

Authentication for the eMayor platform in Dutch municipalities.

A study about authentication techniques for the services “Change of residence” and “Certificate issuance”.



Student: Birgitte E. Catijn Student number: 9156194	Internal Supervisors: Drs. J. Gortmaker Drs. W. G. van den Berg Dr.ir. M.F.W.H.A. Janssen
External Supervisor: Ir. R.L. de Gier	Professor: Prof. Dr. R.W. Wagenaar
Date: 23-11-2004 Version: 2.0 Faculty: Technology, Policy and Management Study: System Engineering, Policy Analysis and Management	

Preface

This thesis is the result of the research I have been carrying out for my graduation project at the University of Technology Delft, faculty of Technology, Policy and Management. For this research I have done an internship at Deloitte Management and ICT Consultants BV, in Amstelveen.

I would like to thank the following people for their advise and feedback: Jeffrey Gortmaker, Wander van den Berg, Marijn Janssen and Rene Wagenaar of TPM; Rene de Gier, my external supervisor at Deloitte, Piet Timmermans, Pim Hengeveld and of course all other colleagues from Deloitte who I could always ask for advise. I would also like to thank everyone I have interviewed. They provided me with information needed for this thesis. Furthermore, I am very grateful for the opportunity my parents gave me to accomplish this degree and not in the least for all their advise and help.

Amstelveen, 23-11-2004
Birgitte Catijn

Summary

eGovernment concerns providing or attainment of information, services or products through electronic means, by and from governmental organisations, at any given moment and place, by offering an extra value for all participating parties (Zweers, 2002). eGovernment offers many advantages for both governments and citizens like: increased efficiency, financial advantages, economic development, stimulation of democracy (because the government becomes more transparent), and better service providing (Bruïne, 2002 and GSA.gov).

Because of these advantages, the national government of the Netherlands set a target of 65%, for services to be online in 2007 (minbzk.nl 01). However, research by overheid.nl shows that this is only 15% at the moment.

eMayor is an European initiative to establish a secure, open, interoperable and cost-effective eGovernment platform for secure communication between small- and medium-sized governmental organisations in Europe. Two services that have been selected in the eMayor project are¹:

1. Certification of residence status. A citizen can request several certificates from a municipality. In eMayor is chosen for certification of residence status, but in this thesis the certification issuance will be used more generally, namely all certificates Gemeentelijke Basis Administratie and Burgerlijke Stand. Examples are certificate of birth, death, residence status, and marriage. It is chosen to do this more in general because the processes are similar and the field of application is larger.
2. Change of residence. Change of residence is concerned with people moving within, into and out of municipalities.

To facilitate online services, authentication is needed. Authentication is defined as: The assurance that the communicating entity is the one that it claims to be (Stallings, 2003). Authentication is needed to know who is requesting a service. This is necessary because the information involved is personal. Furthermore, authentication prevents fraud.

The eMayor platform does not prescribe an authentication technique, although it suggests the use of smart cards. However, the platform will be suitable for the use of passwords, smart card and digital signatures.

The research question of this thesis is formulated as follows:

What is an appropriate way for municipalities to implement authentication for the eGovernment services 'Certificate issuance' and 'Change of residence', while compatible with eMayor?

Appropriate authentication refers to authentication at the right level of security for a service.

In the Netherlands, the tendency is towards using different authentication techniques for different security levels. Some services need a higher level of security and can not be offered at a lower level of security.

An example of a service that requires a high level of security is the issuance of a new passport.

Many services do not require a high level of security. For these services a high level of security would be unnecessarily expensive and complicated. Although there are more important criteria to choose an authentication technique, costs are very important because the funds municipalities have for new initiatives is small.

¹ Actually there is a third service: tax service. This service is not applicable in the Netherlands as the Dutch tax system is organised centrally.

The certification service can be offered online with the use of password authentication. Change of residence is more complicated since Dutch law requires a signature on the service request. Change of residence causes some difficulties for the implementation of authentication in a suitable way. Dutch law (4:1 Awb and articles 65, 66, 68, 80, 81GBA) requires a (hand-written) signature for this service. As long as this law applies, password authentication is not allowed. May 8th 2003 a law is enacted on digital signatures (Wet Elektronische Handtekeningen). This law states that, under certain conditions, a digital signature can substitute the hand-written signature. These requirements determine that a smart card is needed for the secure creation of the key.

However, a centrally organised, nation wide used smart card is not yet available until 2006. Therefore it is difficult to offer the service “change of residence” online within the current legal context. In the near future (end of 2006) it will be possible. However, eMayor will not be available before February 2006 anyway, which makes the gap only a couple of months.

The main research question therefore can be answered as follows:

The most appropriate authentication technique for “Certificate issuance” is a “password and user name” combination. Change of residence can not be offered within the current legal context at the moment but will be in the near future. To comply to current law, the appropriate authentication technique is the use of digital signatures stored on a smart card.

Table of Contents

PREFACE.....	2
SUMMARY	3
1. INTRODUCTION.....	7
2. RESEARCH CONTEXT AND PROBLEM	9
2.1 GENERAL DESCRIPTION OF THE eMAYOR PROJECT.....	9
2.2 DUTCH SITUATION: CONTEXT OF THE RESEARCH AND PROBLEM DEFINITION.....	12
2.3 AIM OF THE RESEARCH & RESEARCH QUESTIONS.....	13
2.4 DELINEATION OF THE PROBLEM	15
2.5 RESEARCH STRATEGY, METHODS AND TECHNIQUES	15
2.5.1 <i>Current situation</i>	15
2.5.2 <i>Authentication techniques, (dis)advantages and initiatives</i>	16
2.5.3 <i>Authentication selection criteria</i>	16
2.6 STRUCTURE OF THE RESEARCH AND PLANNING	16
3. CURRENT SITUATION AND DESIGN OF NEW PROCESSES.....	18
3.1 SERVICES	18
3.1.1 <i>Certification service</i>	18
3.1.2 <i>Change of residence status</i>	21
3.2 TECHNICAL SYSTEMS	22
3.3 DESIGN OF THE EXPECTED ONLINE SITUATION: ONLINE OPPORTUNITIES AND CURRENT SERVICES' BOTTLENECKS	23
3.4 CONCLUSION ON RESEARCH QUESTION 1.....	25
4. AUTHENTICATION TECHNIQUES.....	27
4.1 WHAT IS AUTHENTICATION?	27
4.2 TECHNIQUES, ADVANTAGES AND DISADVANTAGES	28
4.2.1 <i>Password and PIN</i>	29
4.2.2 <i>(Smart) cards and digital signatures</i>	31
4.2.3 <i>Biometrics</i>	36
4.3 CONCLUSION ON RESEARCH QUESTION 2 AND 3	38
5. AUTHENTICATION INITIATIVES	41
5.1 DUTCH INITIATIVES.....	41
5.2 CONCLUSION ON RESEARCH QUESTION 4, 5 & 6	44
6. SELECTION OF AUTHENTICATION TECHNIQUES	46
6.1 SELECTION CRITERIA.....	46
6.2 LEVEL OF SECURITY & LEGAL IMPLICATIONS	47
6.3 DESIGN OF THE SELECTION FRAMEWORK	49
6.4 SELECTION OF AUTHENTICATION TECHNIQUE IN DUTCH SITUATION FOR TWO eMAYOR SERVICES	51
6.4.1 <i>Alternatives that will not be considered</i>	51
6.4.2 <i>Values in the framework</i>	52
6.4.3 <i>Results</i>	53
6.5 REFLECTION ON THE SELECTION FRAMEWORK	54
6.6 CONCLUSION ON RESEARCH QUESTIONS 7 & 8	54
7. CONCLUSIONS & RECOMMENDATIONS	58
7.1 CONCLUSIONS	58
7.2 RECOMMENDATIONS	60
DEFINITION OF CONCEPTS	62

LIST OF FREQUENTLY USED ABBREVIATIONS	65
APPENDIX 1: INTERVIEWEES	66
APPENDIX 2: GBA CERTIFICATES	67
APPENDIX 3: BIRTH CERTIFICATE FRONT SIDE	69
APPENDIX 4: BIRTH CERTIFICATE BACK SIDE.....	70
APPENDIX 5: COPY OF PAPER USED FOR CERTIFICATES.....	71
APPENDIX 6: SYMBOLS ACTIVITY DIAGRAM & DESCRIPTION.....	72
APPENDIX 7: CERTIFICATE BS PROCESS.....	73
APPENDIX 8: CERTIFICATE GBA	76
APPENDIX 9: CHANGE OF RESIDENCE STATUS	80
APPENDIX 10: CERTIFICATE BS ONLINE.....	84
APPENDIX 11: CERTIFICATE GBA ONLINE.....	85
APPENDIX 12: CHANGE OF RESIDENCE STATUS ONLINE	87
APPENDIX 13: SELECTION FRAMEWORK FILLED OUT BY EXPERTS.....	89
LITERATURE	95
BOOKS	95
INTERNET SITES.....	95
REPORTS	98
PUBLICATIONS	98

1. Introduction

The following was found in the news on Monday October 4th (rtl.nl): One third of all passport fraud of people trying to cross the border is caused by people using the passport of someone else.

Clearly, it is difficult to be sure that the person is the one in the picture. Imagine that you have to show who you are while working on a computer.

This could happen when you want to use an online municipal service. About this topic, online authentication of users for municipal web services, this final thesis will be.

The national government in the Netherlands has noticed the need for online services for citizens.

Therefore the Dutch government set the target of 65% of all services to be online in 2007 (minbzk.nl 01).

Also municipalities considered the importance of these online services and started some initiatives to offer their services online.

eGovernment concerns providing or attainment of information, services or products through electronic means, by and from governmental organisations, at any given moment and place, by offering an extra value for all participating parties (Zweers, 2002). eGovernment has a couple of advantages for municipalities and citizens: increased efficiency, financial advantages, economic development, stimulation of democracy (because the government becomes more transparent), and better service providing (Bruïne, 2002 and GSA.gov).

eMayor is an European initiative to establish a secure, open, interoperable and cost-effective eGovernment platform for secure communication between municipalities in Europe. It is partly funded under the Sixth Framework programme from the European Commission. This project focuses on two services: "Certificate issuance" and "Change of residence". Certificate issuance is concerned with the request and processing of a certificate. In the Netherlands, many certificates are available. Examples are a birth certificate or a certificate of residence status. Change of residence is concerned with the change of the home address of a citizen within, into or out of a municipality.

To make use of governmental services online, authentication is necessary. Authentication is the assurance that a person is who he claims to be. This is important because the information involved is personal which makes reading or other misuse of this information by others undesirable.

However, unlike in some other European countries there is no good nationwide used authentication technique in the Netherlands. Authentication is necessary for offering the services online and for the protection of the (personal) information of citizens. This thesis aims to answer the following research question:

What is an appropriate way for municipalities to implement authentication for the eGovernment services 'Certificate issuance' and 'Change of residence', while compatible with eMayor?

To answer this question several steps have to be taken. Firstly the two eMayor services are described for the Dutch situation. The Unified Modelling Language (UML) is used to model these services. Next, Authentication is defined and different techniques are elaborated on. Several authentication initiatives in the Netherlands are described and their applicability is considered. A framework is presented for the selection of authentication methods. Finally an answer will be given to the main research question and its sub-questions.

This thesis consists of the following parts:

Firstly, a description of the eMayor project is given in chapter 2. The participants of the eMayor consortium, the aim of the eMayor project and the advantages of eGovernment services will be described.

This chapter also includes the relevance and aim of the research, the research questions and the delineation. It results in the formulation of the aim of the research and the research questions. Chapter 3 contains the description of the services “Change of residence status” and “Certificate issuance”. The technical systems used for these services are described. Then, the main topic “Authentication” is elaborated on (chapter 4). This will contain the different techniques and their advantages. Dutch initiatives are listed in chapter 5. Next, selection criteria for the selection of authentication techniques are outlined. This resulted in a framework for the selection of an authentication technique (chapter 6). This resulted in the conclusions and recommendations stated in chapter 7.

2. Research context and Problem

In this chapter a short introduction will be given to the eMayor project to understand the background and context of this thesis. In the next sections the problem definition is given, the aim and final result of the research are defined. Also the research questions, the delineation of the problem and the research strategy and methods are described.

2.1 General description of the eMayor project

The eMayor project is an international project with participants in several European countries. These countries are: Belgium, Germany, Greece, Italy, Spain, Switzerland and The Netherlands. The project started in January 2004 and will end in February 2006. It is partly funded under the Sixth Framework programme from the European Commission. The **aim of eMayor** is to develop an open, secure, interoperable and cost-effective eGovernment platform for small and medium sized municipalities.

Platform

Municipalities offer services online. The citizen or companies can get information, contact the civil servants and make use of the services municipalities offer (e.g. requesting a birth certificate), anywhere they have access to a computer with an internet connection.

Furthermore, municipalities communicate with each other, for example to exchange address information of citizens.

A secure communication network is needed to host these communications. The security aspect is very important because of the nature of the information. This is confidential information of citizens. eMayor makes a secure communication amongst the municipalities and between the municipality and the user possible.

Also very important is that the municipalities make agreements with each other about the format of the documents and the security measures. They need to trust documents and the way information will be handled (e.g. privacy policy). This is a requirement for the success of the eMayor platform.

The platform will have three types of interfaces:

1. Interface with the user. The user can view and insert information. A “user” can be a citizen or a civil servant. The citizen might be using a municipal service online, e.g. requesting a birth certificate. The civil servant is using the system because of his profession, he might be assessing the citizen’s request.
2. Interfaces with the different municipalities, this is necessary for the communication between municipalities.
3. Interface with the municipal (legacy) systems (the systems that are currently in use by the municipalities). The services are not implemented in the platform, which avoids that the whole platform needs to be redesigned whenever a municipality want to change something in the service. Furthermore municipalities have different policies and techniques. It would be difficult to redesign the service in such a way that all participants are satisfied. In between the platform and the municipal systems will be a compatibility layer. This layer makes communication between the platform and the municipal legacy system possible.

The eMayor platform can be represented by the following simplified figure (2.1). The platform has interfaces with the other eMayor municipalities, with the municipal (legacy) systems, and with the users. A user can be a civil servant and/or a citizen. In this thesis only authentication of users is considered.

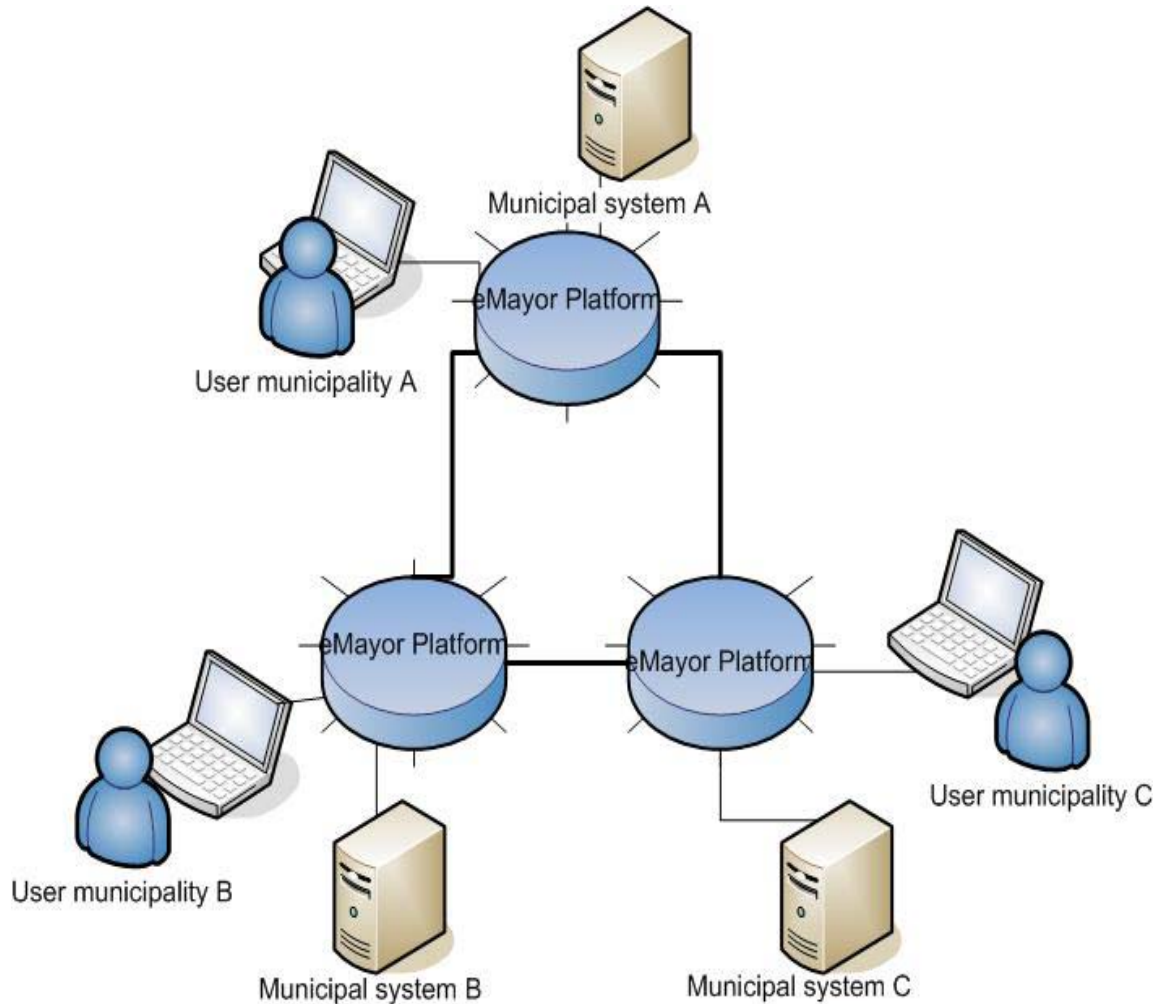


Figure 2.1 Three different types of interfaces in the eMayor platform

The platform also contains several security protocols for secure transport of information. These protocols will not be elaborated on as they are out of scope (see paragraph 3.3 “Delineation of the problem”, which shows that only authentication is within the scope of this research).

The platform offers the combination of the protocols and software that make a secure communication possible. The platform itself will not include any services, it will only make it possible to communicate with them. So, when “services” are mentioned in this thesis, this refers to the municipal services, which are hosted by the municipalities on their legacy systems.

Participants

To realise the eMayor platform, a diverse combination of parties are involved: municipal governments, universities and (commercial) companies. The next table contains all the project participants.

Participant name	Country
Deloitte	The Netherlands
Advanced Encryption Technology Europe B.V.	The Netherlands
Expertnet S.A.	Greece
Fraunhofer Institute for open communication systems	Germany
SADESI	Spain
Ubizen N.V.	Belgium
University of Siegen, Institute of Data Communication Systems	Germany
University of Piraeus Research Centre	Greece
University of Zurich	Switzerland
Municipality of Aachen	Germany
Municipality of Bolzano	Italy
Municipality of Seville	Spain
Municipality of Siena	Italy
Psychiko Municipal Development Corporation	Greece

Table 2.1 eMayor participants

eGovernment

eGovernment concerns providing or attainment of information, services or products through electronic means, by and from governmental organisations, at any given moment and place, by offering an extra value for all participating parties (Zweers, 2002).

A study by the Intergovernmental Advisory Board of the American General Services Administration (GSA) pointed five advantages of eGovernment out as general advantages, suitable for many countries. Although it is an American survey, their research focussed on many countries in the world, comparing them and concluding with general advantages. The GSA mentions that there are more advantages, depending on the place where eGovernment is applied. These five advantages are common in all countries they researched (burger.overheid.nl and GSA.gov) :

1. *Increase efficiency*: eGovernment consolidates and integrates systems. Because of the reduced redundancy the systems become more efficient. Also, eGovernment services reduce the administrative burden, which increases efficiency (Bruïne, 2002).
2. *Financial advantages*. The reason for this advantage is the reduced costs of government operations. By Web-enabling their customer service processes, municipalities can reduce the amount of paperwork and reduce staff needed for the face-to-face servicing of the citizens in the town hall, which results in financial benefits.
3. *Economic development*. “Developing countries and state and local governments view the Internet as critical to developing their regional economies, chiefly by enhancing tourism and by making it easy and convenient for businesses to find information they need and file required reports online (GSA.gov)”. Furthermore eGovernment stimulates mobility of citizens and companies.
4. *Fostering democratic principles*. “The free flow of information permitted by the Internet facilitates transparency and accountability in government. It also increases the accessibility of government at all levels (GSA.gov)”. Furthermore, information and communication technologies offer many possibilities to enhance the participation of citizens in the various democratic processes, e.g. e-voting (Bruïne, 2002).
5. eGovernment *improves the government’s service* to citizens and companies. This is because eGovernment makes it easier, quicker for users to find information or make use of a service.

These advantages show that there are many reasons to stimulate eGovernment services. The platform aims to help the small and medium sized municipalities with this.

Services

A list of potentially interesting municipal services for eMayor has been made. This list is composed after a questionnaire has been sent out to the five participating municipalities: Siena, Aachen, Bolzano, Seville and Psychiko. By means of this questionnaire the municipalities identified relevant services. Out of these services (37), two have been selected, because these two are considered to be the most promising. Actually there is a third service: tax service. This service is not applicable in the Netherlands as the Dutch tax system is organised centrally. From now on only the two services that are relevant for the Netherlands will be mentioned.

The evaluation criteria for the selection of these eMayor services included security and trust, cross border aspects and legal feasibility in a national context. Security and trust is important because the users need to trust the system, otherwise they will not use it. The system is concerned with a lot of confidential information, so strong security measures are required. Services with a big security risk are less preferable than more secure services. However, security is an important aspect in this project and some challenge is needed. The cross border aspect is important because of the international context. Many legal differences have to be considered during the project. The differences in law in several countries, implies that the legal feasibility is also important. More legal differences are less desirable.

The two services that have been selected in the eMayor project are:

1. Change of residence. Change of residence is concerned with people moving within, into and out of municipalities.
2. Certification of residence status. A citizen can request several certificates from a municipality. In eMayor is chosen for certification of residence status, but in this thesis the certification issuance will be used more generally. Examples are certificate of birth, death, residence, and marriage. It is chosen to do this more generally because the processes are similar and the field of application is larger.

After the project is finished and exploitation has started, the platform could be extended to make the hosting of extra services available. For now, this is outside of the project scope.

Suggested authentication technique

The platform does not prescribe an authentication technique, although it suggests the use of smart cards. However, the platform includes support for the use of digital certificates and smart cards, as well as password authentication.

2.2 Dutch situation: Context of the research and Problem definition

There are 483 Dutch municipalities (CBS.nl). The Dutch government has set targets to encourage municipalities to make more services available online. The target set for 2004 is 45%, and in 2007 65% of the municipal services should be offered online (minbzk.nl 01). Some municipalities like The Hague, Tilburg and Dordrecht offer relatively many services online. Others have not developed many interactive services and have static internet sites, which enables you to read information on the site, download and print forms, or send e-mails, but do not offer the possibility to return forms online.

The findings of Dutch survey published on the internet site Overheid.nl shows that only 15% of the 2600 services offered by governments and semi-governments are offered online. This result shows that there is room for improvement of our online government.

The advantages of eGovernment mentioned in the previous paragraph can be applied to the Dutch situation for eMayor. Since the citizen has to fill in the required information himself, there will be less mistakes made by the civil servants who have to copy the written information to a digital format. The service will be more efficient, which results in money and time savings. The civil servant is more flexible

in handling the request for a service, because it does not have to be done at the moment a citizen is at the town hall. Also the municipalities aim to be more customer-oriented. A better service handling will help them achieve this goal. Furthermore, eGovernment can be a way to build an image. The citizen does not have to visit the town hall anymore, which saves time and money. They can retrieve information anywhere, any time, at least when they have access to a computer. They also have better insights in to government services, because they can easily look information up and read it on the internet site of a municipality.

The eMayor project is a European initiative. The actual platform will be implemented in five European cities, in four countries. Dutch municipalities are currently not directly involved in the project. This research will help the Dutch municipalities benefit from this project. The topic addressed will be: *Authentication*. Authentication is necessary to assure that someone is who he claims to be (Stallings, 2003). Because much information is personal it is very important that only authenticated citizens can access the information they are allowed to access or change. For this reason good authentication is required for the municipalities to be able to offer eGovernment services.

Relevance of the research is that eGovernment provides a higher efficiency, financial advantages, economic development, stimulated democracy and provides a better service to users. For most services that are offered online, authentication is required. However, it is not clear which authentication technique is most suitable for Dutch municipalities that want to offer the two eMayor services “Certificate issuance” and “Change of residence status”. Because the information is confidential, good security measures are needed. The municipality needs to be assured that the person working on the computer is the person he claims to be. The **problem definition** can be stated as follows:

It is not evident which authentication technique is most suitable for offering the two eMayor services online in the Netherlands.

The **problem owner** in the research are the municipalities. The Netherlands offer a relatively low number of online services (wmrc.com and overhead.nl). eMayor is an attractive solution to implement an eGovernment environment. To be able to offer services online, it is required that the identity of the user is assured. This is not just an eMayor problem, also other ways in which services are offered online need a good authentication techniques. This means that if municipalities want to offer these services online (Certificate BS, GBA and Change of residence status), they need to implement an authentication technique.

2.3 Aim of the research & Research questions

The Dutch municipalities can benefit from the eMayor platform. The online services need to be secured with an adequate authentication system.

The **aim of this research** is:

Finding an appropriate way in which Dutch municipalities can implement authentication of citizens for the eGovernment services ‘Certificate issuance’ and ‘Change of residence’, and in such a way as to be compatible with eMayor.

The **main research question** is:

“What is an appropriate way for municipalities to implement authentication for the eGovernment services ‘Certificate issuance’ and ‘Change of residence’, while compatible with eMayor?”

Next will be described what is meant by the term “*appropriate*” and “to be compatible with the eMayor platform”.

