. doi: 10.1108/14691930810845777

Android Developers. (2014). Android KitKat. 2014, from https://developer.android.com/about/versions/kitkat.html#svelte

ATKearney. (2013). A Future Policy Framework for Growth: A report for the European Telecommunications Network Operators' Association(ETNO). London: ATKearney.

Au, Y. A., & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications, 7*(2), 141-164. doi: http://dx.doi.org/10.1016/j.elerap.2006.12.004

Bae, E., Banerjee, S., Loozen, T., Murdoch, R., & Saksena, A. (2014). The new digital operator: Accenture.

Baldwin, C. Y., & Clark, K. B. (2006). Architectural innovation and dynamic competition: The smaller "footprint" strategy. *Harvard Business School, Boston, MA*.

Ballon, P. (2009a). *Control and Value in Mobile Communications A political economy of the reconfiguration of business models in the European mobile industry.* Vrije Universiteit Brussel, Brussels.

Ballon, P. (2009b). The platformisation of the European mobile industry. *Communications & Strategies*(75), 15.

Ballon, P., & Van Heesvelde, E. (2010). *Platform types and regulatory concerns in European ICT markets*.

Basole, R. C., & Rouse, W. B. (2008). Complexity of service value networks: conceptualization and empirical investigation. *IBM Syst. J., 47*(1), 53-70. doi: 10.1147/sj.471.0053

Basu, M. (2013). Dubai transport authority enables payment with mobile device. Retrieved 5 February, 2015, from http://events.futuregov.asia/articles/2013/sep/30/dubai-transport-authority-enables-payment-mobile-d/

Boudreau, K. (2010). Open platform strategies and innovation: Granting access vs. devolving control. *Management Science, 56*(10), 1849-1872.

Boudriga, N. (2009). *Security of mobile communications*. Boca Raton, Florida: Taylor & Francis Group LLC.

Bouwman, H., De Vos, H., & Haaker, T. (2008). *Mobile service innovation and business models*: Springer Science & Business Media.

Bouwman, H., Faber, E., Haaker, T., Kijl, B., & De Reuver, M. (2008). Conceptualizing the STOF model *Mobile service innovation and business models* (pp. 31-70): Springer.

Canalys. (2011). Enterprise security market to exceed $22 billion in 2012 [Press release]. Retrieved from http://www.canalys.com/static/press_release/2011/canalys-press-release-201211-enterprise-security-market-exceed-22-billion-2012.pdf

Chen, W. D., Mayes, K. E., Lien, Y. H., & Chiu, J. H. (2011). *NFC mobile payment with Citizen Digital Certificate.* Paper presented at the Proceedings - 2nd International Conference on Next Generation Information Technology, ICNIT 2011.

Cimiotti, M., & Schonowski, J. (2010, 13-14 Sept. 2010). *Telecommunication network driven Ecozone: Enable flexible enhanced services and new operator business models via NGOSS managed control points.* Paper presented at the Telecommunications: The Infrastructure for the 21st Century (WTC), 2010.

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications, 7*(2), 165-181.

De Reuver, M. (2009). *Governing Mobile Service Innovation in Co-evolving Value Networks.* Technische Universiteit Delft, Delft.

De Reuver, M., & Bouwman, H. (2012). Governance mechanisms for mobile service innovation in value networks. *Journal of Business Research, 65*(3), 347-354. doi: http://dx.doi.org/10.1016/j.jbusres.2011.04.016

De Reuver, M., de Koning, T., Bouwman, H., & Lemstra, W. (2009). How new billing processes reshape the mobile industry. *info, 11*(1), 78-93. doi: 10.1108/14636690910933019

De Reuver, M., Verschuur, E., Nikayin, F., Cerpa, N., & Bouwman, H. (2014). Collective action for mobile payment platforms: A case study on collaboration issues between banks and telecom operators. *Electronic Commerce Research and Applications*(0). doi: http://dx.doi.org/10.1016/j.elerap.2014.08.004

Eaton, B. D., Elaluf-Calderwood, S. M., & Sorensen, C. (2010a, 11-14 Oct. 2010). *A methodology for analysing business model dynamics for mobile services using control points and triggers.* Paper presented at the 2010 14th International Conference on Intelligence in Next Generation Networks (ICIN).

Eaton, B. D., Elaluf-Calderwood, S. M., & Sorensen, C. (2010b, 13-15 June 2010). *The Role of Control Points in Determining Business Models for Future Mobile Generative Systems.* Paper presented at the 2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), .

Eaton, B. D., Elaluf-Calderwood, S. M., Sorensen, C., & Yoo, Y. (2015). Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System. *MIS Quartely, 39(1)*, 217-243.

Elaluf-Calderwood, S., Eaton, B., Herzhoff, J., & Sorensen, C. (2011). *Mobile Platforms as Convergent Systems - Analysing Control Points and Tussles with Emergent Socio-Technical Discourses*: InTech.

EMVCo. (2007). EMV mboile contactless payment technical issues and position paer.

Gaur, A., & Ondrus, J. (2012). *The Role of banks in the mobile payment ecosystem: a strategic asset perspective*. Paper presented at the Proceedings of the 14th Annual International Conference on Electronic Commerce, Singapore.

Ghazawneh, A., & Henfridsson, O. (2012). Balancing platform control and external contribution in third‐party development: the boundary resources model. *Information Systems Journal*(23(2)), 173-192.

GlobalPlatform. (2011). GlobalPlatform Card Specification.

GlobalPlatform. (2015). About GlobalPlatform. Retrieved January 13th, 2015, from http://www.globalplatform.org/aboutus.asp

GSMA. (2013a). The Embedded SIM. London.

GSMA. (2013b). The Role of the Trusted Service Manager in Mobile Commerce.

GSMA, & Booz & Co. (2011). Socio-economic benefits of SIM-based NFC. London.

Halinen, A., & Törnroos, J.-Å. (2005). Using case methods in the study of contemporary business networks. *Journal of Business Research, 58*(9), 1285-1297. doi: http://dx.doi.org/10.1016/j.jbusres.2004.02.001

Hawkins, R., & Ballon, P. (2007). When standards become business models: reinterpreting “failure” in the standardization paradigm. *info, 9*(5), 20-30. doi: doi:10.1108/14636690710816426

Herzhoff, J. D., Elaluf-Calderwood, S. M., & Sørensen, C. (2010, 13-15 June 2010). *Convergence, Conflicts, and Control Points: A Systems-Theoretical Analysis of Mobile VoIP in the UK.* Paper presented at the Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference on.

Hjorth, P., & Bagheri, A. (2006). Navigating towards sustainable development: A system dynamics approach. *Futures, 38*(1), 74-92. doi: http://dx.doi.org/10.1016/j.futures.2005.04.005

Hung, S.-Y., Chang, C.-M., & Kuo, S.-R. (2013). User acceptance of mobile e-government services: An empirical study. *Government Information Quarterly, 30*(1), 33-44. doi: http://dx.doi.org/10.1016/j.giq.2012.07.008

Jacobides, M. G., Knudsen, T., & Augier, M. (2006). Benefiting from innovation: Value creation, value appropriation and the role of industry architectures. *Research Policy, 35*(8), 1200-1221.

Jaemin, P., Kiyoung, B., & Cheoloh, K. (2013, 2-6 Sept. 2013). *Secure Profile Provisioning Architecture for Embedded UICC.* Paper presented at the 2013 Eighth International Conference on Availability, Reliability and Security (ARES).

Jaemin, P., Kyoungtae, K., & Minjeong, K. (2008, 13-15 Dec. 2008). *The Aegis: UICC-Based Security Framework.* Paper presented at the Second International Conference on Future Generation Communication and Networking, 2008. FGCN '08. .

Kaplinsky, R., & Morris, M. (2001). *A handbook for value chain research* (Vol. 113): IDRC Ottawa.

Kartseva, V., Hulstijn, J., Tan, Y.-H., & Gordijn, J. (2006). Towards value-based design patterns for inter-organizational control. *BLED 2006 Proceedings*, 22.

Kemp, R. (2013). Mobile payments: Current and emerging regulatory and contracting issues. *Computer Law & Security Review, 29*(2), 175-179. doi: http://dx.doi.org/10.1016/j.clsr.2013.01.009

Klein, G., & Wolf, S. (1998). The role of leverage points in option generation. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 28*(1), 157-160. doi: 10.1109/5326.661098

Kushchu, I., & Kuscu, M. H. (2003). *From E-government to M-government: Facing the inevitable*. Paper presented at the The 3rd European Conference on e-Government.

Lessig, L. (2006). *Code and Other Laws of Cyberspace Version 2.0*. New York: Basic Books.

Li, F., & Whalley, J. (2002). Deconstruction of the telecommunications industry: from value chains to value networks. *Telecommunications Policy, 26*(9–10), 451-472. doi: http://dx.doi.org/10.1016/S0308-5961(02)00056-3

Luhmann, N. (1984). *Soziale Systeme*. Frankfurt: Surhkamp Verlag.

M'Chirgui, Z. e. (2005). Smart card industry: a technological system. *Technovation, 25*(8), 929-938. doi: http://dx.doi.org/10.1016/j.technovation.2004.02.004

M'Chirgui, Z. (2009). Dynamics of R&D networked relationships and mergers and acquisitions in the smart card field. *Research Policy, 38*(9), 1453-1467. doi: http://dx.doi.org/10.1016/j.respol.2009.07.002

Madlmayr, G., Dillinger, O., Langer, J., Schaffer, C., Kantner, C., & Scharinger, J. (2007, 9-11 July). *The benefit of using SIM application toolkit in the context of near field communication applications.* Paper presented at the 2007 International Conference on the Management of Mobile Business

Mallat, N. (2007). Exploring consumer adoption of mobile payments – A qualitative study. *The Journal of Strategic Information Systems, 16*(4), 413-432. doi: http://dx.doi.org/10.1016/j.jsis.2007.08.001

Mantoro, T., & Milisic, A. (2010, 13-14 Dec. 2010). *Smart card authentication for Internet applications using NFC enabled phone.* Paper presented at the 2010 International Conference on Information and Communication Technology for the Muslim World (ICT4M).

Markantonakis, K., & Mayes, K. (2003). An overview of the GlobalPlatform smart card specification. *Information Security Technical Report, 8*(1), 17-29. doi: http://dx.doi.org/10.1016/S1363-4127(03)00103-1

Markendahl, J., Smith, M., & Andersson, P. (2010). *Analysis of roles and position of mobile network operators in mobile payment infrastructure* Paper presented at the 21st European Regional ITS Conference, Copenhagen.

Marwaha, G. (2014). Apple Pay vs Google Wallet: The Secure Element. Retrieved from http://www.gmarwaha.com/blog/2014/10/02/apple-pay-vs-google-wallet-the-secure-element/

Mayes, K., & Evans, T. (2008). Smart cards for mobile communications *Smart Cards, Tokens, Security and Applications* (pp. 85-113).

Meadows, D. H. (1999). *Leverage points: Places to intervene in a system*: Sustainability Institute Hartland, VT.

Moore, J. F. (1993). Predators and prey: a new ecology of competition. *Harvard business review, 71*(3), 75-83.

MPFI. (2008). SIM card report. http://www.mpf.org.in/pdf/general/SIMCard_Report%20PPT.pdf

Noll, J., Calvet, J. C., & Myksvoll, K. (2006, 29-31 July 2006). *Admittance Services through Mobile Phone Short Messages.* Paper presented at the International Conference on Wireless and Mobile Communications, 2006. .

Normann, R., & Ramirez, R. (1993). *Designing interactive strategy: From value chain to value constellation* (Vol. 1998): Wiley Chichester.

Nu.nl. (2015). Overheid start met testen opvolger DigiD. Retrieved March 25th, 2015, from http://www.nu.nl/internet/3989455/overheid-start-met-testen-opvolger-digid.html

Ondrus, J., & Lyytinen, K. (2011, 20-21 June 2011). *Mobile Payments Market: Towards Another Clash of the Titans?* Paper presented at the 2011 Tenth International Conference on Mobile Business (ICMB).

Ondrus, J., Lyytinen, K., & Pigneur, Y. (2009, 5-8 Jan. 2009). *Why Mobile Payments Fail? Towards a Dynamic and Multi-Perspective Explanation.* Paper presented at the System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on.

Ouchi, W. G. (1979). A Conceptual Framework for the Design of Organizational Control Mechanisms. *Management Science, 25*(9), 833-848. doi: doi:10.1287/mnsc.25.9.833

Pannifer, S., Clark, D., & Birch, D. (2014). *HCE and SIM Secure Element: It's not black and white*. Guildford: Consult Hyperion.

Peltoniemi, M., Vuori, E., & Laihonen, H. (2005). *Business ecosystem as a tool for the conceptualisation of the external diversity of an organisation.* Paper presented at the Proceedings of the Complexity, Science and Society Conference.

Peppard, J., & Rylander, A. (2006). From Value Chain to Value Network: Insights for Mobile Operators. *European Management Journal, 24*(2–3), 128-141. doi: http://dx.doi.org/10.1016/j.emj.2006.03.003

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*: Stanford University Press.

Porter, M. E. (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: The Free Press.

Reveilhac, M., & Pasquet, M. (2009, 24-24 Feb. 2009). *Promising Secure Element Alternatives for NFC Technology.* Paper presented at the First International Workshop on Near Field Communication, 2009. NFC '09. .

