Trusting SECaaS in 6G Networks

Exploring Customer Trust and Value Interactions in Security Services Across Different 6G Deployments

Rohit Pandit

Delft University of Technology

TU Delft

Trusting SECaaS in 6G Networks

Exploring Customer Trust and Value Interactions in Security Services Across Different 6G Deployments

by

Rohit Pandit
Student ID: 5928915

Master thesis submitted to Delft University of Technology in
partial fulfilment of the requirements for the degree of
Master of Science
in Management of Technology
to be defended publicly on 18th July 2025

Graduation Committee:

Chairperson:	Dr. A.Y. (Aaron) Ding	Department of ICT
First Supervisor:	Dr.ir. G.A. (Mark) de Reuver	Department of ICT
Second Supervisor:	Dr. J.G. (Johannes) Gartner	Department of DCE

TU Delft

ENSURE-6G

Acknowledgement

Coming from a calculator-wielding mechanical engineering background, I never imagined I'd one day be drawn into exploring how technology functions as a corporate resource, something I came to appreciate through the lens of the Management of Technology programme at TU Delft. I'm especially grateful to those early voices who sparked that shift and opened the door to the complexities and opportunities of the management world, and particularly those who introduced me to the fast-moving world of connectivity, space and spectrum, where my fascination with telecommunications truly began. In the end, I hope to inspire someone reading this thesis to look at technology from an all-new perspective.

I would like to express my deepest gratitude to my thesis supervisor, Mark, for his continuous guidance, thoughtful feedback and steady encouragement throughout this journey. His insights and recommendations helped me navigate the messier parts of the research process, and his trust in my work gave me the confidence to keep pushing forward. I'm especially thankful for his ability to challenge my thinking while always having my back. I'm also incredibly thankful to Johannes and Aaron, whose input at key moments kept the project grounded and moving in the right direction. Their support, sometimes even when delivered over a tight calendar, was always thoughtful and appreciated.

To the industry and academic professionals who agreed to participate in my interviews, this research would not have been possible without your time, openness, and domain expertise. Your perspectives didn't just inform the findings; they brought them to life. More than once, I found myself thinking, "That's the kind of insight I hadn't considered, even after reading countless papers." I'm also deeply grateful to those who helped connect me with these individuals; your behind-the-scenes support and introductions played a crucial role in making this research possible.

To my parents and sister, thank you for always being the calm in the storm. Your patience, unconditional support, and occasional reminders to eat and sleep made more difference than you know. To my peers at MOT and TU Delft, whom I shared long study sessions fueled by an endless supply of coffee, this one's for us. Finally, somewhere between late nights, messy codebooks, stubborn LaTeX errors and too many 'final_final_v4' files, I kept thinking of the quote from an AC/DC record: "It's a long way to the top if you wanna Rock 'n' Roll" Turns out, that applies to a master thesis as well!

Rohit Pandit
Delft, July 2025

Executive Summary

The emergence of Sixth Generation Mobile Network (6G) mobile networks promises unprecedented performance capabilities and novel use cases, such as holographic communication, autonomous driving, and Artificial Intelligence (AI) native operations. To meet these demanding requirements, 6G is expected to adopt decentralised network architectures, supporting distributed data storage and dynamic service provisioning across the network. Whilst such deployments offer significant technical advantages and operational flexibility, they also introduce new security challenges. In particular, the increased complexity and distribution of these networks make it more difficult to detect threats, prevent unauthorised access, and respond effectively to security incidents.

Even in the conventional centralised public 5G mobile networks, concerns around security and privacy have already played a major role in shaping enterprise adoption decisions. These issues are expected to become even more significant in future 6G networks, not only because of the growing number of potential entry points for attacks and increased network complexity, but also due to the integration of AI. Whilst AI is seen as a key component in enabling the capabilities of next-generation networks, it also presents new risks. It may become both a target for attacks and a means through which malicious threats are carried out, adding further pressure to the overall security landscape.

In this context, Security-as-a-Service (SECaaS) presents a promising approach to addressing the security challenges expected in 6G networks. Building on the principles of Software-as-a-Service (SaaS), SECaaS allows enterprise firms to outsource their security needs to specialised providers. This model reduces operational costs by enabling firms to pay only for the security services they use, while ensuring compliance with regulatory and standards requirements. It also provides up-to-date protection through dedicated security experts, removing the need for costly on-site infrastructure or internal expertise.

However, existing research has largely examined SECaaS within centralised cloud environments, offering limited insight into how it must evolve to suit decentralised 6G networks. Unlike traditional centralised architectures, where cloud providers or a Mobile Network Operator (MNO) manage end-to-end connectivity, 6G is expected to support Non-Public Networks (NPNs), networks that can be independently deployed and managed without reliance on a central MNO. These decentralised networks bring intelligence, data storage and service provisioning closer to the user, introducing new challenges around security integration and management that remain largely unexplored in the SECaaS context. In particular, it remains unclear how a SECaaS provider creates value for customers within complex, multi-stakeholder 6G ecosystems.

In research on the evolving 6G standard, a central vision is to embed trust across all elements of the network and its services. Beyond serving as a differentiator, customer trust in a firm offering SECaaS solutions is recognised as a critical factor for service adoption. While existing literature has identified several antecedents of trust in SECaaS providers, it remains uncertain how these are influenced by network decentralisation. Decentralised NPNs create opportunities for local providers to offer more tailored services, yet they may also raise concerns around service quality, both of which can significantly shape customer trust. Moreover, trust and value creation are often linked in a reciprocal relationship: trust fosters collaboration and value co-creation, which in turn strengthens customer trust. However, this dynamic remains unexplored, particularly in the context of SECaaS models in 6G deployments.

This thesis explores what SECaaS would entail in the 6G context, identifying relevant stakeholders and proposing primary and secondary shared responsibilities along with exploring how different 6G deployment models, centralised public networks and decentralised Non-Public Networks (NPNs), shape the interactions among SECaaS stakeholders in co-creating value within a multi-stakeholder ecosystem. It also examines how network decentralisation potentially influences the antecedents of customer trust in SECaaS providers. Framed within the context of the EU-funded Ensure-6G project, the study contributes to both technical and strategic discussions on designing viable business models for security solutions in next-generation mobile networks.

Research Question: How does network decentralisation in 6G deployments influence techno-economic interactions and customer trust in SECaaS providers?

In this highly explorative study, a qualitative methodology was adopted, involving ten semi-structured interviews with stakeholders from the telecom, security, and infrastructure domains. Several participants brought both technical expertise and commercial experience in delivering security solutions and services to customers. The interviews were analysed through thematic coding and structured using two complementary frameworks: the Value Network Configuration (VNC) to map techno-economic roles and interactions, and the Integrative Model of Organisational Trust to examine trust dynamics across varying network deployments.

Findings reveal that SECaaS in the context of 6G encompasses protective, detective, and reactive functionalities that are outsourced from external providers and deployed across both edge locations or user devices and the central network or cloud layers. This distribution ensures that appropriate security solutions are delivered at the right points within the network. In enabling these services, four key stakeholder groups were identified: infrastructure providers, telecom providers, security technology vendors, and SECaaS providers. While ambiguity remains regarding the exact responsibilities for provisioning and managing network infrastructure, connectivity, and security services in 6G, this study proposes a set of primary and shared secondary responsibilities for each actor.

In summary, the security technology vendor is primarily responsible for developing and provisioning the security hardware and software tools, such as firewalls and threat detection systems. The SECaaS provider acts as an intermediary between these vendors and the end users, integrating various security tools into a cohesive, bundled solution tailored to the specific requirements of each customer. This process of integration and customisation represents the core mechanism through which the SECaaS provider creates value within the 6G network ecosystem.

Moreover, in centralised public network deployments, the MNO typically assumes the role of the SECaaS provider, offering both connectivity and security services. This concentrates value creation around the MNO, despite the broader shift away from MNO-centric business models in 6G networks. In contrast, decentralised NPNs offer greater flexibility, enabling users to contract local providers for connectivity and security services, potentially operating entirely independently of a central MNO. However, the VNC analysis reveals that such decentralised architectures require enhanced stakeholder coordination frameworks due to the increased number of actors involved. For example, additional mechanisms are needed to enable an external SECaaS provider to securely access customer data and operate within a local network managed by a separate local network provider.