In the Netherlands, the tendency is towards using different authentication techniques for different security levels. Not all services require the same level of security and thus different authentication techniques will be applied. Some services need a high level of security and can not be offered at a lower level of security. An example of a service that requires a high level of security is the issuance of a new passport. Although a high level of security could serve more services, this is unnecessarily expensive. The request for a certificate requires a lower level of security, thus this service requires an other level of security. *Appropriate authentication* is a technique that takes into account the different levels of security. This thesis will pay attention to the fact that different levels of security can be applied and that appropriate authentication takes into account that there are different levels of security.

The platform does not prescribe an authentication technique. It does suggest one, namely the use of smart cards, but also supports for the use of digital certificates and password authentication. It will be researched whether these techniques are suitable in the Dutch situation (as can be seen from the research sub-questions). As there are no Dutch municipalities involved in the eMayor project this is not done in the eMayor project itself. *To be compatible with the eMayor platform* means that the authentication technique chosen in the Netherlands has to be supported by the eMayor platform

The **final result** of this research will be a report with the descriptions and models of the services chosen in the eMayor project, an overview of several authentication techniques and several Dutch authentication initiatives, selection criteria, resulting in a conclusion on appropriate authentication techniques for the two eMayor services in the Netherlands.

The main research question will be divided into separate research questions. The research **sub-questions** to be addressed are:

1. Current situation:
 - a) What processes do the two eMayor services in the current situation consist of?
 - b) What can be improved by offering the two eMayor services online?
2. Which techniques for authentication can be found in literature?
3. What are the advantages and disadvantages of these authentication techniques?
4. Which Dutch authentication initiatives are currently initiated?
5. Are current Dutch authentication initiatives useful for the Dutch eMayor services?
6. Is the suggested authentication technique of the eMayor project suitable for Dutch municipalities?
7. What are the selection criteria for choosing suitable authentication?
8. How can a selection of an authentication technique be made?

These sub- questions will be answered in the next chapters. In paragraph 2.4 the research strategy is elaborated on and in this paragraph can also be found in which chapters the sub-questions will be answered.

2.4 Delineation of the problem

Delineation in research is always necessary. The scope of the research is determined by the following:

- Some services are for *citizens* as well as for companies available. In this thesis the focus is on citizens, not companies. However, the process descriptions are similar for companies.
- Only *two services* chosen by the eMayor consortium (*certificate issuance, change of residence status*) are analysed, no other services are part of this research. eMayor also includes a tax service. This service is different in the Netherlands and therefore will not be researched.
- The topic of this thesis is *authentication*, not access control which covers a larger area of security measures.
- This thesis focuses on authentication for *municipal* eGovernment services, not at national government, provinces or “Waterschappen”.
- Authentication of *citizens* is researched, not authentication of civil servants.
- A user can be authenticated, but also a sent message. This thesis focuses on user authentication, message authentication is out of scope.
- Authentication of users using a *computer* with a browser are considered, mobile log on is delineated.

2.5 Research strategy, methods and techniques

Next a description will be given of the research strategy, methods and techniques that are used.

2.5.1 Current situation

Firstly, in chapter 3, the current Dutch situation is described with regard to the two eMayor services (Change of residence, Certificate issuance).

The following research question will be answered:

- 1) Current situation:
 - a) What processes do the two eMayor services in the current situation consist of?
 - b) What will be improved by offering the two eMayor services online?

UML (Unified Modelling Language) is used to model the current situation. UML is a world wide standard, which makes communication between different parties easier. Furthermore this language is the standard for the eMayor project.

Within UML there are different types of models, like sequence diagrams, class diagrams and activity diagrams. The municipal processes are modelled using activity diagrams. Activity diagrams are useful in describing behaviour, especially when much processes are parallel. For this reason they are very useful to depict workflow.

Interviews are held to gather information about the services. Later on interviews are held to verify whether the UML models made correspond to the actual services they deliver. These interviews are held with civil servants from the municipalities of The Hague and Hoorn. With both cities at least one interview is held to verify the models. This were semi-structured interviews with a small questionnaires. This questionnaire will contain questions about the services of the municipalities Hoorn and The Hague.

2.5.2 Authentication techniques, (dis)advantages and initiatives

Secondly, research on authentication is performed, and can be found in chapter 4 and 5. The following research questions will be answered:

2. Which techniques for authentication can be found in literature?
3. What are the advantages and disadvantages of these authentication techniques?
4. Which Dutch authentication initiatives are currently initiated?
5. Are current Dutch authentication initiatives useful for the eMayor services?

Questions 2 and 3 are answered in chapter 4, question 4 in chapter 5.

A literature study is done about authentication. This background study is used to discover which techniques for authentication are in use in Europe. Dutch initiatives will be analysed. The literature study is also used to know more about the advantages and disadvantages of these techniques. Furthermore, interviews are held about several Dutch authentication initiatives. The interviewees are employees of BKWI, ECP and ICTU. These were all semi-structured interviews.

2.5.3 Authentication selection criteria

Interviews are held with ICTU and civil servants of the municipality of The Hague, to determine the selection criteria. The literature study on authentication is also used in this stage. The score card and SMART method will be used to evaluate the different authentication techniques. A section framework is designed to evaluate different authentication techniques. The following research questions will be answered in chapter 6:

6. What are the selection criteria for choosing suitable authentication?
7. Is the suggested authentication technique of the eMayor project suitable for Dutch municipalities?
8. How can a selection of an authentication technique be made?

2.6 Structure of the research and planning

The following table shows the structure of the research. For every chapter the methods and techniques which are used and the expected results are shown.

Chapter	Research method and techniques	Expected results
2. eMayor project, Problem & context	<ul style="list-style-type: none"> Internal literature study and interviews 	<p>Description of eMayor project and background</p> <p>Description of problem</p> <p>Aim of the research, Delineation</p> <p>Research strategies, techniques</p> <p>Research questions</p>
3. Current situation (services, systems, chances and bottlenecks)	<ul style="list-style-type: none"> UML Activity Diagrams Interviews with municipalities The Hague & Hoorn 	<p>Description of situation: description and models of services of municipalities Answer Research Question 1 a) and b): What processes do the two eMayor services in the current situation consist of?</p> <p>What can be improved by offering the two eMayor services online?</p>
4. Authentication techniques and (dis-)advantages	<ul style="list-style-type: none"> Literature study about authentication 	<p>Answer Research Questions 2 & 3: Which techniques for authentication can be found in literature?</p> <p>What are the advantages and disadvantages of these authentication techniques?</p>
5. Authentication initiatives	<ul style="list-style-type: none"> Interviews BKWI, eNIK, ECP.nl, The Hague 	<p>RQ 4 & 5 & 6: Which Dutch authentication initiatives are currently initiated?</p> <p>Are current Dutch authentication initiatives useful for the Dutch eMayor services?</p> <p>Is the suggested authentication technique of the eMayor project suitable for Dutch municipalities?</p>
6. Authentication selection	<ul style="list-style-type: none"> Score card /SMART method Interviews ECP.nl, The Hague 	<p>RQ 7 & 8: What are the selection criteria for choosing suitable authentication?</p> <p>How can a selection of an authentication technique be made?</p>
7. Conclusions & Recommendations		<p>Conclusions</p> <p>Recommendations</p>

Table 2.2 The structure of the research

3. Current situation and design of new processes

This chapter will outline the current situation as it is in Dutch municipalities. This is necessary to understand the background of the services and the systems used. For example, the procedures used are important for the determination of the security level of the authentication technique. Furthermore, the description of this situation is needed to point out where changes have to be implemented in the new online situation.

Several aspects of the current situation will be described. Firstly, in paragraph 3.1, the change of residence status and the certification service will be described. In the Netherlands, there are two important categories of certificates: GBA (Gemeentelijke Basis Administratie) certificate and BS (Burgerlijke Stand) certificate. These two categories are modelled separately, which, in combination with the change of residence, will result in three models. Interviews are held to gather the required information. Civil servants of the municipality of The Hague have been interviewed (appendix 1). More about these models and the explanation of the GBA and BS will be described in section 3.1.1. The change of residence status is described in section 3.1.2.

Secondly, the technical details of the networks and systems will be described (paragraph 3.2). These details are important for the level of security and to get a better understanding of the way the systems work. The GBA system will be explained and the communication networks within and between municipalities will be described.

Thirdly (in paragraph 3.3), the bottlenecks in the current situation will be described and the design of the processes in an online situation are described. The process bottlenecks will be mentioned and the (expected) changes and improvements in the situation after the services are offered online will be pointed out.

Lastly, conclusions on research question 1 will be drawn in paragraph 3.4

3.1 Services

Three different services will be described. These services are modelled in UML activity diagrams. UML is used because UML is a world wide standard, which makes communication between different parties easier. Furthermore, this language is the standard for the eMayor project. The processes will be modelled using an activity diagram. Activity diagrams are useful in describing behaviour, especially when much processes are parallel. For this reason they are very useful to depict workflow. Furthermore, by the use of swim lanes the different roles (civil servant, citizen, employee in the safe) can be depicted. It will be clear which actor implements which tasks in which order.

These models can be found in the appendices 7 to 12. Appendix 6 contains a page with the symbols, their names and a description how the models should be read.

These models and descriptions are made for the change of residence status, GBA (Gemeentelijke Basis Administratie) certificate and BS (Burgerlijke Stand) certificate processes. The last services are both types of the certification service. They will be described first.

3.1.1 Certification service

The certification service offers the citizen the ability to make a request for a certificate and receive the certificate from the municipality. There are many different certificates issued in Dutch municipalities.

Examples are birth certificate, death certificate, certificate of residence. A full list of GBA- certificates is included in appendix 2.

Certificates originate in two administrations. These are called the Gemeentelijke Basis Administratie (GBA) and the Burgerlijke Stand (BS).

The latter administration can contain the following information about the citizen, corresponding the occurrences in a persons life: birth, marriage, divorce, emigration and death. Different aspects will be included: date of birth, city of birth, the parents' names; date and city in which the person married, the name of the partner; divorce date; address and date of emigration; date and place in which a person passed away.

This information is kept in books in a room called the safe, in the municipality where the event happened. For example if a person is born in The Hague, he or she will be registered in the Hague. When this person marries in Hoorn, his/her marriage will be registered in Hoorn. This implicates that this person needs to get his birth certificate in The Hague and if he needs a marriage certificate, he also has to visit Hoorn.

The GBA contains more information. It also includes the persons address, drivers licence number, "SoFi number", passport number, etc. These categories will be explained in more detail in paragraph 3.2 "GBA-system". This information is stored in the municipality the person is living in (actually: the municipality the person is registered to be living in). A GBA-certificate is issued in this municipality. This certificate can contain different parts of the information kept in the GBA; just that part the citizen requests will be printed, e.g. the address. All the information about one person together is called the Persoonslijst (PL), which can be entered by giving in the persons name. However, the information can be accessed in different ways. To give an example: it is also possible to enter an address. The system will return the names of everyone living at that address.

Next, the processes to apply for and to issue the certificate will be described. The models made of these services in UML activity diagrams are added to the appendices 7 and 8.

Certificate BS process

This process is modelled in appendix 7.

Request done by citizen

The citizen has two options to request for a certificate: go to the town hall or send it (by post, mail or fax). When the citizen decides to send the request, he needs to add a copy of his passport. The civil servant working in the safe receives the request and will determine the identity of the citizen. The municipality of the Hague asks citizens to identify themselves, but this is not made mandatory by law.

Identification

The identification can be done with or without (a copy of) a passport. The latter one is only possible if the civil servant is able to ask the citizen questions to verify his identity. For this reason this is only possible in case the citizen comes to the town hall or when he calls. A sub model is made of the identity check, to make the main model more readable.

When the *citizen carries a passport*, the document is checked to see whether it is issued by a legal issuer and whether the person looks like the picture. If not, the process is stopped. When the document is issued by a legal issuer, it is checked whether the passport is issued in the Netherlands. When this is the case, the document should be registered on the persons PL. If not; the process is stopped. When the document is registered on the PL or when the document is not Dutch, the next step will be taken.

The identity can also be checked *without a passport*. The citizen will be asked questions on the basis of the information in the GBA. However, it is clear that this offers the risk of fraud.

Gathering information and approval/rejection of request

After the identity is determined the required information is gathered. What information this exactly is, depends on the kind of certificate requested. Then, the request will be assessed. This could lead to the rejection of the request. In that case, the citizen can ask for a copy of the rejection. This copy of the rejection can either be sent by mail or given to the citizens.

Payment and processing of the request

If the request is approved the civil servant will consider whether the citizen has to pay for the certificate. In some cases the law makes exceptions and no fee has to be paid. For example, some certificates are for free when the citizen has reached the age of 65. The fee has to be paid at the service desk or can be paid afterwards in case the citizen is not at the town hall.

Now the civil servant will look up the document and make a scan. The civil servant will print it and either send it by post or hand it over to the citizen. This print is made on special paper, which makes it hard to copy the document. Whenever a copy is made the words “copy” and “kopie” will appear. Appendix 3 contains a birth certificate copied on this paper. The next appendix (4) contains the back side of this certificate, showing safety instructions. Appendix 5 shows the paper many of the certificates are copied on. The words “copy” and “kopie” can be seen very clearly.

In case the citizen did not visit the town hall, the civil servant will arrange the payment. This is a payment by means of an enclosed giro slip or (in case the citizen already filled out a payment form) sending the form to the bank.

Certificate GBA process

This process is modelled in appendix 8.

Request done by citizen

The citizen is able to authorize other people to request for the certificate GBA. In this description of the certificate request the word “citizen” will be used: this can be a person requesting a certificate for himself or for someone else in case he is authorized to do this.

Again the citizen has two options to request for a certificate: go to the town hall or send it (by post, mail or fax).

Identification

The identification procedure is the same as in the BS certification procedure, so this will not be explained again.

Processing of the request

By means of the information in the GBA, the personal information can be researched when there seem to be mistakes.

The GBA certificate will be produced. This consists of the following steps: firstly, it will be determined which information has to be printed (depending on the type of certificate requested). Secondly, the data will be printed, and in case of confidentiality this will be mentioned on the document. In the last step the document is checked on mistakes.

After the document is produced, there are two scenarios. In the first scenario, the person is at the town hall, in the second the person made the request by mail, fax or email.

Scenario 1 person is at the town hall

In case the person is at the town hall, the civil servant will give him the certificate and will return his passport. The civil servant will determine whether the citizen has to pay him a fee. If so, the citizen will have to pay the fee.

Scenario 2 person sent the request

In case the citizen did not visit the town hall, the civil servant will determine whether the citizen has to pay a fee. The certificate will be sent to the person's home address, accompanied by an enclosed giro slip or (in case the citizen already filled out a payment form) sending the form to the bank.

3.1.2 Change of residence status

The change of residence service offered by municipality is for citizens moving within this municipality (intra municipal), citizens moving from another municipality to this municipality (inter municipal) and or citizens from this municipality moving abroad. This service changes the address to the new address and will store this new address on the person's PL. In case the citizen moves abroad, the PL will be stored on a special place for people moving abroad. This is called: freezing the account. A description will be given of the process, the model made in a UML activity diagram is added to the appendix 9.

Change of residence status process

This process is modelled in appendix 9.

Request done by citizen and Identification

To change the residence status the citizen first has to fill out a form and sign it. He can send it or go to the town hall.

The civil servant will receive the form and will check the identity of the citizen first. Again, this is the same procedure as in the BS certification procedure.

Comparison of information and digital GBA-form

After the identity is determined, the form will be compared with the information in the GBA. When no mistakes are found, the civil servant will fill out a digital GBA-form with the name, date of birth, date of moving, possible family members who also move, the old address and the new address information.

When a person moves to the Netherlands Antilles a special change of address card has to be sent.

Assessment of change of address

The change of address will be assessed, which can lead to an investigation of the information. The investigation can have different causes, for example when there are already people living at the citizen's new address.

When everything is fine, the civil servant has to check whether the citizen moves now or in the near future.

Person moves in the (near) future

In case the person moves in the future, the request is stored in the system and the real change of address will only be made at the right date (the date the person actually moves). The system automatically checks this list of people moving in the future, and changes the information at the right time.

Person moves now

When the person does not move in the future, the civil servant will check whether this person comes from another municipality. If so, the civil servant has to contact this municipality to get the citizen's PL. Then, the civil servant checks if this person has "relationships" in the municipality. A relationship is only a formal relationship like a parent, sister, or husband. If there are any, the system will automatically add these relationships to the citizen's PL. When the system fails to add the contacts, the civil servant will do it manually.

Updating and Error check

Now, the citizens PL will be updated. The new information is stored in the GBA. Then, the civil servant checks whether there are investigations on the change of address request. If so, he needs to know if this can be closed, he will contact the other municipality when the investigation is done by that municipality. When research is finished, the change of address will be checked by another civil servant. If this civil servant finds a mistake, he will return it to the first civil servant with a description of the mistake. After the change is completed and rectified, it will be stored.

3.2 Technical systems

Several systems are involved concerning the services. The most important aspect of these systems is the security aspect. The next sections describes the diverse systems.

GBA system:

The GBA is developed according to a logical design made by the Basis registratie Personen- & Reisdocumenten (BPR). This organisation is a part of the Department of the Interior (Dutch: Ministerie van Binnenlandse Zaken). They prescribed the functionality of the system, for example security topics, the way backups have to be made and how often this is needed, etc. By means of this prescription, three software developing companies made a GBA application. These three companies are Pink Roccade, Centric and Procura. Every municipality chooses one of these suppliers. The exchange of information between municipalities with different GBA systems does not cause any problems.

The municipalities have the responsibility of gathering the information of its inhabitants. They have to make sure the information they store are up to date and correct.

Some other organisations can get access to this information. An example of such organisation is “de Belastingdienst”, an organisation that collects tax. Not every organisation has access to the GBA information. Which organisations do have access is determined by law (“Wet GBA”). These are mostly governmental or semi-governmental organisations that need the information to do there (public) activities. No citizens have access to an other citizen’s PL. This is determined in the privacy laws in the “Wet GBA”. Municipality A does not have access to the GBA-system of municipality B. The municipalities can communicate with each other using a “mailbox system”. This means that they can send each other messages and get replies, but can not access each others systems. The format of these messages is determined as well. This facilitates the automation of the processing and sending of the messages.

The GBA-system in a certain municipality contains information on the citizens living in that municipality. This information is divided in 15 categories:

1. Person (information about this person like name, date of birth, etc)
2. Parent 1
3. Parent 2
4. Nationality
5. Marriage
6. Dead
7. Registration
8. Address
9. Child
10. Legal residency (Dutch: “Verblijfstitel”)
11. Power relationship (Dutch: “Gezagsverhouding”)
12. Travel document
13. Right to vote
14. “Afnemers indicatie” (contains references needed for information supply)
15. Notes (not in use anymore)

As mentioned earlier, the GBA can also be used in a different way. It is also possible to look up an address and see who is living at that address. Every address with one or more people living there is registered in the “address list” (BPRBZK.nl 01). This topic will not be elaborated on, because it is not important for the research.

There are two other information data bases in the GBA, they will also not be elaborated on. They are the “Landelijke tabellen” and the references (“verwijzingen”). The latter one contains some information of people who used to live in this municipality, and moved to another municipality after October first, 1994. It also contains information of people born in this municipality after October first 1994, but who do not live in this municipality.

The “Landelijke tabellen” are lists with codes. Every category in the registration is represented by a code. These codes are determined for different categories, for example the municipality of The Hague has it’s own number. This is done because so many people live in the Hague, it is easier to use a code. These codes are the same all over the country.

Communication networks:

The GBA-systems communicate with each other. For example, they send each other PLs. This has to be done in a secure way, so eavesdroppers will not get the chance to read the information.

The communication between different municipalities is sent on a secure connection. Within municipalities, the different offices send each other information using an intranet. This network can only be accessed by people of this municipality that are attached to this network. This makes interception of messages more difficult.

3.3 Design of the expected online situation: Online opportunities and current services’ bottlenecks

This thesis also proposes a redesign for the services in case they are offered online. First some issues concerning the change of residence status process and the expected changes for the online process will be described. Models are made that show how the services are expected to be when they are offered online. Next the certificate BS process and the certificate GBA process will be elaborated. This chapter will end with a conclusion about the online services “Change of residence” and “Certificate issuance”.

In general

There are risks of fraud in the current situation. When the citizen has no passport, the civil servant will ask him questions to identify whether this is the same person as the person he claims to be. This is done by asking questions obtained from the information about this person in the GBA. The civil servant can ask questions in the following categories: name, date of birth, name of the parents or children, address, etc. It is not difficult to imagine that a person might know this about someone else. This means that here is an opportunity for fraud.

Expected changes for the online process:

The citizen does not have to come to the town hall any more, which saves him time and travelling costs. He can request the service any moment he want, and is not bound to opening hours of the town hall. Furthermore, democracy is increased by making the municipality more transparent. The services, and their legal implications can be viewed online. This makes them accessible and visible to everybody (with a computer and browser).

The advantage for the municipality is that it saves time of the processing of the service and helping the customer. This might even result in a reduced number of desk workers, so a reduction of cost. These time savings are obtained because the forms are already filled out by the citizens on a digital format and

therefore less mistakes will be made by copying the information done by the civil servant. Moreover, the identification process does not have to take place as this is done online in the authentication step. Offering the service online is a service the municipality offers to the citizens. These citizens will appreciate that they can get their address changed online without leaving the house. These advantages can be gained by changing the following.

Change of residence status online

The process of changing the residence status online is modelled in appendix 12. This is a model of the expected situation.

The process will be shorter because the identification process is redundant after a citizen has logged in and authenticated on the internet site.

In the current situation two forms have to be filled out. First the citizen has to fill one out (the former “PTT-aangifte formulier”), and sign this form. Later when the request reached the civil servant, this servant needs to fill out the digital GBA- form in the system. When the service will be offered online this double effort is not necessary anymore. The citizen just fills out the form on the internet and this will arrive at the town hall.

Certificate BS online

The process of acquiring the certificate BS online is modelled in appendix 10. This is a model of the expected situation.

One thing is actually misleading in the certificate BS process. The municipality of The Hague asks the citizen to identify himself, which can be seen from the model. Actually this is not mandatory by law.

When a citizen does not want to identify himself, he will still be allowed to get the certificate.

Furthermore, the identification process itself can cause some problems as well. This is the same problem as described in the change of residence status process. The questions a civil servant asks to identify the citizen can be studied which is a risk for fraud.

Offering this service online might help preventing this fraud. In that case the citizen has to log in and can only be the person allowed to have this certificate.

Other changes to the process when offered online will be summed up in the next section:

The citizen has to log in at the internet site of the municipality. On this site the citizen can choose the services he desires and has to fill out the required information for this services in a form on this site. He will send it by pushing a button and the request will arrive at the town hall almost immediately. Because the citizen fills out the required information for the service he wants on the internet site, the civil servant does not have to gather the required information from the citizen. He automatically receives the right information. This saves the civil servant time. Because the citizen has to authenticate himself to the system online, the identification process does not have to be done by the civil servant.

The citizen is that he does not have to go to the town hall anymore. He will be able to request the certificate anytime and does not have to take into account the opening times of the town hall. Also, there is no waiting time in a queue anymore.

Since the identification process is right at the beginning of the service request, no time will be wasted on citizens that can not identify themselves.

Certificate GBA

The process of acquiring the certificate GBA online is modelled in appendix 11. This is a model of the expected situation.

Again, the identification process can cause problems. In the process of requesting the certificate GBA, identification is obliged. But this can be done by asking the citizens questions, which can lead to fraud when a person studies the answers of somebody else. Offering the service online could help preventing this fraud in retrieving the certificate GBA.

Other changes to the process when offered online will be summed up next:

Many of the changes in the process are the same as the changes in the certificate BS process.

The citizen has to log in at the internet site of the municipality and fill out the required information. This saves the civil servant time, because he does not have to gather them himself.

Also, the identification process is not necessary anymore.

Again the advantage for the municipality and for the citizen is saving time because of increased efficiency. Time savings can result in decreased cost because the civil servant can use the saved time for some other task. This might even result in a lower number of required desk workers. The municipality offers the citizens better service by offering the certification service and change of residence online and at the desk.

3.4 Conclusion on research question 1

Research question 1 was formulated as follows:

1. Current situation:
 - a) What processes do the two eMayor services in the current situation consist of?
 - b) What can be improved by offering the two eMayor services online?

The main process steps are:

Certificate issuance (BS and GBA)

- Request by citizen
- Identification
- Approval/rejection request
- Payment and processing of the request

An important difference between BS and GBA process is that for the request of a certificate GBA an identification is obliged. Unlike in the BS process where this is not necessary.

Change of address

- Request by citizen
- Identification
- Check GBA information matches request form and produce digital GBA form
- Approval/rejection request (possibly followed up by an investigation)
- Store in temporary file (if necessary)
- Ask for PL and update file
- Check data

Offering the services online has some implications on the processes. There are a couple of steps in the old process that do not have to be taken care of anymore. They will be summed up next:

- The identification process is redundant (this will be an automated process online)

- The civil servant does not need to retrieve the required information, because the citizen already fills these out in digital format
- Knock-out moments are at the beginning of the process, which avoids the handling of citizens that can not properly identify themselves or that are not authorized to request a service.
- In the change of address process: only one form has to be filled out instead of two

Offering the services online provides the following **advantages**:

- Knock-out moments are at the beginning of the process, partly in the identification process. Persons who can not identify themselves at the desk take time of the civil servant without any service being offered. By filtering these people out by authentication online, the civil servants only spend time on actual service handling and transactions
- Offering services online could help remedy fraud in the identification process (GBA certificate and change of address)
- Municipality saves time and money (e.g. because processes are shorter and more efficient)
- Municipality offers the citizen better service
- Municipality is more flexible in doing their work (they can handle the request at a certain point in time convenient for them, not just when the citizen arrives at the desk)
- Citizen saves time and money (does not have to go to the town hall, no waiting time in the queue)
- Citizen more flexible in requesting the service (they can determine when to request themselves and do not have to take into account opening hours of the town hall)
- The municipality becomes more clear/ transparent, which enforces democracy.