Rijksoverheid. (2015a). Het eID scheme: een nieuwe standaard voor toegang tot online dienstverlening. Den Haag.

Rijksoverheid. (2015b). Kabinet start pilots met het eID Scheme. Retrieved 27 February, 2015, from http://www.rijksoverheid.nl/nieuws/2015/02/09/kabinet-start-met-pilots-voor-eID scheme.html

Rongyu, H., Guolei, Z., Chaowen, C., Hui, X., Xi, Q., & Zheng, Q. (2009). A PK-SIM card based end-to-end security framework for SMS. *Computer Standards & Interfaces, 31*(4), 629-641. doi: http://dx.doi.org/10.1016/j.csi.2008.06.011

Sein, M., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS Quartely, 35*(1), 37-56.
Smart Card Alliance. (2014a). Host Card Emulation
Smart Card Alliance. (2014b). NFC Frequently Asked Questions. Retrieved 18 November, 2014, from http://www.smartcardalliance.org/publications-nfc-frequently-asked-questions/
Smart Card Alliance. (2015). Smart Cards Applications. Retrieved 27 January, 2015, from http://www.smartcardalliance.org/smart-cards-applications/
Solaimani, S. (2014). *The alignment of business model and business operations within networked-enterprise environments.* (PhD), TU Delft, Delft.
Solaimani, S., & Bouwman, H. (2012). A framework for the alignment of business model and business processes. *Business Process Management Journal, 18*(4), 655-679. doi: doi:10.1108/14637151211253783
Stabell, C. B., & Fjeldstad, Ø. D. (1998). Configuring value for competitive advantage: on chains, shops, and networks. *Strategic management journal, 19*(5), 413-437.
Stamp, M. (2006). *Information security: principles and practice*: John Wiley & Sons.
Statista. (2012). Global mobile payment transaction volume from 2010 to 2017. Retrieved February, 2015, from http://www.statista.com/statistics/226530/mobile-payment-transaction-volume-forecast/
Steffens, E. J., Nennker, A., Zhiyun, R., Ming, Y., & Schneider, L. (2009, 26-29 Oct. 2009). *The SIM-based mobile wallet.* Paper presented at the 13th International Conference on Intelligence in Next Generation Networks, 2009. .
Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research Commentary---Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Info. Sys. Research, 21*(4), 675-687. doi: 10.1287/isre.1100.0323
Trossen, D., & Fine, C. (2005). Value Chain Dynamics in the Communication Industry: MIT Communications Futures Program.
Tsai, Y.-R., & Chang, C.-J. (2006). SIM-based subscriber authentication mechanism for wireless local area networks. *Computer Communications, 29*(10), 1744-1753. doi: http://dx.doi.org/10.1016/j.comcom.2005.09.016
UL TS. (2014a). mCommerce ecosystems. Leiden.
UL TS. (2014b). Secure Element based NFC payments.
UL TS. (2015a). Apple's embedded SE. Leiden: UL TS.
UL TS. (2015b). White paper HCE payment implementation. Leiden.
Wiedemann, D. G., Palka, W., & Pousttchi, K. (2009). Business models for mobile payment service provision and enabling *Mobile and Ubiquitous Commerce: Advanced E-Business Methods* (pp. 29-47): IGI Global.
Wireless Watch. (2014). How iPad's soft SIM lets Apple pit carriers against each other. 2014, from http://www.theregister.co.uk/2014/10/27/ipads_soft_sim_is_the_thin_end_of_the_wedge_for_carriers/
Woodard, J. (2008). *Architectural Control Points*. Paper presented at the Third International Conference on Design Science Research in Information Systems and Technology (DESRIST 2008), Atlanta, GA.

Appendix A – Scientific article

The SIM Card as Control Point in the Dutch eID scheme

Joan Sebastiaan Blok
Faculty of Technology, Policy and Management, Delft University of Technology, the Netherlands

Abstract – The SIM is a secure module within the handset that can be used to offer authentication and identification services. These capabilities offer opportunities for MNOs to exploit the SIM as revenue source. This paper researches whether MNOs can exploit the SIM in the Dutch eID scheme by applying the concept of control points. By analysing interviews with authentication and identification experts, this paper provides empirical data on the concept of control points. The results show that the SIM technology is a suitable means to provide authentication and identification in the eID scheme but that uncertainties related to the revenue model are barrier to exploit these qualities.
Keywords: eID, SIM card, control points, value networks, authentication

1. Introduction

Mobile Network Operators (MNOs) are facing difficult times. Currently their revenues are declining as the use of SMS and regular phone calls are being replaced by over-the-top (OTT) services such as Whatsapp and Viber. Forecasts show an expectation of a 1.5 per cent revenue decrease per year for mobile networks in Europe in the coming decade (ATKearney, 2013). These forecasts do not show a bright future for the MNOs and therefore they need new sources of revenue if they are to sustain or grow their profitability.

A possible new source of revenue for MNOs could be to provide mobile authentication and identification services. In order to provide such services the Subscriber Identity Module (SIM) card could be of value. The SIM is used to identify and authenticate devices such as mobile handsets. The SIM is a tamper resistant independent part of the mobile phone, which can become a trusted entity guarding personal information and identifying each user (Mantoro & Milisic, 2010). The SIM, in the form of a Universal Integrated Circuit Card (UICC) can take over functions of plastic smartcards since it is able to hold a number of applications (Jaemin, Kyoungtae, & Minjeong, 2008). Hence, the SIM card can be used for services such as ID cards, bank cards, bus tickets or even a security element that confirms a person's identity online without the need to introduce new hardware elements in the mobile handset (Mantoro & Milisic, 2010; Reveilhac & Pasquet, 2009). This shows that the SIM can be used to provide mobile authentication and identification services.

There are, however, technical alternatives in the market that offer similar functionalities as the SIM: embedded secure elements (SE) and cloud-based solutions. The embedded SE is a hardware module that is soldered onto the mobile handset and offers the same level of security as the SIM (Reveilhac & Pasquet, 2009). In a cloud-based solution the credentials are stored in the cloud environment of the service provider rather than on a hardware module (Pannifer, Clark, & Birch, 2014). Both solutions are capable of providing mobile authentication and identification services. This shows that the SIM is not the only option for mobile authentication and identification services and that MNOs face fierce competition.

This paper is part of a larger research conducted by UL Transaction Security and Delft University of Technology to identify new opportunities for the SIM. During this research the eID scheme in the Netherlands was marked as possible opportunity for MNOs to exploit the SIM by providing mobile authentication and identification services. The eID scheme is new standard for online identification that is being developed by the Dutch government in co-operation with the business sector (Rijksoverheid, 2015b). The eID scheme contributes to the government's ambition that by 2017 all government transactions with citizens and businesses can be conducted electronically (Rijksoverheid, 2015a). The eID

scheme allows for multiple login sources with have a high level of assurance and offers the possibility that these means are provided by public and private organizations (Rijksoverheid, 2015b). This means that the scheme offers the possibility to login with an ID card or even a bankcard, as long as these means comply with the requirements of the eID scheme. This shows that the eID scheme could be an opportunity for MNOs to provide authentication and identification services for the government by leveraging the SIM. Therefore this paper aims to determine whether MNOs could exploit the SIM in the eID scheme.

As such, the concept of control point seems relevant for this research, as it helps to analyze business models and to identify potentially profitable sources of revenue to MNOs (Eaton, Elaluf-Calderwood, & Sorensen, 2010a). This concept is first discussed in a white paper of the Value Chain Dynamics Working Group (VCDWG), which is part of the MIT Communications Futures Program (Trossen & Fine, 2005). This group aimed to develop a methodology to detect positions of economic power for services within the telecommunications industry and to understand their sustainability. Based on this goal, the group developed the concept of control points. Eaton et al. (2010a) embed the concept within existing business model literature and define control points as functional areas where power can be exercised within value networks. Control points have been applied in a number of studies. For example, Eaton, Elaluf-Calderwood, and Sorensen (2010b) use control points for a high level analysis of the business model of two mobile service platforms: Apple's App store and the Android Market Place. Next to that, Woodard (2008) uses it to characterize architectural design decisions. In general, it shows that control points explain why and how members of the value network can extract value (Cimiotti & Schonowski, 2010; Eaton et al., 2010a; Woodard, 2008). So, if the SIM would qualify as control point in the eID scheme, it should be able to generate value to the MNO.

In this paper, we apply the concept of control points to determine whether the SIM qualifies as a control point, which MNOs can exploit as an authentication and identification means in the eID scheme. As the eID scheme is still under development, there is limited data available. That is why we use interviews as a research approach. This allows us to acquire knowledge of practitioners and experts related to mobile authentication and identification as well as the eID scheme domain.

Theoretically, this paper contributes to the concept of control points, as there is a lack of empirical data (Eaton et al., 2010a). By conducting interviews with in industry experts empirical data can be gathered that can help to further develop the concept of control points. Furthermore, this research contributes to the domain of mobile authentication and identification as well as eID services.

The remainder of the paper is organized as follows. First, an understanding of the theoretical basis of the research is discussed. Second, an overview of the domain regarding mobile authentication and identification and the eID scheme is provided. Next, we discuss the research approach, after which we discuss the results of the interviews. Finally, a conclusion and discussion is presented.

2. Theoretical background

Eaton et al. (2010b) frame control points as socio-technical objects, which are driven by the need to share resources and content over networks. In addition, Bouwman, De Vos, and Haaker (2008) argue that a service cannot be offered by a single company and that a number of companies have to work together to create and deliver a service. All this this relates to the Resource Dependence Theory (RDT) of Pfeffer and Salancik (1978). They explain that organizations cannot own all resources and capabilities needed for its business but they can have access to resources of other firms, which creates interdependency. This means that the resources one organization needs are often owned by other organizations and therefore organizations depend on each other. Hence, resources are a basis of power (Pfeffer & Salancik, 1978). Control points are elements or resources on which other players in the value network depend to conduct their business and therefore control points are sources of economic power (Eaton et al., 2010a). According to Ballon (2009a) and Kartseva, Hulstijn, Tan, and Gordijn (2006), power is manifested through control and can be operationalised through different patterns such as authorisation, confirmation and compensation. Based on Ouchi (1979), control can be defined as the design and improvement of mechanisms through which an organization can be managed, so that it moves towards its objectives. In a control point control is exerted through business, regulatory and/or technical means (Eaton et al., 2010a).

Control points exist within value networks and therefore it is necessary to first define value networks. As explained, organizations have to collaborate to create and deliver a service. Li and Whalley (2002) explain that organizations working together in the telecommunications industry can be viewed as a value network. According to De Reuver (2009, p. 12) value networks can be defined as "*a dynamic network of actors working together to generate customer value and network value by means of a specific service offering, in which tangible and intangible value is value exchanged between the actors involved"*. A value network can be seen as an economic mechanism that converts one form of value to another (Allee, 2008). Value networks are thus networks in which value conversion takes place with the goal to deliver a specific service or product. The concept of value networks is closely related to Porter's (1985) concept of value chains. However, for this research the concept of value networks seems more valuable as Li and Whalley (2002) argue that telecommunications is a competitive market where companies not only compete in a conventional way (linear chain) but also compete with companies from other industries that operate under different value propositions and economics, therefore the industry can better be described as a value network rather than a value chain. Furthermore, the focus within value chains is on the exchange of tangible assets and that the flow of intangible assets is not considered (Allee, 2000, 2008). Intangible assets are becoming more important in today's economy and should therefore be included when describing and analysing networks (Allee, 2002). In this research we use value networks to analyse the value exchanges among the actors involved with SIM-based authentication and identification for the eID scheme.

Ballon (2009a) argues that not all positions within a value network carry the same 'weight' and therefore the positions must be analysed to fully take into account power relations and structural asymmetries. As discussed, control points can help to explain the positions of economic power within a value network. Control points are defined and evaluated by four parameters (Eaton et al., 2010b; Trossen & Fine, 2005):

- *Interchangeable or scarcity:* The ease by which alternative players can own a similar control point asset
- *Demand:* The extent to which a control point is accessed by players within a value network.
- *Value:* The amount of tangible and intangible value that a control point is able to capture.
- *Time*: Affecting the other parameters, as they are dynamic and may change over time.

Another aspect that Trossen and Fine (2005) take into account in their theory is triggers. Triggers help to explain changes and the sustainability of the business models. Triggers are external factors that cause a transition from one set of control points.

Based on these characteristics, it is concluded that control points show a lot of resemblance with bottlenecks. Bottlenecks have been discussed in a wide range of studies (Baldwin & Clark, 2006; Ballon, 2009b; Jacobides, Knudsen, & Augier, 2006). Bottlenecks have been researched in fields varying from transaction cost, supply chain management, economics, anti-trust law, platform theory to design science and are thus well documented (Ballon, 2009a). Jacobides et al. (2006, p. 1209) define a bottleneck as *"a segment in a system where mobility (both in terms of switching costs and potential entry) is limited and competition is softened"*. When owning and controlling a bottleneck the owner is provided with bargaining and economic power as bottlenecks are critical resources that are limited in supply and high in demand (Ballon, 2009a; Boudreau, 2010). This shows that the bottlenecks have similar characteristics as control points. However, a difference is that not every control point is limited in supply and high in demand. Eaton et al. (2010a) shows that every actor in the value network has at least one control point and not all of them are limited in supply and high in demand. We conclude that bottlenecks can be viewed as strong control points. This means that a value network member does not need to own a bottleneck to capture value. However, they do need to own a control point to capture value.