Trust in SECaaS providers was found to be a prerequisite for service adoption, with a reciprocal dynamic observed: trust enables value co-creation with the customer, which in turn reinforces trust in the provider. The interviews identified several antecedents of customer trust, which were grouped into three main categories. Relational factors are shaped through direct interactions between the provider and the customer. Organisational factors relate to the firm's perceived reputation, capability, accountability and track record of delivering reliable services. Finally, external factors represent a newly proposed category, encompassing elements such as regulatory certifications and geopolitical influences, which typically lie beyond the direct control of the firm.

The study finds that network decentralisation does not directly alter the identified antecedents of customer trust. Participants noted that many customers are not technically or security aware and therefore tend to base their trust in a provider on organisational and external factors, regardless of how the network is deployed. However, the study suggests that decentralisation could indirectly strengthen relational trust. Decentralised NPN deployments create opportunities for local connectivity and security providers, who are better positioned to leverage their proximity, customer intimacy, and contextual understanding. These elements can enhance customer relationships and foster greater trust in the SECaaS provider.

The study makes three key academic contributions. First, it proposes a set of primary and shared secondary responsibilities for the main stakeholders involved in deploying SECaaS solutions. Second, by analysing value network configurations across varying levels of network decentralisation, it maps how the SECaaS provider co-creates value in different deployment models and highlights how this

co-creation becomes more fragmented in decentralised 6G NPNs. Third, it advances the understanding of customer trust in SECaaS providers by identifying emerging antecedents, such as geopolitical influences and regulatory certifications, and by exploring how decentralised network architectures can indirectly strengthen relational trust through proximity, contextual awareness, and customer intimacy.

From a managerial perspective, the study provides practical guidance for firms seeking to adopt the SECaaS model. It enables prospective providers to map key stakeholders on a power-interest matrix, helping them assess the influence of each stakeholder and manage their requirements effectively. For large multinational firms, the study highlights the importance of adopting flexible organisational structures that preserve brand reputation while enabling operational agility. This balance allows them to foster customer intimacy and proximity, both of which are essential for building trust. Additionally, since trust is a prerequisite for service adoption, the study recommends that all SECaaS providers, regardless of size, ensure compliance with regulatory certifications. These certifications not only demonstrate a minimum standard of security but also serve as a critical foundation for establishing customer trust.

Additionally, this study supports the development of a viable SECaaS business model by examining how value is created through the integration and delivery of security services. Understanding this value creation process is a crucial component of any business model and serves as a foundation for evaluating the feasibility of offering SECaaS in 6G networks. The study also identifies a potential strategic opportunity for SECaaS providers to support the transition from centralised to decentralised security architectures by offering services that facilitate the migration of existing tools and solutions in 5G networks into decentralised 6G deployments.

Like any study, this research has its limitations. A key limitation lies in the disconnect between academic expectations of 6G networks and current industry practices, where many stakeholders are still focused on deploying and realising use cases within 5G networks. As a result, some participants perceived 6G as a distant or even dystopian concept, often characterised by overly ambitious visions and fragmented decentralised networks. Furthermore, due to the highly explorative nature of the study and the complexity of the topic, no single participant could provide comprehensive expertise across both technical and commercial dimensions. Instead, insights emerged through complementary perspectives across interviews, technically focused participants often lacked detailed awareness of how customer trust is built or varies across contexts, whereas commercially aligned participants, such as sales engineers, could speak to customer relationships but were less familiar with the technical potential and challenges of future 6G networks.

Finally, the study recommends that future research investigate the interrelationships between the identified antecedents of trust, particularly how they may influence one another. Quantitative research could be used to statistically evaluate the relative importance of each group of antecedents in shaping customer trust in a SECaaS provider. Additionally, longitudinal studies across different industries are encouraged to examine whether sector-specific use cases lead to varying techno-economic interactions and distinct security and privacy requirements. Lastly, as this study finds no major direct impact of network decentralisation on the antecedents of trust, possibly due to current limited stakeholder and customer awareness, it proposes that a similar study be conducted once the 6G standard is finalised but before widespread deployment of decentralised NPNs, to assess whether these findings remain consistent in a more mature technological context.

Contents

List of Figures

List of Tables

Abbreviations

5G Fifth Generation Mobile Network
5G-SA 5G-Standalone
6G Sixth Generation Mobile Network

AI Artificial Intelligence
API Application Programming Interface

BCDR Business Continuity and Disaster Recovery
BCI Brain Computer Interactions

CRAS Connected Robotics and Autonomous Systems
CSA Cloud Security Alliance

DDoS Distributed Denial of Service
DLP Data Loss and Prevention

eMBB Enhanced Mobile Broadband
EN Encryption
ES Email Security

HAP High Altitude Platform

IaaS Infrastructure-as-a-Service
IAM Identity and Access Management
IIoT Industrial Internet of Things
IM Intrusion Management
InP Infrastructure Providers
IoT Internet of Things
IRS Intelligent Reflecting Surfaces
ITU International Telecommunications Union

KPI Key Performance Indicator

M2M Machine to Machine
Massive MIMO Massive Multiple Input Multiple Output
MDR Managed Detection and Response
MEC Multi-access Edge Computing
ML Machine Learning
mMTC Massive Machine Type Communications
mmWave Millimetre Wave
MNO Mobile Network Operator

MTD Moving Target Defence
MVNO Mobile Virtual Network Operator

NFV Network Function Virtualisation
NIST National Institute of Standards and Technology
NPN Non-Public Network
NS Network Security
NTN Non Terrestrial Network

O-RAN Open Radio Access Network

PaaS Platform-as-a-Service
PNI-NPN Public Network Integrated Non-Public Network

QKD Quantum Key Distribution

RAN Radio Access Network

S-NPN Standalone Non-Public Network
SA Security Assessment
SaaS Software-as-a-Service
SASE Secure Access Service Edge
SD-WAN Software Defined Wide Area Network
SDN Software Defined Network
SECaaS Security-as-a-Service
SIEM Security Information and Event Management
SLA Service Level Agreement

THz Terahertz
TN Terrestrial Network

UAV Unmanned Aerial Vehicle
UE User Equipment
URLLC Ultra Reliable Low Latency Communications

VNC Value Network Configuration

WS Web Security

XAI Explainable Artificial Intelligence
XR Extended Reality

1 Introduction

1.1. Background

While global Fifth Generation Mobile Network (5G) networks continue to be deployed, the academic and industry research communities have already begun exploring the next generation of mobile communications, Sixth Generation Mobile Network (6G). Early visions of 6G suggest that it will not only be an evolution of the current 5G standard but a significant transformation in mobile communications (Letaief et al., 2019). With network deployments expected to roll out by 2030 this new generation of mobile networks is expected to enable innovative new applications like smart healthcare, massive Internet of Things (IoT), digital twins and autonomous mobility (Jiang et al., 2021). These demanding applications are expected to require intense computational power at multiple layers in the network chain, leading to the emergence of end-to-end service applications (Nguyen et al., 2021).

Furthermore, in shaping the future of 6G, Latva-aho and Leppänen (2019) and Yrjölä et al. (2020) advocates for a human-centric approach that prioritises the seamless integration of the physical and digital worlds. This vision underpins the development of advanced use cases such as extended reality Extended Reality (XR), holographic communication, and immersive digital experiences (Veith et al., 2023; Xiang et al., 2024). To enable these demanding applications, research outlines ambitious technical targets for 6G, including end-to-end latency of 1 millisecond and throughput speeds approaching 1000 Mbps (Latva-aho & Leppänen, 2019; Letaief et al., 2019). Additionally, 6G aims to provide ubiquitous global coverage by integrating satellite and cellular networks into a unified network. A defining feature of this generation will be its AI-native approach, where AI is not merely an add-on but embedded at every layer of the network (Siriwardhana et al., 2021).