The following **risks** should be considered:

- No matter which authentication techniques is used, there will always be people able to commit fraud. However, good authentication mechanisms can make authentication more secure. So, it is about the degree in which authentication provides security, and it is never 100% secure.

4. Authentication techniques

In the previous chapter the municipal services chosen for the eMayor platform are described. From these descriptions it became clear that authentication of the user of the services is an important issue. Municipalities want to offer services online. To verify the identity of a user who applies for the service, authentication is necessary.

This chapter will elaborate on different ways to authenticate users to a system. Authentication is important because unauthenticated persons should not be able to access systems, read or access information or in other ways can interfere with someone's privacy.

In this chapter different authentication techniques are described. Firstly, an answer will be given for the question: What is authentication? Next, several authentication techniques are described (paragraph 4.2). In paragraph 4.3 research questions 2 and 3 will be answered.

4.1 What is authentication?

Authentication of the user of a service is an important issue. Consequently, the next question to be answered is: What is authentication?

To answer this question, the preceding question has to be answered first: What is identification? And more generally: What is access control?

“Access control is the ability to limit and control the access to host systems and applications via communication links” (Stallings, 2003). To limit access to host systems and applications, several techniques and policies have to be applied. Authentication is one of the possibilities to limit access. Also, the protection of the network by the use of firewalls and the physical security of the system are important ways to control access. By physical security is meant the protection of the machines and devices themselves, not through the network, but the physical machine. They should be protected from damage, theft or people using the machine for unauthorized purposes.

Access to the host system and applications can be controlled by making authorization rules. Authorization is the act of giving authority or permission (Check Point Software Technologies, 2003). To give an example, user A and B might both be able to authenticate and log on to a system, but A might have the right to read property on this network, and B might be authorized to read this property and edit files as well. A and B have different rights.

Access control also includes security policy with regard to computer access, as can be seen from the following definition: Access Control is a mechanism and policy that restricts access to computer resources (Check Point Software Technologies, 2003).

Most people are familiar with the meaning of identification. In many occasions identification is necessary, for example at the airport passengers have to identify themselves using their passport. Different definitions of identification can be found in literature. According to Woodward (2003), identification systems answer the following question: “Who is X?”

This can be determined in various different ways like asking someone's name or checking a passport.

However authentication goes a bit further. Stallings (2003) defines authentication as follows: “The assurance that the communicating entity is the one that it claims to be.”

Although these definitions seem very similar, there is a slight difference. The authentication process puts emphasis on *assuring* that someone is who he claims to be.

Check Point Software Technologies (2003) puts it a bit different: “Identification is the process of subjects establishing who they are to an access control”. They define authentication as follows: “Authentication is the technical control that requires subjects prove they are who they claim to be.”

This means that in this definition the *technical control* determines the difference between identification and authentication.

However in other literature identification and authentication are used interchangeably.

In this thesis a distinction will be made between identification and authentication. Identification is the answer to the question: “Who is X?”. Authentication puts emphasis on the assurance that this person is who he claims to be and is defined as follows: “The assurance that the communicating entity is the one that it claims to be.”(Stallings, 2003)

This assurance can be obtained by the use of technical controls like authentication techniques (passwords, PINs, smart cards, biometrics) to prove this identity. These techniques are necessary in case a person has to be authenticated while working on a computer.

The word identification will be avoided to prevent confusion. Only in chapter 3 the word identification is used because the municipal process descriptions use this word.

4.2 Techniques, advantages and disadvantages

There are different types of authentication. They are based on the following (Woodward, 2003):

- Authentication based on something you *know*
- Authentication based on something you *have*
- Authentication based on something you *are*

A typical way to authenticate yourself using something you *know* is the use of a password. In paragraph 4.2.1 passwords will be elaborated on.

Authentication by means of something you *have* is often done by a (smart) card or certificate. This topic will be described in paragraph 4.2.2.

Something you *are* involves biometrics. These are bodily characteristics that are typical for every individual. This will be described in paragraph 4.2.3.

The next figure (4.1) depicts authentication and the three different techniques to authenticate. However, combinations of these three categories exist as well, e.g. smart cards with PINs or with biometric information on it. Combining different types of authentication is called *two-factor authentication*. Combining different techniques increases the level of security. To use the above example; without the PIN-code it is difficult to get money from a stolen (bank) card.

In the next sections (4.2.1 to 4.2.3) the separate types of authentication are described.

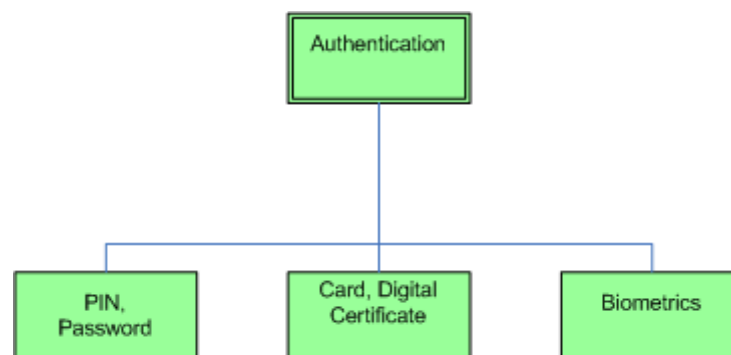


Figure 4.1 Different ways of authentication

4.2.1 Password and PIN

A password is something you know. The use of passwords is a way to authenticate that is regularly used. A password can be defined as: a supposedly secret string used to prove one's identity (Stallings, 2003). Another example of "something you know" is a PIN-code. A PIN (Personal Identification Number) is actually a variation on the password, but only consists of numbers.

To authenticate a person A, A has to give in the character string (or PIN). This string is compared with the stored string. If they are the same, A is authenticated. When the two strings do not match, A will not get access to the system.

The fact that a password or PIN is something you know, implies that there is a chance to forget the password (or PIN). A password should not be written down, but also not be so easy that it is able to guess them, for example names, or dates of birth. This is a difficult issue, because when the password is easy to remember, it is also easy to crack. It seems better to make the password more difficult to guess or crack, but when the password is hard to remember, the user will start writing it down. Most people can remember up to 7 or 8 digits. In case the password is longer, the users might write it down, which is another chance for hackers.

Users often use the same passwords for multiple applications, so they only have to remember one password. This means that the hacker only has to find one password to access all applications.

Furthermore, some people share passwords on purpose. For example, when different people are participating with others in a project group. Even if they do not give the password on purpose, some people have passwords which are easy to guess if you know a bit about this person. Examples are dates of birth, the name of a child, etc. Hackers can also get the password by just looking at the person who is typing his password on the keyboard, called "shoulder surfing" (Beaver, 2004).

"Social engineering" is another way in which the password can be obtained for fraudulent purposes. Someone gets the password by "asking" and pretending that they need it to help the owner with some problem, e.g. by pretending to be a bank employee or a policeman. Unwary people might tell the password to the criminal.

A hacker can also obtain the password across the network, by using password-cracking software. An example is a "dictionary attack". This software enters all the words in the dictionary and will reveal the passwords if this is a word which is in this dictionary. A brute-force attack is an attack using software that tries every possible character combination that the password might consist of. Since every possible combination is tried, it might take a long time to find the right password. This depends on the computing power of the computer trying to crack the password, the length of the password and whether the password consists of different types of characters (e.g. numbers, letters, capitals and symbols).

Moreover the password database itself should also be protected. In case the database is not protected properly, hackers can get access to all user accounts, which is highly undesirable. There are two aspects to this, namely the protection of the physical machine and the protection of the access to the machine through the network it is connected to. The physical machine has to be protected by securing the room it is in. The network can be protected in several ways, like using firewalls, encryption, etc. Because this is outside of the scope of this thesis, this topic will not be elaborated on.

It is clear that there are many ways to compromise a password. There are also ways to prevent this. Maybe one of the most important is making the users aware of the problems, and risks. Users should not write passwords down, share them, or choose easy to guess passwords. Passwords with numbers, characters, capitals and symbols are preferable. Almost 3 trillion eight-character password combinations are possible by using the numbers 0-9 and 26 characters of the alphabet (Beaver, 2004). This makes it

difficult to forge the password by guessing and takes a long time and computing power when password-cracking software is used.

The implementation of PINs and passwords only require additional software. For this reason this technique of authentication is relatively affordable compared to cards or biometrics in which more than software is required. Passwords and PINs often require a helpdesk to help people who forgot their password or PIN, which can be costly. This can be reduced to a minimum by offering the users good education on the use of passwords and PINs. Besides, the generation of passwords becomes automated more and more nowadays.

Personal Identification Numbers (PINs) consists of numbers out of the range 0-9. Usually the PIN code consists of only four digits. According to the ISO 9564-1 standard the PIN should consist four to twelve alpha-numerical characters in order to reduce the risk on fraud by trial and error (Rankl, 2000). However, the use of non-numeric characters is not possible in most PIN stations (for example ATMs). Furthermore, the more characters are used, the more difficult it will become to remember the code. Users will start writing the code down, which makes the risk of fraud bigger.

Theoretically, the chance to guess a four digit pin code in three tries (before the system blocks the card) is 0.03% (Rankl, 2000). However, it turned out that some digits are used more often than others and that some combinations of numbers are not allowed, resulting in less different passwords. This makes the percentage 0.66% that the PIN can be guessed in three times, which is 22 times higher.

The following table shows the PINs and passwords with various lengths and coding, and the number of possible combinations (Rankl, 2000).

Type of PIN or password	Range of values or coding of the PIN or password	Number of possible PINs or passwords
1-digit PIN	PIN $\in \{0...9\}$	10
1-Character password	Password $\in \{0...9, "A"... "Z"\}$	36
1-Character password	Password $\in \{0...9, "a"... "z", "A"... "Z"\}$	62
1-Character password	Password $\in \{0...9, "a"... "z", "A"... "Z", 20 \text{ arbitrary special characters}\}$	82
4-digit PIN, no leading 0	PIN $\in \{1000...9999\}$	9.00×10^3
4-digit PIN	PIN $\in \{0000...9999\}$	1.00×10^4
4-Character password	Password $\in \{0...9, "A"... "Z"\}$	1.68×10^6
4-Character password	Password $\in \{0...9, "a"... "z", "A"... "Z"\}$	1.48×10^7
4-Character password	Password $\in \{0...9, "a"... "z", "A"... "Z", 20 \text{ arbitrary special characters}\}$	4.52×10^7
5-digit PIN, no leading 0	PIN $\in \{10000...99999\}$	8.90×10^4
5-digit PIN	PIN $\in \{00000...99999\}$	1.00×10^5
6-digit PIN, no leading 0	PIN $\in \{100000...999999\}$	8.99×10^5
6-digit PIN	PIN $\in \{000000...999999\}$	1.00×10^6
6-Character password	Password $\in \{0...9, "A"... "Z"\}$	2.18×10^9
6-Character password	Password $\in \{0...9, "a"... "z", "A"... "Z"\}$	5.68×10^{10}
6-Character password	Password $\in \{0...9, "a"... "z", "A"... "Z", 20 \text{ arbitrary special characters}\}$	3.04×10^{11}

Table 4.1 PINs and passwords with various lengths and coding, and the number of possible combinations

The above table shows several PIN and passwords combinations. The second column specifies the type of characters the password consists of. The third column represents the number of possible combinations.

When this number is higher, the chance that the password or PIN can be compromised is smaller. As can be seen from the table, a six character password with numbers, letters, capitals and symbols is the most difficult to guess. However, as described earlier, the way people use their passwords is very important. For example, when a person writes the password down on a post-it next to the computer, even a twelve digit password will not suffice.

4.2.2 (Smart) cards and digital signatures

There are many different types of cards and digital signatures. Five different types of cards will shortly be discussed. The sixth card is a hybrid; a combination of different cards. The other five cards are all members of the family of cards with the ID-1 format, specified in the ISO standard 7810. This standard prescribes the card characteristics like size, flexibility and temperature resistance (Rankl, 2000). This ID-1 format is the standard for smart cards, which has the size of a credit card: length $\approx 85.6\text{mm}$; width $\approx 54\text{mm}$; thickness $\approx 0.76\text{mm}$.

The five cards of the ID-1 format are the embossed card, the magnetic-strip card, the optical card, memory card and the Smart card.

The different types of cards can be subject to theft, which makes a “two-way protection” important. This two-way protection is a combination of two different ways of authentication, for example the combination of using the card as well as a password or PIN. This combines “something you know” with “something you have”.

Lastly, digital signatures will be explained in this paragraph.

Embossed card

The Embossed card is a card with numbers embossed on it. The relief is made so an easy copy of the card can be made. The old credit or Visa cards had this relief, and the copy was made by putting it in a holder putting special paper on top of it and pulling an ink strip over the card and paper. Now a print was made, and the copy was ready to send to the credit card company. It does not require electricity or connection to a telephone network. Clearly, the copies of the embossed card give a lot of paper overload and it is not digital (Rankl, 2000). Credit cards are often embossed cards. These cards are not an option for authentication for eGovernment services as the information is printed on the card and therefore to easily readable.

Magnetic strip card

A solution for the paper overload is to code the information on the embossed card and store it on a magnetic strip on the card. The magnetic strip cards are swiped through a reader after which the information is used for the transaction. The strip has three tracks in which the information of the user is stored. There is also space to store information on the latest transactions. Tracks 1 and 2 are read-only after the card has been issued, while data may also be written to track 3 while the card is in normal use. The total storage capacity of the magnetic strip is about 1000 bits (Rankl, 2000). A disadvantage of the magnetic strip card is that 1000 bits is not very much and that information can easily be altered and read. The technique of the magnetic strip is similar to that of a tape recorder. The specifications of the equipment and card technology are public, and because the technology is not very difficult, it is relatively easy to make a card reader and copy information of the card. Readers are available for less than \$1000. The information copied from a card can be used to reproduce the card and make fraudulent transactions (Hendry, 2001). Especially unattended machines (for example ATMs) are a risk because the fake cards can be used here without anybody noticing it is a copy. Some manufacturers of magnetic strip cards have developed techniques to prevent this fraud, but they increase cost considerably.

The amount of money lost in fraud all over the world is estimated to be billions of dollars a year. Magnetic strip cards are often used as banking cards to withdraw money from an automated teller machine (ATM). However a new standard based on smart card technology for bank cards is on its way (Kelfkens).

Because of these security issues, the magnetic strip card is less suitable for authentication of eMayor services.

Optical cards

Hendry (2001) mentions the optical card as a way to store information. It is based on the same technique as used in compact disk players. A laser “reads” the little holes in the surface of the card. These cards can store a relatively large amount of information (6Mb), but also have disadvantages. The information on the card can be accessed without further security measures like passwords. Furthermore the cards and equipment are expensive.

The advantage, namely the large storage capacity, is not very relevant for authentication. What is relevant is security, which makes this card less suitable for application in this field.

Memory card

A memory card is defined as: A card with a chip that has a simple logic circuit with additional memory that can be read and/or written (Rankl, 2000). This type of smart card is relatively simple (compared to the smart card) and sometimes called “chip card”. It does not have a CPU but is able to make some small transactions. Big application areas of the memory card are (pre-paid) telephone cards.

The information on this card can easily be read in case the card is stolen or lost. The information is hardly protected which makes it less suitable for authentication.

Smart cards

Many slightly different definitions can be found in literature. Hassler (2001) defines the smart card as follows: “A microprocessor and storage system realized in a microcircuit embedded in a plastic card the size of a credit card. The card operates when inserted into an external terminal device with which it interfaces electrical contacts. Through these contacts, the terminal provides electrical power and communicates with the card processor using a low-speed serial asynchronous character protocol. The basic physical, electrical and communications aspects of the interface have been standardized by ISO/IEC.”

This definition is rather technical, and besides, it does not covers all sorts of smart cards.

The following definition of a smart card is given by Rietdijk (2001):

“A smart card is a plastic card equipped with a chip which provides storage and communication of data between smart card and terminal.”

The next definition adds power supply to it:

“Smart cards are essentially devices that allow information storage and processing, but need to interact with an active device providing the necessary power supply.” (Bolchini, 2003)

In this paper the following **definition of a smart card** will be used, which is a combination of the definitions of Bolchini and Rietdijk:

“A smart card is a plastic card equipped with a chip that allows data storage and processing, and communication of data between smart card and terminal, but needs to interact with an active device providing the necessary power supply.”

As can be seen from this definition, smart cards contain memory and a microprocessor or CPU. Because of its microprocessor power this card can apply more security mechanisms than the other cards and therefore it is more secure. The processor can calculate encryption algorithms.

The memory functions of writing, erasing and reading can be restricted and linked to specific conditions by both hardware and software. The smart card has the ability to compute cryptographic algorithms (because it contains a CPU), which makes them much more secure than the other cards (Rankl, 2000). This security aspect is important for authentication.

Smart cards need reading equipment. Card readers come in different shapes and sizes. These readers can be integrated in computers or provided as separate devices.

Three types of smart cards are: Microprocessor cards, Crypto cards and Contactless cards.

Microprocessor card

The microprocessor card has a contact chip which it uses to communicate with the reading equipment. These cards are applied in sectors where a higher security level is needed, like financial services and in hospitals.

Crypto cards

A crypto card is very similar to the microprocessor card. It contains memory to store information and a CPU which makes the calculation of encryption algorithms possible. The difference between the microprocessor card and the crypto card is that the cryptographic coprocessor of the processor card is substituted by a more advanced one. The improvement in the crypto cards allows public key encryption, whereas microprocessor cards only provide private key encryption (Bolchini, 2003).

Contactless card

This type of card does not have the visible chip because it does not have to be put in a reader. Instead it has to be put on a reader surface (different type of reader as the contact smart card reader) or some cards do not have to make contact with a reader at all. The distance between card and reader can be up to 10 meters. This distance depends on the equipment used. The technology used to make contact between reader and card is called Radio Frequency Identification (RFID). This technique is a bit more complex because it has to deal with some problems like interference between different cards.

This card is often used for efficiency purposes. When a large group of people passes a certain point where the reading equipment is located, the system can register the identities of the passant at once. The system actually checks the *cards* passing the system and not whether the card and the person belong to each other. Furthermore, this type of card raises questions about the privacy of citizens as it feels as if they can be checked everywhere without knowing. For this reason the contactless card is often used for different purposes than the other types of smart cards.

A characteristic of the smart card is the embedded chip in the card. Memory card also have a chip but not the processor power the smart cards have. For that reason the memory card is distinguished from the other smart cards. This computing power makes a difference in the security the card offers because it is this processor power that enables several security protocols and cryptographic calculations. The following table (4.2) depict the differences. The green coloured rows show the different types of smart cards. The blue colour depicts the memory card.

	Plastic card with chip	Contact points	Memory	Processor power (CPU)	Advanced cryptographic coprocessor
Memory card	Yes	Yes	Yes	No	No
Microprocessor	Yes	Yes	Yes	Yes	No
Crypto card	Yes	Yes	Yes	Yes	Yes
Contactless card	Yes	No	Yes	Yes	No

Table 4.2 Differences between several types of cards

Hybrids

Another possibility is to combine different technologies in one card. An example of a hybrid is a card with a magnetic stripe and a chip. Also other combinations are possible. In this way the advantages of the different techniques can be combined to get the best result (synergy). An example of a hybrid card with a chip and a magnetic stripe is included in figure 4.2. An important aspect is that the hybrid card has to contain some logic that determines which of both techniques is applied first. This will depend on the use of the card and the required level of security. Sometimes cards are hybrids because of changing standards and the difficulty to change the system at once. Both techniques will be in use till the system totally adapted to the new technology.



Figure 4.2 A hybrid card with on the left a chip and on the right a magnetic strip

Digital signature

A digital signature is usually based on public key cryptography. To understand what a digital signature actually is, *public key cryptography* needs to be explained.

A user “A” will get a private key (also called “secret- key”). He is (should be) the only one that has this key and keeps it secret. A message encrypted with this private key can only be sent by user A. To read this message another user “B” needs to have A’s public key. B can also use this key to encrypt messages and send it to A. A is the only one that can decrypt this message. B encrypts this message with his private key, so A knows the sender was B (A needs to have B’s public key).

The encrypted message from A is A’s digital signature, because it is encrypted using his private key and it can only be made readable by using A’s public key.

Everyone that has A’s public key could read A’s message. A can send his public key to a person he wants to communicate with, or publish it, so everyone can read his messages or use it to send him a message.

The following figure (4.3) depicts the encryption of data using A’s private key (gu.edu.au). The plain text data is encrypted by the private key. The public key can be used to decrypt the encrypted text into plain text. The purple paper in the figure is the encrypted text.

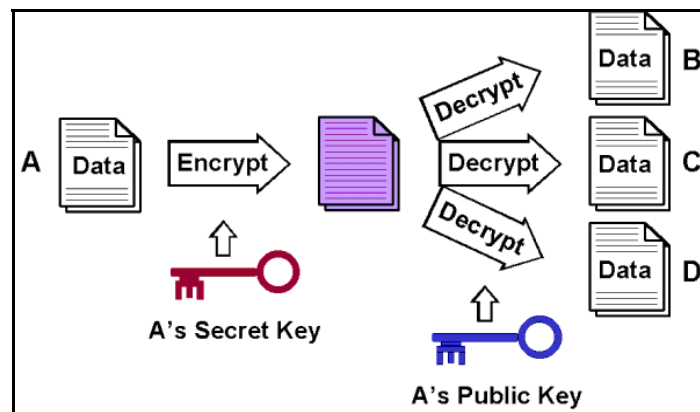


Figure 4.3 Encryption of data used A's private key (private key = secret key)

Persons B,C and D can use A's public key to encrypt a message meant for A. Only A can read this message as he is the only person possessing his private key. This can be seen from figure 4.4 (gu.edu.au)

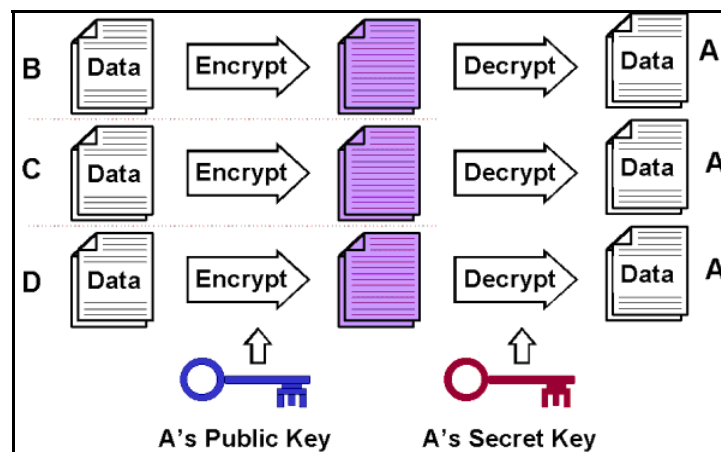


Figure 4.4 Decryption of data used A's public key

In the situation mentioned above, it is not sure whether the key actually belongs to the person who claims it is his key. C could pretend to be A, to gain (confidential) information mentioned for A. He can publish his own key and state that it is A's key. In this case people might respond to C while they actually think it is A.

To avoid that a third user "C" pretends to be A, the public key needs to be build into an "certificate". The certificate is issued by a trusted party (called a Certificate Service Provider). This party has to be trusted by the users so they know that A's public key is authentic. The certificate contains the following:

- A public key
- A name (of user A but this can also be a computer or organisation)
- A validity period (the time the certificate is valid)
- The location of a revocation centre (this URL site contains a list of certificates that are expired or revoked, and is managed by the Certificate Service Providers)

There are two Certificate Service Providers (CSP) in the Netherlands that can deliver high quality certificates, namely PinkRoccade and Diginotar.

In a Public Key Infrastructure (PKI), the certificate issuer is called a Certificate Authority (CA). This certificate authority is a trusted party that issues certificates and updates the Certificate Revocation List (CRL). This list contains the certificates that are expired or revoked.

Certificates exist in different quality levels. This depends on a couple of factors: the technology used to compute the key (the encryption algorithm used to make the key) and the status of the CSP. For example user A can act as a trusted CSP, however this is not as safe as when an official CA issues the certificates. The law on digital signatures (Wet Elektronische Handtekeningen, May 8th 2003, implementation of the European directive 1999/93/EG) distinguishes between two types of certificates: an advanced certificate and a not-advanced certificate. The advanced certificate has requirements on the quality (like the chosen encryption algorithm), that are comparable with PKI quality. The not-advanced certificate has less quality requirements. The law states that this type of certificate can be used when parties agree with each other on the use of this less secure type of certificate. In cases of disagreement about the security level, a judge has to decide in court.

A certificate can be saved on a computer's hard-disk or on a smart card. The latter option is the most secure. This is because the computer can more easily be accessed by unauthenticated users and viruses can attack the computer. In case the certificate is saved on the computer, the computer has to be secured. This is usually done by the use of passwords. Furthermore, computers are located in an office or house, which gives them physical protection. However, this does not protect it from other people that have access to the building. Moreover, a citizen needs to have his own computer to access municipal services, because certificates can not be stored on computers in public places (e.g. internet cafes). For this reason, Dutch law on electronic signatures determined that, to be "safe", the certificates have to be stored on a smart card (justitie.nl and wetten.nl).

Although the storage on a smart card is not 100% secure either, it is more secure than the storage on the hard disk of the computer. A risk of the storage on a card is that the card can be lost.

Certificates issued by a CA in a Public Key Infrastructure are considered to be very safe, however a disadvantage is the high maintenance costs.

4.2.3 Biometrics

The International Biometric Industry Association (IBIA) defined biometric authentication as follows (IBIA.org):

"It is the automatic identification or identity verification of an individual based on physiological or behavioural characteristics. Such authentication is accomplished by using computer technology in a non-invasive way to match patterns of live individuals in real time against enrolled records. Examples include products that recognize faces, hands, fingers, signatures, irises, voices, and fingerprints."