Other concepts that are closely related to control points are gatekeepers (Ballon & Van Heesvelde, 2010) and boundary resources (Ghazawneh & Henfridsson, 2012), which deal with access control of platforms or resources. These concepts can be seen as specific control points, as they allow an organization to capture value by granting parties access to a resource or platform. However, control points are not limited to these functionalities. This research uses control points as means of analysis, as it a comprehensive concept that can be used to analyse a broad spectrum of possible value sources.

We are aware that in order for MNOs to play a role in the eID scheme other factors might play a role such as revenue models or governance issues. However, in this research the focus is on whether the SIM can generate value in the eID scheme rather than on the business model itself. Therefore we use the concept of control points, as it helps to gain insight in the control and economic power that the SIM offers to MNOs.

3. Domain

As explained in the introduction, the Dutch eID scheme is a new standard for online identification that is being developed by the Dutch government in cooperation with business sector. Currently, the eID scheme is in a pilot phase, which will run till the beginning of 2016 (Nu.nl, 2015). The aim of the scheme is to establish an identity electronically with a sufficient level of assurance to process and protect personal data. The eID scheme can be used to identify a user at government websites but also at commercial websites such as webshops by using attribute provisioning (Rijksoverheid, 2015b). For example, an online liquor store needs to know whether a user is old enough. Attribute provisioning makes it possible that the liquor store will receive a 'yes' or 'no' by relying on the eID. In the eID scheme the user can decide what personal data is shared with the website. Besides, the website is only allowed to ask for data that is needed for their service (Rijksoverheid, 2015c).

In order for a user to identify himself at a website, he has to login to verify his identity. An interesting feature of the eID scheme is that it allows for multiple login means. This makes the system flexible and less vulnerable for malfunctions (Rijksoverheid, 2015c). The government wants to offer the possibility to login with government issued documents such as a driver's license and ID card. Next to that, the government wants to allow login means of private organizations such as bankcards. Within the eID scheme the government wants to stimulate a free market and therefore they want private organizations to join the scheme (Rijksoverheid, 2015d). According to the government, all means that comply with the eID criteria are allowed to connect to the system. Therefore this research aims to determine whether the SIM would be a suitable means to provide authentication and identification in the eID scheme.

4. Research approach

As this research focuses on new applications of the SIM, it is explorative of nature and there is limited data available. Therefore this research uses semi-structured interviews as a way to capture knowledge of practitioners and experts related to mobile authentication and identification and the eID scheme. Semi-structured interviews allow room for new theoretical insights while the information can be analyzed in a structured way. This allows us to incorporate findings beyond the concept of control points that might be of value to determine whether the SIM can be exploited.

The interviews candidates were acquired in a number of ways. First, the client network of UL Transaction Security was consulted. Second, the network of academics from the Delft University of Technology was contacted. Third, the personal network of the researcher was used to make contact with industry experts. Finally, interviewees were asked if they knew experts that could be of value for the research. This led to a diverse group of 12 experts. The number of experts is the result of the saturation principle. The respondents were senior level experts and had knowledge of mobile authentication and identification services and/or the eID scheme. This helped to assess the capabilities of the SIM as well as the requirements for the login means in the eID scheme. As this research was part of a larger research, the mobile authentication and identification experts were asked to assess multiple markets where the SIM could be of value i.e. mobile payment and enterprise ID. We interviewed two MNOs and one government organization. Unfortunately, we were unable to interview more directly involved stakeholders. Therefore we tried to close this gap by interviewing a number of independent experts. An additional benefit is that these experts could speak more freely, as they are not directly involved with the service development. All respondents were located in the Netherlands, with one exception. This could lead to imbalance, however, as this expert was an academic he mainly focused on the capabilities of the SIM and analyzed the role of MNOs in general. An overview of the respondents can be found in table 1.

The interviews were conducted by making use of an interview protocol but the respondents were allowed to deviate from the list to provide their own insights. The interview questions focused on the control point criteria, i.e. viability value network, level of uniqueness, demand, value, time and triggers. An overview of the protocol can be found in the appendix. The interviews have transcribed by making use of notes and audio recordings. After which, the gathered data was structured by making use of coding. The coding helps to build a theory to answer the research question. In the first round of coding important elements related to authentication and identification services were highlighted. In the second round of coding the focus was on finding communalities and differences related to the SIM and the MNO in regard to the concepts of control points and value networks. Finally, selective coding was done where the findings of the interviews are coupled to the control point criteria. Based on the findings in the interviews, the researcher established links with the control point criteria, as some explanations are hidden between the lines.

Code	Organization	Position	Expertise
MNO1	MNO	Manager mCommerce	mCommerce
MNO2	MNO	Manager mCommerce	mCommerce
GOV	Government	Chief Security Officer	Government services
IE1	Independent expert	Managing consultant	Authentication
IE2	Independent expert	Consultant	mCommerce
IE3	Independent expert	Consultant	Government services
IE4	Independent expert	Card scheme manager	mCommerce
IE5	Independent expert	Business developer	mCommerce
IE6	Independent expert	Managing partner	Authentication
IE7	Independent expert	Associate professor	mCommerce
IE8	Independent expert	Program Director	mCommerce
IE9	Independent expert	Senior consultant	ICT Government

Table 0-1: Overview of respondents

5. Results

This section presents the main findings from the interviews. The results are discussed by the means of the control point criteria. During the analysis of the interviews it showed that the control point parameters overlap. The level of uniqueness has a direct affect on the strength of a control point but also indirect. The level of uniqueness affects the parameters demand and value because if there are alternatives for the SIM then this will likely lead to less market share. Next to that, if the level of uniqueness that the control point offers is low, then the value that the control point represents will be less. The parameter demand also influences the value of the control point, as the scarcity principle shows that more demand leads to higher pricing. Since these parameters have overlap, a number underlying factors influence multiple parameters. These factors have been derived from the interviews and are discussed next in relation to the SIM as possible control point. The statements and quotes presented in this chapter are linked to codes that have been assigned to the respondents in table 1. The remainder of this section is structured according the control point criteria: level of uniqueness, demand, value and time. Finally, the viability of the value network is discussed.

5.1 Level of uniqueness

As this paper is part of a larger research on SIM-based mobile authentication and identification services, we initially marked embedded SEs and cloud-based solutions as competitors for the SIM. However, during the interviews it became apparent that banks and governments should be seen as competitors for providing eID services. Banks have the ability to provide eID services by using the bankcards as authentication and identification means [GOV, IE1, IE4, IE6, IE9], while the government provides its citizens with ID cards and driver's licenses, which could connect to the eID scheme [GOV, IE1, IE2, IE9]. However, the government wants to create a system, which offers the possibility to log in with multiple means and to which businesses could connect. This leads to a more robust system because different means can be used to log in [GOV, IE3]. Therefore the government can be seen as a competitor

for the MNO, as they would supply their own authentication means, but also as a customer, as they want businesses to connect to the system to create robustness.

Handset manufacturers, who control the embedded SE, are not seen as competitors because the government has a preference for local players due to privacy issues (e.g. patriot act). Next to that, the fragmentation of handsets weakens the position handset manufacturers because the government wants a standardized solution [GOV, IE1, IE3, IE9]. They do not want to differentiate per authentication means, as this leads to limited reach and high costs. Furthermore, a cloud-based solution is currently not seen as a competing technology for the SIM [GOV, IE3].

Therefore we define the level of uniqueness of the SIM by comparing it to bankcards and ID cards. Based on the interviews, we conclude that the SIM is unique because it combines a number of key characteristics. First, is that the SIM is present in every handset and this is valuable as because people are more attached to their phone than bankcard [MNO2, IE9]. The MNO logically values his own product above others and as only one other expert mentioned this, one could doubt the value of this view. Second, is that the SIM has reach, as many consumers own a SIM. Reach is a key requirement for authentication services, as the government wants to serve all its citizens [MNO1, MNO2, GOV, IE1, IE2, IE3, IE4, IE6, IE7, IE9]. Third, the SIM is a secure means for authentication and identification [MNO1, MNO2, IE3, IE4, IE5, IE6, IE7]. The government must be able to trust that a person is really who he says he is and therefore a secure authentication and identification is needed. To determine the level of assurance of the authentication means the government uses the STORK framework [MNO1, GOV, IE1, IE6, IE7]. This is a framework developed by the EU, which is used to determine the quality of assurance that an authentication means offers. For the eID scheme the government requires that a person's identity has been confirmed, which complies with STORK level 3 and 4. The SIM technology is able to meet the STORK requirements, as it securely stores secrets and could be linked to a person [MNO1, GOV, IE6, IE7]. The final feature that makes the SIM unique is that it is able to provide connectivity [MNO1, MNO2, IE6]. This connectivity can increase the security of the authentication and identification process, as the SIM provides a separate communication channel and therefore a man in the middle attack is less likely [GOV, MNO2]. All the discussed characteristics contribute to the level of uniqueness of the SIM. It is the combination of characteristics that makes the SIM unique compared to other solutions such as a bankcard or ID card.

5.2 Demand

The section on the level of uniqueness shows that the SIM is has reach and that the technology can comply with STORK level 3 or 4. As discussed, these are key characteristics for authentication and identification services. Therefore these characteristics are a cause of demand, as long as the SIM complies with the eID standards. However, based on the interviews a number of limiting factors have been identified for demand. The first limiting factor has been addressed in the previous section, as the SIM is not the only means that can offer authentication for the eID scheme.

Second, is that a SIM swap is needed as most of the deployed SIMs are technically not suitable to offer authentication and identification services [MNO1, MNO2, IE7]. A SIM swap is an extensive process that leads to high costs. A MNO explained that this is a real barrier as it hard to let consumers swap their SIM. Market research shows that most consumers will not to come to the shop for a new SIM [MNO1]. If most of the SIMs are not suitable for to offer authentication for the eID scheme, then the reach is also small and this is unwanted by the government. The needed SIM swap thus affects the costs of the SIM but also the reach of the solution.

Another limiting factor is the fragmentation of MNOs in the Netherlands. Cooperation with three MNOs is needed to serve most of the market [MNO2, IE2, IE6 IE7]. The government does not want a fragmentation of solutions because it limits reach and requires adjustments per authentication and identification means. Therefore the service must be standardized [GOV, MNO1, IE1, IE2, IE9]. As one of the respondents said: *"The operators must offer the same level of service because if they don't then their reach becomes really small"* [IE1]. Therefore a number of the respondents argued that the MNOs must collaborate together to create an independent authentication standard that could connect to the eID scheme [IE1, IE2, IE4, IE7]. Then the MNOs would be able to offer the same level of service and the government

would not have to differentiate per MNO. However, [GOV] said that it is not essential for MNOs to create a standard, as MNOs could individually connect to the eID scheme. This would mean that the eID requirements would lead to standardization. If a party is able to meet these requirements they could join the eID scheme. [GOV] estimated that MNOs would be able to serve over a third of the eID market due to their reach and presence in the handset. However, the government wants the MNOs to join the eID scheme and therefore this estimation could possibly be too positive. Overall, it shows that most of the respondents think that there can be demand for the SIM in the eID scheme.

5.3 Value

As explained, the value parameter is influenced the already discussed parameters of uniqueness and demand. Therefore the same factors that impact the demand affect the value of the SIM. It is because of qualities that the SIM has that it creates demand and it is because of these qualities that it represents value. Furthermore, if there is more demand for the SIM then it becomes more valuable. However, for the MNOs it is key that the SIM will lead to revenue [MNO1, MNO2]. This means that a revenue model is needed. "*The idea is that authenticators will earn money by the provisioning of attributes and that the party asking for the authentication will pay"* [GOV, IE3, IE6]. However, the revenue model of the eID scheme is uncertain, as the eID scheme it is still under development [GOV, MNO2, IE1, IE2, IE4, IE6, IE9]. It is uncertain what the system should look like and for what services it can be used, as it is currently in a pilot phase.

5.4 Time

The fourth control parameter is time, as the strength of a control point can change over time. During the interviews, a number of aspects have been discussed that could possibly influence the strength of the SIM as control point over the next couple years. However, none of these factors were widely addressed during the interviews.

5.5 Viability value network

As control points exist within value networks, a condition is that the value network is viable. Therefore the respondents were asked to give their view on the role that MNOs could have within the eID scheme. The interviews showed a number of complications that should be overcome in order for the SIM to be part of eID scheme.

A key condition is that MNOs must comply with STORK level 3 or 4, as the eID scheme is build around this standard [MNO1, GOV, IE1, IE4]. As discussed, the security of the SIM can be STORK compliant. However, to reach STORK level 4 a physical meeting is needed, where the identity of the consumer is confirmed. According to the respondents the MNOs have an issuing process that can meet the STORK requirements, as they have face-to-face enrolment [MNO1, GOV, IE1, IE4]. However, a number of respondents pointed out that not every SIM is linked to a person [MNO1, IE4, IE6, IE7]. The purchase of a pre-paid subscription does not require the user to physical identification. Furthermore, phone subscriptions can be passed on to other users (e.g. father pays subscription for daughter or company for employee). So, although MNOs have face-to-face enrolment, the SIM is not necessarily linked to a person. To meet the STORK requirements MNOs must upgrade their issuance process in such a way that the SIM is indeed linked to a person.