To support its performance and resilience requirements, 6G architectures are expected to adopt decentralised network designs, enabling distributed data storage and dynamic service migration across nodes (Qiao et al., 2020). However, whilst these designs offer technological flexibility and scalability, they also introduce significant security challenges. The complexity and heterogeneity of such distributed infrastructures make it increasingly difficult to detect malware, prevent intrusions, and respond effectively to breaches. Notably, even within the relatively centralised architecture of 5G, security and privacy were already identified as critical factors influencing enterprise adoption (Jiang et al., 2021). These concerns are magnified in 6G, not only due to the expansion of attack surfaces and infrastructural fragmentation but also because of the integration of AI. Although AI is envisioned as a core enabler of in 6G, it also introduces novel vulnerabilities. Literature warns that AI could act as both a target and a tool for malicious activity within these networks, further intensifying the security landscape (Benzaïd & Taleb, 2020).

To address these emerging security challenges, researchers propose two major developments anticipated in the 6G landscape. The first is the broader adoption and simplified deployment of a service-based model for security solutions commonly known as Security-as-a-Service (SECaaS) across the network (Nguyen et al., 2021). As a subset of the Software-as-a-Service (SaaS) paradigm, SECaaS is a commonly adopted service model in the cloud computation domain which enables organisations to outsource their security operations to specialised providers (Ngo-Ye et al., 2020). The second devel-

opment involves the advancement of AI models, enhancing their ability to proactively learn from and respond to diverse and evolving threats (Nguyen et al., 2021). AI is expected to serve as a foundational component of 6G networks, driving intelligent operations across various network deployments (Letaief et al., 2019; Qiao et al., 2020).

The SECaaS model offers several advantages to users, enabling them to subscribe only to the security services they require, thereby avoiding the need for costly on-site infrastructure. It also allows organisations to delegate security responsibilities to specialised providers, ensuring that their systems remain updated and compliant with evolving regulatory standards (Ngo-Ye et al., 2020). For SECaaS providers, customer trust has been identified as a critical factor influencing market adoption (Ngo-Ye et al., 2020; Senk, 2013). This emphasis on trust becomes even more significant in the context of 6G, where early visions advocate for embedding trust mechanisms directly into the network design, building upon the work done in 5G and further promoting a secure-by-default architecture from the outset (Latva-aho & Leppänen, 2019; Ylianttila et al., 2020).

Furthermore, for SECaaS providers, it is essential to differentiate their offerings by creating additional value for end users (W. Wang & Yongchareon, 2020). However, the evolving future 6G ecosystems mark a fundamental shift in how value is created and distributed (Yrjölä et al., 2020). Unlike traditional models where a single actor was responsible for delivering end-to-end connectivity and services, 6G envisions a collaborative, multi-stakeholder environment (Xiang et al., 2024). In this ecosystem, value is co-created and shared among actors with diverse roles and capabilities (Aagaard et al., 2024; Porambage et al., 2025) through a sharing of technical and economic interactions across the network (Basaure et al., 2024). Consequently, 6G is increasingly regarded as a general-purpose technology that enables both horizontal and vertical value co-creation, moving away from linear value chains towards more dynamic, network-based models (Yrjölä et al., 2022). As the SECaaS model was originally developed for centralised cloud computing domains (Chaisiri et al., 2015), its evolution into decentralised networks with multi-stakeholder ecosystems in 6G environments creates a complex dynamic and a new area of active exploration and development for how SECaaS providers can co-create value.

In summary, the vision for 6G presents a compelling yet complex transformation of mobile networks, characterised by decentralised architectures, AI-native operations, and integrated trust mechanisms. These technological and structural shifts create a dynamic and fragmented environment in which security must be reimagined. As the SECaaS model is expected to gain prominence, it should offer a flexible and scalable means of addressing these security needs. However, the adoption of SECaaS in the 6G context introduces new challenges for providers. These include managing emerging AI-driven threats, operating within increasingly decentralised infrastructures, and navigating trust relationships across a diverse set of stakeholders co-creating value within the network. As such, offering SECaaS solutions in 6G requires firms to not only adapt to novel technological demands but also to reposition themselves within a rapidly evolving value ecosystem, making it a timely and strategic challenge for future research and industry alike.

1.2. Context of the Present Study

Research into securing next-generation mobile networks is already gaining traction across Europe. A key example is the Ensure-6G project, funded under the EU Horizon Europe programme, which brings together a broad consortium of academic and industry stakeholders to develop and validate security and privacy solutions for 6G networks. The project contributes to foundational academic work aimed at building a secure-by-default and trustworthy 6G ecosystem (Ensure-6G, 2024). As part of this initiative, TU Delft is actively involved in exploring one of the project's scientific objectives: assessing how 6G security and privacy solutions affect business models and the economic viability of delivering security solutions in 6G. Situated within this evolving research landscape, this thesis contributes by examining how firms offering SECaaS solutions must navigate the complex challenges introduced by emerging threats, novel technologies and multiple stakeholder involvements in future 6G ecosystems.

Whilst the SECaaS model has been widely studied within cloud-based architectures, research examining its application in mobile communication networks, especially in the context of 6G, remains limited. Existing studies primarily address SECaaS from a traditional centralised deployment perspective, which fails to reflect the decentralised, distributed nature envisioned for future 6G architectures. This

presents a critical gap in understanding how SECaaS models must evolve to align with the technical and organisational transformations 6G is expected to bring. As 6G networks move towards service-based, decentralised deployments, potentially integrating cellular and satellite components, the mechanisms through which SECaaS can deliver value, and ensure resilience require renewed investigation from a technological and economic standpoint.

In addition to architectural shifts, the complexity of stakeholder interactions in 6G further complicates the landscape for SECaaS providers. 6G is expected to be shaped by highly collaborative ecosystems, where security responsibilities are increasingly distributed across multiple actors. These actors are likely to co-create both horizontal and vertical value propositions, enabled by the general-purpose nature of 6G technology. Understanding how such actors interact, technologically and economically, is therefore essential. Yet, current research offers limited insight into these techno-economic interactions: the dynamic relationships between technological dependencies, economic incentives and organisational responsibilities that define how value is co-created in 6G security contexts.

Moreover, the complexity of stakeholder interactions in 6G further complicates the landscape for SECaaS providers. As 6G networks are expected to emerge through collaborative ecosystems, security responsibilities become increasingly fragmented, particularly as firms explore both horizontal and vertical value propositions enabled by 6G as a general-purpose technology. In this context, trust will be a critical factor influencing the adoption of SECaaS solutions. However, the decentralised and distributed nature of 6G networks raises new questions about how trust dynamics may vary across different deployment scenarios. While existing studies provide insights into the antecedents of trust in SECaaS providers, they are largely confined to the cloud computing domain and assume traditional, centralised architectures, thus failing to account for the structural and relational complexities introduced by decentralised mobile networks.

1.3. Research Gap

Given the expected development of SECaaS models in 6G networks (Nguyen et al., 2021), this thesis addresses the emerging gap in understanding how these models can be adapted to decentralised 6G network architectures. It presents an exploratory study conducted from the perspective of a firm seeking to become a SECaaS provider in 6G, aiming to understand how best to position itself within this evolving ecosystem. While W. Wang and Yongchareon (2020) provides a comprehensive review of SECaaS categories and functional groupings in the cloud computing domain, existing research does not sufficiently examine how SECaaS might operate within the context of 6G, nor does it identify the key stakeholders involved in deploying such solutions. This gap stems from the fundamental differences between cloud and 6G environments: cloud-based SECaaS models are built around centralised infrastructures, whereas 6G introduces decentralised architectures, edge-native deployments, and context-specific end-to-end service delivery. These shifts fundamentally reshape how security services are provisioned, managed, and consumed, rendering a direct transfer of cloud-based knowledge insufficient without adaptation.

Furthermore, while Basaure et al. (2024) provide a valuable perspective by comparing techno-economic interactions in centralised and localised 6G deployments for digital twin applications, existing literature does not yet examine how such interactions evolve within the more complex and collaborative SECaaS ecosystems, particularly as networks shift from centralised to decentralised architectures. Additionally, although trust is widely recognised as a critical factor influencing the adoption of SECaaS solutions, and existing studies propose frameworks for categorising the antecedents of trust in SECaaS providers (Ngo-Ye et al., 2020; Senk, 2013), these insights are primarily derived from cloud-based environments. There remains a limited understanding of how trust in SECaaS providers is shaped within the dynamic and distributed context of mobile networks, particularly those envisioned for 6G. Moreover, how trust dynamics differ across centralised, decentralised, or hybrid deployments has not been adequately explored. As decentralisation enables greater user-specific customisation and potentially enhances network security, it may also introduce new concerns around service provisioning and quality assurance, factors that can significantly influence customer trust in SECaaS providers.