However, different people might have different opinions about whether biometric identification is invasive. For this reason the following definition is used in this thesis: "Biometrics is the automated use of physiological or behavioural characteristics to determine or verify identity". (Nanavati, 2002)

In the current situation the civil servant checks the photo on the passport of the citizen manually to verify the citizen's identity. The "automated use" (in the above definition) means that only computers or machines are used to verify the identity. This has some implications. Firstly, the identification process will take less time. Biometric systems are able to compare thousands of records per second (Nanavati, 2002). Secondly, no human errors will be made. However, some people might have difficulties only being in contact with machines.

Biometrics can be divided in two categories of characteristics: physiological characteristics and behavioural characteristics.

Examples of physiological characteristics used for biometrics are:

- facial characteristics
- hand characteristics
- fingerprints
- iris characteristics
- retina characteristics

Identification using behavioural characteristics can be done by making:

- voice scans
- keystroke scans
- signature scans

The different types of biometric authentication techniques have different advantages and disadvantages. There are three factors determining whether the initial scan will match the same person later in the verification process. These are (Nanavati, 2002): *changes in a user's biometric data*, *changes in user's presentation* and *changes in environment*. The latter one can be caused by variations in background light, noise, etc. Changes in a user's biometric data are changes to what is measured: e.g. a voice or a fingerprint. Examples of situations that cause those changes are sore throats, scars, change of body hair (beards), weight changes and surgery. Another factor that can cause a mismatch is a change in user representation. Putting the finger on the reader in a different angle, change in the distance between face and camera, speaking at a different tone.

Some biometric scans are more susceptible to those changes than others. The different scans and their characteristics are as follows (Nanavati, 2002):

Physiological characteristics:

- Facial scans. This scan is made by standing in front of a camera. The facial scan is not the most secure authentication technique because both the changes to the biometric data as well as changes to the environment hamper the recognition of a person. When a person makes changes to his/her face, e.g. facial hair, glasses, scars and aging make facial scans less reliable. Furthermore lighting and background composition make identification harder. However there is a lot of experience with the use of this technique.
- Hand scan. The hand has to be put on a reader. This reader measures the height and width of the hand and fingers. The hand scan is relatively secure, however subject to changes of biometric data when the citizen has some job or hobby that damages the hand.
- Fingerprint scan. Same as for the hand scan, taken on a reader. The fingerprint is relatively secure, but subject to changes of biometric data when the citizen has some job or hobby that damages the hand. Advantages are that this technique is not expensive, mostly perceived as non intrusive and there is a lot of experience with the use of fingerprints.
- Iris scan. The iris scan is a scan of the coloured part of the eye. The camera comes pretty close to the eye which might be experienced as intrusive. Also the person has to stand in the right position to be scanned correctly so this technique is more than moderately susceptible to changes in user representation. However this is a very safe way of authentication, because the chances of changes in the biometric data and of the environment are very small. The difficulty with regards to the iris scan is that it is a patented technology, which means that governmental organisations are stuck to private organisations and costs are higher than for other authentication techniques.
- Retina scan. This scan checks the blood vessel pattern on the back inside of the eye. To scan the blood vessel pattern a light has to be shone in the eye. The changes to the user representation are challenging to get the person in the right position to make the scan. But overall this is a very secure authentication mechanism.

Behavioural characteristics:

- Voice scan. The analogue pattern of waves is made in a digital code. The voice can be recorded by a recorder. It is medium safe, as the voice record is subject to changes in voice by smoking or a cold, emotion and stress. Furthermore, background noises can hamper the scan. So both changes in user representation and changes in the environment can cause mismatches. This scan is convenient and not intrusive.
- Keystroke scan. This scan records the patten of typing, the speed, the time the person holds a key and the time between keystrokes. This technique is medium save, because it is not susceptible to environmental changes but it is not clear whether changes come from change in biometric data or from user representation. Furthermore, typing patterns can change and also different types of keyboards influence the pattern. An advantage of this technique is that it makes use of broadly used hardware, so less new equipment has to be developed and bought.
- Signature scan. Copies a signature and compares it to the stored signature. Also the stroke order, speed and pressure are measured. This technique is medium save because signatures can change over time.

Also combinations of biometric authentication techniques are possible for identification. A initiative of the Dutch government is to apply a passport with a fingerprint and a facial scan. This is because it is very hard for impostors to conquer two biometric scans. The Dutch government wants to be consistent with the European plan for passports, for that reason the facial scan is chosen. Furthermore, to improve the level of security, the government decided to add a fingerprint. Two different authenticators make it more difficult to compromise the information. More about this Dutch passport initiative is described in chapter 5 “Authentication Initiatives”.

eGovernment services should be scalable because no citizens can be excluded. Although there are many biometric authentication initiatives, fingerprint scans and facial scans are the only techniques applied on a large scale. Because of the lack of experience in the other techniques these might not be very suitable for large scale application and thus for authentication of the two eMayor services in the Netherlands.

4.3 Conclusion on research question 2 and 3

In this chapter research questions 2 and 3 are answered:

2. Which techniques for authentication can be found in literature?
3. What are the advantages and disadvantages of these authentication techniques?

The previous section pointed out that there are some advantages and disadvantages of the use of passwords or PIN- codes for authentication. A disadvantage of the PIN and password is that they are not very secure. Not only because it is only “something you know”, but also because passwords are easy to compromise.

The chance that a 4-digit PIN is guessed in three times is 0.66%. This is not very high. However there is a difference between the technical and the social aspect of the passwords and PIN. Technically the chance that a password or is compromised is not very big. Although special password cracking software can be used to crack this, a large computing power is needed when the passwords are more complicated. The largest risk to passwords and PINs is the social aspect. Users write passwords down, share them and store them in non- secure places. This can be prevented by making the users aware of the issues concerning password security. Also, forcing the user to change password frequently and forcing users to choose more difficult combinations of numbers, letters, capitals and symbols will help preventing fraud. The combinations should not be too difficult, as this enforces people to write them down.

An advantage of the use of passwords or PIN- codes is that they are relatively affordable. No extra cards and readers have to be bought and installed. Furthermore only simple software will be used. This makes it easy to implement. Lastly, citizens are comfortable with the use of passwords and PINs because of years of experience and use. The acceptance of this technique is high.

Because passwords usually have more characters than PINs, passwords are more secure. Of course, this is only the case when users use the passwords properly; no sharing, writing down or simple combinations like names or dates of birth should be used.

Different families of cards exist, each having their own advantages and disadvantages. The embossed card does not need electricity or a telephone. It produces a big paper flow, which makes it less suitable for large scale application. Furthermore it is not digital. For these reasons this card is not suitable for authentication of the two eMayor services.

The magnetic strip card has limited storage space and is subject to copying the information. Furthermore, the magnetic strip card is subject to magnetic fields, which could delete (parts of) the stored information (Hendry, 2001). The optical card has a large storage capacity but is less secure than the smart card. The memory card is very useful for simple transactions. It has some memory capacity in which it holds the user's information and where it can store information. Therefore it is useful for telephone booths but less suitable for authentication.

There are different types of smart cards. The contactless card is often used for efficiency purposes. A large group of people can be checked at the same time. However, this causes privacy issues.

Microprocessor smart cards have a CPU or microprocessor which makes it possible to calculate more difficult encryption algorithms. They also have a larger storage capacity. This type of smart card is very suitable for the transactions which require higher level of security. An even higher level of security is offered by the crypto card, which has a more advanced cryptographic coprocessor than the microprocessor card.

Lastly digital signatures and certificates are mentioned as an authentication technique based on "something you have". They come in different security levels, but the PKI standards are considered to be very safe. Especially when the certificate is stored on a smart card, this technique is very secure. Nevertheless, this maintenance cost (management of the keys, certificates and the CRL) are high.

There are a couple advantages of smart cards over passwords. Smart cards are often used in combination with passwords or PINs. This combination provides higher level of security, because it combines something you know with something you have. Furthermore smart cards can have more advanced security mechanisms. Passwords are easy to crack. Dictionary attacks, social engineering or just the way users treat passwords makes them not very trustworthy.

Anyway, smart cards are more expensive. To use smart cards, reading equipment is necessary. PINs and passwords are also less secure than PKI certificates, but these are cheaper.

Most types of biometrics provide a higher level of security than passwords and cards. The possible problems with these two authentication techniques are described earlier. Biometric identifiers can not be forgotten, stolen or shared. A person always carries them around. According to Nanavati (2002), biometric identifiers also provide increasing convenience. A person does not have to carry around a card or does not have to remember a password. Also for the system (administrator) this saves the burden of storing and securing all the passwords. The factor causing the high administrative burden for passwords is the helpdesk and the work of the administrator. This is because people can forget their passwords. Biometric characteristics have to be saved but this is done only once because it is not possible to forget the biometric characteristic.

In addition, biometrics is a good technique to prevent certain types of fraud. Some people use multiple identities to use public benefits. Using biometric information the database can be searched for the same biometric information. In this way it is not possible to register twice under different names.

Another form of fraud is "look-alike" fraud. Using a passport of another citizen who looks like the picture in the photograph a person can pretend to be someone else. Biometric identification will make this harder.

Some people are concerned about their privacy when their biometric characteristics are copied and stored. Especially unauthorized storage and usage are concerns. The risk of privacy invasiveness is depending on a couple of factors: the owner of the biometric data (user or institution), the duration of the project, the place where biometric data is stored, the type of biometric (physiological or behavioural) applied and the question whether biometrics are deployed in the public or the private sector.

However, some state that the use of biometrics provide privacy (Woodward, 2002). For example, when a password is compromised the user can loose information or money, even without knowing. Biometrics make identity theft harder.

Furthermore, the use of biometrics for access control can keep intruders away from personal information. Because of the privacy issues and because the technique is not used as broadly as the other alternatives (password and card) the user acceptance is not as large yet. This will probably change after people get used to the technology.

The systems needed for most types of biometric identification cost more money than password or smart card technologies. The price of the equipment drops which makes large scale application in the future possible.

There are many trials with biometric characteristics done, but hardly any with very big databases of persons participating. This means there are no results of such trials, which makes it difficult to apply these biometrics on a large scale. The only biometric identifier applied on a large-base with enough accuracy is the fingerprint (CWI, 2003). This makes this technique the only suitable biometric authentication technique for nationwide used eGovernment applications.

This results in the following table (4.3) containing the most suitable techniques and their advantages and disadvantages.

Technique	Advantage	Disadvantage
PIN	Affordable, easy implementation, high usability and acceptance/trust	Low level of security
Password	Affordable, easy implementation, high usability and acceptance/trust	Low level of security
Smart card	Secure, usable	Cost
Certificate	Secure, suitable substitute for hand-written signature	Cost
Fingerprint	Secure, not possible to forget, enough experience to use for large-scale applications	Cost, low trust/acceptance (privacy issues)

Table 4.3 Suitable authentication methods and their advantages and disadvantages

5. Authentication Initiatives

In the following section (5.1) an overview of some Dutch authentication initiatives will be given. This overview gives an indication of the current state of development and implementation of authentication techniques in the Netherlands. It has to be stated that these are some of the important authentication initiatives, but the list is not exhaustive.

In paragraph 5.2 the answers to research questions 4, 5 and 6 will be given.

5.1 Dutch initiatives

2b or not 2b, Biometric characteristics in passport

2b or not 2b is initiated by Minister de Graaf (“Bestuurlijke Vernieuwing”). The test started September 1st 2004, citizens in the following six municipalities are able to participate in this initiative, namely Almere, Apeldoorn, Eindhoven, Groningen, Rotterdam and Utrecht. 15.000 participants are needed. The International Civil Aviation Organisation (ICAO) decided that a facial scan should be added to passports. However, the European Union decided that that is not reliable enough and decided to add a fingerprint. The Dutch passport will contain a finger scan and a facial scan. However, the citizen can not take the passport home, it is only used for the tests. The experiment consists of tests with recognition equipment. The goal is to determine the usefulness of biometrics in the passport. The experiment ends at February 28, 2005. (minbzk.nl 02 and BPRBZK.nl 02)

This experiment is a way to test the equipment needed for the use of biometrics. However, the technology is not developed far enough to consider this an alternative for authentication of the two eMayor services.

Biometric identification at Schiphol airport

Frequent flyers at Schiphol can use iris scans to save time at the customs. By scanning their iris, these passengers do not need to show their passports. The passengers will get a Privium card, on which these biometric characteristic is stored. The card has to match the iris to give access to the gates.

This initiative is very useful for this purpose (small-scale authentication). Passengers are identified and authenticated while they actually save time at the customs. This technique is expensive and not yet applicable on a large-scale. Therefore it is not suitable for authentication of “certificate issuance” and “change of residence”.

Dutch municipal initiatives

Some municipalities initiated their own authentication mechanism. An example is the municipality of The Hague (www.denhaag.nl). This municipality is far with the development of online services. The Hague performs several initiatives to become the municipality with the best customer service in 2007. An initiative called “het Glazen Stadhuis”, makes online services possible. These online services are accessible using password & username authentication. To accomplish that citizen will be able to access services online, several studies have been carried out. The Raad van State made an analysis of the legal implications of the online services. Not all services can be offered online, as the law prescribes citizens to identify at the town hall for some of the services. According to the legal study the following services can be offered online: certificate GBA, certificate BS, applying for marriage. Services that The Hague will offer online, but which legally have to be applied for on paper are: change of postal address, change of name (geslachtsnaam), re-burial at another place or cremate (after burial has taken place) and make changes in the GBA (like change of address). For these services research will be undertaken to find out which actions have to be taken to offer the service online.

Another study carried out by Deloitte (Eikenboom, 2004), concluded that the interests of the citizens in The Hague closely matches the services this municipality is interested in offering.

The Hague aims at services that are used frequently. They used the following argument: using the lowest level of security (which is the most affordable), which services can this municipality offer? It turned out that the most affordable services like certificate BS and GBA are also the services most requested for. In the near future the above mentioned services will be offered online (Douma, interviewee).

The Hague is not the only municipality offering electronic services. Other municipalities that run in front in the Netherlands are Dordrecht (www.dordrecht.nl), Enschede (www.enschede.nl), Hoorn (www.hoorn.nl) and Tilburg (www.tilburg.nl). Examples of services that the municipality of Hoorn offers online are: change of address, reservation of marriage facilities, certificate GBA. The municipality of Enschede offers services online and participates in the NAV/DigiD initiative, a trial started on July 13th. The municipalities of Dordrecht and Tilburg also offer certificates (GBA and BS), change of address, possibility to make an appointment with a civil servant, and many other services.

Internet banking

Several Dutch banks offer online payment options. ABN-Amro, Rabobank, Postbank, Fortis are examples of banks that offer the opportunity to pay online. Most of these banks apply systems with (smart) cards. ABN-Amro supplies the online banking users with a smart card and a smart card reader. Fortis supplies its users with a portable reader, which enables the users to use every computer to make their online transactions. Postbank does not use smart cards but supplies lists with codes which have to be used in combination with a password to make transactions.

Banks offer the online banking service to provide better customer service and save money by reducing the paper flow.

Although internet banking is a good way to manage your financial administration, these internet banking techniques are less suitable for authentication of citizens to municipalities. There are a couple of reasons for this. In case governments want to use internet banking techniques, arrangements with many different banks have to be made. This is not feasible. Furthermore, citizens prefer not to use their bank card or credit card online.

Nieuwe Authenticatie Voorziening (NAV)/ DigiD

The goal of the NAV is to provide every citizen with a password & user name combination for many (semi-)governmental services, so citizens will not be given heaps of passwords at all the different organisations. At the moment the log in name is based on the SoFi (social security) number. From January 1st, 2006 the “Burger service nummer (BSN)” will be used instead of the SoFi number. The NAV plans to be available to every citizen on January 1st, 2005. The NAV is an initiative undertaken by several big governmental organisations: Centrale Organisatie Werk en Inkomen (CWI), Informatie Beheer Groep (IBG), the Belastingdienst, College voor Zorgverzekeringen (CvZ), de Sociale Verzekeringsbank (SVB) and the Uitvoeringsinstituut Werknemersverzekeringen (UWV). Also several municipalities are participating. A trial has started in Enschede; citizens are able to access municipal services by using a password provided by NAV. During this trial there are not very many users of the NAV.

There are a couple of reasons the NAV chose the user name & password combination. Firstly, the username and password are easy to implement. Secondly, Dutch citizens do not have a smart card for eGovernment services yet. A smart card is less easy to implement than a password. Furthermore, many citizens are used to passwords, and passwords are easy to understand. A government aim for 2006 is that 65% of all services are available online. The online services should offer the citizen better “customer service”, but not at cost of security. That is why not all services can be offered online when using the NAV password. Some services, like renewing your passport, need a higher level of security. The decision whether NAV is secure enough for a service is up to the organisation that will use it. Therefore there will be difference between municipalities in which services they offer using the NAV.

Citizens can enrol at the NAV-site (www.burgerpin.nl). They have to submit their name, date of birth, SoFi number and address. The password will be sent to the address stored in the GBA. This secures that no other person will get the password. However, some scenarios are imaginable in which some other person might get the password. According to Ghosh this is a very small percentage and for that reason is not significant. There will be checks in the process to prevent fraud as well. An example is charging a fee before the certificate is sent.

The names “Burgerpin” and “NAV” are used interchangeably, but since October 5th the new name of this initiative is DigiD. (Ghosh, interviewee and burgerpin.nl)

The NAV has a few clear advantages and disadvantages. The advantages are that it is easy to implement, that it does not cost very much money and it can be used for all municipalities and semi-governmental organisations.

Although this initiative sounds promising, there are a couple disadvantages. There are hardly any requirements on the password a user chooses. Only numbers and letters have to be used, which easily results in passwords that are easy to guess, like names with a number, e.g. one of the children’s first name with a number. Passwords like that are very easy to encompass.

An other disadvantage is that the password is sent to the home address mentioned in the GBA. Other people at this address therefore have access to this password or could even request the password.

Although the chance that this happens is not very big, there are occasions imaginable that it happens. For example a couple living together but considering a divorce.

Furthermore NAV does not prescribe the services that can be offered using this initiative. This responsibility is up to the municipalities using NAV. This will result in reduced transparency as municipalities will implement this differently, and will offer different services.

Lastly, it has to be noted that it is not yet determined who is going to pay for NAV. The question is whether it is going to be paid by the national government or the individual municipalities/semi-governments. In the latter case it is not sure whether the size of this municipalities matters to the cost.

Elektronische Nederlandse Identiteits Kaart (eNIK)

The former NIK (Dutch Identity Card) will be replaced by the eNIK (electronic Dutch Identity Card).

This is an identity card the size of a banking card. The aim of the card is to make electronic services available in a high quality fashion. The card will only contain information that does not change over time. For example, the name and date of birth of the holder, but not the driver’s licence number. For this reason it is not possible to use it for many different purposes, but the information on the card will always be correct because the information does not change. The card will be a smart card with two chips; one contact chip and one contactless. The contact chip will contain the holder’s information (name, date of birth, SoFi number), the contactless chip will contain the biometric data of the holder. This implies that for user identification and authentication, the contact chip will be used. The contactless chip has an efficiency function. To give an example, when many people pass a certain point, the reader gets all the signals and knows who is going through in less time than when every person has to put the card in a reader. As described in chapter 4 this raises privacy issues. The contactless chip with biometric information will be used for travelling; the customs can see if an undesired person passes the reader. This initiative is expected to start at the end of 2006. Exact details are unknown because the eNIK design plans not finished yet. (‘t Eind, interviewee).

This card seems a good way to authenticate services that require a higher level of security. A disadvantage is that it will take up to two years before the eNIK card will be available.

ECP framework / e-ok initiative

Many different authentication initiatives exist. The ECP platform developed a framework, to prevent citizens from having multiple cards and passwords. This framework makes authentication solutions

comparable. First, companies that supply solutions assess their technique, using the framework. When another company needs an authentication solution they can access the results of the assessment and compare it to other solutions. Also, they will compare it to their own needs. In case there is a match, the searching company can contact the company with the best solution and make arrangements to implement it.

When more authentication solutions are “recycled”, the citizen can use the same smart card for multiple solutions. This will make an overload of mechanisms, smart cards or passwords unnecessary.

The ECP framework offers the opportunity to make different authentication initiatives comparable by offering the framework.

This initiative is very useful as it makes different methods comparable and provides understanding of the security level of these initiatives. Furthermore, it aims to stimulate reuse of existing authentication methods, which prevents the growing number of different cards and passwords users have to remember. It has to be remarked that the methods are scored by the organisation that provides this method. Therefore it is questionable whether the e-ok framework is reliable. Although there will be committee investigation complaints, not all methods are checked.

PKI Overheid

PKI Overheid is an initiative by the Dutch national government. It aims to establish a PKI infrastructure for communication with the government and between governments.

This PKI infrastructure is a system of architecture, technique, management, procedures and rules based on public key encryption (PKIoverheid.nl). Emphasis is put on *reliable* communication.

This initiative facilitates secure communication and authentication. Though it is an expensive method.

5.2 Conclusion on research question 4, 5 & 6

In this paragraph the following research questions are answered.

4. Which Dutch authentication initiatives are currently initiated?
5. Are current Dutch authentication initiatives useful for the eMayor services?
6. Is the suggested authentication technique of the eMayor project suitable for Dutch municipalities?

Research Question 4:

In this chapter described several authentication initiatives, such as NAV/DigiD, internet banking, eNIK, 2b or not 2b, iris scans at Schiphol airport ECP/e-ok initiative, PKIoverheid and some municipal initiatives. The most important initiatives will be described under research question 5.

Research Question 5:

Many organisations are currently occupied with the topic of authentication of users. Therefore there are many authentication initiatives.

As described above, eNIK can be useful for the authentication of services that require a higher level of security because it aims at providing citizens with a identification smart card. However, it will take two years before it will be available.

NAV/DigiD is useful for the authentication of services that require a low security level. This password based initiatives aims to provide citizens with a password they can use for multiple governmental organisations. Furthermore it will save individual organisations money as they do not have to develop an authentication implementation themselves.

PKIoverheid

PKI makes the use of digital signatures and certificates possible. These are necessary to substitute the hand-written signature.

Research Question 6:

The smart card is suitable for services that require a higher level of security.

A problem is that we do not have a national authentication smart card yet. The eNIK is expected in 2006.

This Dutch Identity card could be used for authentication of services that require more security than a password can offer.

Furthermore, some services require a digital signature. These can be stored on the smart card.

eMayor suggests the use of smart cards. The answer to this research question therefore is: yes, but only after the eNIK is introduced, which will be at the end of 2006.

6. Selection of authentication techniques

A selection framework is designed in this chapter. This framework will facilitate the selection of an authentication technique for the services “Change of residence” and “Certificate issuance” in the Netherlands. Selection criteria have to be chosen to determine which authentication mechanism is the most suitable. These criteria are determined by studying literature and articles on this topic and information gathered in interviews with civil servants and security experts. The selection criteria are summed up in paragraph 6.1. Paragraph 6.2 contains more information on the differences in security levels distinguished for services. Legal implications on the selection of the authentication techniques are also explained in this paragraph. Then, the general framework for selection of authentication techniques is presented (6.3). This framework can be used to score the authentication techniques using the criteria defined in paragraph 6.1. In paragraph 6.4 the selection framework will be applied for the two eMayor services in the Netherlands. A reflection on this framework is given in paragraph 6.5. This reflection is based on interviews with experts in the field of security and governments. Lastly, in paragraph 6.6 research questions 7, 8 and the main research question will be answered.

6.1 Selection criteria

The following selection criteria are found. This is a general list of criteria for the selection of an authentication technique. In the next paragraphs the difference in importance of several criteria for the two eMayor services will be explained.

- **Cost.** There are different types of cost: cost of implementation, cost of maintenance, initial cost. Cost can be distinguished between the parties that actually have to pay. Especially municipalities do not have a large budget for these developments (Douma). Furthermore, this criterion is also important because it is (a part of) the aim of eMayor to be cost-effective.
- **Ease of implementation** (Douma). Do the municipalities need specialised knowledge they do not have? Does it cost much time to implement?
- **Level of security.** Depending on the service requested by the citizen a level of security is needed. Some services require a higher level of security than others. The level of security determines the requirements of the security techniques. This criterion is also part of the aim of eMayor. More about this criterion is described in paragraph 6.3
- **Interoperability/standardisation** (ECP.nl). In the growing development of the European Union it is important to gear to development in the *EU*. Furthermore it is important not to get too many different initiatives within *the Netherlands*, so people will not have multiple cards/passwords. Money can be saved by using the same techniques again. To be interoperable with the other eMayor municipalities it is interesting to consider which technique they use. This criterion is also part of the aim of eMayor.
- **Ease of use/ usability.** Usability is important because eGovernment aims to provide better service to the citizens. If the ease of use is low, citizens will not use the offered services, which makes them less useful.
- **Level of trust/ Acceptance.** An important aspect is the level of trust the citizens have in the system. People will not use the online services when they do not trust the system, and will not send their (personal) information online. For this reason it is important that the citizens feel comfortable with the system. Furthermore, is the authentication technique an accepted technique? If not, (some) citizens will not make use of it.
- **Scalability.** Scalability concerns the size of the group of users that are able to use the authentication technique. It also involves the ease in which a group of users can be enlarged to

make use of the service. The Netherlands have 16.3 million inhabitants (CBS.nl 02) which requires a large group to be able to use the technology. Since governmental services are studied in this thesis, no one can be excluded and therefore the authentication technique has to be scalable.

The criteria will be used to design a selection framework which is presented in paragraph 6.3.

6.2 Level of security & Legal implications

Most services require a certain level of security. For some services this level is higher than for others. In the Netherlands, the tendency is towards using different authentication techniques for different security levels. Some services need a high level of security and can not be offered at a lower level of security. An example of a service that requires a high level of security is the issuance of a new passport. Although a high level of security could serve more services, this is unnecessarily expensive and complicated. The request for a certificate requires a lower level of security.