Another factor that could influence the role of the MNO is that they need to become a trusted service provider [IE1, IE2, IE4, IE6, IE9]. "*Trust is essential for authentication because the company that requires authentication has to trust that the company, which facilitates the authentication, can verify the user. For instance, a web shop has to trust that they will receive a payment when the consumer purchases something. They have to trust the authentication and identification mechanism of the bank*" [IE1]. From a consumer perspective trust is important as well because they want their information handled carefully and securely. Most respondents thought that the MNOs were able to gain the trust of their customers as they are known brands and are seen as technically capable [MNO1, MNO2, IE2, IE4, IE9]. The view of the MNOs could be biased, as they have a clear interest to present themselves as credible companies. However, three independent experts share this view and even said that banks have more trust issues due bonus scandals.

Based on the interviews, three other factors have been identified that influence whether the MNO could function as authenticator. These factors have already been discussed in the previous paragraphs and

therefore a brief overview is given. The first factor is that there are competitors for providing an eID. Another limiting factor could be the fragmentation of MNOs in the Netherlands. The third factor is the uncertain revenue model.

Based on the interviews, it seems that the MNO in the role of authenticator can be of value in the eID scheme. With some adjustments to the enrolment procedure, MNOs are able to offer STORK level 4 authentication. However, a barrier is that the revenue model for the eID scheme is still unknown and this leads to hesitation among MNOs to join the project. Nevertheless, one of the MNOs is actively pursuing the eID scheme and therefore the designed value network seems viable. An overview of the findings is presented in figure 1.

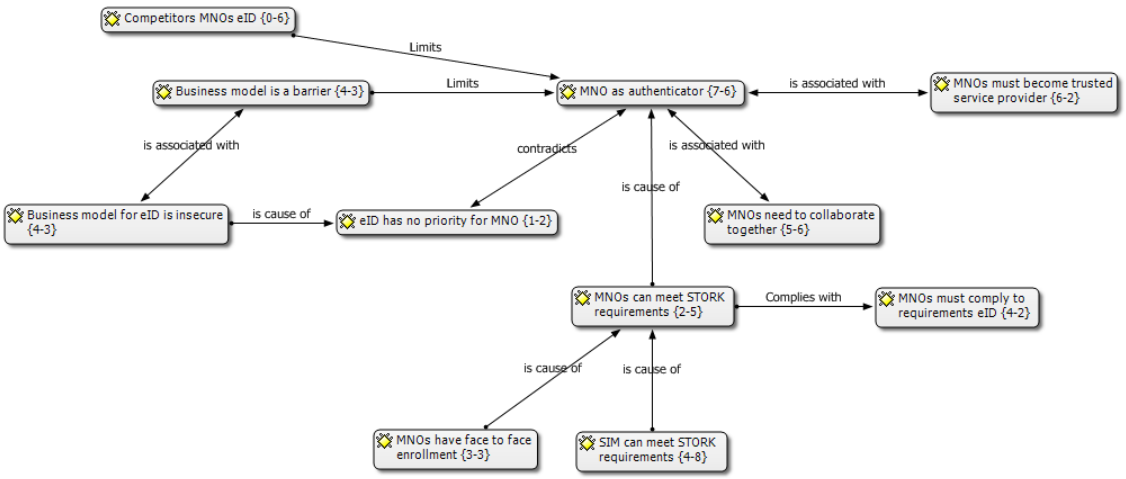


Figure 1: Overview role MNO in the eID scheme

In figure 1 an overview is presented, which summarizes the role that the MNO can play in the eID scheme. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned to the transcripts and the second number the links with other codes. Furthermore, the relation have been drawn by the researcher based on a secure analysis of the interviews.

6. Discussion and conclusions

This paper aimed to determine whether the SIM could qualify as a control point in the Dutch eID scheme that could be exploited by MNOs. This research was part of a larger researcher that aimed to identify possible opportunities for SIM-based authentication and identification services. Therefore 12 industry experts have been interviewed that had knowledge of mobile authentication and identification and/or the eID scheme. Based on the interviews, it is concluded that the SIM scores well on the control point criteria but whether it qualifies as a control point remains indefinite. The viability of the value network is uncertain due to an unknown revenue model. Therefore private companies are hesitant to join the eID program. Nevertheless, this research shows that the SIM can be of value in the eID scheme to provide authentication and identification.

From a theoretical aspect this research shows that the concept of control points helps to explain the added value of the SIM for mobile authentication and identification services. However, this research showed that the emergence of a value network could be a barrier for the existence of a control point. Therefore this research proposes that for future studies first the viability of the value network is researched. If that is the case, then the control point's concept can be used to determine how much value an organization can extract from the value network. Furthermore, this research identifies a complexity related to the evaluation of control points. This research shows that the control point parameters are interrelated. However, each parameter does add a new dimension to the control point and therefore a control point should be evaluated on all three parameters. For example, a unique control point might not

be able to extract value or have demand. Therefore all parameters should be incorporated when evaluating a control point. However, for the ease of the analysis the parameters should be assessed consecutively:

1. Level of uniqueness/scarcity
2. Demand
3. Value
4. Time

This research has a number of limitations. As this research was part from a larger research which focused on three markets and this comes at the expense of the research depth. If the interviews would focus on one market, more market specific industry experts could have been consulted. This could provide more insight in the viability of the designed value networks, as they could have been discussed in more detail. Next to that for this research it would have been valuable to interview more directly involved stakeholders. Unfortunately, it was only possible to interview MNOs that actively developing mCommerce solution. There is a risk that there is biased view on the added value of the SIM because only two MNOs have been interviewed that have a positive attitude towards mCommerce services. In relation to this, it was only possible to interview one government organization. For the research it would have been useful to conduct interview multiple government organizations. Especially, an interview with the ministry of Binnenlandse Zaken would seem valuable, as they are the initiator of the eID scheme. However, this research tried to cover this gap by interviewing multiple independent experts.

Finally, based on this research some recommendations for further research are done. This research showed that the emergence of a value network could be a barrier for the existence of a control point. Therefore this research proposes further research on how the viability of value networks can be assessed. In relation to that, it was concluded that control points are not suitable to determine whether a resource can be exploited in value networks that are bound to uncertainties. However, the concept could possibly be applied to evaluate control points in existing value networks. It could help to identify positions of power in existing value networks. With this in mind, it is proposed that case studies in which the concept of control point is applied to existing value networks. This should lead to empirical data and help in the further development of the concept. Furthermore, the researcher would propose a study regarding the strategic feasibility and viability of the eID scheme and how to implement a successful business model.

Appendix Interview. Topic list

Table 2 shows the interview protocol that was followed during the interviews. The protocol shows the questions related to the control point criteria. This protocol has been used to assess different markets and therefore gives a general overview of the questions.

Concepts	Question
Introduction	• Is audio recording allowed? • Explain the research and the research objective • Explain structure of the conversation
SIM	• What is your opinion on the function of the SIM in regard to mobile authentication and identification services?
Application markets	• What do you find interesting markets to target with mobile authentication and identification services and why? • Are the following service markets options for your company to offer mobile authentication and identification services considering the market size, potential revenue and needed security: o Enterprise ID (e.g. Physical access, intranet) o Government services (e.g. online identity, mobile passport) o Mobile payment (e.g. online, proximity) • What do you see as requirements when offering mobile authentication and identification services to the specific markets?
Value network	• What is your opinion of the value networks and do you see a role for your company? • What role is the most likely role for the MNO in the different service markets: o As cloud authentication provider? o As SE provider? o Or no role at all?
Control point criteria	
Uniqueness/scarcity	• What added value can the SIM provide to your company in regard to mobile authentication and identification services? • What technical alternatives would you consider when offering authentication services and why? • What technical solution would have you preference and why? • Why not another solution?

Demand	• For what service would the SIM be of added value and in what technical form? • What market share would the MNO be able to capture with the SIM for this service? • What are limitations of the SIM when offering authentication and identification services on a business and organizational level?
Value	• What influence does the SIM give the MNO in the value networks? • Can the SIM function as a revenue source to the MNO? • What would be a revenue sharing model that is likely to be supported by the service providers?
Time	• Do you see the SIM as a long-term solution for mobile authentication and identification services?
Triggers	• What are external (technical, organizational, business, social acceptance) factors that may influence the SIM as control point? • How do you estimate the chances of these factors indeed influencing the SIM as control point?
Concluding	• Do you have additional remarks or thoughts that you want to share?

References

Allee, V. (2000). Reconfiguring the value network. *Journal of Business Strategy, 21*(4), 36-39. doi: doi:10.1108/eb040103

Allee, V. (2002). *A value network approach for modeling and measuring intangibles*. Paper presented at the Transparent Enterprise, Madrid.

Allee, V. (2008). Value network analysis and value conversion of tangible and intangible assets. *Journal of Intellectual Capital, 9*(1), 5-24. doi: 10.1108/14691930810845777

ATKearney. (2013). A Future Policy Framework for Growth: A report for the European Telecommunications Network Operators' Association(ETNO). London: ATKearney.

Baldwin, C. Y., & Clark, K. B. (2006). Architectural innovation and dynamic competition: The smaller "footprint" strategy. *Harvard Business School, Boston, MA*.

Ballon, P. (2009a). *Control and Value in Mobile Communications A political economy of the reconfiguration of business models in the European mobile industry.* Vrije Universiteit Brussel, Brussels.

Ballon, P. (2009b). The platformisation of the European mobile industry. *Communications & Strategies*(75), 15.

Ballon, P., & Van Heesvelde, E. (2010). *Platform types and regulatory concerns in European ICT markets*.

Boudreau, K. (2010). Open platform strategies and innovation: Granting access vs. devolving control. *Management Science, 56*(10), 1849-1872.

Bouwman, H., De Vos, H., & Haaker, T. (2008). *Mobile service innovation and business models*: Springer Science & Business Media.

Cimiotti, M., & Schonowski, J. (2010, 13-14 Sept. 2010). *Telecommunication network driven Ecozone: Enable flexible enhanced services and new operator business models via NGOSS managed control points.* Paper presented at the Telecommunications: The Infrastructure for the 21st Century (WTC), 2010.

De Reuver, M. (2009). *Governing Mobile Service Innovation in Co-evolving Value Networks.* Technische Universiteit Delft, Delft.

Eaton, B. D., Elaluf-Calderwood, S. M., & Sorensen, C. (2010a, 11-14 Oct. 2010). *A methodology for analysing business model dynamics for mobile services using control points and triggers.* Paper presented at the 2010 14th International Conference on Intelligence in Next Generation Networks (ICIN).

Eaton, B. D., Elaluf-Calderwood, S. M., & Sorensen, C. (2010b, 13-15 June 2010). *The Role of Control Points in Determining Business Models for Future Mobile Generative Systems.* Paper presented at the 2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), .

Ghazawneh, A., & Henfridsson, O. (2012). Balancing platform control and external contribution in third-party development: the boundary resources model. *Information Systems Journal*(23(2)), 173-192.

Jacobides, M. G., Knudsen, T., & Augier, M. (2006). Benefiting from innovation: Value creation, value appropriation and the role of industry architectures. *Research Policy, 35*(8), 1200-1221.

Jaemin, P., Kyoungtae, K., & Minjeong, K. (2008, 13-15 Dec. 2008). *The Aegis: UICC-Based Security Framework.* Paper presented at the Second International Conference on Future Generation Communication and Networking, 2008. FGCN '08. .

Kartseva, V., Hulstijn, J., Tan, Y.-H., & Gordijn, J. (2006). Towards value-based design patterns for inter-organizational control. *BLED 2006 Proceedings*, 22.

Li, F., & Whalley, J. (2002). Deconstruction of the telecommunications industry: from value chains to value networks. *Telecommunications Policy, 26*(9–10), 451-472. doi: http://dx.doi.org/10.1016/S0308-5961(02)00056-3

Mantoro, T., & Milisic, A. (2010, 13-14 Dec. 2010). *Smart card authentication for Internet applications using NFC enabled phone.* Paper presented at the 2010 International Conference on Information and Communication Technology for the Muslim World (ICT4M).

Nu.nl. (2015). Overheid start met testen opvolger DigiD. Retrieved March 25th, 2015, from http://www.nu.nl/internet/3989455/overheid-start-met-testen-opvolger-digid.html

Ouchi, W. G. (1979). A Conceptual Framework for the Design of Organizational Control Mechanisms. *Management Science, 25*(9), 833-848. doi: doi:10.1287/mnsc.25.9.833

Pannifer, S., Clark, D., & Birch, D. (2014). *HCE and SIM Secure Element: It's not black and white*. Guildford: Consult Hyperion.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*: Stanford University Press.

Porter, M. E. (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: The Free Press.

Reveilhac, M., & Pasquet, M. (2009, 24-24 Feb. 2009). *Promising Secure Element Alternatives for NFC Technology.* Paper presented at the First International Workshop on Near Field Communication, 2009. NFC '09. .

Rijksoverheid. (2015a). The eID scheme. Retrieved 7 June, 2015, from http://www.eIDscheme.nl/snelbuttons/english/

Rijksoverheid. (2015b). Het eID stelsel: een nieuwe standaard voor toegang tot online dienstverlening. Den Haag.