Addressing this gap is essential not only from a technical and architectural perspective but also from a strategic and organisational one. As SECaaS providers seek to enter or expand within the 6G space,

they must navigate a changing landscape where value is co-created with diverse actors and trust becomes an enabler of adoption. Understanding how decentralised deployments affect value co-creation and trust relationships is thus critical for developing viable business models. By exploring how trust dynamics and stakeholder roles vary across centralised and decentralised deployments, this thesis aims to support firms in shaping viable business models for SECaaS solutions in the 6G networks.

1.4. Research Objective and Question

This research aims to explore the techno-economic interactions between stakeholders and the trust dynamics that characterise SECaaS solutions across centralised and decentralised 6G network deployments. To achieve this aim, the research is utilises the following main research question:

"How does network decentralisation in 6G deployments influence techno-economic interactions and customer trust in SECaaS providers?"

Additionally, based on this main question, further sub-research questions are developed to guide the research as follows:

SQ1: "What constitutes SECaaS in the context of 6G networks?"

SQ2: "Who are the key stakeholders involved in deploying SECaaS solutions in 6G networks?"

SQ3: "How does network decentralisation influence techno-economic interactions between SECaaS stakeholders in 6G deployments?"

SQ4: "How does network decentralisation influence the antecedents of customer trust in SECaaS providers?"

1.5. Remaining Structure of the Thesis

Having arrived at the main research question and the guiding sub-research questions, this remaining thesis is structured in the following way: Chapter 2 covers the existing literature about the topic specifically looking at the technical concepts in Chapter 2.1, followed by the related theoretical publishing are discussed in Chapter 2.2 and is concluded with the emerging literature gap in Chapter 2.3.

Following this, in Chapter 3, the research methodology adopted for this study is presented, describing the qualtiative resrarch approach used in this study in Chapter 3.1. This is followed by Chapter 3.2 describing how the data is collected in this thesis using interviews, including the sampling strategy employed and interview protocol used. Lastly, this is concluded with Chapter 3.3, discussing how the gathered data is analysed using thematic coding to form emerging themes.

Subsequently, in Chapter 4, the insights and findings from the data analysis of the interviews are presented. Finally, in Chapter 5 each sub-research question, and therefore by extension the research question, is answered based on the findings and discussions. The chapter concludes by addressing the limitations of the study in Chapter 5.2, the recommendations for future research domain in Chapter 5.3 and concludes with Chapter 5.4 which reflects on the alignment between this thesis and the Management of Technology programme.

2

Literature Review

This section will explore the existing literature about the technical and theoretical domains. First, in Chapter 2.1, the technical concepts are discussed to help explain terminologies in 6G mobile networks, network deployments, security concerns, Artificial Intelligence (AI) in 6G security and Security-as-a-Service (SECaaS). Next, in Chapter 2.2, the related theoretical academic publishings regarding 6G stakeholder analysis, value interactions and customer trust are discussed. Finally, after examining and analysing the key concepts, the literature gap is identified and discussed in Chapter 2.3.

2.1. Technical Background

The advent of 6G networks represents a significant evolution in wireless communication, characterised by diverse network deployment models ranging from centralised to decentralised architectures. This transformation brings new security challenges and opportunities, particularly with the increasing integration of Artificial Intelligence (AI) to enhance security capabilities. Understanding these technical dimensions, including the fundamentals of SECaaS, is essential for framing the stakeholder interactions, value creation and trust dynamics within 6G ecosystems. This section provides a foundational overview of these key concepts, setting the stage for a deeper exploration of SECaaS and its role in addressing emerging security demands.

2.1.1. Current 5G Mobile Networks

The standardisation body responsible for mobile communications, 3GPP, finalised the first phase of 5G with Release 15 at the end of 2019 (3GPP, 2022). 5G introduces a comprehensive transformation in both radio access and core network architecture, moving beyond incremental enhancements to previous LTE networks. It is designed to meet diverse requirements through three core service categories: Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (mMTC), and Ultra Reliable Low Latency Communications (URLLC) (Agiwal et al., 2021; Liu et al., 2020). To support these capabilities, 5G leverages new spectrum bands defined under the 5G New Radio (5G NR) specification, including both sub-6 GHz and Millimetre Wave (mmWave) frequencies, which offer high capacity but also pose technical challenges such as limited range and sensitivity to blockage (Pi & Khan, 2011).

In its initial rollout, 5G has largely followed a non-standalone (NSA) deployment model, which builds on existing 4G infrastructure to accelerate adoption while minimising costs (Agiwal et al., 2021). A key enabler in this transition is dual connectivity, allowing user devices to connect simultaneously to 4G and 5G base stations (Access, 2015), thereby improving reliability and throughput, particularly in urban hotspots. Over time, the goal is to shift toward 5G-Standalone (5G-SA), which relies fully on the 5G Core and is built on virtualisation and software-defined networking principles (Agiwal et al., 2021). These standalone networks offer advanced capabilities such as network slicing and are seen as foundational for the future beyond-5G and 6G networks, supporting more demanding use cases across industries and domains (Aagaard et al., 2024).

2.1.2. Envisioned 6G Mobile Networks

As 5G continues to mature and expand globally, attention from researchers and industry has increasingly turned to the next generation of mobile communications, Sixth Generation Mobile Network (6G) (Chowdhury et al., 2020; Jiang et al., 2021). The ongoing deployment of 5G has exposed certain limitations and with the rapid rise in connectivity demands, interest in 6G as the next major technological advancement is accelerating (Chowdhury et al., 2020; M. Wang et al., 2020). With commercial deployment anticipated around 2030, Latva-aho and Leppänen (2019) envisioned 6G as a fundamentally transformative shift in mobile communications, setting it apart from earlier generations.

The 6G vision is already being shaped in research, aiming to seamlessly blend the digital and physical worlds, with humans at the centre of an array of network-driven applications (Veith et al., 2023). A central vision is the integration of ubiquitous wireless intelligence, where 6G will facilitate novel connections between the physical and digital domains in real-time by linking biological systems and expanding human sensory experiences (Latva-aho & Leppänen, 2019; Yrjölä et al., 2020). Furthermore, it will build upon existing 5G methods to support higher data rates, massive connectivity and reliability (Jiang et al., 2021; Letaief et al., 2019; Xiang et al., 2024).

The key driver for 6G is the predicted exponential growth of mobile network traffic and subscriptions, especially due to the introduction of data-intensive applications, cloud services, smart devices and Machine to Machine (M2M) communications (Chowdhury et al., 2020; Jiang et al., 2021). For instance, the International Telecommunications Union (ITU) estimates that by 2030, every mobile user will consume nearly 250 Gigabytes (GB) per month, as compared to 5 GB per month in 2020 (International Telecommunication Union (ITU), 2015). In a recent report, Ericsson revised this to around 280 GB per month (Ericsson, 2025). With estimates of around 6.5 billion unique mobile subscribers in 2030, as compared to 5.8 billion in 2024 (GSMA, 2025a), global mobile data traffic is expected to exceed nearly 1.6 Zettabytes (ZB) per month[1] in 2030. Furthermore, M2Ms communication will only further add to this with an expected 97 billion subscriptions adding over 600 EB/month in traffic volume by 2030 (Chowdhury et al., 2020; Jiang et al., 2021).