It has to be noted that the trend towards different authentication techniques for different security levels, is in contrast with other initiatives, namely to stop the expansion of all kinds of different initiatives resulting in people having multiple passwords and cards.

It is difficult to determine which security level a service needs. Several Dutch initiatives determined different security levels. NAV/DigiD made a distinction between four different security levels, namely: zero, low, middle and high. Level zero does not need an authentication method. An example of a service in this category is the ability to send an e-mail. Level low is the level supported by the DigiD; a password and username combination. Medium level can be offered with PKI software (digital certificate stored on the hard-disk of the computer). The highest level could be provided with PKI in combination with a card (digital certificate stored on a card). This could be served by the PKIoverheid initiative in combination with a eNIK card.

ECP also has its own level of security scheme, in which three levels are described, namely: low, medium and high. ECP states that two factors determine the strength of the authentication technique. The first is the security or reliability of the technique itself. The second is called the life-cycle of the authentication technique. This refers to the processes during the life-cycle of the authentication technique. The ECP-framework enumerates several processes related to the life-cycle and security of the authentication technique. For every process different options are mentioned that provide “low”, “medium” or “high” scores. However, it is not clear how the distinction between the different levels is made. In other words it does not state why a certain process scores “high” and another “medium” or “low”.

In this thesis the different security levels are based on the following (this categorisation is also supported by surfnet.nl):

- A low level of security is provided by techniques that are based on “something you know”
- A medium level of security is offered by techniques that are based on “something you have” (preferably in combination with “something you know”)
- A high level of security can be obtained by the use of techniques that are based on “something you are”

The following figure demonstrates this division (figure 6.1):

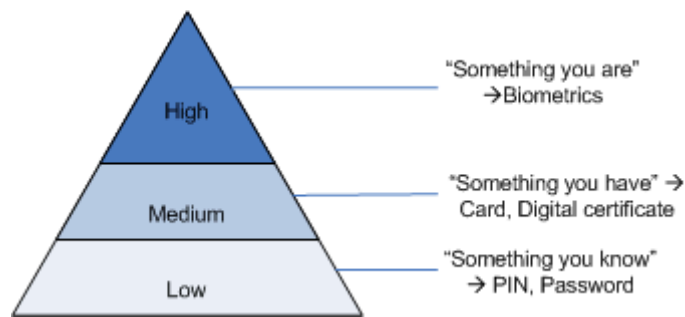


Figure 6.1 Three security levels

Three security levels are distinguished, namely low-medium-high. An argument could be whether there is a fourth level “zero”. This would be the same as the level zero defined by the NAV/ DigiD. This level does not need an authentication technique and therefore is less interesting in this thesis.

A service determines the requirements of the security. This depends on the “damage” in case of fraud. The possible damage depends on the risk of fraud and the size of the damage/ consequences in case of fraud. This damage can be expressed in material and non-material damage. Material damage could be the loss of money caused by the fraud. Non-material damage could be the damage to someone’s image or leaked out information.

The risk of fraud and the consequences are influenced by the difficulty to practise fraud (e.g. determined by the process steps in the service) and the value of the fraud for the person practising fraud. Some services might be subject to legal requirements.

The two eMayor services both have relatively simple processes as can be seen from the process descriptions in chapter 3 and the UML models in appendices 8 to 12. Only passport identification is required in the current situation. The information the citizen fills out is checked by the civil servant to determine whether extra research on the information is required. Change of residence also requires a (hand-written) signature on the request.

Both change of residence and certificate issuance offer some risk of fraud. The risk on fraud is not high because the advantage gained in case of fraud is pretty small. These statements are supported by a risk analysis carried out by de Raad van State. De Raad van State researched made a risk analysis and concluded that the risk is small.

These findings are also supported by other initiatives. NAV/DigiD and the municipality of the Hague suggest to offer certificate issuance at security level low.

However, laws apply on the services. The service Change of residence needs a signature (law 4:1 Algemene wet bestuursrecht (Awb) and article 65,66,68,80,81GBA), which makes it impossible to be served with a PIN or password.

The law on digital signatures (Wet Elektronische Handtekeningen) determined that a digital signature can substitute these handwritten signatures. This law states that, under certain conditions, a digital signature can substitute the hand-written signature. This signature can be offered in two fashions. Firstly, organisations can make arrangements with each other and state these in covenants. This is done between municipalities and organisations. This however seems not feasible on such a large scale with all citizen. Secondly, the certificate has to fulfil certain requirements e.g. for computation and the storage and creation of the signature. These requirements determine that a smart card is needed for the secure creation of the key. this means that for the service “Change of residence” the medium level is required.

The services that require a low level of security are the services requested for most, according to BKWI. 80% of the transactions can be offered at this level. This 80% is not 80% of the different types of services but actually 80% of the transactions. The percentages for higher level authentication are higher, more transactions and services can be offered. A large percentage of the transactions can be done by low level

authentication; medium and high level authentication add extra services to this. These are actually relatively small contributions. Although these contributions are small, they are required in case services are offered that require a higher level of security.

According to the study by de Raad van State the following services can be offered within the lowest security level: certificate GBA, certificate BS, applying for marriage. Services that The Hague will offer online, but which legally have to be applied for on paper are: change of postal address, change of name (geslachtsnaam), burial at another place or cremate (after burial has taken place) and make changes in the GBA (e.g. change of address). For these services research will be undertaken to find out which actions have to be taken to offer the service online. However, some other municipalities like Tilburg, Hoorn and Enschede also offer change of address online. From the study by de Raad van State actually turned out that this is not legal.

For this can be concluded that municipalities not employ the same rules to determine whether services can be offered online (and under which conditions they are offered). Municipalities have their own (illegal) initiatives to be able to offer services online.

The security levels determine the minimal required security level. After the minimal level is determined, the techniques are scored to determine which one is preferable. For example, in case the service needs a security level “low”, all techniques could be applied for this service. Then, it depends on the criteria (paragraph 6.1) which technique is the most suitable. So the security level and the legal aspects are preconditions.

This selection can be made by the use of the framework presented in the following paragraph.

6.3 Design of the selection framework

A framework for the selection of an authentication technique is presented in table 6.1. This framework makes it possible to easily score several authentication techniques using the criteria that are determined in paragraph 6.1.

Description of symbols and meaning of the **Framework**:

The framework is based on two evaluation methods: the score card and the SMART method (Simple Multi-Attribute Rating Technique) (Bots, 1998). As the name might seem to suggest, the SMART method has nothing to do with a “smart card”.

These two techniques are both used to score alternatives using criteria. The score card method uses colours, that show the order of importance of the alternatives. The SMART method also adds values to the criteria because some are more important than others. A higher number indicates that this criterion is more important. These values combined with the scores of the alternatives will result in a row with the total score and in a row with an order of importance.

The framework lists the alternatives horizontally and the criteria vertically. Parallel to the column with the criteria is a column with the values. The two bottom rows are used to show the score of an alternative. The first one shows the total score, the second one the order of ranking compared to the other alternatives.

The alternatives are scored using +1, 0 and -1. In this scale +1 means that this is the most positive score. -1 is the worst score. For example, +1 does not mean the highest cost but the best score at the criterion cost, so the lowest “cost”. This might be confusing, but in this way the simplest overview is given which authentication technique scores well. For a better visual representation colours can be added to the scores in the framework. Red is used for low scores, yellow for scores in the middle of the spectrum and green for high scores.

For the values a range from one to four is used. A higher score indicates that this criterion is considered to be of higher importance.

Service:														
Security level:														
	Value	PIN (4-digit)	Password (min 6 letters, symbols, numbers)	Memory card	Smart card	Certificate	Fingerprint	Hand	Face	Iris	Retina	Keystroke	Signature	Voice
Cost		+1	+1	0	0	0	-1	-1	-1	-1	-1	-1	-1	-1
Ease of implementation		+1	+1	0	0	0	-1	-1	-1	-1	-1	0	-1	-1
Security		-1	0	0	+1	+1	+1	+1	0	+1	+1	+1	+1	+1
Interoperability NL		-1	+1	0	0	0	-1	-1	-1	-1	-1	-1	-1	-1
Interoperability eMayor		-1	0	+1	+1	+1	-1	-1	-1	-1	-1	-1	-1	-1
Usability		+1	+1	+1	+1	+1	0	0	0	-1	-1	+1	0	+1
Trust/ Acceptance		+1	+1	+1	+1	0	0	-1	-1	-1	-1	-1	-1	-1
Scalability		+1	+1	+1	+1	+1	+1	-1	-1	-1	-1	-1	-1	-1
Total score →														
Order of ranking/ importance →														

Table 6.1 Authentication alternatives and criteria framework without value

6.4 Selection of authentication technique in Dutch situation for two eMayor services

In this paragraph the framework will be filled out for the Dutch situation. In paragraph 6.4.1. the alternatives that are mentioned in the general framework are considered whether they are suitable for the Dutch eMayor situation. This result in the framework for the Dutch situation. In paragraph 6.4.2 this framework is filled out and scored. In paragraph 6.4.3 the results are presented.

6.4.1 Alternatives that will not be considered

“Certification issuance” requires a low level of security and “Change of residence” the medium level. Since both services do not require the same level of security, they are scored in different tables (table 6.2 and 6.3).

There are more important criteria to score the authentication technique on. One criterion is a *precondition* for the authentication techniques used for governmental services, namely *scalability*. This is because for governmental services a large group needs to be supported and nobody can be excluded. The general selection framework (table 6.1.) is filled out for the situation of the two eMayor services in the Netherlands. Which criteria and alternatives are considered for this situation is explained in the following section.

The different authentication mechanisms will be scored in a table using the above described criteria. However, some authentication techniques are not suitable in the current Dutch situation. Alternatives that will not be considered are: the embossed card, magnetic strip, optical card, contactless card and many of the biometric authentication techniques.

The *embossed card* will not be considered. There are a couple of reasons for that. Firstly, the embossed card brings about a large stream of paper work. The technique is not digital, which is a requirement for online transactions. Secondly, the information of the citizen is embossed on the card, which does not offer any privacy. The information can be read for the card as soon as someone holds it in his hand. For these reasons the embossed card is no option for secure online authentication for municipal services.

The *magnetic strip* card has some difficulties that make this alternative not suitable too. This card is not as secure as, for example, the smart card. This is because information can easily read from the card.

The *optical card* has a lot of storage capacity. It is difficult to protect this information. Furthermore it is the question whether so much storage capacity is needed for authentication. This technique is not an option either.

The *memory card* is not considered because the smart card is considered to be a better alternative. Although the memory can is slightly cheaper, the difference is not big as the required card and reading equipment is still necessary. Moreover it is less secure than the smart card.

The *contactless card* is often used for efficiency purposes. Because it actually authenticates the card instead of the user, it is not an option for authentication of the user for the use of the two eMayor services.

Many of the *biometric* authentication techniques are still in an early stage of development. There is no experience with large scale trials and therefore no results. For this reason many biometrics are not available for large scale utilization. The only biometrics tested on large databases of people are the fingerprint and the facial scan (CWI, 2003). The facial scan is not accurate enough (CWI, 2003). For this

reason the only biometric considered is the fingerprint; all the other biometrics will not be included in the framework for eMayor.

6.4.2 Values in the framework

Cost:

Value: Cost is an important criterion. Municipalities often have small budgets for innovation (Douma). Therefore the value for this criterion is high.

Score: The cost of PIN/password are very low. A helpdesk and the administrator are the only factors really causing any cost. The production and implementation cost are very low for PINs. This is because the only required equipment is a computer with special software for the PIN/password, and the eMayor platform.

Microprocessor cards are more costly than the PIN/password. Several reason are: the necessary card reading equipment, the card issuer and a certificate authority. The cards themselves have to be produced, which is done by the card issuer. These extra facilities make the cards more expensive than the PIN/passwords.

Certificates are more expensive than passwords. The maintenance cost are higher, because of the management of the certificates and keys.

To make fingerprint authentication work, there needs to be an organisation taking the biometric identifier and recording it. Furthermore a certificate authority is needed. A fingerprint reader is necessary. The storage of the prints needs good security. The fingerprints are used for year now, which makes the equipment less expensive as it used to be. However, this alternative is more expensive than passwords or smart cards.

Security:

Value: Level of security is very important. The personal information has to be secured. However it is important to note that the required level of security depends on the service delivered. The services researched in this thesis therefore do not have the same values. The value for change of residence is higher as it requires a higher security level.

Score: The required security level causes the distinction between the two tables (table 6.2 and 6.3). The certificate issuance table can be offered at security level “low”. Change of address requires security level “medium”. Some services require higher security levels than others. For these services security is of higher importance than for services that do not require a high level of security. This implicates that the value for this criterion changes as the security level changes.

The security level that can be offered using password or PINs is the lowest level. Smart cards and certificates can offer more security and biometrics can offer the highest level of security.

Note that every technique invites new risks.

Interoperability:

Score: In this thesis interoperability has two levels: National and eMayor/European. At the eMayor level, there are many countries implementing smart cards. The UK, Belgium, Finland and Italy already have a national identification (smart) card. Spain and Greece adopted EU directive CWA 14890, a directive on Secure Signature Creation Devices (SSCD) for electronic signatures. Smart cards are examples of SSCDs as are USB tokens. However, the eMayor platform aims to support both password as well as smart cards and digital signatures.

At a national level it is important to notice that there are many password and smart card initiatives, however no nation wide used authentication technique is in use in the Netherlands that is suitable for the two eMayor services. The DigiD aims to be a nationwide used authentication technique. This technique uses user name and password combination.

Biometrics are hardly implemented on a large scale in Europe.

Value: Many initiatives will lead to many different authentication techniques. This is not very desirable. Users have to remember many different codes and have to keep different cards. Being interoperable in the Netherlands is less important than being interoperable with the platform.

Ease of implementation:

Value: The ease of implementation is of minor importance. For small and medium sized municipalities it is harder to implement systems themselves because they lack the knowledge or means. The system only has to be implemented once, which makes it of minor importance.

Score: The ease of implementation of the password and PIN is higher than for the smart cards. This is because less facilities are required, e.g. readers. The technique is more complicated and therefore requires educated personnel to be able to work with this technique. There are even more facilities required for biometrics. The biometric identifiers have to be recorded and stored. This makes that this alternative has the lowest score at the criterion “ease of implementation”.

Usability:

Value: Usability is not one of the most important criteria. However, the system has to be usable to be utilized by the citizens. The authentication technique should not be too difficult to use or too intrusive.

Score: The usability is the degree in which the equipment allows ease use of this authentication technique. The password or PIN scores high at this criterion.

Biometrics require more intrusive techniques. Therefore the usability is lower.

Trust/Acceptance:

Value: Trust/Acceptance is of minor importance. Though the citizens have to trust and accept the system to make use of it, this criterion is not as important as security or scalability.

Score: Passwords and smart cards are commonly used and therefore is the acceptance of these techniques high. The acceptance of biometrics is less, this has several reasons: firstly, biometrics not used at such a large scale as other authentication techniques. Secondly, some people experience biometrics as being intrusive. Furthermore, privacy issues cause a lower score at this criterion

Scalability:

Value: The value for scalability is high as it is important that all Dutch (or even European!) citizens need to be provided, and no one can be excluded.

Score: Scalability is a precondition for authentication techniques. A score -1 means that the alternative will not be considered. Most biometric authentication techniques are not scalable because there is no experience with large scale application. Alternatives scoring -1 at this criterion are not considered. The scores 0 and +1 are possible and determine the degree in which it is scalable. The alternatives scoring -1 (many of the biometrics) are therefore not considered for the two eMayor services. The other alternatives are all very scalable.

6.4.3 Results

The best authentication technique for the service “certificate issuance” is the “password”, which scores +10. The score is close to the score for the smart card. That is because the smart card is more secure and better interoperable with eMayor. However, security is of less importance at a low security level. This authentication technique provides a low level of security, which suffices for this service. A criterion which is important is cost. The costs of passwords are low, the lowest of all alternatives (only PIN is affordable as well). Password scores at none of the criteria -1.

Change of residence needs the medium level of security. Actually, the password, smart card and the certificate have high scores. However, the law requires a digital signature as a substitute for the hand-written signature. Therefore this alternative is suggested to use in combination with the smart card for the secure storage and creation of the digital signature. This alternative scores high and complies with the law.

6.5 Reflection on the selection framework

To reflect on the framework, it is filled out by several experts in the field of security and governments. The frameworks can be found in appendix 13. From these frameworks can be seen that there are some similarities and some differences.

Some notes have to be made. The interviewees could not fill out the row for interoperability eMayor since most of them are not familiar with the design of the platform. Only one interviewee filled this row in because he interpreted it as being interoperable on EU level. Because the interviewees could not fill in this row, this row also has to be deleted in the scores made in this thesis as it is not possible to compare them otherwise. This actually did not influence the three best scores.

The six frameworks compared give the following result:

- Three out of six people score the password to be the best authentication technique; two others score the password second best
- Fingerprints score the lowest mark for three times
- The most popular three authentication techniques are: password, smart card and digital certificate

Differences in scores can be explained by the following:

- The scores are influenced by personal preferences and differences in knowledge. Some interviewees gave cost the lowest possible value(1), while others suggested that this criterion is so important it needed the highest score(4).
- The perspectives of the interviewees were not the same, as some were more into governments and others were security experts.
- The framework does not exclude subjectivity

Although there are some differences, the results mostly pointed in the same directions. Therefore the framework is valuable and the suggested authentication methods are maintained.

6.6 Conclusion on research questions 7 & 8

The following research questions will be answered:

7. What are the selection criteria for choosing suitable authentication?

The following research question and the main research question can be answered next:

8. How can a selection of an authentication technique be made?

The following selection criteria are used in the selection framework 6.1: cost, usability, ease of implementation, trust/acceptance, level of security, interoperability and scalability.

The levels of security are defined based on the characteristics of the techniques: level low is based on “something you know”, medium on “something you have” and high on “something you are”. A service determines the requirements of the security. De Raad van State performed a risk analysis on the services

change of residence and certificate issuance. Change of address needs medium security because a digital signature is required. For the service certificate issuance, level low will suffice.

After the minimal security level is determined, an authentication technique has to be selected. Using the criteria a framework is made to score the different techniques and make the required selection.

The best authentication technique for the service “certificate issuance” is the “password”. This authentication technique provides a low level of security, which suffices for this service (Raad van State). The costs of passwords are low. Furthermore, they are easy to implement and the acceptance is high.

“Change of residence” needs the medium level of security. The password, smart card and the certificate have high scores. However, the law requires a digital signature as a substitute for the hand-written signature. Therefore this alternative is suggested to use in combination with the smart card for the secure storage and creation of the digital signature. This alternative scores high and complies with the law.

Although there are some differences in the scores by the experts, it can be concluded that the framework is very useful. The results mostly pointed in the same directions. Three out of six times the experts also score the password best and two times second best. The three most popular techniques are password, smart card and digital certificate.

Service: Certificate issuance						
Security level: low						
	Value	PIN (4-digit)	Password (min 7 letters, symbols, numbers)	Smart card (Microprocessor, crypto card)	Digital Certificate	Fingerprint
Cost	3	+1	+1	0	0	-1
Ease of implementation	1	+1	+1	0	0	-1
Security	2	-1	0	+1	+1	+1
Interoperability NL	1	0	+1	0	0	-1
Interoperability eMayor	2	-1	0	+1	+1	-1
Usability	1	+1	+1	+1	+1	0
Trust/ Acceptance	1	+1	+1	+1	0	0
Scalability	3	+1	+1	+1	+1	+1
Total score →		+4	+10	+9	+8	-2
Order of ranking/ importance →		4	1	2	3	5

Table 6.2 Authentication alternatives scored for “Certificate issuance” in the Netherlands

Service: Change of address						
Security level: medium						
	Value	PIN (4-digit)	Password (min 6 letters, symbols, numbers)	Smart card (Microprocessor, crypto card)	Certificate	Fingerprint
Cost	3	+1	+1	0	0	-1
Ease of implementation	1	+1	+1	0	0	-1
Security	4	-1	0	+1	+1	+1
Interoperability NL	1	0	+1	0	0	-1
Interoperability eMayor	2	-1	0	+1	+1	-1
Usability	1	+1	+1	+1	+1	0
Trust/ Acceptance	1	+1	+1	+1	0	0
Scalability	3	+1	+1	+1	+1	+1
Total score →		+3	+10	+11	+10	0
Order of ranking/ importance →		3	2	1	2	4

Table 6.3 Authentication alternatives scored for “Change of residence” in the Netherlands

7. Conclusions & recommendations

This chapter contains the conclusion and recommendations. In paragraph 7.1 the conclusions will be drawn. Paragraph 7.2 contains the recommendations.

7.1 Conclusions

The aim of this thesis is answering the following research question:

What is an appropriate way for municipalities to implement authentication for the eGovernment services 'Certificate issuance' and 'Change of residence', while compatible with eMayor?

To gain knowledge and insight to this question, the following sub-questions have to be answered.

1. Current situation:
 - a) What processes do the two eMayor services in the current situation consist of?
 - b) What will be improved by offering the two eMayor services online?

The main process steps Certificate issuance and Change of residence are:

- Request by citizen
- Identification
- Approval/rejection request, possible further research
- Payment and processing of the request (processing of the requests is different for Certificate issuance and Change of residence)

An important process step in the current services is the identification of the citizen. This process will be automated in the online situation. This will save the civil servant time. Other advantages of offering the service online are: the knock-out moments are at the beginning of the process; municipality offers the citizen better service, money and time savings by both citizen and civil servant; increased flexibility and increased transparency.

2. Which techniques for authentication can be found in literature?
3. What are the advantages and disadvantages of these authentication techniques?

Authentication techniques can be divided in the following categories:

- Authentication based on something you *know*
- Authentication based on something you *have*
- Authentication based on something you *are*

Passwords and PINs are examples of “something you know”. They are easy to implement, relatively affordable, but less secure than the other alternatives.

Smart cards, and certificates are examples of “something you have”, although often used in combination with passwords or PINs (two-factor authentication). They are more secure than passwords, but also more expensive as reading equipment is necessary.

Biometrics is based on “something you are”. Therefore you can not forget them. A disadvantage is that many or not yet applied on a large scale. Although, costs are decreasing, they are still expensive.

4. Which Dutch authentication initiatives are currently initiated?
5. Are current Dutch authentication initiatives useful for the Dutch eMayor services?

There are several authentication initiatives: 2b or not 2b; NAV/DigiD, e-ok framework, eNIK, PKIoverheid and several municipalities have their own initiatives. Most useful for eMayor are PKIoverheid, eNIK and NAV/DigiD. The latter one is useful for low security authentication, as it aims to provide passwords that can be used for multiple governmental organisations. eNIK offers an identification smart card, but this will actually take till 2006 before it is implemented. PKIoverheid makes authentication with the use of digital certificates possible. This is very useful as digital certificates can legally substitute hand-written signatures.

6. Is the suggested authentication technique (smart cards) of the eMayor project suitable for Dutch municipalities?

The smart card is suitable for services that require a higher level of security. A problem is that we do not have a national authentication smart card yet. The eNIK is expected in 2006. This Dutch Identity card could be used for authentication of services that require more security than a password can offer. Furthermore, some services require a digital signature. These can be stored on the smart card. eMayor suggests the use of smart cards but also supports the use of digital signatures and passwords. These can be supported by the NAV/DigiD and PKIoverheid initiatives. The answer to this research question therefore is: yes, but smart cards can only be supported after the eNIK is introduced, which will be at the end of 2006.

7. What are the selection criteria for choosing suitable authentication?
8. How can a selection of an authentication technique be made?

The following selection criteria are used in the selection framework 6.1: cost, usability, ease of implementation, trust/acceptance, level of security, interoperability and scalability.

Levels of security are based on the characteristics of the techniques: level low is based on “something you know”, medium on “something you have” and high on “something you are”. De Raad van State performed a risk analysis on the services change of residence and certificate issuance. Change of address needs medium security because a digital signature is required. For the service certificate issuance, level “low” will suffice.

After the minimal security level is determined, an authentication technique has to be selected. A framework is made to score the different techniques and make the required selection.

The answers to the sub-questions result in the following analysis:

“Certificate issuance” requires a low level of security (Raad van State). For this level of security the authentication technique “password + user name” will suffice. This techniques scores the best in the selection framework and therefore is suggested for the eMayor service certificate issuance.

Change of residence causes some difficulties for the implementation of authentication in a suitable way. Dutch law (4:1 Awb and articles 65, 66, 68, 80, 81 GBA) requires a (hand-written) signature for this service. As long as this law applies, password authentication is not allowed. May 8th 2003 a law is enacted on digital signatures (Wet Elektronische Handtekeningen). This

law states that, under certain conditions, a digital signature can substitute the hand-written signature. These requirements determine that a smart card is needed for the secure creation of the key.

A centrally organised, nation-wide used smart card is not yet available until 2006 (the eNIK). Therefore it is difficult to offer the service “change of residence” online within the current legal context. In the near future (end of 2006) it will be possible. However, eMayor will not be available before February 2006, which makes the gap only a couple of months.

Since eMayor supports the use of digital certificates, password and smart card authentication both solutions for the Dutch situation are also compatible with eMayor.

The main research question therefore can be answered as follows:

The most appropriate authentication technique for “Certificate issuance” is a “password and user name” combination. Change of residence can not be offered within the current legal context at the moment but will be in the near future. To comply to current law, the appropriate authentication technique is the use of digital signatures stored on a smart card.

Since there currently is no centrally organised authentication technique in the Netherlands, some municipalities just offer change of residence online without an appropriate authentication technique. This is actually not allowed.