Rijksoverheid. (2015c). Kabinet start pilots met het eID Stelsel. Retrieved 27 February, 2015, from http://www.rijksoverheid.nl/nieuws/2015/02/09/kabinet-start-met-pilots-voor-eid-stelsel.html

Rijksoverheid. (2015d). Uitgangspunten van het eID stelses. Retrieved 7 June, 2015, from http://www.eID scheme.nl/over-eID scheme/uitgangspunten-voor-het-scheme/

Trossen, D., & Fine, C. (2005). Value Chain Dynamics in the Communication Industry: MIT Communications Futures Program.

Woodard, J. (2008). *Architectural Control Points*. Paper presented at the Third International Conference on Design Science Research in Information Systems and Technology (DESRIST 2008), Atlanta, GA.

Appendix B – Card architecture

In 1999 the GlobalPlatform has been established by companies from the payments and communications industry, the government sector and the vendor community (GlobalPlatform, 2011). It is a non-profit association that promotes a global infrastructure for smart card implementation across multiple industries with the goal to reduce the barriers, which are hindering multiple application smart cards (GlobalPlatform, 2015). For that reason GlobalPlatform has developed a standard for smart cards that provides a common security and card management architecture. The card architecture is useful for multi-application cards and is depicted in Figure 1.

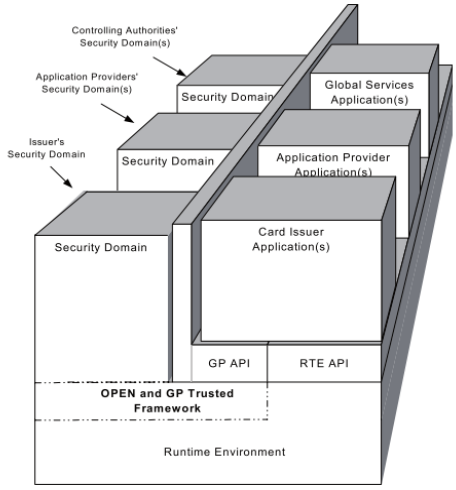


Figure 1: Card architecture (GlobalPlatform, 2011)

According to Alimi and Pasquet (2009, p. 3) "the GlobalPlatform card architecture consists of logical and physical components that aim to provide application interoperability and security, in an issuer controlled environment." As the architecture shows in Figure 1, multiple applications can be hosted on the card with each having its separate security domain. Security domains reflect on-card representatives of off-card authorities and can be split into three different types (GlobalPlatform, 2011):

- Issuer Security Domain (ISD)
- Supplementary Security Domains (SSD)
- Controlling Authority Security Domains (CASD)

The ISD is the first application that is installed on a card and is mainly used to perform all issuer related card management. The ISD performs cryptographic operations when card content changes and holds the issuer's keys. In the case of a SIM card the MNO is the issuer and the first application on the card is used to authenticate to the network. The SSD is a secured environment where a Service Provider (SP) or application provider is allowed to download, install and maintain applications following their own lifecycle. The CASD has the role to enforce the security policy on all application code that is loaded on the card (Alimi & Pasquet, 2009). The GlobalPlatform card specification allows the card issuer to delegate the card content management to the SP. SPs are able to manage their own applications on the card while issuers are protected from unauthorized changes (GlobalPlatform, 2011; Markantonakis & Mayes, 2003).

Appendix C – Application markets

This chapter identifies different markets where the SIM could possibly be of value as a secure authentication and identification means. The markets have been identified because they currently use smart cards for authentication purposes. However, the opportunities for authentication and identification are not limited to these markets but due to practical reasons such as time constraints, this research focuses on major industries that use smart cards. For the same reasons, we chose to only to an in-depth research on three markets. All these markets require a secure authentication and identification means and therefore they could prove to be an opportunity for MNOs. Smart Card Alliance (2015) defines major industries in which authentication and identification is needed:

- Enterprise ID
- Financial
- Government
- Healthcare
- Online identity
- Telecommunications
- Transportation

The market of enterprise ID consists of organizations of all sizes and all industries who want to identify and authenticate users of their networked systems (Smart Card Alliance, 2015). These systems vary from physical access to a company's office to access to the intranet. As companies have resources and information that should only be accessed by authorized persons, security is important. Nowadays, smart cards and passwords are often used to authenticate users at enterprises (Smart Card Alliance, 2015). This means that it could prove to be an interesting market for MNOs to target with SIM authentication.

The financial market is a big user of smart cards in the form of payment cards (M'Chirgui, 2005; Smart Card Alliance, 2015). Banks and credit card companies supply users with debit and credit cards. Smart cards provide a secure way to pay. Furthermore, authentication is needed in this market when accessing an online bank account or when conducting a transaction. For this market several initiatives have been deployed in which the SIM is used to store the payment application(Dahlberg et al., 2008).

Governments are other interesting markets that require secure authentication and identification. Governments supply their citizens with passports, driver licenses, ID cards but also DigiD (online authentication in the Netherlands for government services). For these services it is important that the user can identify himself and is who he claims to be. The mobile phone and the SIM have the capability to securely bring all these services to the handset and therefore it is an interesting market to MNOs.

The fourth market that is identified is the healthcare sector. According to Smart Card Alliance (2015) in the healthcare sector smart cards are implemented to support a wide variety of features and applications such as portable medical records, secure access to medical information or physical access to buildings. All the medical records are confidential and privacy related and therefore the infrastructure for healthcare identity management requires a secure authentication mechanism whether that interaction is in person or over the internet (Smart Card Alliance, 2015).

Another market that requires authentication is the online identity market. Examples of places where online authentication is needed are websites such as Facebook or web shops as Amazon. Online authentication for services that fall under government, finance or enterprise ID do not fall within this market as they require a different level of security. This market consists of websites that use a single

step authentication method such as passwords. Examples of such websites are social media as Facebook or LinkedIn.

The telecommunication market is one of the biggest users of smart cards as the SIM is widely used across the industry. The SIM is used to authenticate mobile handsets to the network. As this research focuses on new sources of revenue for MNOs by making use of the SIM, the telecommunications market is not taken into account as a new application market. It is a market in which MNOs and the SIM are already well represented.

Transportation is the final market that is discussed. In the transportation market smart cards are widely used in the form of transit fare payment but also for parking fee payment. Examples are the Oyster card in London and the OV chipkaart in the Netherlands. The transportation market is thus not limited to public transport alone but can also be used for services such as parking and toll. In Dubai there have already been initiatives where the mobile phone is used for authentication and identification in the transportation market (Basu, 2013).

Appendix D – Conceptualization SE value networks

This chapter is related to the conceptualization of the existing value networks. In chapter 5, three value networks have been conceptualized and named after the SE:

- Value network SIM SE
- Value network embedded SE
- Value network cloud-based solution

In this appendix an overview is presented of the resource ownership related to the technical infrastructures that have been discussed in chapter 5. Furthermore, the processes related to mobile payments are schematically depicted and explained per value network. First, the SIM SE is discussed. Second, the embedded SE value network related to Apple pay infrastructure is presented. Finally, the process and resources related to a cloud-based solution are discussed.

SIM SE

In the technical infrastructure multiple resources that contribute to the service have been identified. In Table 1 an overview of the resources and the actors that control them is given. It shows that the MNO and the SP control multiple assets within this infrastructure. The MNO issues the SE and is therefore a tier 1 player in this value network. The SP also plays a key role as they offer the application service to the end user. In order to provision the application on the handset the MNO and SP both have a TSM. The owner of the wallet is often a MNO or SP. The MNO and SP thus control the major resources in this infrastructure. Other parties help to enable the service and have a less dominant role. The OS provider provides the interface to access the mobile wallet. The contact point is controlled by the merchant or SP (depends on the service application) and provides access to the service network.

Resource	Owner/control/issuer
SE	MNO
Mobile wallet	MNO/SP
SEI TSM	MNO
SP TSM	SP
Service application	SP
Contact point	Merchant/SP
Handset (specifications)	Handset manufacturer
Handset (ownership)	User
OS	OS provider

Table 1: Resources and actors MNO value network

Processes

In order for the service to be up and running a number of processes need to be completed. The processes are distinguished in two categories: provisioning and use of service. Based on the process display the key resources related to authentication and identification are determined. The resources used during the provisioning are mostly controlled by the MNO and SP (e.g. SIM and TSM). In brief, the provisioning is as follows. The user has to acquire a handset in which he installs the SIM with SE to connect to the MNO network. Next, the user has to install a mobile wallet and register at the SP to sign up for the service, after which the service application installed on the SE. The SP TSM can then personalize and manage the application on the SE by communicating with MNO TSM.

For the use of service the SP plays a dominant role as they offer the service to the user. To use the service, the user must take his handset and open the mobile wallet to access the service application. Next, the transaction is initiated at the point of interaction and the user needs to unlock his

credentials (e.g. by making use of a pin) stored on the SE application to give his approval. Finally, the transaction is verified and authorized at the SP systems through the service network. The processes and related resources show that the resources owned by the MNO play a large role in the underlying service infrastructure. This shows that with the actual use of the service the MNO is less involved. A schematic overview is presented on the next pages.