Moreover, 6G's development will also be influenced by societal needs such as resilience, sustainability, inclusivity and empowerment. These aspects will be shaped by broader political, economic, social, technological, legal and environmental (PESTLE) drivers (Latva-aho & Leppänen, 2019; Yrjölä et al., 2020; Yrjölä et al., 2022). The human-centric focus will seamlessly integrate the digital and physical worlds, enabling promising novel use cases including multisensory XR applications, Connected Robotics and Autonomous Systems (CRAS), wireless Brain Computer Interactions (BCI), holographic telepresence, advanced health services, smart manufacturing and real-time digital twins (Campoy et al., 2025; Chowdhury et al., 2020; Christopoulou et al., 2025; Jiang et al., 2021)

To support these novel applications, 6G networks aim to deliver significant performance improvements over 5G, guided by a new set of Key Performance Indicators (KPIs). These enhancements are summarised in Table 2.1, based on insights from Chowdhury et al. (2020), Jiang et al. (2021), and Letaief et al. (2019). Peak data rates are expected to rise dramatically from 10 Gbps in 5G to a projected 1000 Gbps (1 Tbps) in 6G, while the actual experienced data rate for the user is expected to rise tenfold, from 100 Mbps to 1000 Mbps. End-to-end latency will be reduced from 10 milliseconds in 5G to as low as 1 millisecond, with some proposals targeting an ultra-low 0.1 milliseconds, enabling near-instantaneous communication. Connection density is expected to grow from 10^6 to 10^7 devices per km^2, accommodating the exponential rise in devices.

[1] 1 zettabyte (ZB) = 1,000 exabytes (EB), 1 EB = 1,000 terabytes (TB), 1 TB = 1,000 gigabytes (GB)

Table 2.1: Performance Metrics and Technology Comparison in 4G, 5G and 6G

Metric	***4G***	***5G***	***6G***
Peak Data Rate (Gbps)	1	10	1000
User Experienced Data Rate (Mbps)	10	100	1000
End-to-End Latency (ms)	100	10	1
Connection Density devices/ km^2	10^5	10^6	10^7
Energy Efficiency (Bit/Joule)	1X	100X	1000X
Reliability (success probability)	99.99%	99.999%	99.99999%
Area Traffic Capacity (Mbps/ m^2)	0.1	10	1000
Mobility Support (km/hr)	350	500	1000
Integration of NTN	None	None	Complete
AI Usage	None	Partial	Complete
Integration of Autonomous Vehicles	None	Partial	Complete
Use of Extended Reality	None	Partial	Complete
Use of Haptic Communication	None	Partial	Complete

Adapted from European Science-Media Hub (2021), Jiang et al. (2021), Krasniqi et al. (2019), and Latva-aho and Leppänen (2019)

To materialise these ambitious KPIs for 6G, a wide range of advanced technologies will need to be developed and integrated. Chowdhury et al. (2020) and Jiang et al. (2021) identify five categories of these technologies: (i) new spectrum to achieve ultra-high-speed communication, notably mmWave and Terahertz (THz) frequencies above 100 GHz; (ii) new networking methods, including the widespread adoption of Network Function Virtualisation (NFV) techniques like Software Defined Network (SDN), enabling functions like Radio Access Network (RAN) slicing and the use of Open Radio Access Network (O-RAN) frameworks; (iii) improvements in the air interface such as Massive Multiple Input Multiple Output (Massive MIMO), and Intelligent Reflecting Surfaces (IRS) to improve signal coverage and spectral efficiency; (iv) novel architectures incorporating Non Terrestrial Networks (NTNs) such as satellite mega-constellations, High Altitude Platforms (HAPs) and Unmanned Aerial Vehicles (UAVs) to ensure ubiquitous and resilient connectivity; (v) new operational paradigm, characterised by the deep integration of communication, computing and storage functions powered by AI, blockchain and digital twins, all operating in tandem with mobile networks.

Unlike previous generations where Mobile Network Operators (MNOs) held end-to-end responsibility, the 6G landscape is shaped by distributed responsibilities across a multi-actor ecosystem, raising fundamental questions about who builds security solutions, who deploys them and who is responsible for managing them. To understand the emerging roles within 6G ecosystems, Yrjölä et al. (2023) identify twenty key stakeholder groups, including conventional stakeholders like MNOs, infrastructure providers and network equipment vendors, but also new emerging stakeholders like marketplace providers, security and privacy enhancing service providers and cloud computing service providers.

By analysing attributes such as power, urgency, and legitimacy, Yrjölä et al. (2023) categorise these stakeholders into three categories: (i) incumbent-born platform, (ii) platform-born adjacent platform and (iii) the novel born-platform and show how they would interact with each other as denoted in Figure 2.1. A multi-sided platform mediates involved stakeholders, such as buyers and sellers, fostering network effects where participation of others increases the value for one stakeholder group (de Reuver et al., 2018). In the emerging 6G ecosystems, multi-sided platforms can be classified by their origin, either developed by incumbents, adjacent to existing platforms, or entirely new ventures and by their position in the value chain, either upstream or downstream (Yrjölä et al., 2023). Incumbent-born platforms usually operate upstream and rely on a core product. Platform-adjacent ones focus downstream, delivering innovative services. Born-digital platforms are independent from the start, built to create new markets with a digital-first approach. For instance, infrastructure providers deliver connectivity and computing power to cloud service providers, who then enable app developers to build novel services for the broader ecosystem.

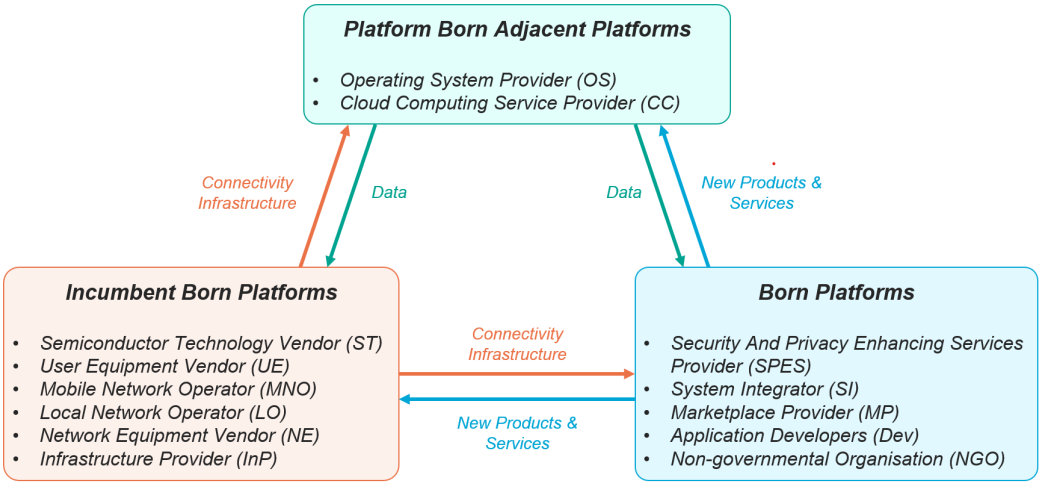

Figure 2.1: 6G Stakeholder Interactions
Adapted from (Yrjölä et al., 2023)

Finally, one of the key defining features of 6G is its deep integration of AI, positioning it not just as a support tool but as a core component of the network itself (Chowdhury et al., 2020; Siriwardhana et al., 2021). Unlike 5G, where AI was limited by conventional architectures and applied more sporadically, 6G aims to be truly "AI-empowered." AI and Machine Learning (ML) will be embedded throughout the architecture - from network design and protocol optimisation to service orchestration and real-time operations, enabling intelligent orchestration and adaptive service management (Siriwardhana et al., 2021; Yrjölä et al., 2020). This shift supports autonomous systems and highly efficient, flexible networks. Additionally, Jiang et al. (2021) note that AI at the network edge will be crucial for achieving low-latency, context-aware processing and decision-making.

2.1.3. Network Deployments

In 6G networks, it is essential to differentiate between traditional centralised deployment models, typically operated by public MNOs, and the emerging decentralised approaches, such as Non-Public Networks (NPNs) (Frank et al., 2022; Qiao et al., 2020). Traditionally, mobile networks serving the general public have been deployed and operated by Mobile Network Operators (MNOs) using a centralised architecture. These networks also followed a vertically integrated supply chain model where the MNO managed the entire infrastructure, essentially creating an MNO-centric system (Basaure et al., 2024; Yrjölä et al., 2020).