7.2 Recommendations

The following recommendations to the municipalities can be made:

- The degree in which passwords are secure (also) depends on the requirements for the passwords. The municipality should restrict the choice of the characters of the password. Preferably they need to consist of three out of the following four categories: letters, capitals, numbers and symbols. They should be six to eight characters long and they need to be changed periodically (e.g. once in six months).
- Good instructions need to be given to make citizens aware of the security risks of the use of passwords. Issues like social engineering, shoulder surfing, etcetera, are important to be understood.
- Additional checks build into the process will reduce the number of false request. Examples are arranging the payment before the document is sent, and sending the requested certificates or confirmation to the address stated in the GBA.
- The NAV/ DigiD is a good initiative, able to offer password security for municipalities and semi-governmental organisations. In case municipalities want to implement password authentication, the NAV/DigiD initiative is recommended.
- A clear framework with all municipal services and the required security level should be developed. Further research should be done on the required security levels.
- Further research is recommended on the legal issues concerning the “Change of residence” service. Although the service seems quite simple, it requires high security measures because of the required signature. Maybe regulation on this topic can be reconsidered to facilitate the provision of services online.
- Italy, Belgium, Finland and the UK already have a national smart card implementation. It would be very useful to study these implementations to learn from their experience. This can be used to avoid pitfalls.

- The chosen technique could be used for other purposes than municipal authentication, like authentication for other (governmental) organisations.
- The possibility to further automate the services could be researched, so the citizens request can be handled without or with less interference of the civil servant. This might make the processes more efficient.

Definition of concepts

Access control

Access control is the ability to limit and control the access to host systems and applications via communication links (Stallings, 2003).

Authentication

Authentication is defined as follows: The assurance that the communicating entity is the one that it claims to be (Stallings, 2003).

Authenticator

A data item which can only be provided by one person (Woodward, 2003).

Biometric authentication

It is the automatic identification or identity verification of an individual based on physiological or behavioural characteristics (IBIA.org).

Chip card

A card with a chip that has a simple logic circuit with additional memory that can be read and/or written (Rankl, 2000). This type of card is also called “memory card”.

Cross-border aspect of the eMayor services

The certificates from other municipalities will be accepted in the different countries. Because services will be accessed online, a person does not have to travel back to its native country to get the required certificate, form of information.

eGovernment

Electronic government concerns providing or attainment of information, services or products through electronic means, by and from governmental organisations, at any given moment and place, by offering an extra value for all participating parties (Zweers, 2002).

Identification

Identification systems answer the following question: Who is X? (Woodward, 2003)

Legacy systems

The old systems used by the municipalities.

Magnetic-strip card

A card with a magnetic strip on which data may be read and subsequently read. The magnetic strip holds three data tracks with differing data recording densities. Tracks 1 and 2 are only read after the card has been issued, while data may also be written to track 3 while the card is in normal use. The magnetic material in the strip may have either high-coercivity characteristic or a low-coercivity characteristic (Rankl, 2000).

Memory card

A card with a chip that has a simple logic circuit with additional memory that can be read and/or written. Memory cards can also have supplementary security logic blocks, which for example make authentication possible (Rankl, 2000).

Microprocessor card

A microprocessor card is a card with a micro controller chip, which contains a CPU, volatile memory (RAM) and non-volatile memory (ROM, EEPROM and the like). A microprocessor card can also contain a numerical coprocessor (NPU). So that it can quickly execute public-key cryptographic algorithms (Rankl, 2000).

Password

A password can be defined as: A supposedly secret string used to prove one's identity (Stallings, 2003).

Service

A services is a general concept which has different explanations depending on the field of study it is used in. In this research the following definition of a service is used:

A service is the non-material equivalent of a good. Service provision has been defined as an economic activity that does not result in ownership, and this is what differentiates it from providing physical goods. It is claimed to be a process that creates benefits by facilitating either a change in customers, a change in their physical possessions, or a change in their intangible assets. By supplying some level of skill, ingenuity, and experience, providers of a service participate in an economy without the restrictions of carrying stock (inventory) or the need to concern themselves with bulky raw materials. On the other hand, their investment in expertise does require marketing and upgrading in the face of competition which has equally few physical restrictions (wordiq.com).

Small to Medium sized Governmental Organisations (SMGOs)

By the term *Small to Medium sized Governmental Organisations (SMGOs)* we refer to governmental bodies that share the following characteristics:

- Small-sized public organisations that cover a geographic area serving several thousands of citizens, that may be located in rural or isolated areas.
- Medium-sized public organisations that cover a geographic area serving approximately between 200.000 and 500.000 citizens, that are normally located in urban or metropolitan areas. Examples include larger municipalities or chambers of commerce under public law.
- Interact frequently with citizens and/or businesses, to offer paper-based and electronic services utilizing a limited number of available resources (employees and funds).
- Interact with each other, in local or cross-border transactions, to exchange information on behalf of citizens, businesses or the organisation itself. (eMayor 01, 2004)

Smart Card 1

A microprocessor and storage system realized in a microcircuit embedded in a plastic card the size of a credit card. The card operates when inserted into an external terminal device with which it interfaces electrical contacts. Through these contacts, the terminal provides electrical power and communicates with the card processor using a low-speed serial asynchronous character protocol. The basic physical, electrical and communications aspects of the interface have been standardized by ISO/IEC (Hassler, 2001).

Smart Card 2

Rietdijk (2001): a smart card is a plastic card equipped with a chip which provides storage and communication of data between smart card and terminal.

Smart Card 3

Smart cards are essentially devices that allow information storage and processing, but need to interact with an active device providing the necessary power supply (Bolchini).

List of frequently used abbreviations

Awb

Algemene wet bestuursrecht

BPR

Basis registratie Personen- & Reisdocumenten

BS

Burgerlijke Stand

CA

Certificate Authority

CRL

Certificate Revocation List

CSP

Certificate Service Provider

eGovernment

Electronic Government

eNIK

elektronische Nederlandse Identiteits Kaart

GBA

Gemeentelijke Basis Administratie

NAV

Nieuwe Authenticatie Voorziening

PIN

Personal Identification Number

PKI

Public Key Infrastructure

PL

Persoonslijst

UML

Unified Modelling Language

Appendix 1: Interviewees

DATE	NAME	ORGANISATION	TOPIC
18-06-2004	Mr. Rob van der Velde	Municipality of The Hague	GBA, BS and services
23-07-2004	Mr. Peter Douma	Municipality of The Hague	eGovernment policy, plans and projects Municipality of The Hague
03-08-2004	Mr. Rob Van der Velde	Municipality of The Hague	Check Activity Diagrams
04-08-2004	Mr. Jacob Boersma	ECP.nl	Authentication initiatives in the Netherlands
01-09-2004	Ms. Sheila Ghosh	BKWI	Nieuwe Authenticatie Voorziening (NAV)
03-09-2004	Mr. F. van Barneveld and Mr. H. van Rijn	Municipality of Hoorn	GBA, models, differences between municipalities
03-09-2004	Mr. Gerrit Jan van 't Eind	eNIK (ICTU)	Elektronische Nederlandse identiteitskaart (eNIK)
05-11-2004	Mr. D. Wieringa	Deloitte	Selection Framework
05-11-2004	Mr. P. van Eijk	Deloitte	Selection Framework
09-11-2004	Mr. S. Daskapan	TU Delft	Selection Framework
11-11-2004	Mr. P. Hengeveld	Deloitte	Selection Framework
17-11-2004	Mr. P. Timmermans	Deloitte	Selection Framework

Appendix 2: GBA Certificates

PIV uittreksels

pagina 1 van 2

PIV uittreksels

PIV uittreksels	Soort papier
U001 Uittreksel basisadministratie	beveiligd
U002 Uittreksel met datum adres en gemeente, vestiging, huwelijks- en kindgegevens met een apart tekstveld voor datum begin geldigheid Ned. Nationaliteit	beveiligd
U004 Uittreksel t.b.v. huwelijksaangifte	beveiligd
U005 Uittreksel met burgerlijke staat	beveiligd
U006 Uittreksel met datum adres en gemeente	beveiligd
U007 Uittreksel met burgerlijke staat en nationaliteit en gezag	beveiligd
U008 Uittreksel met nationaliteit(en)	beveiligd
U009 Uittreksel Vertrek Aruba / Nederlandse Antillen	beveiligd
U010 Attestatie de Vita	beveiligd
U011 Attestatie de Vita met partner	beveiligd
U012 Attestatie de Vita Engels, Duits, Frans	beveiligd
U021 Uittreksel met nationaliteit, gezag en kiesrecht	beveiligd
U025 Uittreksel met een overzicht van alle reisdocumenten	beveiligd
U026 Uittreksel t.b.v. rijvaardigheidsexamen	beveiligd
U030 Uittreksel internationaal Ned/Frans/Duits/Engels	beveiligd zonder logo
U031 Uittreksel internationaal Ned/Spaans/Italiaans/Turks	beveiligd zonder logo
U032 Uittreksel internationaal Ned/Frans/Duits/Engels Archief (voor personen die niet actueel ingeschreven staan)	beveiligd zonder logo
U033 Uittreksel internationaal Ned/Spaans/Italiaans/Turks Archief (voor personen die niet actueel ingeschreven staan)	beveiligd zonder logo
U040 Uittreksel met historische adressen	beveiligd
U050 Uitgifte PL bij geboorteaangifte	wit logo papier
U060 Aangifte van voorgenomen vertrek naar buitenland (Verklaring)	beveiligd
U065 Pas 65	voordruk
U070 Inlichtingen basisadministratie	beveiligd
U071 Inlichtingen basisadministratie met huwelijksgegevens	beveiligd
U072 Inlichtingen basisadministratie met nationaliteitsgegevens met een apart tekstveld voor datum begin geldigheid Ned. nationaliteit	beveiligd



<http://intranet.denhaag.nl/smartsite.dws?id=36072>

26-05-2004



U090	Verklaring Turks/Marokkaans consulaat ivm acceptatie voornamen	wit zonder logo
U091	Verklaring Burgerlijke Staat	beveiligd
U092	Verklaring Burgerlijke Staat niet ingeschrevene	beveiligd
U093	Verzoek wijzigen burgerlijke staat	wit zonder logo
U094	Verzoek brondocumenten	wit zonder logo
U356	Brief toezenden persoonslijst	wit logo papier
U360	Onderzoek	beveiligd
U400	Brief Naamgebruik	wit logo papier
U401	Brief na wijziging naamgebruik	wit logo papier
U450	Verzoek geheimhouding	wit zonder logo
U451	Verzoek tot geheimhouding bij FIOM-kinderen	wit zonder logo
U600	Uittreksel basisadministratie tbv woningtoewijzing alleenstaande	beveiligd
U601	Uittreksel basisadministratie tbv woningtoewijzing gezin	beveiligd
U650	Laissez-Passer voor lijken	wit zonder logo
U651	Verlof tot lijkbezorging	beveiligd
U652	Verlof tot lijkbezorging geen inwoner wel hier begraven/cremeren	beveiligd
U700	Garantverklaring inwoner met partner	beveiligd zonder logo
U701	Garantverklaring zonder partner	beveiligd zonder logo
U702	Garantverklaring blanco	beveiligd zonder logo
U800	Huwelijksbevoegdheid inwoner	aparte voordruk
U801	Huwelijksbevoegdheid niet ingeschrevene	aparte voordruk

Appendix 3: Birth Certificate front side

Nr. A 2318	
Op	vierentwintig december negentienhonderd negenenzeventig,
te	7 uur, 45 minuten, is geboren in de gemeente 's-Gravenhage,
Bronovolaan 5, Catijn, Birgitte Eva, dochter van:	
Catijn, Robertus Antonius, systeemontwerper en	
zijn echtgenote: van Zuidam, Hendrina Josina	
Jacoba, beiden wonende te 's-Gravenhage.--	
De aangifte van deze geboorte is mij, ambtenaar van de burgerlijke stand van 's-Gravenhage, gedaan door: de vader voornoemd, oud 29 jaar.	
Waarvan akte op 27 december 1979.	
 	

7

MAKTE DE BURGERSCHAP VAN 'S-GRAVENHAGE

Appendix 4: Birth certificate back side

Bij twijfel over de authenticiteit van dit document kunt u de volgende controles uitvoeren:

Kijk goed naar de voorzijde van het document

U ziet een patroon van grijze zeshoeken.

Daartussen is uiterst kleine tekst in groen en oranje gedrukt; onder een loep moet deze tekst netjes en scherp zijn.

Het laatste geldt trouwens ook voor alle andere lijntjes en patronen in het document.

In het papier bevinden zich verder vezeltjes in verschillende kleuren

Houd het document tegen het licht

Overal in het papier is een watermerk in de vorm van een honingraat zichtbaar.

Maak een fotokopie.

Als u van een echt document een fotokopie maakt zal in de grijze zeshoeken de tekst COPY - KOPIE verschijnen.

Gebruik een UV-lamp

Onder UV-licht worden kleine blauwe en groene vezeltjes in het papier zichtbaar.

De oranje bedrukking in het midden van het document licht geel op.


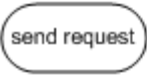


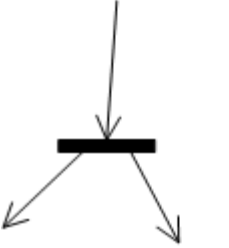
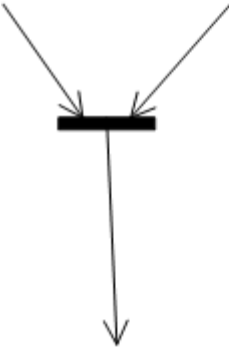

Verder licht het nummer van het document rood op.

Is op de voorzijde de tekst COPY - KOPIE duidelijk zichtbaar?

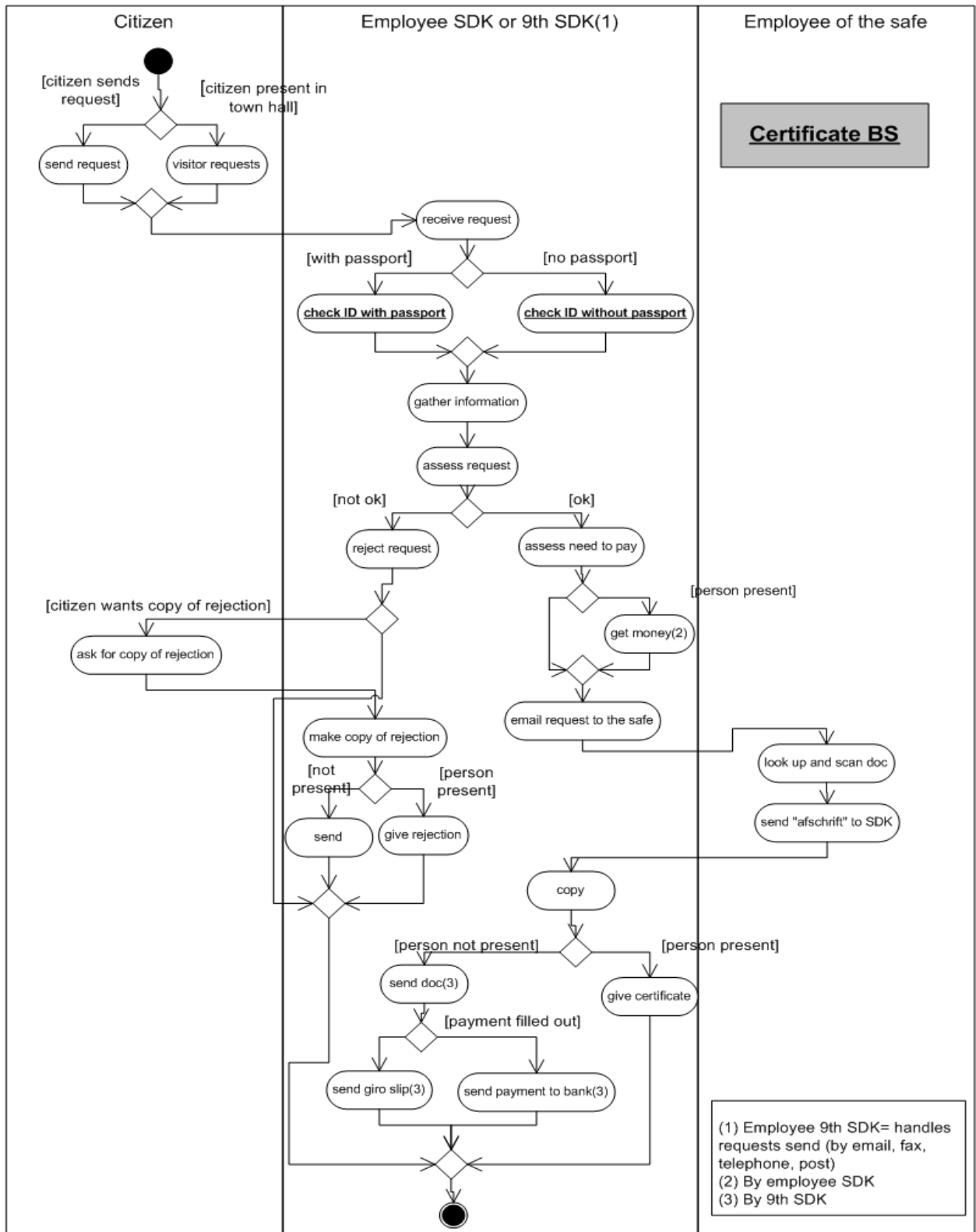
Dan heeft u met een fotokopie te maken!

U kunt altijd de controles zoals hierboven beschreven uitvoeren om zekerheid te verkrijgen.

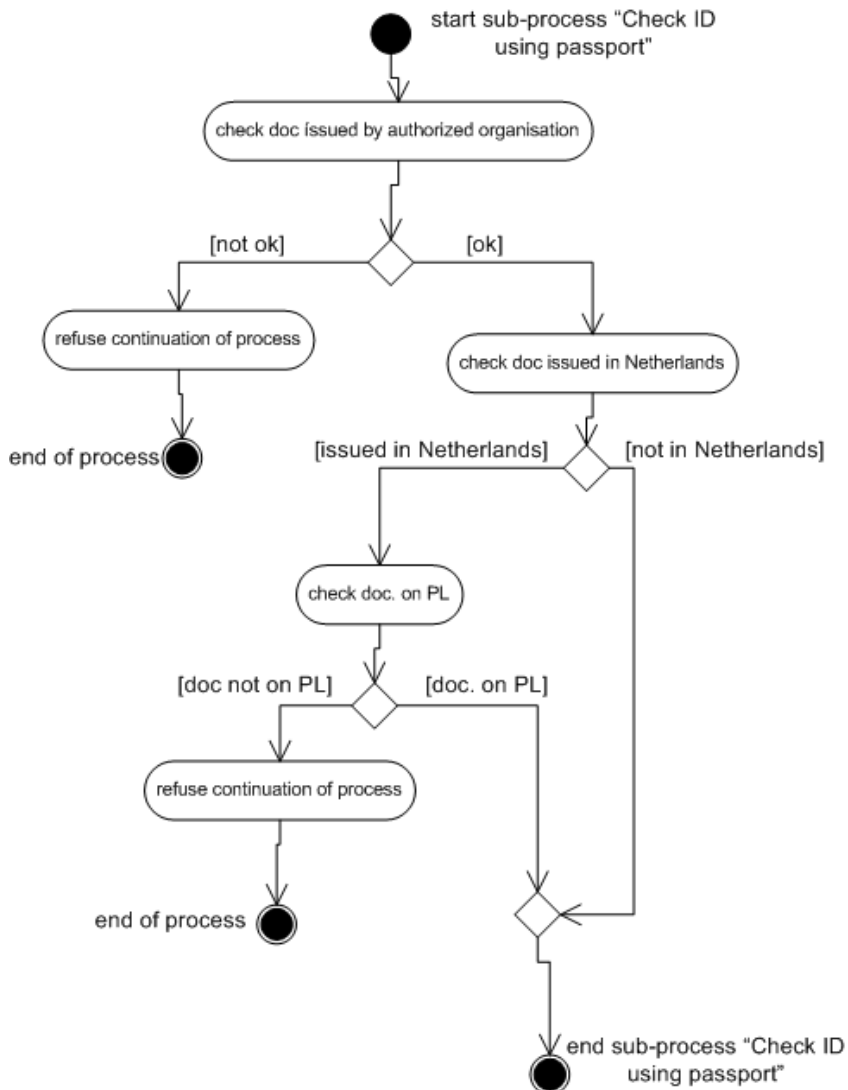
Appendix 6: Symbols Activity Diagram & Description

	Transition	<p>Top-down the models depict time. A task at the top of the page is done before a task at the bottom of the page. A diamond has either one incoming transition and two out going transitions or two incoming transitions and one out going. The first one indicates a decision to be taken. The process will follow either one or the other transition.</p> <p>Two transitions coming together in a diamond means that the two firstly separated transitions come together again.</p> <p>A fork also has two out going transitions, but these occur in parallel. This means that both processes or done and that there is not an order which one happens first. A join combines these two paths again. The process will only go on after both paths are finished.</p> <p>In some models the activities are bold and underlined, this means that that activity has a sub-model. This is done to make the model more readable.</p>
	Action	
	Initial state	
	Final state	
	Fork	
	Join	
	Diamond	

Appendix 7: Certificate BS process

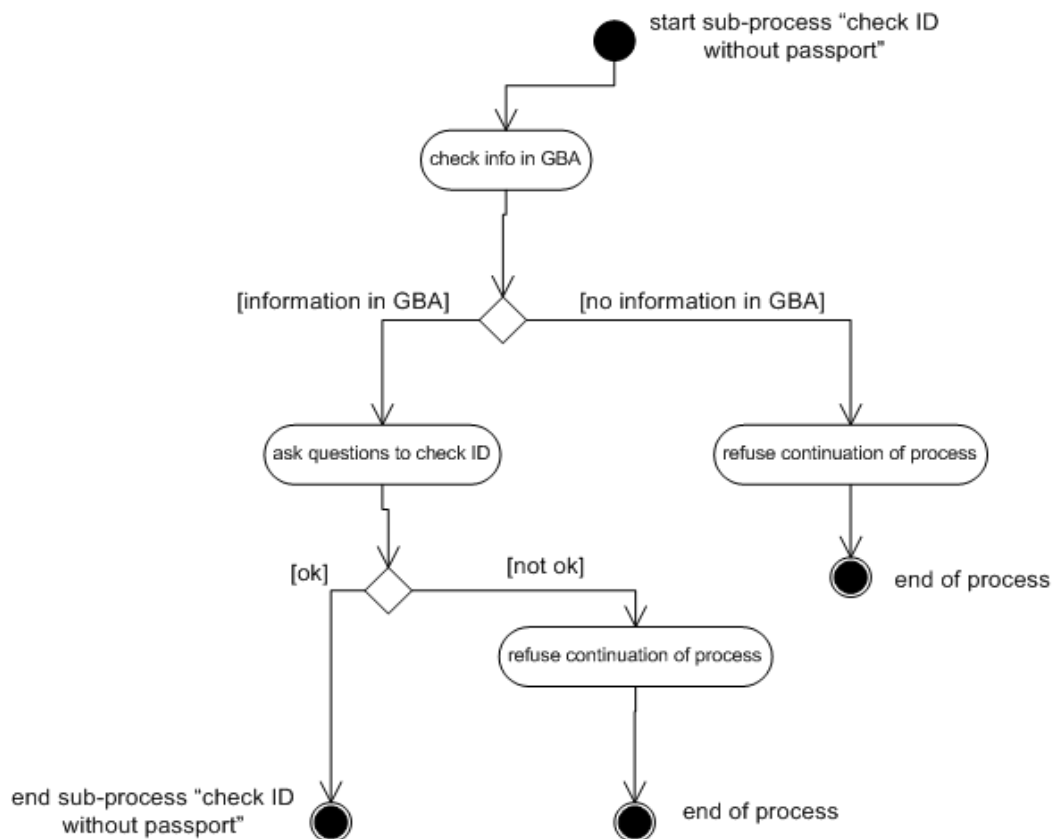


check ID using passport



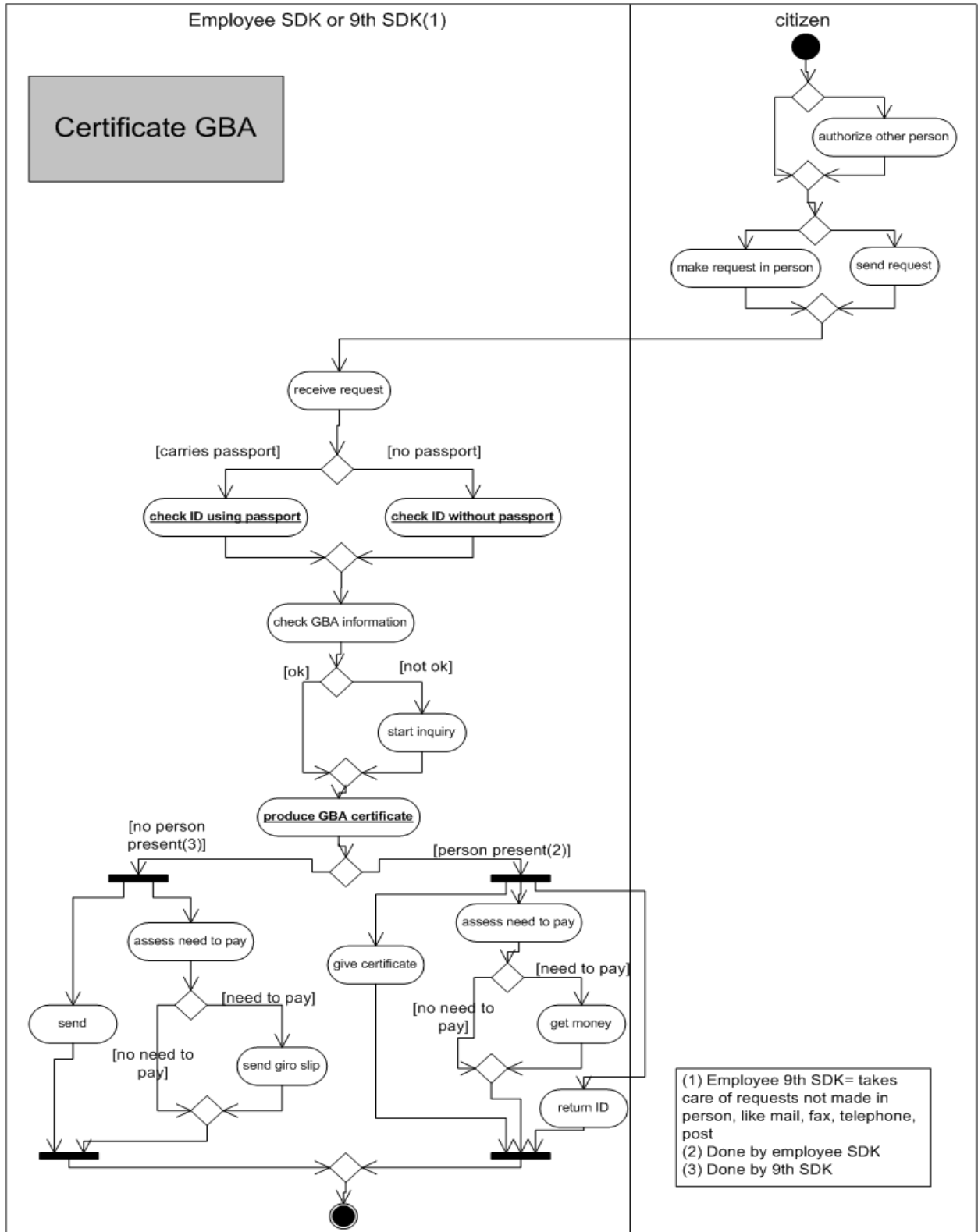
- (1) Employee 9th SDK= handles requests send (by email, fax, telephone, post)
- (2) By employee SDK
- (3) By 9th SDK