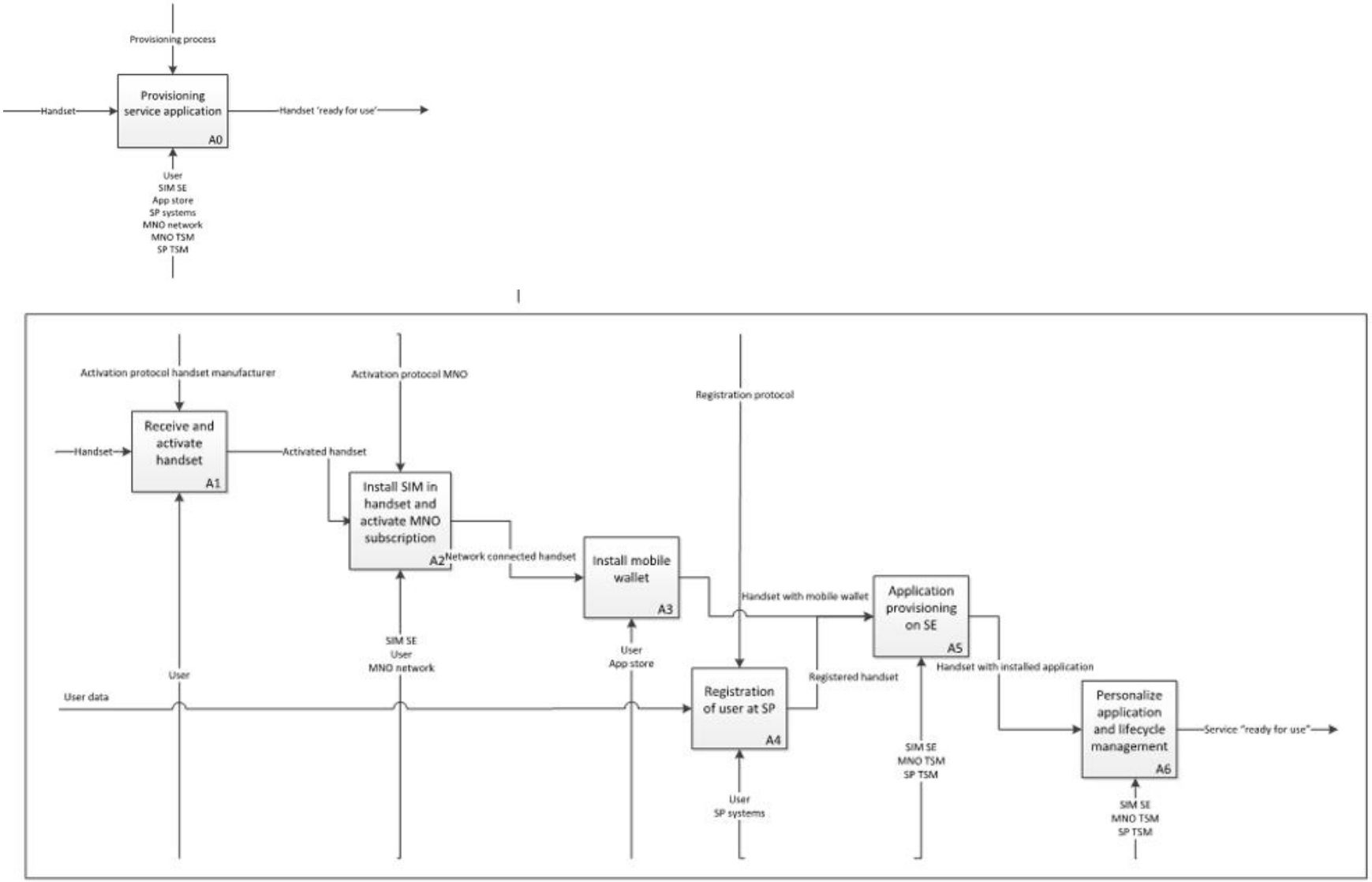


Figure 2:Provisioning process SIM SE

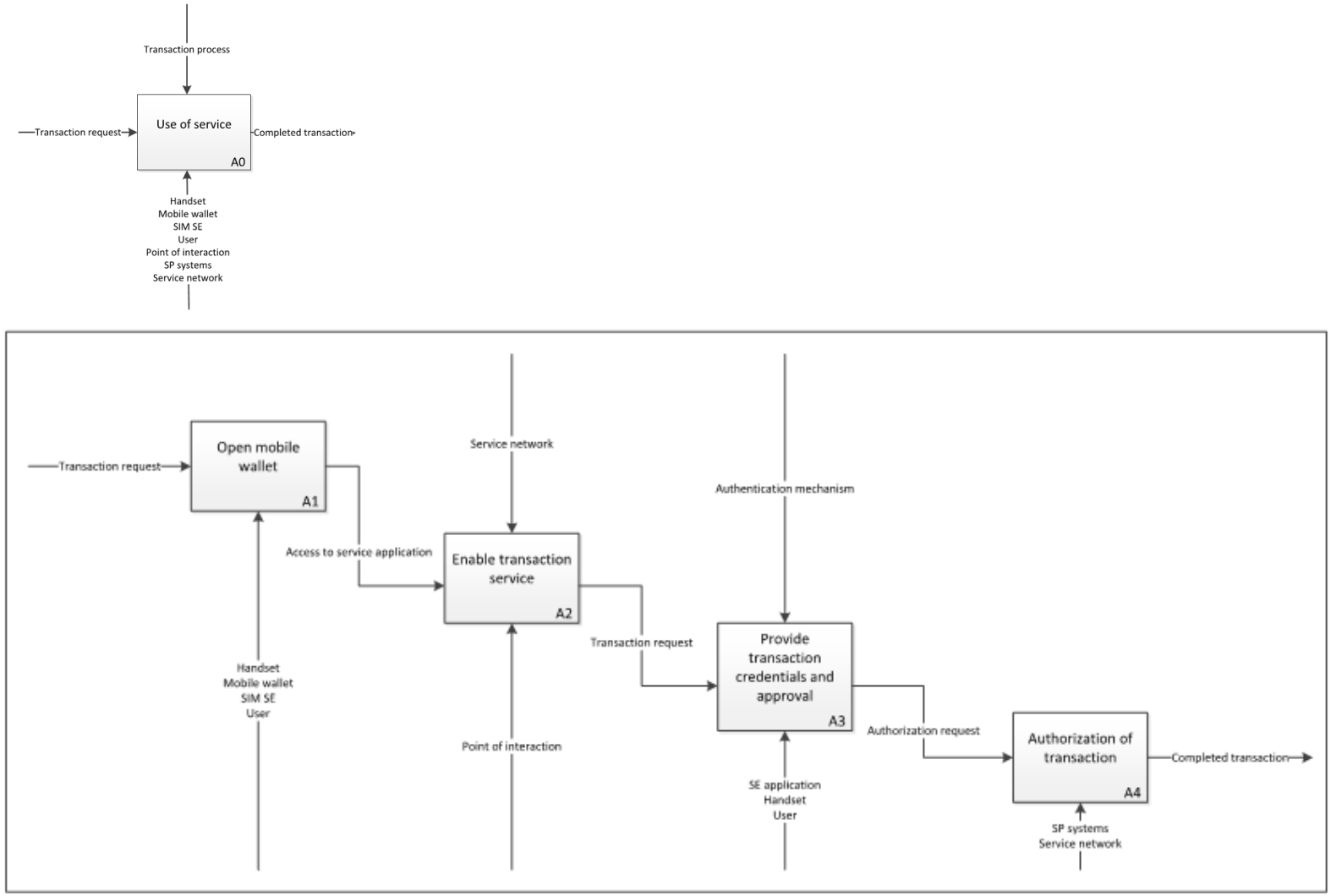


Figure 3: Use of service SIM SE

Embedded SE

Based on the technical infrastructure of the embedded SE the necessary resources have been identified. These resources are owned, controlled or used by the different actors and this shown in Table 2. By identifying the actors it becomes clear that Apple is a large player in this infrastructure, as it owns most of the resources. Apple owns the SE, passbook, a TSM and issues the handset with its own OS. Apple is clearly the focal organization within this solution. If a SP wants to offer a service on the Apple handset, it has to comply with the demands of Apple and the TSM operator. For the SP this means that it is easier to connect to the system but it reduces their potential revenue as Apple and the TSM supplier take a percentage per transaction (UL TS, 2015a).

Resource	Owner/control/issuer
SE	Apple
Mobile wallet/Passbook	Apple
Apple (SEI) TSM	Apple
TSM	TSM operator
Service application	SP
Point of interaction	Merchant/SP
Handset (specifications)	Apple
Handset (ownership)	User
OS	Apple

Table 2: Resources and actors Apple value network

Processes

Figure 4 is an overview of the provisioning process for a service stored on the embedded SE. The provisioning process is quite similar to provisioning on a SIM SE. There are, however, some changes as the different resources and actors are involved. When the user acquires the handset and activates it, the next step is that he creates a user account at Apple. This enables him to make use of passbook, Apple's mobile wallet. In order to use the service the user must register himself at the SP, after which the application is provisioned on the embedded SE by making use of Apple's TSM. Finally, the SP can personalize the application by using the TSM of the TSM operator.

The processes related to the use of the service are shown in Figure 5. It is quite similar to use of a SIM SE stored service application. The main differences are that the mobile wallet is Apple's passbook and that an embedded SE is used instead of the SIM. The process steps are the same. The user has to use his handset for the transaction by opening passbook. Next, he holds the handset at the point of interaction and unlocks the credentials, after which the underlying service network authorizes the transaction. The processes show that with an embedded SE there is no role for the MNO, as their resources are not used. In this case Apple owns most of the resources and plays a focal role.

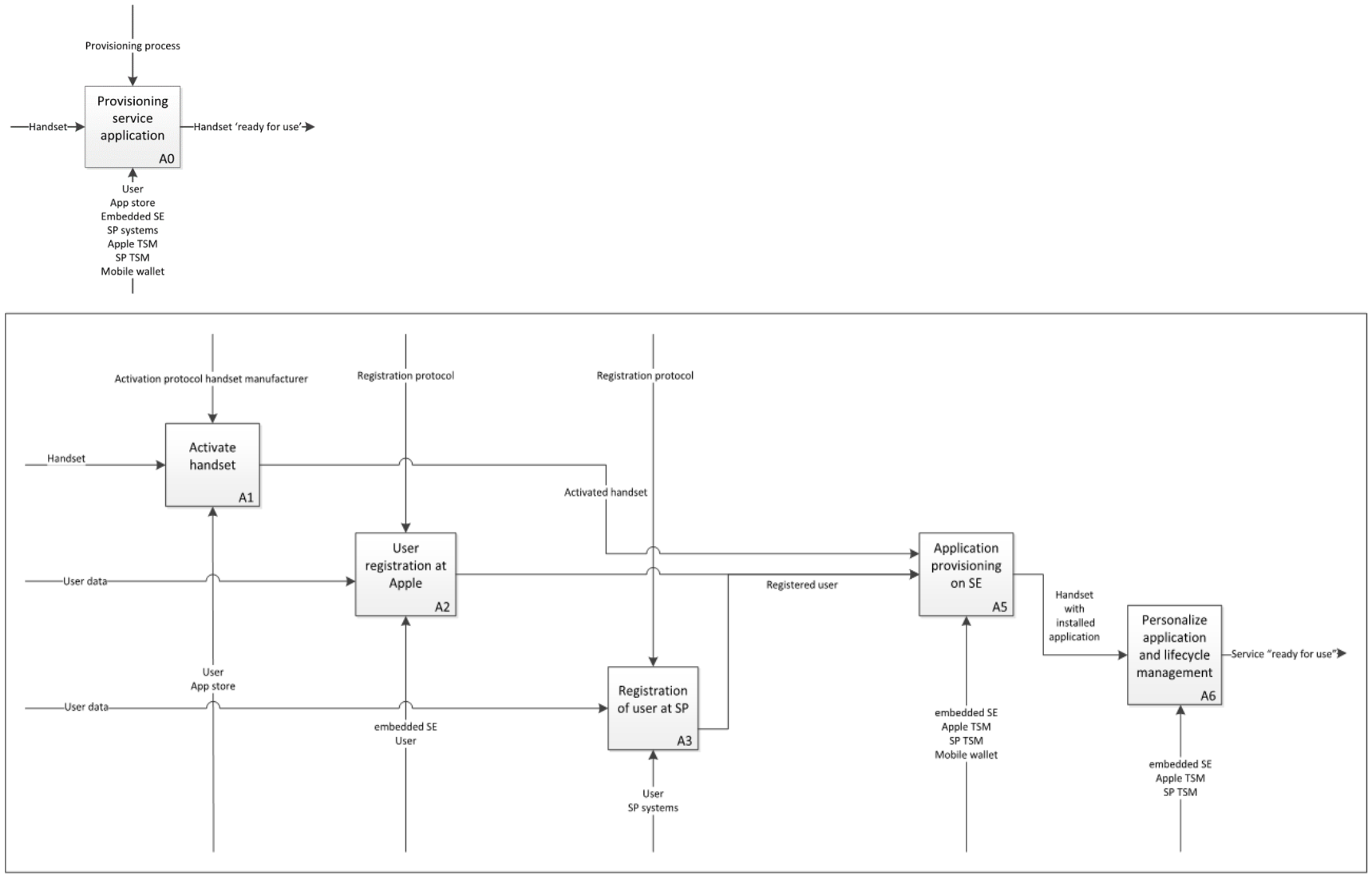


Figure 4: Provisioning process embedded SE

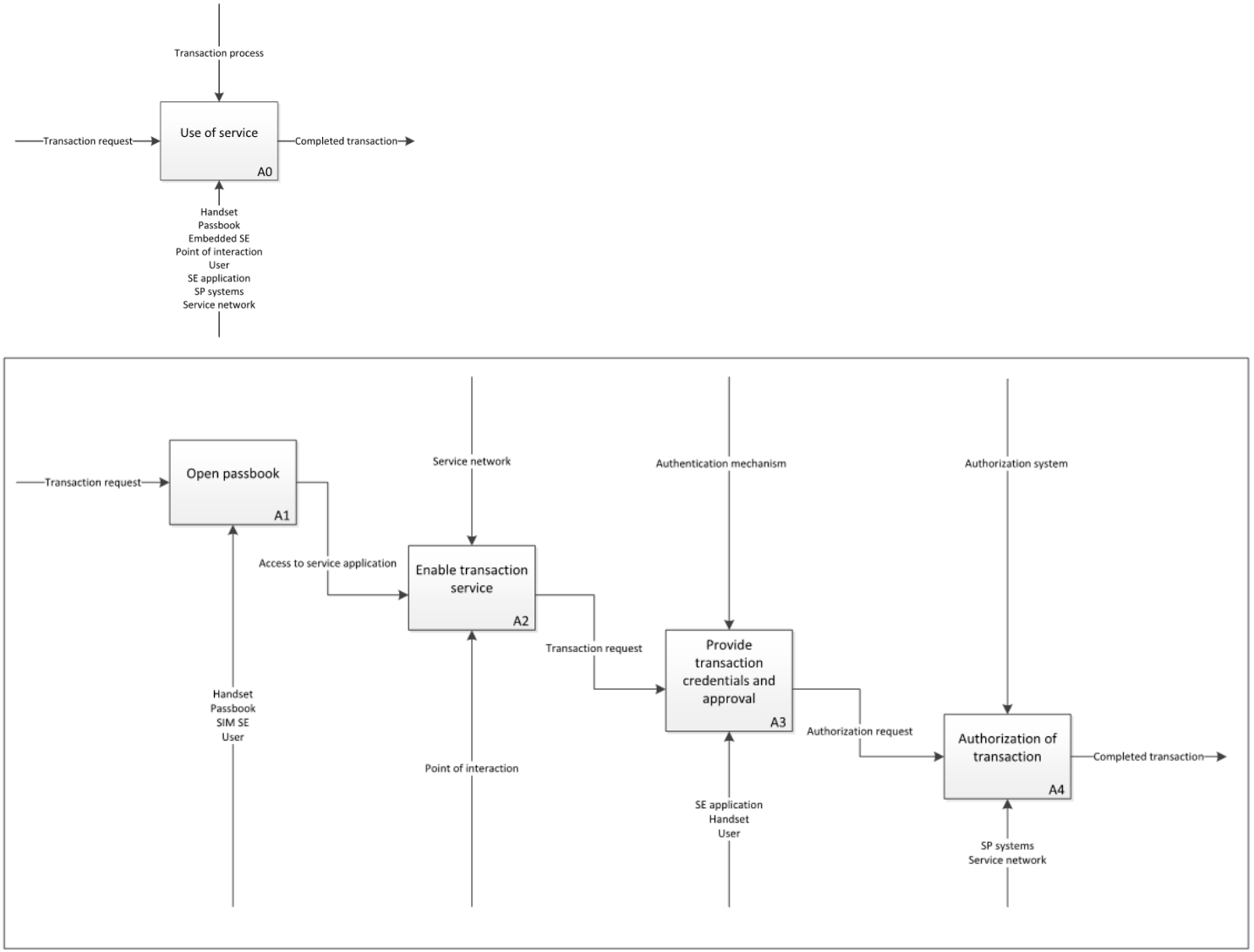


Figure 5: Use of service embedded SE

Cloud-based solution

The figures of the technical infrastructure show the resources that are used to facilitate the service. In Table 3 the actors that own, control or issue the resource are shown. The SP owns most of the resources. This technical solution is only possible when the handset makes use of the Android KitKat OS, which is offered by Google. The OS enables cloud solutions so that SPs can develop their own service on the handset. Therefore with a cloud solution the SP takes on a focal role and the SP is less dependent on other organizations.