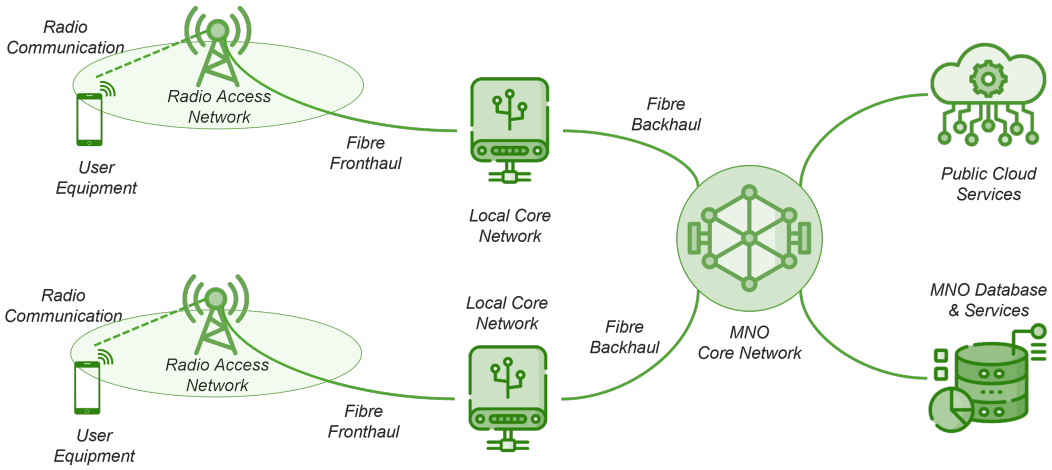

Figure 2.2: Traditional Public Mobile Network Deployment
Adapted from Lam et al. (2022)

In these conventional public networks, as described in Lam et al. (2022), data flow follows through a centralised architecture shown in Figure 2.2. The MNO will distribute a region into cells, providing a local Radio Access Network (RAN) to wirelessly connect to various User Equipment (UE). These individual RANs are connected to a local core network via optical fibre fronthaul, and multiple such local cores are connected to the central core network for the region using optical fibre backhaul. In these public networks, the central core acts as the hub through which traffic is directed either to external networks like the internet and public cloud services or to internal MNO-managed services and databases (Walia et al., 2019). The MNO oversees and manages the entire network infrastructure, from the RAN to the core, ensuring end-to-end control over service delivery.

However, with new emerging and localised use cases in 6G, different network deployment modes are expected to evolve to serve these applications. Networks will be developed and deployed with infrastructure flexibility and resource sharing in mind (Basaure et al., 2024). Therefore, 6G is being designed as a fundamentally distributed, decentralised and intelligent network (Qiao et al., 2020). This evolution leads to diverse deployment models beyond the traditional MNO-centric public network. For instance, 5G has already started to see the adoption of private 5G networks or NPNs boosting digital transformation across industries, which will be the foundations in private 6G networks (Frank et al., 2022; Veith et al., 2023). NPNs can be categorised into four broad categories (5G-ACIA, 2019) :

- Standalone Non-Public Network (S-NPN) which operates independently without relying on any public network infrastructure and may optionally connect to the wider public network or services using a firewall. All network functions from the RAN to the core network are deployed within the premises of the local boundary.
- NPN Shared RAN also known as Public Network Integrated Non-Public Network (PNI-NPN) shares the RAN infrastructure between the public and non-public networks. A logical boundary is set between the two networks and the network functions are separated, thus the NPN has its own network identity, spectrum bands and data flows.
- NPN Shared RAN and Control Plane is another PNI-NPN that not only shares the RAN infrastructure but also the control plane network functions. In this case, only the traffic generated locally is contained and managed on the premise of the local boundary
- NPN hosted by a Public Network using technologies like network slicing and NFV is where all the non-public traffic is managed using the public network infrastructure and logical functions, but is treated as if it were a completely different network.

The fundamental difference between these deployment models lies in how UE within a NPN accesses the public network (Frank et al., 2022). In an S-NPN, as the network is fully self-contained, as shown in Figure 2.3, the UE only connects to the local core network through the locally deployed RAN. Whilst typically entirely disconnected from the public network, an S-NPN can optionally connect to public services via a firewall, which is usually deployed at the boundary of the network, allowing the UE to connect to a public service if needed. These network enables high-quality of service (lower latency and higher bandwidth), providing the local network operator maximum flexibility of configurations and ensuring the security of the network. However, this kind of network is more expensive to deploy and requires highly specialised experts to configure, operate and maintain the network (Frank et al., 2022)

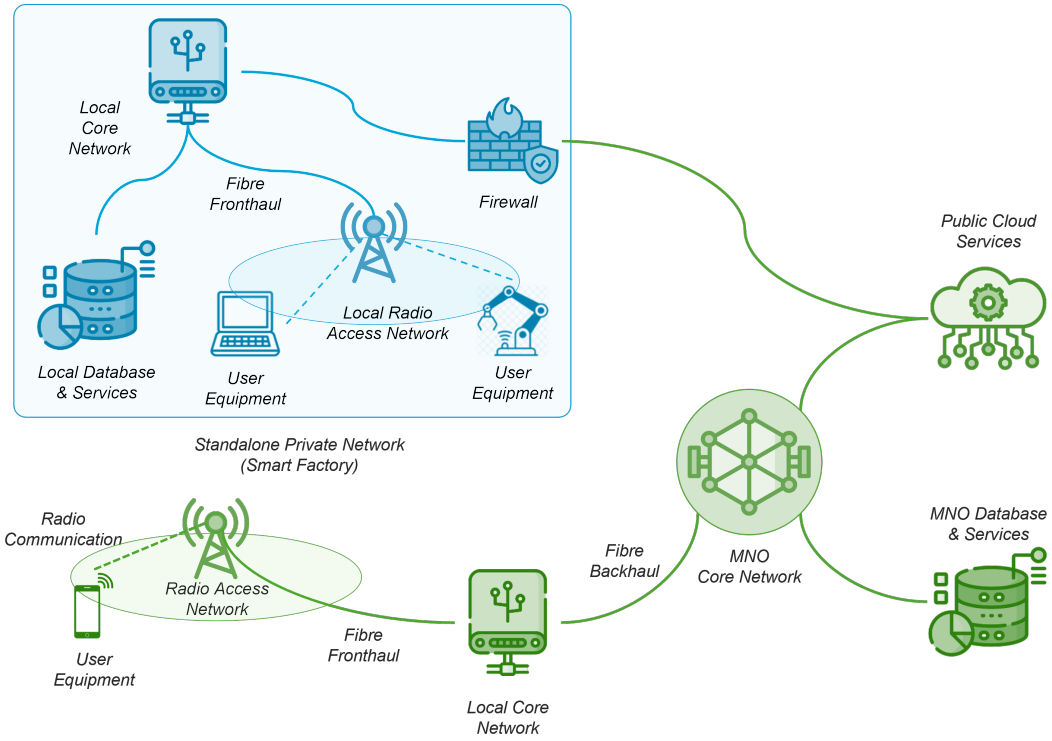

Figure 2.3: Standalone Non-Public Network Deployment
Adapted from 5G-ACIA (2019)

In contrast, a PNI-NPN is established in collaboration with a public network, where elements of the private and public infrastructures are combined based on agreed terms. The UE typically needs a subscription to a public network to gain access, which can be selectively managed based on the SLA between the local operator and the MNO operating the public network (Frank et al., 2022). Such a network deployment is illustrated in Figure 2.4 where the NPN replies on the public RAN equipment, but all other network control functions, including spectrum, are independently managed locally on the customer's premise. The benefit of configuring a network in this manner is that deployment costs are significantly reduced whilst still maintaining network performance (low latency benefits). However, as the network is only partially isolated, it is more reliant on external stakeholders, which could increase the attack surface and raise some security concerns (Frank et al., 2022).