check ID without passport

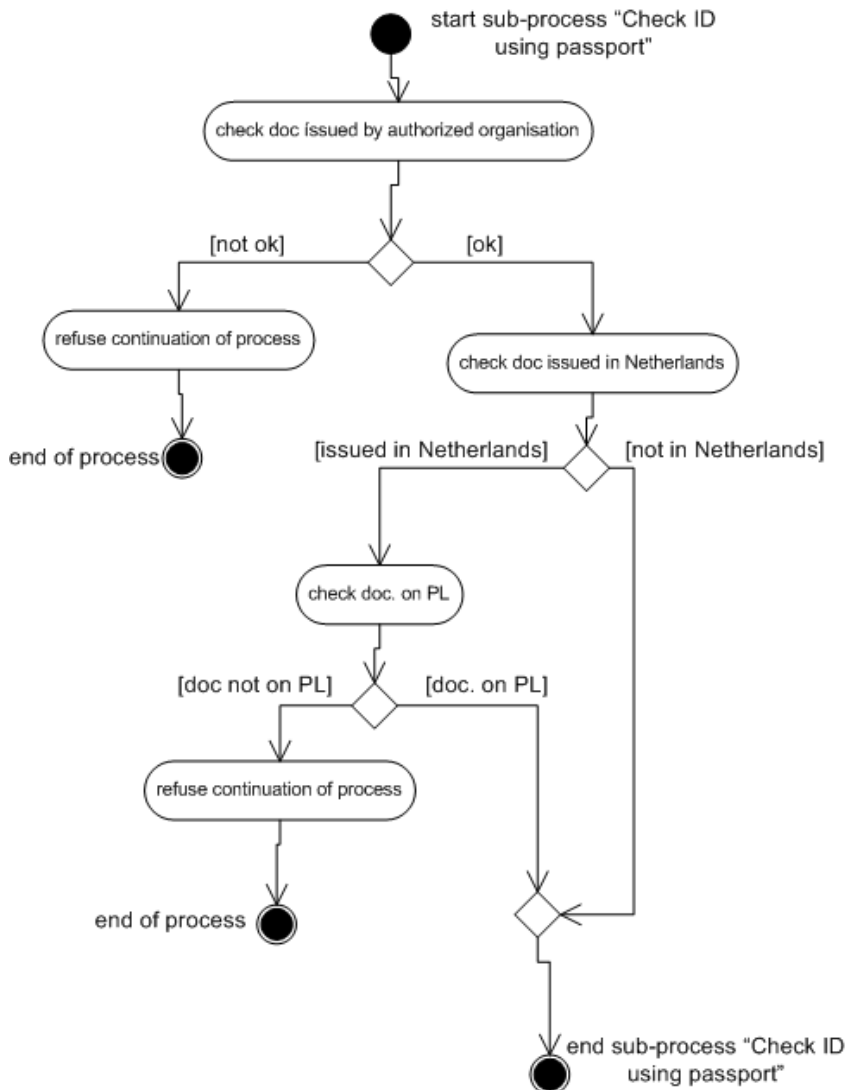


- (1) Employee 9th SDK= handles requests send (by email, fax, telephone, post)
- (2) By employee SDK
- (3) By 9th SDK

Appendix 8: Certificate GBA

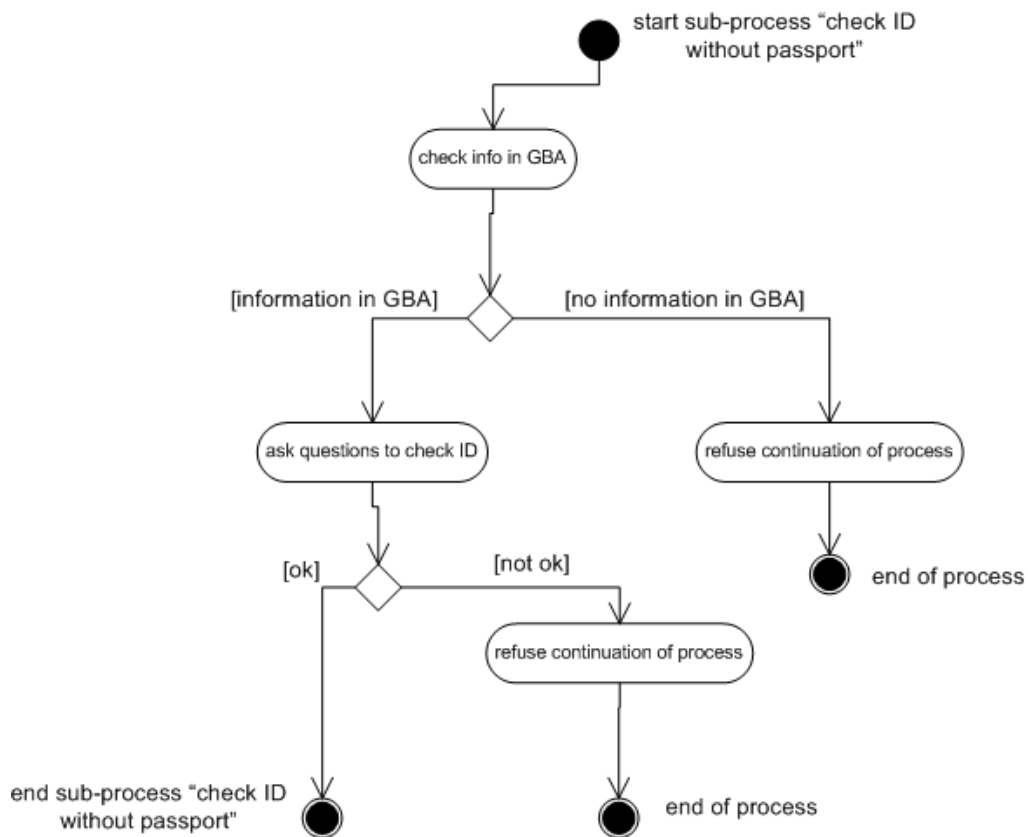


check ID using passport



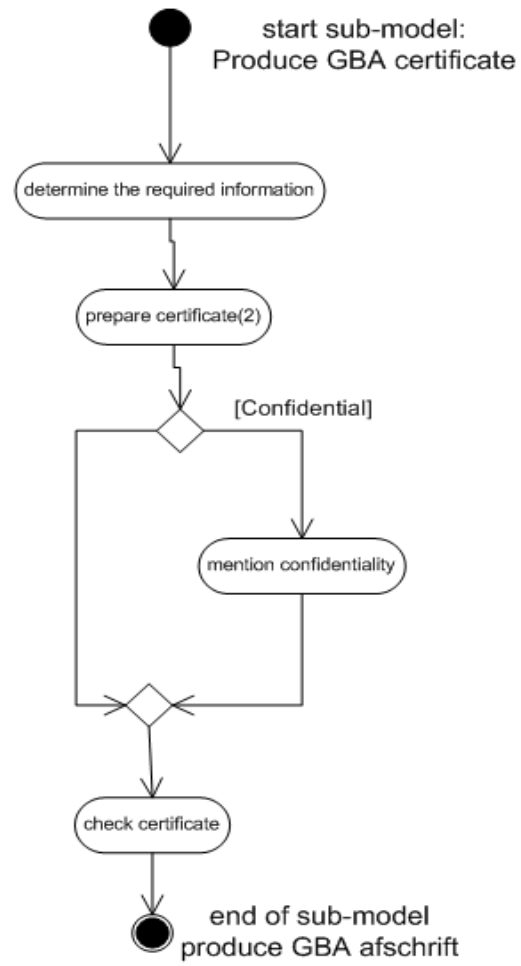
- (1) Employee 9th SDK= handles requests send (by email, fax, telephone, post)
- (2) By employee SDK
- (3) By 9th SDK

check ID without passport



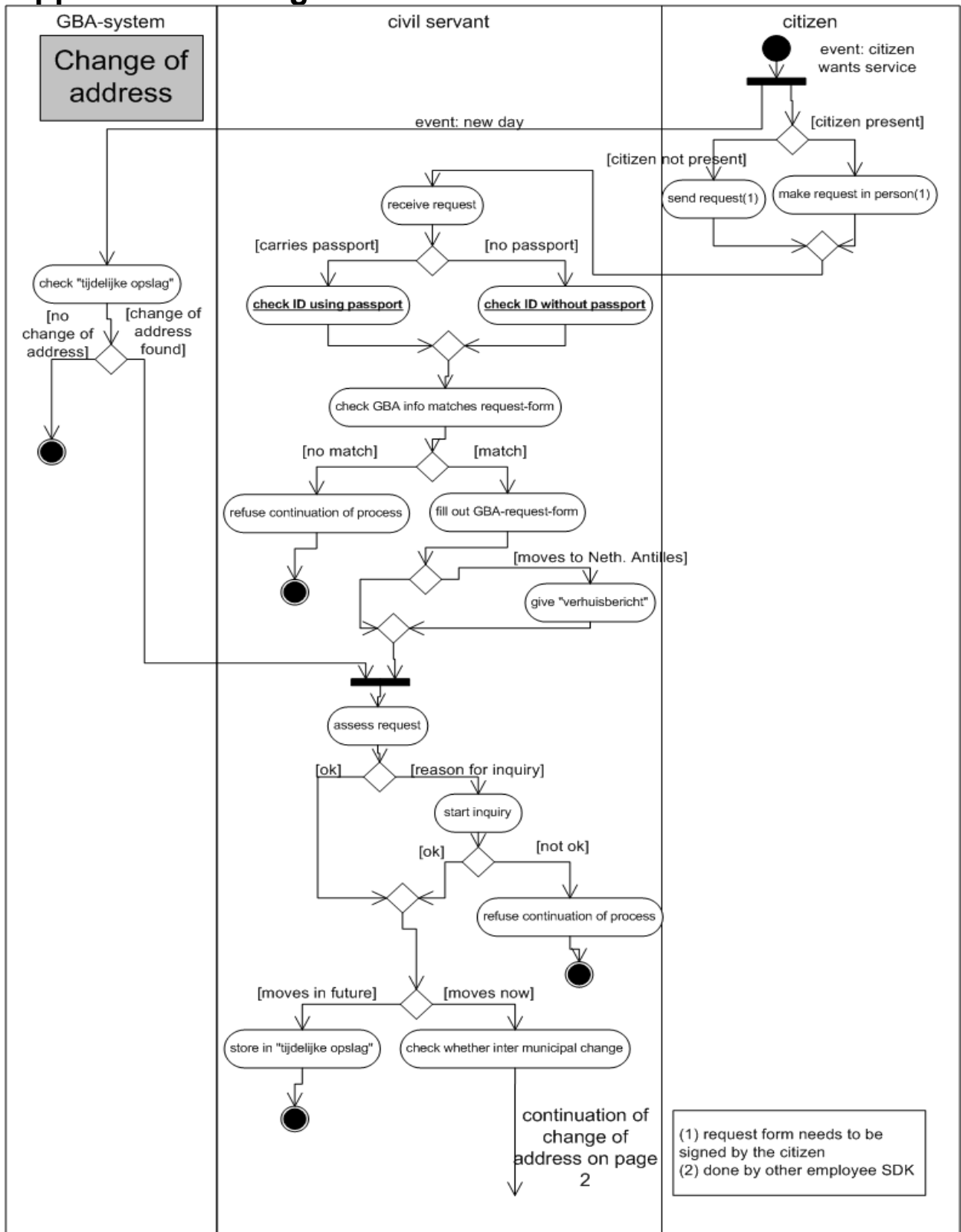
(1) Employee 9th SDK= takes care of requests not made in person, like telephone, fax, post or, online
(2) not yet printed on paper, but stored in digital document first

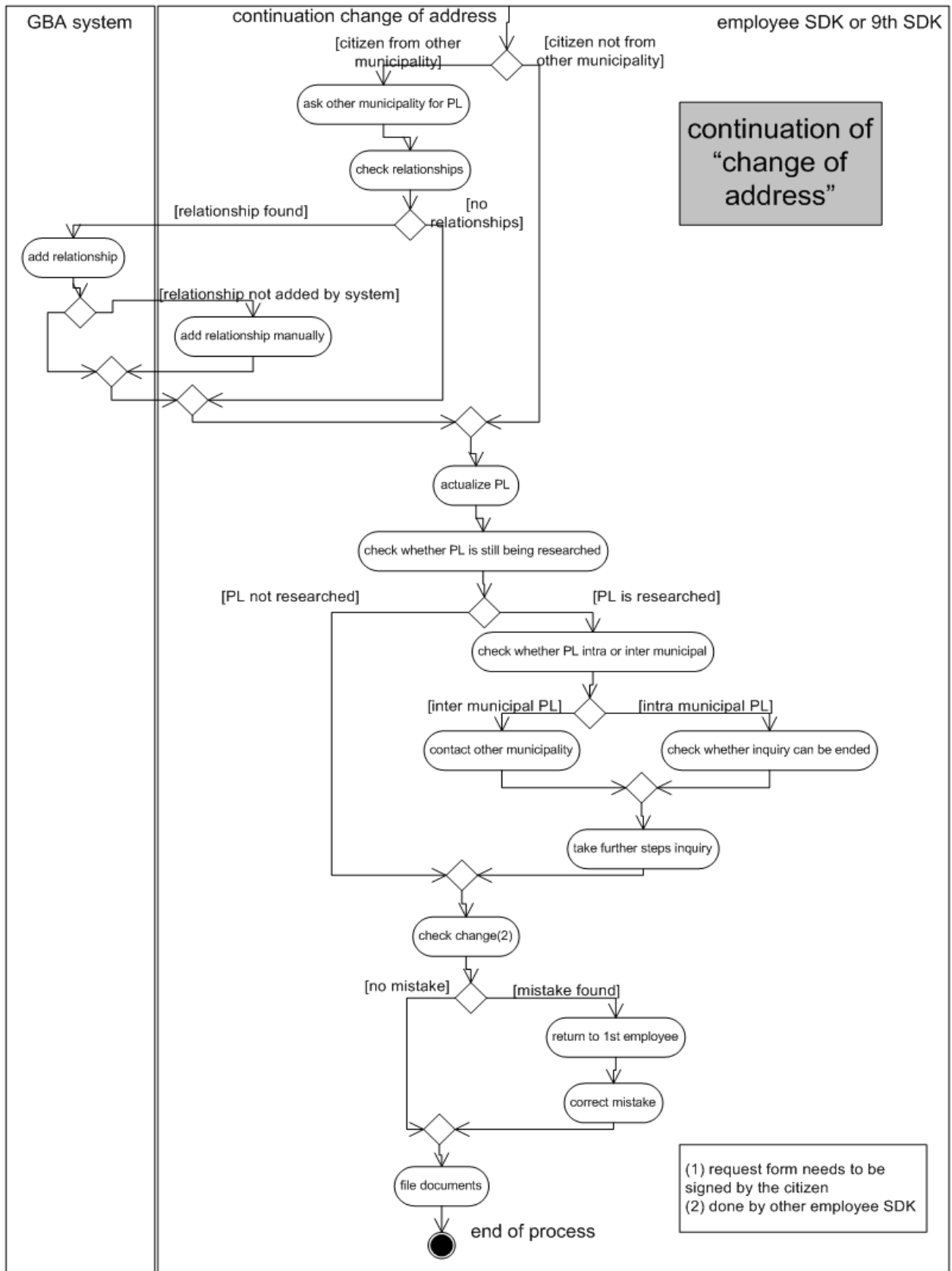
Produce GBA certificate

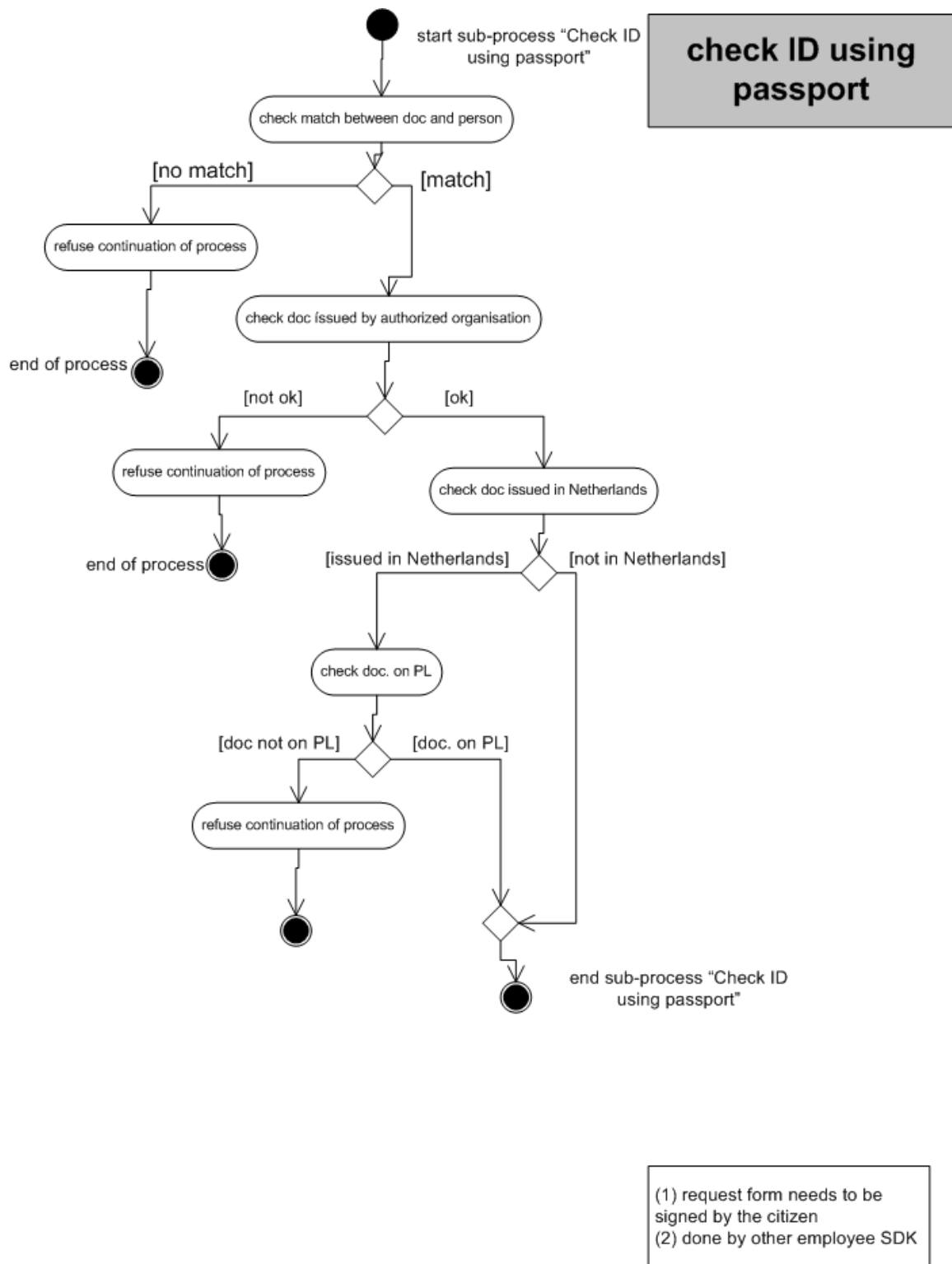


(1) Employee 9th SDK= takes care of requests not made in person, like telephone, fax, post or, online
(2) not yet printed on paper, but stored in digital document first