Resource	Owner/control/issuer
Cloud	SP
Mobile wallet	SP/Third party
Service application	SP
Point of interaction	Merchant/SP
Handset (specifications)	Handset manufacturer
Handset (ownership)	User
OS	Google
Tokens	Token provider

Table 3: Resources and actors Cloud value network

Processes

The processes for a cloud solution can also be split into provisioning and use of service. For a cloud solution the provisioning process is a lot simpler than for a physical SE as the user only needs to download the application and register at the SP systems. There are no TSMs involved with the provisioning. This is because the application is stored on the OS instead of the physical SE and only an Internet connection is necessary.

The use of the service for a cloud solution consists of extra steps compared to using a physical SE. This is because the tokens or keys that enable the transaction need to be downloaded in advance before the service can be used. This process is shown in Figure 6 and the main difference with the other solutions is that the user needs to download the keys needed for the transaction in advance. Depending on the solution of the SP multiple keys that can be used for multiple transactions can be downloaded at once. However, to ensure the security the keys are valid for limited time. Besides, the need to download the transaction keys the use of service is similar to the other solutions. The user needs open the mobile wallet on his handset and download the transaction keys. Next, the user can use the handset at the point of interaction after which the transaction is authorized by making use of the SP systems.

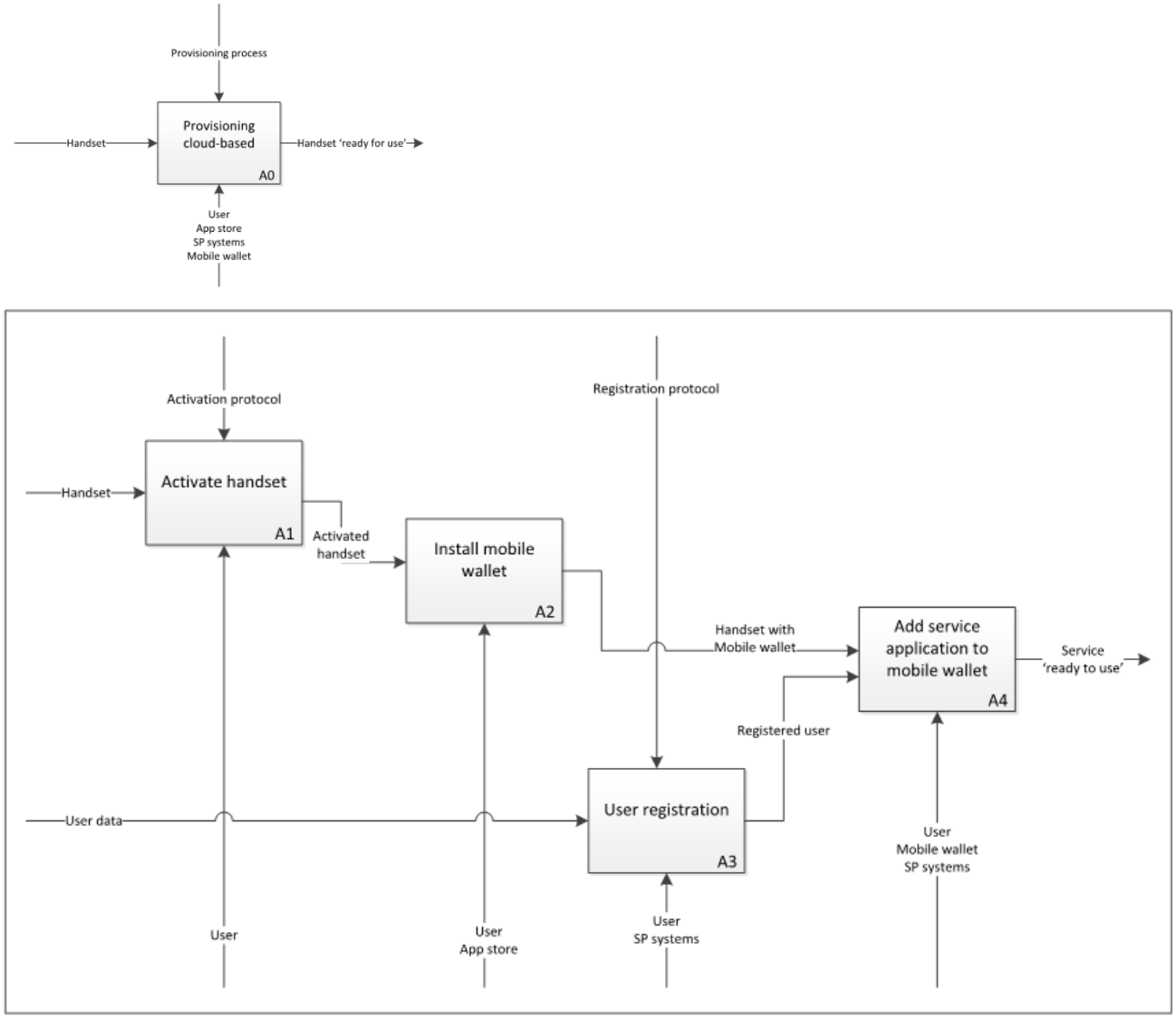


Figure 6: Provisioning process Cloud-based solution

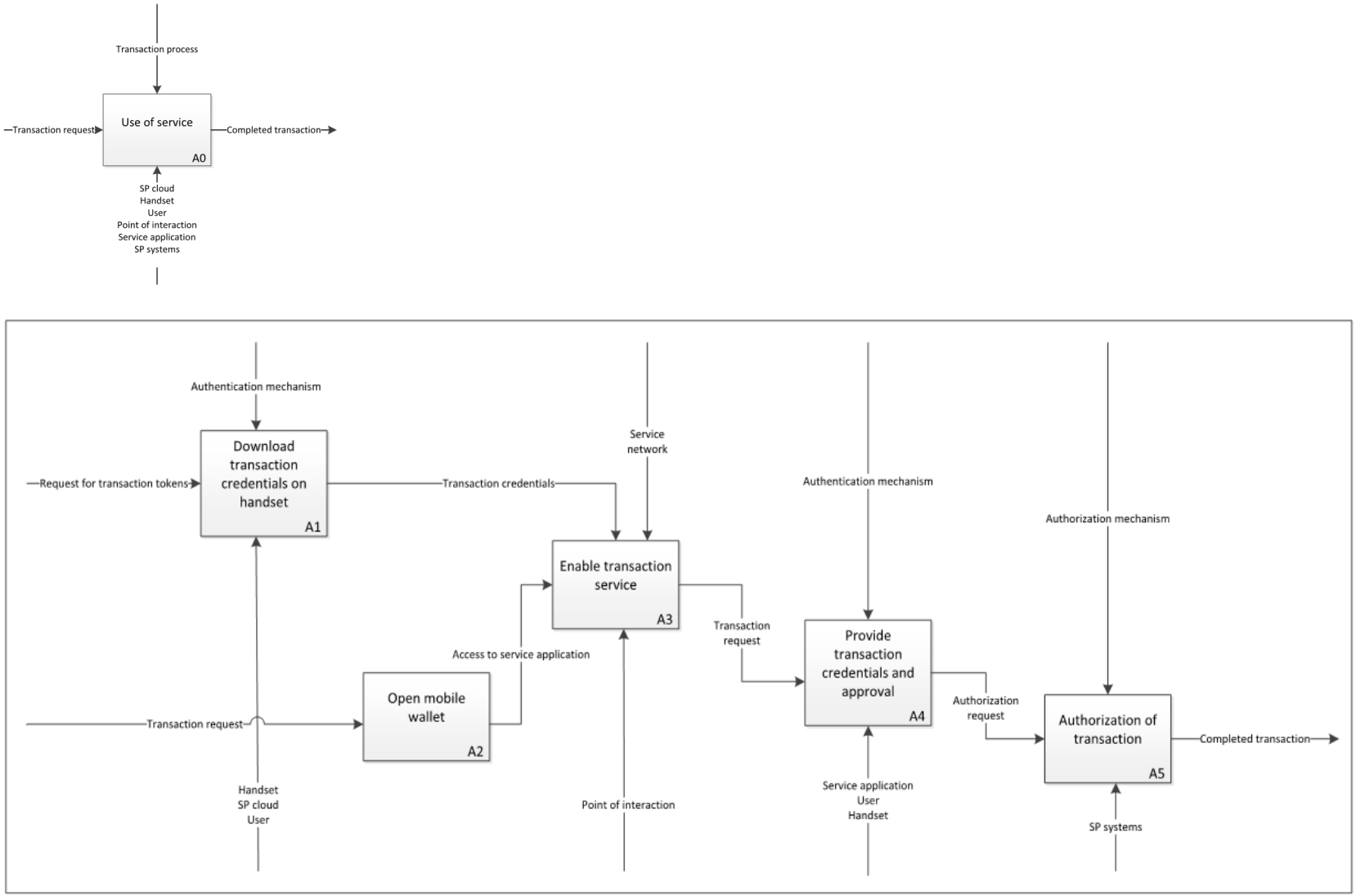


Figure 7: Use of service cloud-based solution

Appendix E - Results

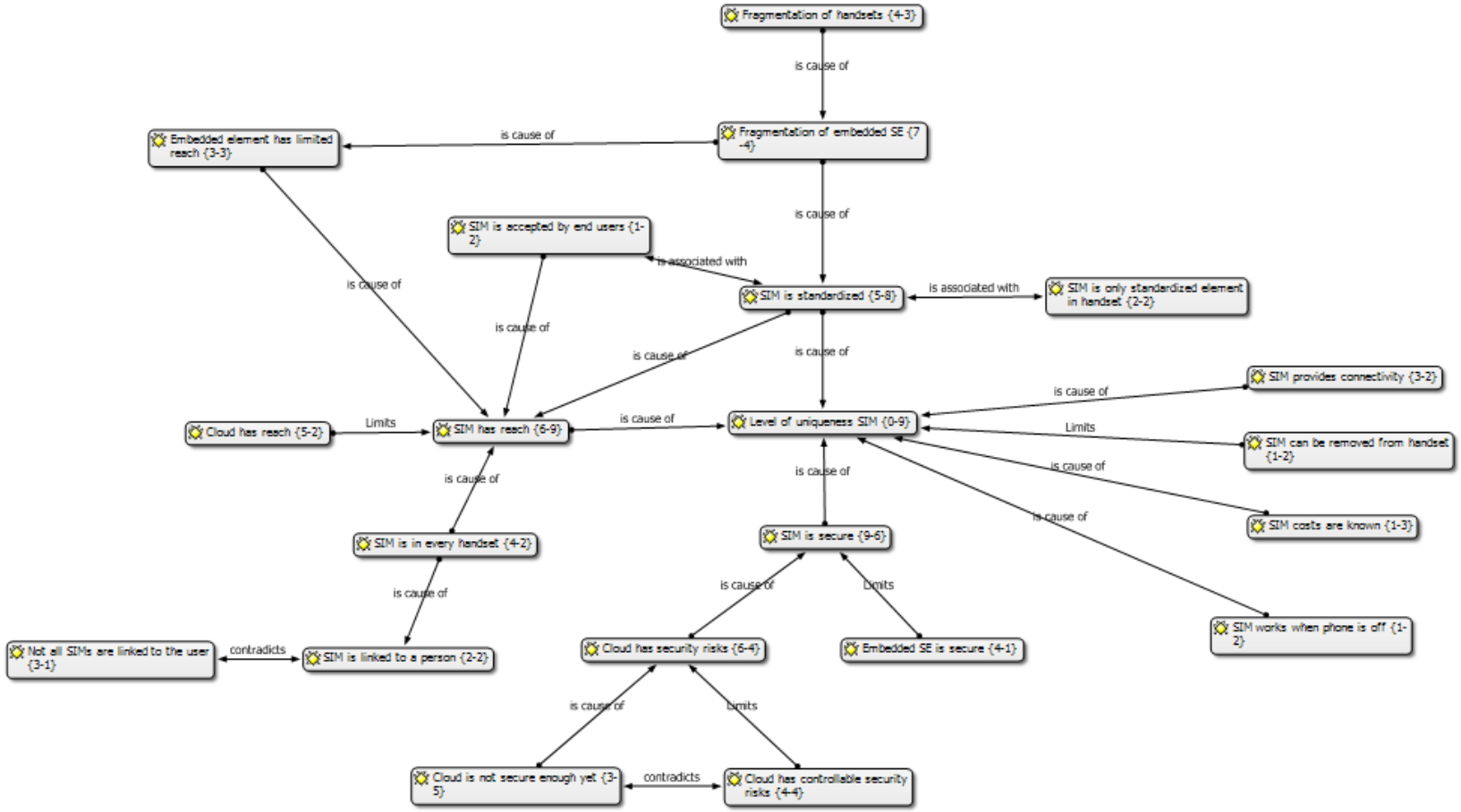
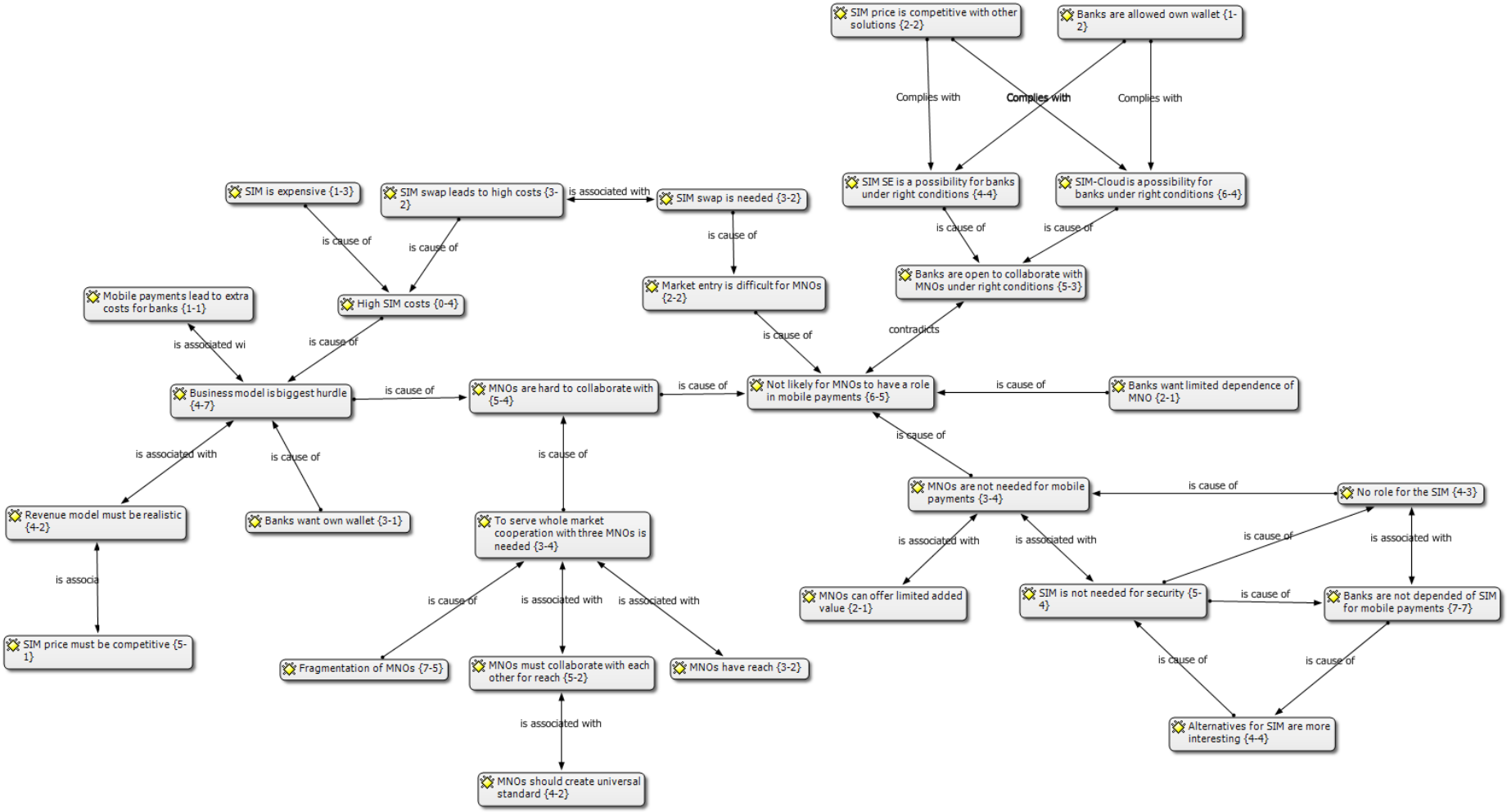