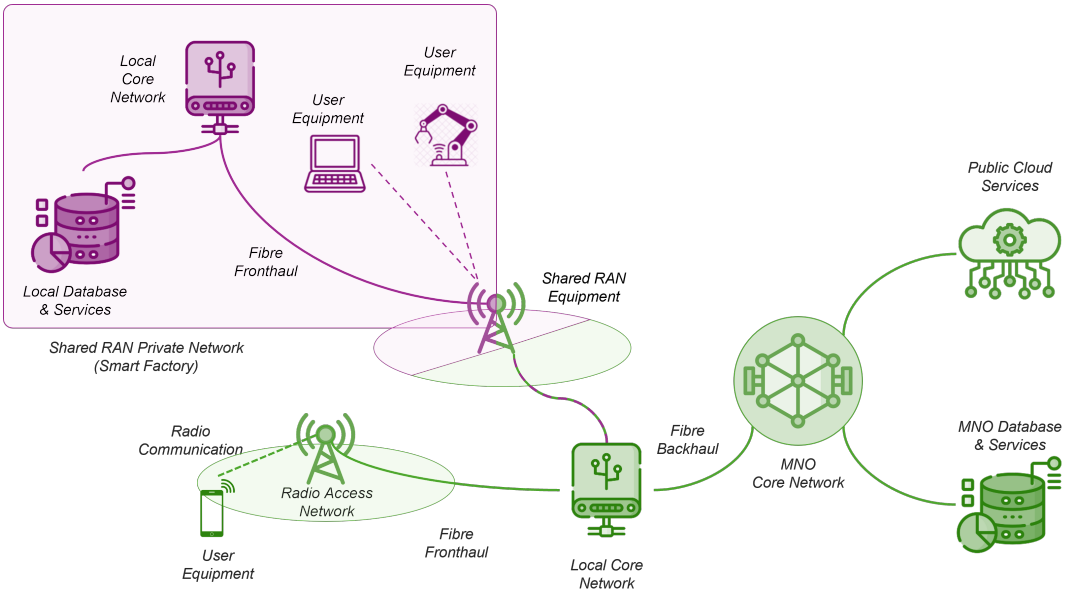

Figure 2.4: Non-Public Network Deployment sharing Public RAN Equipment
Adapted from 5G-ACIA (2019)

2.1.4. Security in 6G

The security of 6G mobile networks is critical, particularly as it must meet demanding performance standards (Benzaïd et al., 2022). Security and privacy already play a key role in ensuring business continuity in 5G and therefore are expected to become even more critical in 6G, which will require multi-layered protection and networks with embedded trust (Jiang et al., 2021; Latva-aho & Leppänen, 2019). Early visions of 6G expect security and privacy prevention measures to require significant upgrades, which can be better understood by classifying security challenges and defence techniques across the three layers of network architecture: the physical, connection (or network) and service (or application) layers as shown in Figure 2.5 (Nguyen et al., 2021).

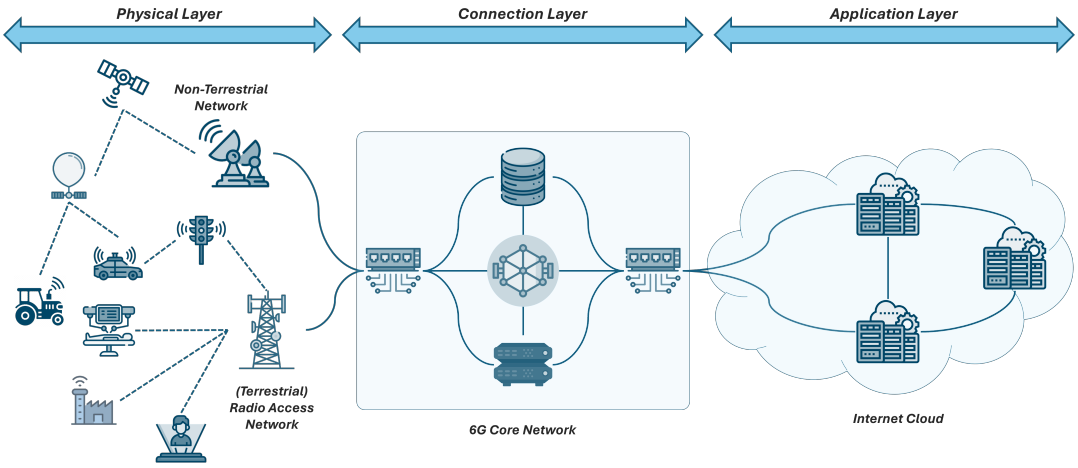

Figure 2.5: Security Across Network Layers
Adapted from Nguyen et al. (2021)

The physical layer serves as the foundation of the network for wireless communication, enabling devices to establish a connection with different nodes on the network. Protecting information in the physical layer, such as defending against fundamental attacks like eavesdropping and jamming threats, is relevant to nearly all 6G use cases (Nguyen et al., 2021). The security of the physical layer improves confidentiality and low-level authentication, which is particularly useful in cost-effective IoT de-

vices which may lack the resources on the device to perform advanced authentication (Ylianttila et al., 2020). Implementation can occur at various points in the network, such as base stations, IoT gateways or on the device itself. However, as 6G introduces new human-centric applications, like XR and bio-integrated sensing, it introduces novel physical layer threats that cannot be addressed by existing mechanisms alone. Thus, new countermeasures tailored to these unique 6G scenarios are essential to ensure secure and resilient connectivity (Ylianttila et al., 2020).

Security of the connection layer, often called the network layer, focuses on securing communication routes and managing control over the network infrastructure. This layer addresses security issues between the user equipment and the services it requests (Nguyen et al., 2021). This layer has faced significant security threats, including signalling data manipulation, spoofing and large-scale Distributed Denial of Service (DDoS) attacks that can overwhelm core network components and disrupt access for legitimate users. 6G is expected to incorporate technologies like quantum-resistant cryptography, like Quantum Key Distribution (QKD) (Kavaiya et al., 2024). Moreover, secure Software Defined Wide Area Network (SD-WAN) is expected to enhance network control by separating the control plane (the routing process) from the data plane (the packet forwarding process) (Nguyen et al., 2021)

At the service or application layer, the primary goal is to protect the broader service infrastructure, which spans from hardware and operating systems to virtual environments and Application Programming Interfaces (APIs). Security at this layer requires a broader strategy including authentication, data encryption, application-layer protocols, firewall deployment and service identity and access management (Nguyen et al., 2021). With 6G introducing highly dynamic, distributed and service-based architectures, security systems must evolve to be more intelligent and automated. Protecting against malware, intrusions and data breaches becomes increasingly complex in a ”Service Everywhere” approach, where services are deployed across various decentralised computing nodes.

6G networks are also expected to carry forward some of the security issues seen in earlier generations (Nguyen et al., 2021; Siriwardhana et al., 2021; Ylianttila et al., 2020). To strengthen 6G systems, it is important to build on the security lessons learned through 5G. As 6Gs is also expected to utilise network softwarisation and slicing technologies like SDN and NFVs, the security vulnerabilities associated with these technologies will also persist. For instance, SDN will continue to face the risk of attacks targeting their controllers and communication interfaces, whereas network slices can be subject to DDoS attacks (Siriwardhana et al., 2021; M. Wang et al., 2020). Furthermore, 6G networks will face a range of new and amplified security threats. Threats will stem from the massive scale and high device density, with forecasts estimating up to 100 billion connected devices significantly broadening the attack surface (Nguyen et al., 2021; Ylianttila et al., 2020). The rise of ultra-dense deployments, including small cells, mesh topologies and multi-connectivity, increases the number of vulnerable endpoints, offering attackers more entry points across a widely distributed infrastructure (Siriwardhana et al., 2021).

In addition, the envisioned “Service Everywhere” paradigm, where services run across decentralised edge nodes, complicates intrusion detection and data leakage prevention, demanding adaptable, embedded security solutions. Moreover, the anticipated convergence of Terrestrial Network (TN), Non Terrestrial Network (NTN) and virtual network domains, alongside the proliferation of resource-constrained IoT and bio-devices, raises concerns about weak authentication and insufficient cryptographic protection (Nguyen et al., 2021). Tackling these new security and privacy challenges in 6G will demand innovative strategies, including greater automation, real-time protection, support for interoperability and the adoption of Zero Trust frameworks.