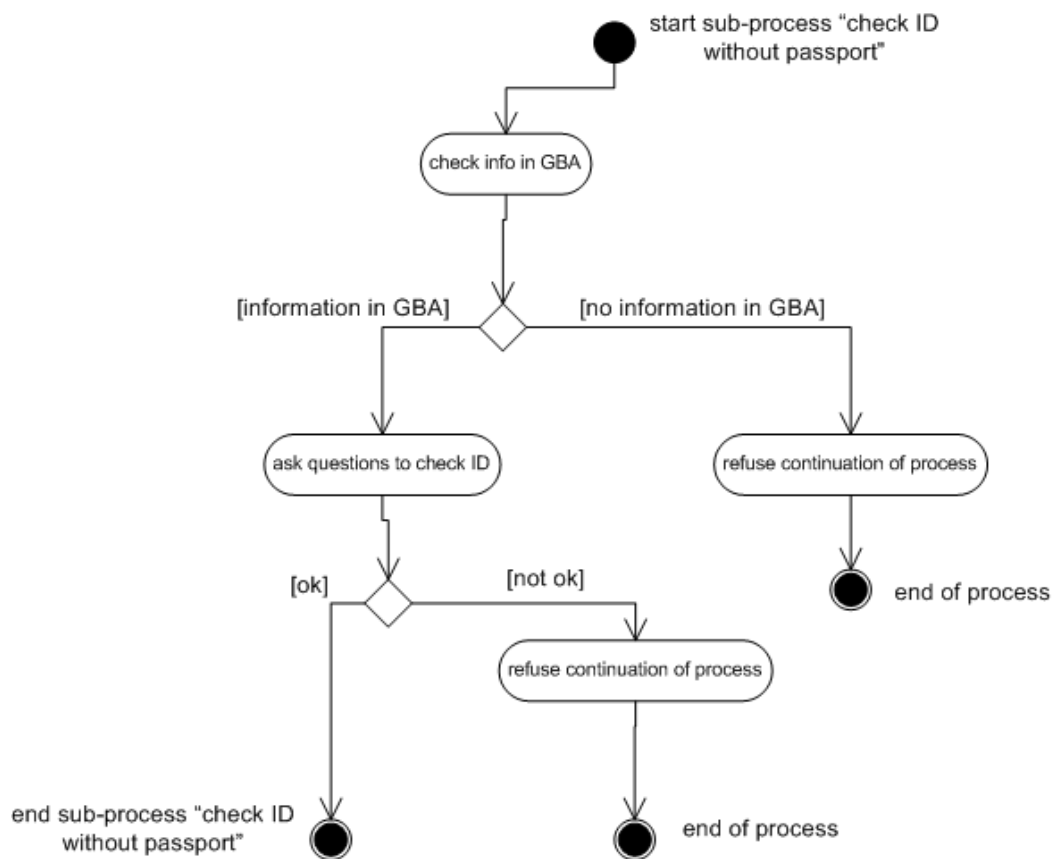
Appendix 9: Change of residence status





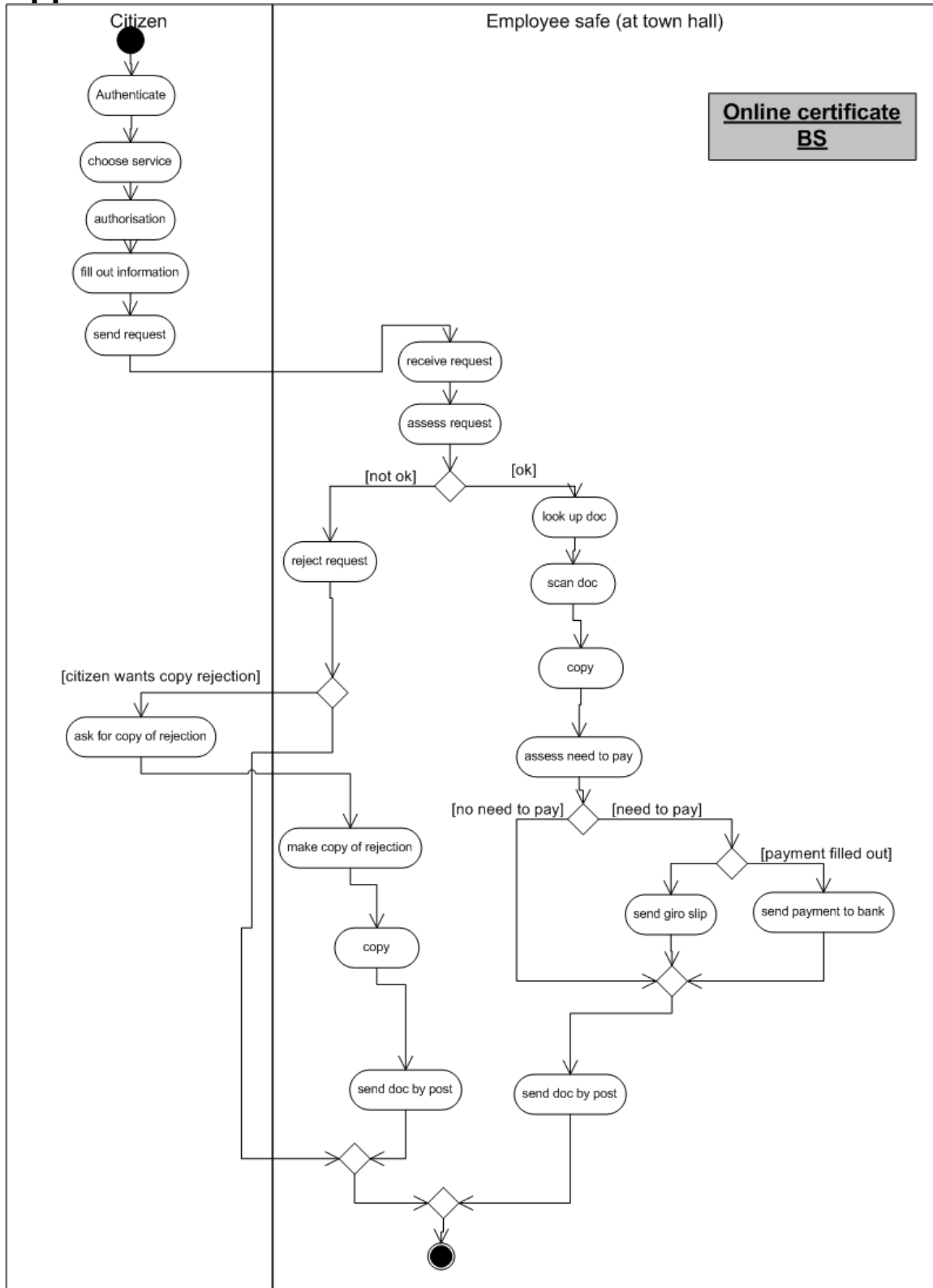


check ID without passport

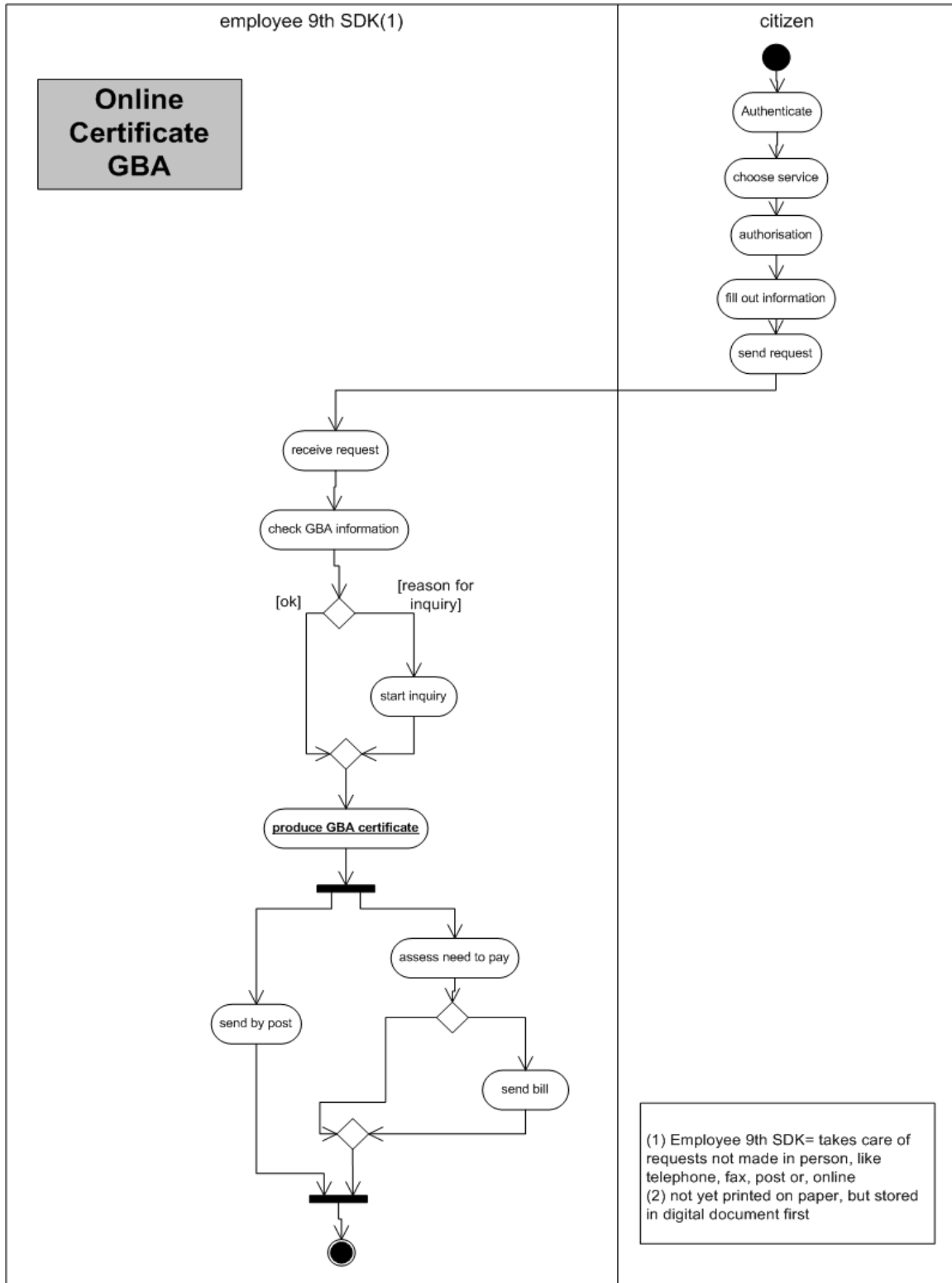


(1) request form needs to be signed by the citizen
(2) done by other employee SDK

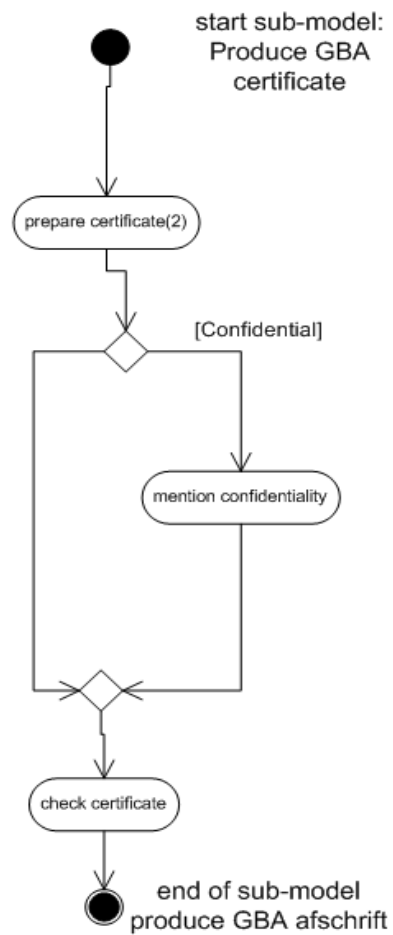
Appendix 10: Certificate BS online



Appendix 11: Certificate GBA online

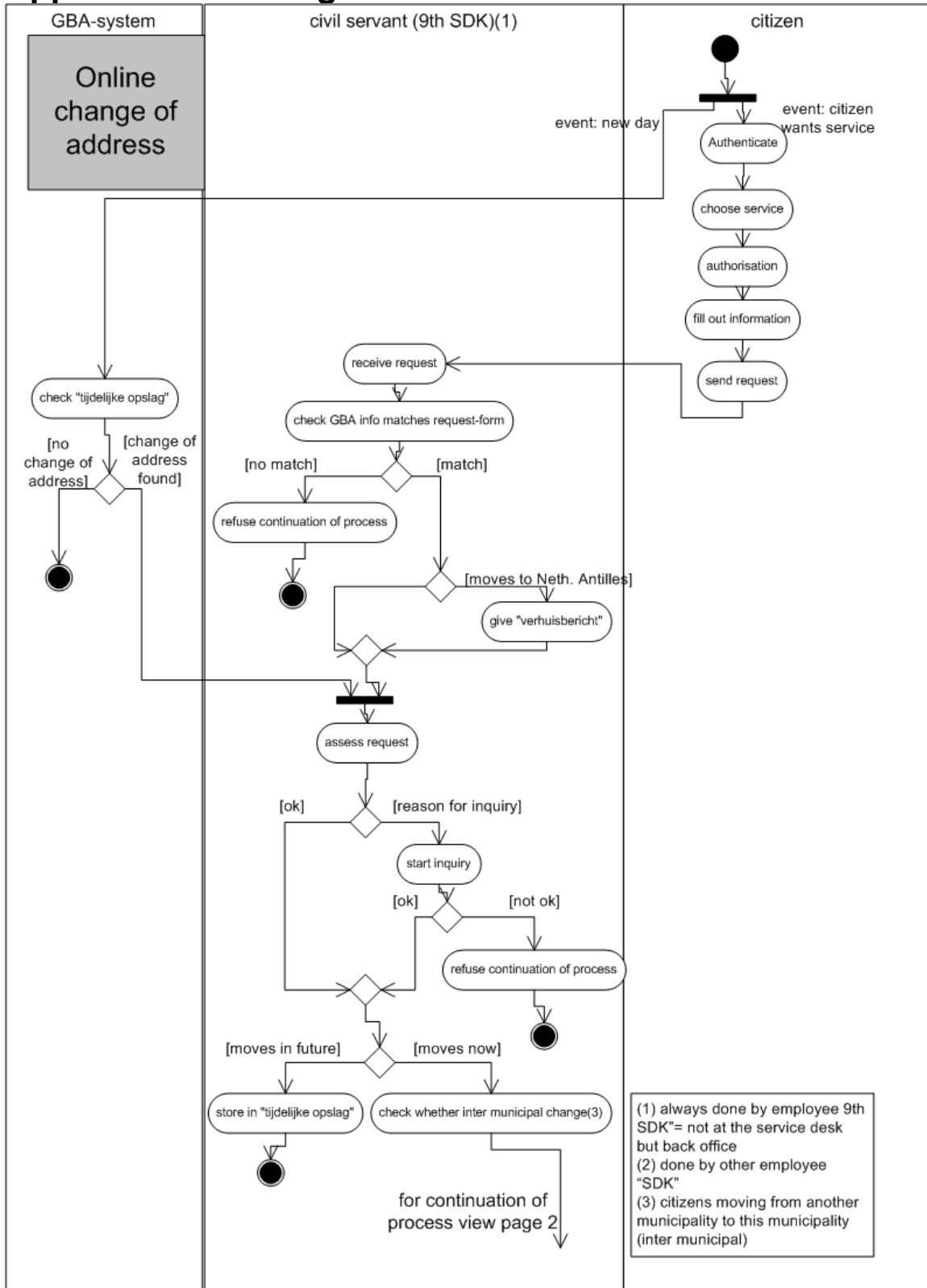


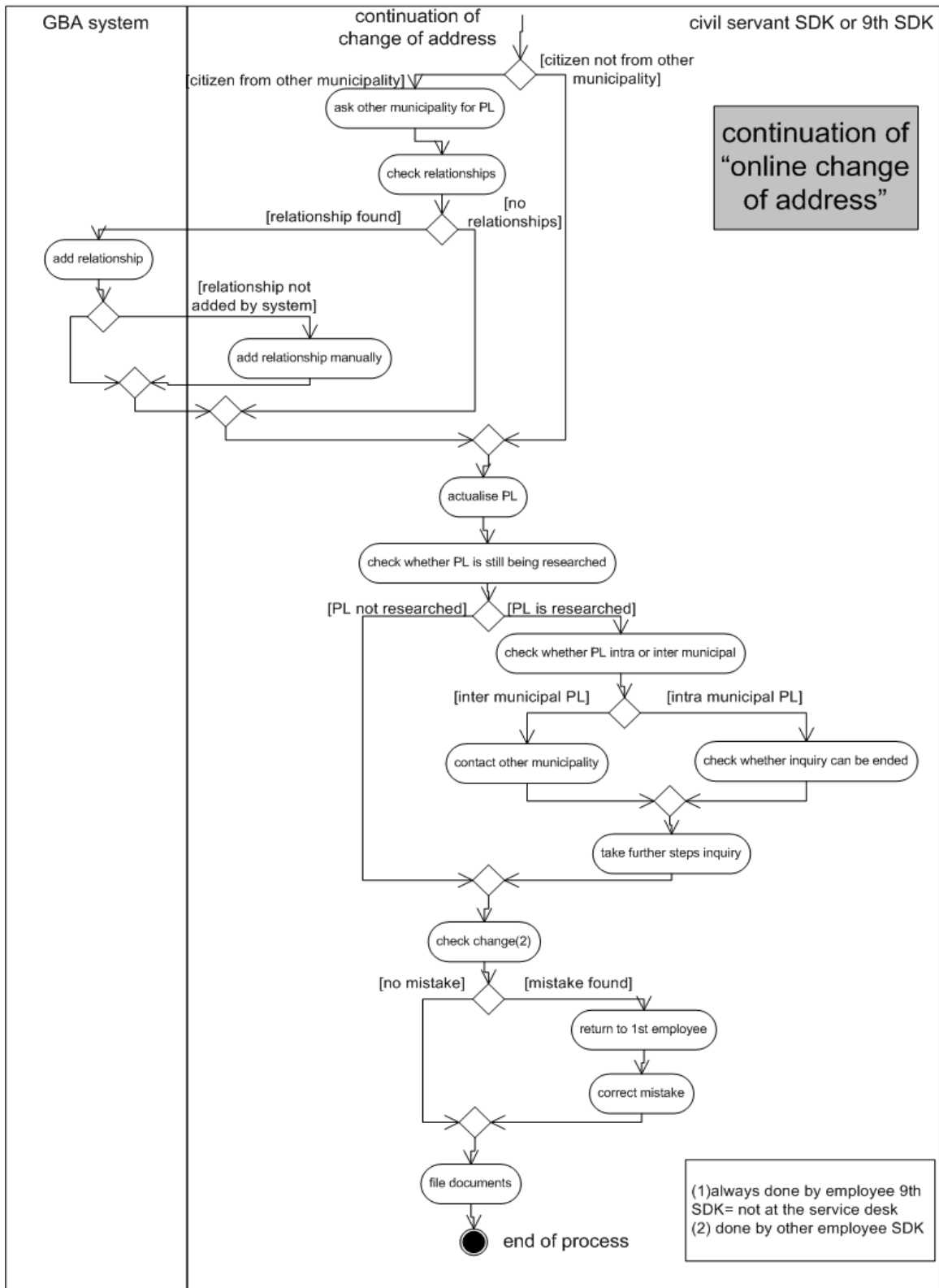
Produce GBA certificate



(1) Employee 9th SDK= takes care of requests not made in person, like telephone, fax, post or, online
(2) not yet printed on paper, but stored in digital document first

Appendix 12: Change of residence status online





Appendix 13: Selection framework filled out by experts

The following people have filled out the framework. This is done to reflect on the selection framework which is designed in chapter 6.

Dr. P.H.J. van Eijk
Drs. D.M. Wieringa
Ir. S. Daskapan
Dr. W. Hengeveld
P.G.J. Timmermans RA

Peter van Eijk							
	Value	PIN (4-digit)	Password (min 6 letters, symbols, numbers)		Smart card (Microprocessor, crypto card)	Certificate	Fingerprint
Cost	2	+1	+1		0	0	-1
Ease of implementation	3	+1	+1		-1	0	-1
Security	3	-1	0		+1	+1	+1
Interoperability NL	2	1	+1		0	1	1
Interoperability eMayor	3						
Usability	4	+1	+1		0	0	0
Trust/ Acceptance	4	-1	0		+1	+1	+1
Scalability	1	+1	+1		+1	+1	0
Total score →		+5	+12		+5	+10	4
Order of ranking/ importance →		3	1		3	2	4

Derk Wieringa							
	Value	PIN (4-digit)	Password (min 6 letters, symbols, numbers)		Smart card (Microprocessor, crypto card)	Certificate	Fingerprint
Cost	4	+1	+1		0	-1	-1
Ease of implementation	4	+1	+1		0	-1	0
Security	3	-1	-1		0	+1	+1
Interoperability NL							
Interoperability eMayor							
Usability	3	+1	0		0	-1	0
Trust/ Acceptance	4	+1	+1		0	-1	1
Scalability	1	+1	+1		0	0	0
Total score →		+13	+10		0	-12	3
Order of ranking/ importance →		1	2		4	5	3

Semir Daskapan							
	Value	PIN (4-digit)	Password (min 7 letters, symbols, numbers)	Memory card	Smart card (Microprocessor, crypto card)	Digital Certificate	Fingerprint
Cost	1	1	1	1	0	1	0
Ease of implementation	2	1	1	1	1	0	1
Security	4	-1	1	1	1	1	0
Interoperability NL	3	1	1	1	1	1	1
Interoperability eMayor	4	1	1	1	1	-1	1
Usability	3	1	1	1	1	-1	1
Trust/ Acceptance	3	1	1	1	1	0	1
Scalability	3	1	1	1	1	1	0
Total score →		15	23	23	22	4	15
Order of ranking/ importance →		3	1	1	2	4	3

Pim Hengeveld							
	Value	PIN (4-digit)	Password (min 7 letters, symbols, numbers)	Memory card	Smart card (Microprocessor, crypto card)	Digital Certificate	Fingerprint
Cost	4	0	0	0	0	1	-1
Ease of implementation	4	0	0	-1	-1	0	-1
Security	3	-1	-1	0	1	0	1
Interoperability NL	2	1	1	-1	-1	0	-1
Interoperability eMayor	2	1	1	+1	1	1	1
Usability	2	1	1	1	1	0	0
Trust/ Acceptance	3	0	0	1	1	-1	1
Scalability	2	1	1	1	1	1	1
Total score →		5	5	3	6	5	0
Order of ranking/ importance →		2	2	3	1	2	4

Piet Timmermans							
	Value	PIN (4-digit)	Password (min 7 letters, symbols, numbers)	Memory card	Smart card (Microprocessor, crypto card)	Digital Certificate	Fingerprint
Cost	1	1	1	1	0	0	-1
Ease of implementation	1	1	1	1	1	1	0
Security	4	-1	-1	0	0	0	1
Interoperability NL	2	-1	1	-1	-1	+1	-1
Interoperability eMayor	3						
Usability	2	1	1	1	1	1	1
Trust/ Acceptance	2	1	1	1	1	1	1
Scalability	3	1	0	1	1	1	1
Total score →		3	4	7	6	10	8
Order of ranking/ importance →		6	5	3	4	1	2

Literature

Books

- Beaver, K., and S. McClure, Hacking for dummies, Wiley Publishing, Indianapolis, 2004
- Bots, P.W.G., Inleiding Technische Bestuurskunde (TB111), TUDelft, 1998
- Bruïne de, F., E-Government: A European Priority, in: J.E.J. Prins (ed.), Designing e-Government, On the crossroads of technological innovation and institutional change, Kluwer Law International, The Hague, 2002, p. 121-126
- Ellings, R., and B. Andeweg, J. de Jong, C. Swankhuisen, Rapportage techniek, Wolters-Noordhoff, Groningen, 1994
- Hassler, V., Security fundamentals for e-commerce, Boston Artech House, 2001
- Hendry, M., Smart card security and applications, Second edition, Artech house, Norwood, 2001
- Nanavati, S., and M. Thieme, R. Nanavati, Biometrics Identity verification in a networked world, John Wiley & sons, Chichester, 2002
- Rankl, W., and W. Effing, Smart Card handbook, Second edition, John Wiley & Sons, Chichester, 2000
- Rietdijk, J., and F. Spoelstra, Smart cards in de reële en virtuele wereld, ten Hagen & Stam, Den Haag, 2001
- Stallings, W., Network security essentials, Applications and standards second edition, Prentice Hall, New Jersey, 2003
- Verschuren, P., and H. Doorewaard, Designing a research project, Lemma, Utrecht, 1999
- Woodward, J., and N. Orlans, P. Higgins, Biometrics, Identity assurance in the information age, McGraw-Hill, Osborne, 2003
- Zweers, K., and K. Planqué, Electronic government in the US. From an organization-based perspective towards a client oriented approach, In: J.E.J. Prins (ed.), Designing e-Government, On the crossroads of technological innovation and institutional change, Kluwer Law International, The Hague, 2002, p. 91-120

Internet sites

- Abitz.com
Der Schlüssel für Ihren Rechner, 23-08-2004, <http://www.abitz.com/peripherie/rainbow.php3>

BPRBZK.nl 01

De gegevens verzameling van de GBA, 22-07-2004, www.bprbzk.nl

BPRBZK.nl 02

2b or not 2b, Doe mee aan de praktijkproef biometrie en ontvang 10 € korting!, 27-08-2004, <http://www.bprbzk.nl/downloads/BPR001.ex.FolderA5.DEF.040621.pdf>

burger.overheid.nl

Wereldwijd vijf voordelen van e-government, 31-05-2004, <http://www.burger.overheid.nl/nieuws/?id=358>

Burgerpin.nl

Wat is de Nieuwe Authenticatie Voorziening (NAV)?, 28-07-2004, <http://www.burgerpin.nl/allesoverNAV.htm>

CBS.nl

Gemeentelijke indeling op 1 januari 2004, Wijzigingen in de gemeentelijke indeling per 1 januari 2004, 19-05-2004, <http://www.cbs.nl/nl/standaarden/classificaties/gemeentelijke-indelingen/gemeenten2004-inleiding.htm>

CBS.nl 02

Bevolkingsteller, 16-09-2004, <http://www.cbs.nl/nl/cijfers/bevolkingsteller/popclocknl.asp>

cordis.lu 01

Information Society Technologies, 08-06-2004, <http://www.cordis.lu/ist/home.html>

cordis.lu 02

Instruments, 08-06-2004, <http://www.cordis.lu/fp6/instruments-print.htm>

Den Haag.nl

24-07-2004, www.denhaag.nl

Dordrecht.nl

06-09-2004, www.dordrecht.nl

Ecp.nl

Vertrouwen krijgen in eNederland met e-Ok keurmerk, 30-07-2004, <http://www.ecp.nl/persbericht.php?id=28>

enschede.nl

06-09-2004, www.enschede.nl

GSA.gov

E-gov delivers benefits on many fronts, 04-10-2004, http://www.gsa.gov/Portal/gsa/ep/contentView.do?noc=T&contentType=GSA_BASIC&contentId=8943

Gu.edu.au

11-11-2004, www.int.gu.edu.au/courses/2010int/crypto.html

hoorn.nl
06-09-2004, www.hoorn.nl

IBIA.org
International Biometric Industry Association, Frequently Asked Questions about Biometric Technology, 02-07-2004, www.IBIA.org

Justitie.nl
19-10-2004,
http://www.justitie.nl/publicaties/brochures_en_factsheets/elektronische_handtekeningen.asp

Minbzk.nl 01
“Zo snel mogelijk naar een elektronische overheid”, 14-06-2004,
http://www.minbzk.nl/ict_en_de_overheid/overheid_on_line/inspringthema_s/betere_dienstverlen_i/persberichten/kabinet_presenteert

Minbzk.nl 02
Biometrie in reisdocumenten, brief aan de tweede kamer, 27-08-2004,
http://www.minbzk.nl/contents/pages/1010/brief_tk_biometrieinreisdocumenten.pdf

Mycom.nl
Mobiele opslag; USB drives, 20-09-2004,
<http://silverappl.mycom.nl/MyCom/Store/productdetailedinfo.do?productID=57470&productType=1>

NICTIZ.nl
27-08-2004, www.NICTIZ.nl

Overheid.nl
15-09-2004, www.overheid.nl

PKIOverheid.nl
19-10-2004, www.pkioverheid.nl

Rtl.nl
23-10-2004,
[www.rtl.nl/\(/actueel/editienl\)/components/actueel/editienl/2004/week41/0510045.xml](http://www.rtl.nl/(/actueel/editienl)/components/actueel/editienl/2004/week41/0510045.xml)

Surfnet.nl
22-11-2004, <http://www.surfnet.nl/publicaties/bulletin/02-4/h6.shtml>

tilburg.nl
06-09-2004, www.tilburg.nl

Wetten.nl
Wet- en regelgeving, Wet elektronische handtekeningen (geldend op: 15-10-2004),
<http://wetten.overheid.nl/cgi-bin/sessioned/browsercheck/continuation=26570-002/session=775463174013336/action=javascript-result/javascript=yes>

wmrc.com

Global survey shows USA takes the lead in online government, Independent analysis shows that even the leaders have failed to deliver effective online government, 25-05-2004,
http://www.wmrc.com/press_release/20011018-5.pdf

Wordiq.com

Wordiq, where words have meaning, encyclopedia, 03-06-2004,
<http://www.wordiq.com/definition/Service>

Reports

CWI

Albrecht, A. et al, BioVision: Roadmap for Biometrics In Europe to 2010, CWI Report PNA-E0303, 08-12-2003

Eikenboom

Eikenboom, M., and M. van Dam, Eindrapport Nulmeting elektronische dienstverlening gemeente Den Haag, project Majesteit, 26-01-2004

eMayor 01

eMayor Consortium, eMayor project report D2.1 Municipal services- Analysis, requirements and usage scenarios, 15-04-2004

eMayor 02

eMayor Consortium, eMayor project report Specific Targeted Research or Innovation Project, Annex I- "Description of work", Electronic and Secure Municipal Administration for European Citizens, 17-12-2003

eMayor 03

eMayor Consortium, eMayor project report D2.2, Analysis related to security and PKI services for SMGOs, p. 85-86, 04-06-2004

Raad van State

Raad van State, Elektronisch aanvragen VIND producten Burgerzaken, 12-09-2003

Publications

Bolchini

Bolchini, C., and F. Salice, F. Schreiber, L. Tanca, Logical and Physical Design Issues for Smart Card Databases, ACM Transactions on Information Systems, Vol. 21, No. 3, 07-2003, pages 254-285

Kelfkens

Kelfkens, G., Chip op pasjes zet fraudeurs de voet dwars, Automatiseringsgids # 35, 27-08-2004, page 9