Figure 8: SIM level of uniqueness mobile payment extensive

The figure shows an overview of the factors that make the SIM unique. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. Not all codes are shown in this figure. A more extensive overview can be found in the Appendix. The relations have been drawn by the researcher and are based on analysis of the interviews and a comparison of the authentication and identification means. The figure shows that the combination of characteristics makes the SIM unique. Similar characteristics of other solutions limit the uniqueness. As the level of uniqueness represents a control point parameter it has not been assigned codes in the transcripts but is linked to codes that influence the uniqueness of the SIM



.

Figure 9: Role mobile payment MNO extensive

The figure provides an overview of the interview findings regarding the viability of the value network and the role of MNOs in mobile payments. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews.

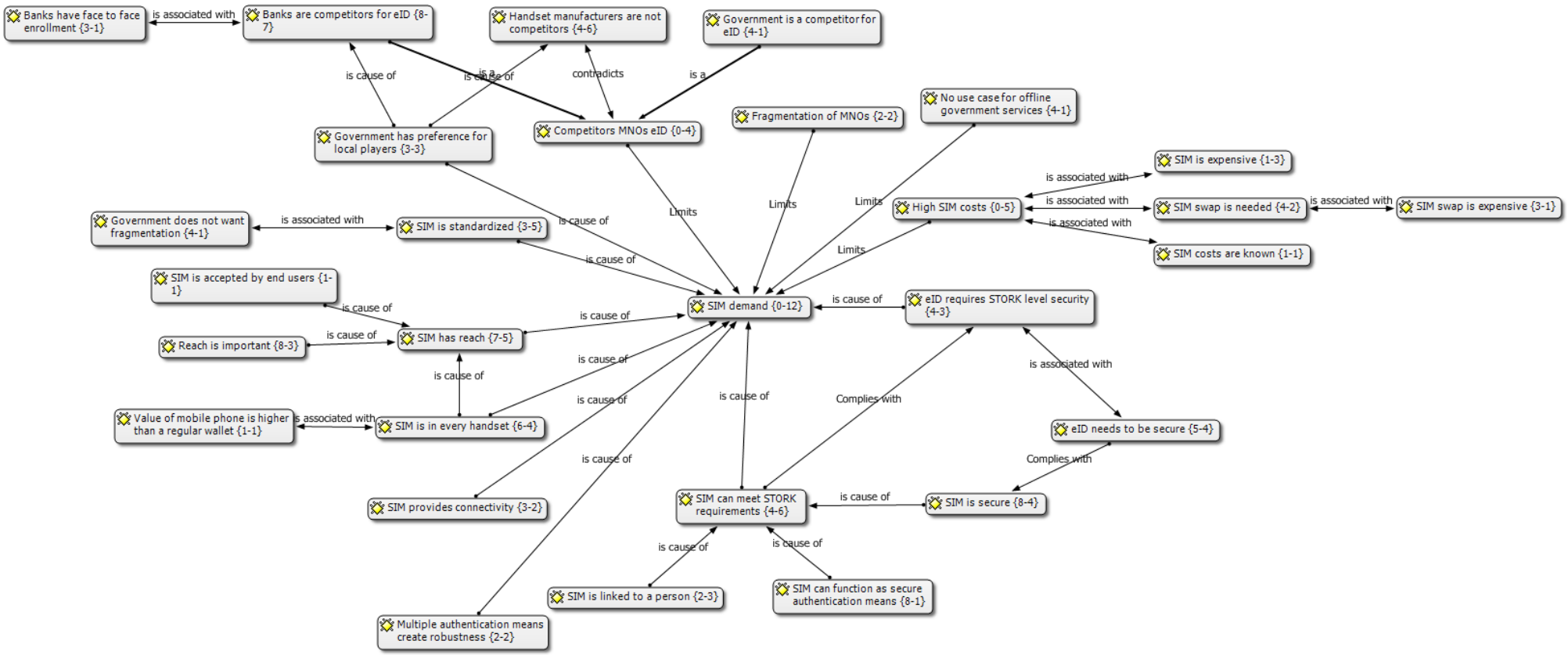


Figure 100-1: Demand SIM government services extensive

The figure provides an overview of the interview findings regarding demand of the SIM. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews. As demand is a control point parameter it has not been assigned codes in the transcripts but is linked to codes that influence the demand for the SIM.

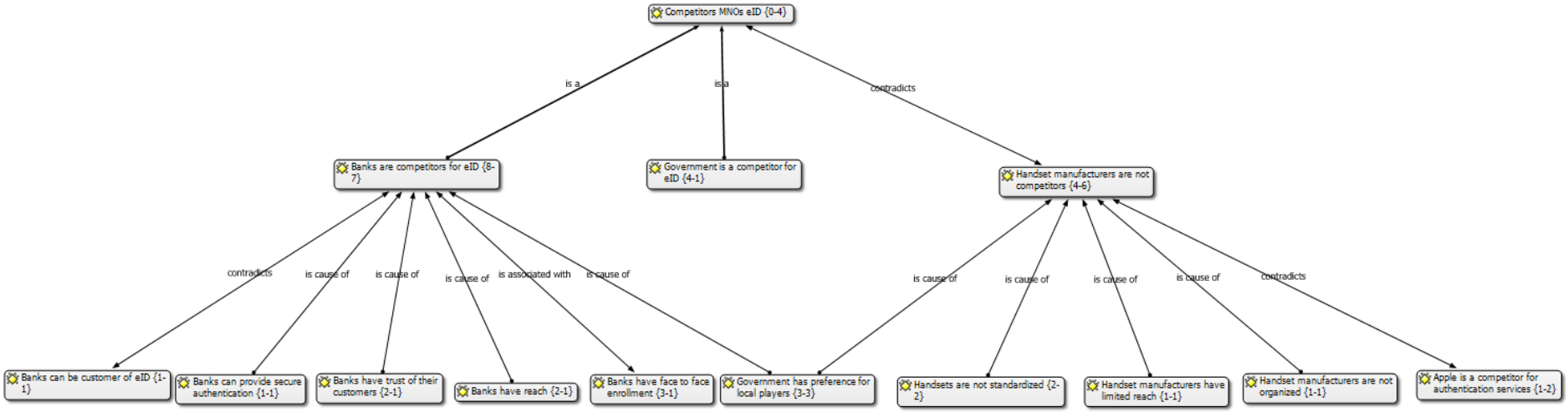


Figure 11: Competitors MNO eID scheme extensive

The figure provides an overview of the interview findings regarding the competitors of MNOs in the eID scheme. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews.

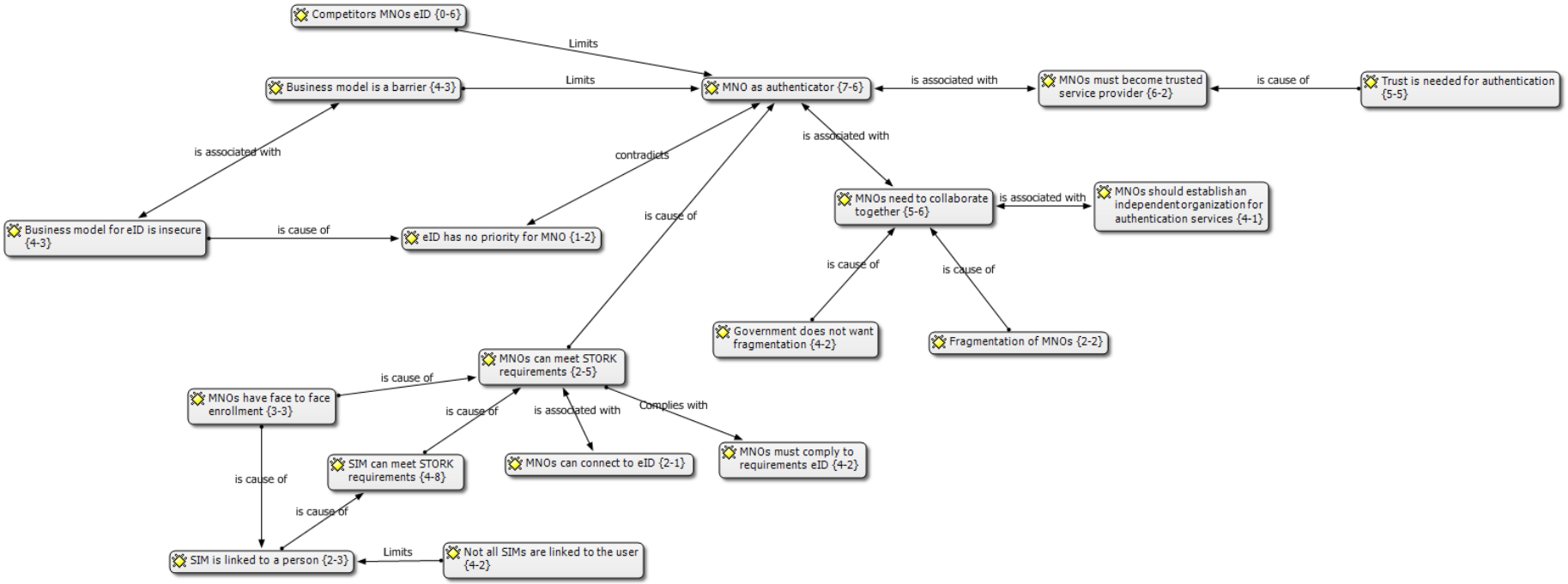


Figure 12: Role MNO eID scheme extensive

The figure provides an overview of the interview findings regarding the viability of the value network and the role of MNOs in the eID scheme. The labels represent codes that have been assigned by the researcher on the basis of the interviews. The first number within the label represents the number of codes assigned in the transcripts and the second number the links with other codes. The relations have been drawn by the researcher and are based on analysis of the interviews.