2.1.5. AI in 6G Security

As highlighted in Chapter 2.1.2, Artificial Intelligence (AI) is expected to be deeply integrated throughout 6G networks, playing a central role in enabling intelligent automation, optimisation, and security functions (Chowdhury et al., 2020; Siriwardhana et al., 2021). This shift marks a transition from the 5G focus on “connected things” to a 6G vision of “connected intelligence,” where AI oversees most network operations and elements (Letaief et al., 2019). These AI-driven systems will be capable of autonomous decision-making, peer-to-peer interactions, decentralised data handling and dynamic service adaptation (Qiao et al., 2020; M. Wang et al., 2020). Moreover, the AI-native design is argued to allow the network to self-learn and adjust in real-time, functioning as a flexible collection of subnetworks, with local adaptability and intelligent radio features powered by AI (Letaief et al., 2019; Yrjölä et al., 2020).

In terms of security, AI is expected to be fundamental to the management of smart, adaptive and automated security required in dynamic 6G networks. AI will be leveraged to identify and mitigate security threats in a timely and cost-effective manner (Benzaïd et al., 2022). Specifically, Identify Authorisation is a use case where AI is argued to facilitate constant user authentication and policy enforcement based on user and context-aware attributes (Benzaïd & Taleb, 2020). Additionally, AI would also enhance API security by proactively monitoring for threats and automating responses to attacks (Benzaïd & Taleb, 2020). With strong pattern recognition strength, AI would support early detection of anomalies and intrusions to prevent malicious activities (Benzaïd et al., 2021).

Furthermore, techniques such as genetic algorithms and Machine Learning (ML) will drive smarter Moving Target Defence (MTD) strategies that balance protection with resource efficiency (Benzaïd & Taleb, 2020). Automated, closed-loop security systems relying on AI are considered essential for securing 6G networks. Benzaïd et al. (2022) propose that systems typically consist of four components: a monitoring system, an analytics engine, a decision-making engine, and a service enforcement element, suggesting that AI and ML are primarily embedded within the analytics engine to enable intelligent security analytics and inform adaptive, real-time decisions across the loop.

However, AI is frequently characterised in the literature as a "double-edged sword" as whilst it offers significant potential in threat detection and prevention, it simultaneously introduces new vulnerabilities and attack surfaces (Benzaïd & Taleb, 2020; Siriwardhana et al., 2021). Given that 6G networks are expected to rely heavily on AI-driven functions, these systems themselves may become high-value targets for malicious actors (Benzaïd & Taleb, 2020; Nguyen et al., 2021). One prominent risk involves adversarial manipulation of ML algorithms, such as data poisoning or algorithm poisoning, where corrupted training data results in inaccurate or misleading model predictions (Nguyen et al., 2021; Siriwardhana et al., 2021). In such scenarios, attackers may aim to: (i) evade detection while maintaining the illusion of normal operation (integrity attacks), (ii) degrade system performance or usability (availability attacks), or (iii) extract confidential information from training datasets, models or users (privacy attacks) (Benzaïd & Taleb, 2020).

Additionally, AI systems themselves can be used as an offender, leading to new security attacks that are scalable and faster to deploy (Benzaïd & Taleb, 2020; Siriwardhana et al., 2021). For example, the literature suggests that AI could be potentially used to exploit zero-day vulnerabilities by deploying a massive Distributed Denial of Service (DDoS) attack. Moreover, attackers could leverage AI to carry out fast and efficient reconnaissance of a network, identifying and logging details like connected devices, operating systems, open ports and user accounts, which could then be used to exploit administrative privileges. Furthermore, attacks could also include identity spoofing by using an AI model, where malicious actors learn and mimic the behaviour of legitimate entities to gain unauthorised access (Benzaïd & Taleb, 2020).

6G also emphasises decentralised intelligence and the move away from traditional centralised models, highlighted in Chapter 2.1.3. In the 6G environment, each network node will serve both as a data provider and consumer in a decentralised service, distributed AI approaches will help address data heterogeneity, ensure privacy and support autonomous decision-making in these decentralised environments (Qiao et al., 2020). Moreover, techniques like federated learning allow training across multiple devices without moving raw data, enhancing privacy and security (M. Wang et al., 2020). Edge intelligence, which represents processing data closer to the user, will be vital for real-time responsiveness (Nguyen et al., 2021; Siriwardhana et al., 2021). Furthermore, the ongoing trend of network softwarisation will continue, with 6G networks adopting cloud-native principles such as micro-services and containerisation to support more agile and scalable deployments of networks and security functions (Benzaïd et al., 2022; Nguyen et al., 2021).

2.1.6. Security-as-a-Service

Security-as-a-Service (SECaaS) is a service model to address data security concerns where the security needs and management are outsourced to guarantee cloud security (Al-Aqrabi et al., 2012). This model was initially conceptualised by Hussain and Abdulsalam (2011) by adopting a user-centric approach specifically for cloud-based applications (Ngo-Ye et al., 2020). Based on a service-oriented architecture, SECaaS provides cloud users with increased control over securing their applications and data. Moreover, despite the different levels of cloud computing, namely Infrastructure-as-a-Service

(IaaS), Platform-as-a-Service (PaaS) and SaaS, SECaaS can be applied across all three levels. In their work, the authors propose a central component called a security manager between the cloud users and the different cloud services responsible for managing the security clouds (Hussain & Abdulsalam, 2011).

SECaaS is also viewed as a sub-category of Software-as-a-Service (SaaS), allowing customers to choose and contract an outside organisation to manage their security needs. Compared to traditional cloud services offering access to an application or platform, SECaaS allows users to services that run on the cloud and protect the customer's operations, data and services (Ngo-Ye et al., 2020). This idea is built upon the work of Hussain and Abdulsalam (2011), who suggested that users, rather than relying solely on their main provider's security, could subscribe to the security measures provided by other cloud providers. Therefore, the customer can choose which security services they use, allowing them to pay-per-use, similar to various other cloud services (Lee et al., 2015). As SECaaS solutions can be a complex domain, the Cloud Security Alliance (CSA) offers some standardised definitions and implementation guidance to support their adoption (Cloud Security Alliance, 2019). This framework proposes ten categories of SECaaS functions and features, which are as follows:

- Identity and Access Management (IAM): This helps manage who can access what by setting rules, checking user identities, keeping records and using single sign-on to ensure people get the right level of access.
- Data Loss and Prevention (DLP): This is about protecting information from being seen, changed, deleted or damaged by unauthorised individuals with the help of enforcing policies, encryption and keeping logs.
- Web Security (WS): This is designed as an additional layer over existing protection, aiming to secure Web-based traffic through the cloud.
- Email Security (ES): This ensures safe email use by blocking spam, harmful attachments and dangerous links with the help of policy-based encryption.
- Security Assessment (SA): This involves reviewing cloud services, often with help from third-party experts, to find and fix security problems, which helps raise security awareness for both the cloud provider as well as the user, involving monitoring events and keeping logs.
- Intrusion Management (IM): This focuses on spotting and reacting to attacks, using both human and automated actions by reconfiguring system components to halt and prevent an intrusion
- Security Information and Event Management (SIEM): This gathers logs and alerts from many tools like servers and firewalls, analyses the data, and helps detect and respond to threats.
- Encryption (EN): This is the process of converting information by changing it into an unreadable code that only the right key can unlock.
- Network Security (NS): This area is about handling threats to networks, especially in cloud setups where data travels online, including unauthorised access, modification, denial and protection of network resources.
- Business Continuity and Disaster Recovery (BCDR): This category covers planning and testing to keep systems running during problems or recover quickly afterwards through redundancy.

Furthermore, these ten categories can be classified into three main groups of SECaaS based on the security control perspectives (W. Wang & Yongchareon, 2017). The first is known as protective measures, which are measures before a security threat occurs and include categories like IAM, DLP, and EN. The second category is known as detective, which are security measures that evaluate and study threats whilst they are ongoing and includes categories like SA and SIEM. Finally, the last group is known as reactive, which includes measures to incorporate the learnings and response after the security threat has been encountered and includes categories like WS, ES, IM, NS and BCDR (W. Wang & Yongchareon, 2020). These three groups are not mutually exclusive but rather have some shared characteristics amongst them as depicted in Figure 2.6. For instance, the activities under the detection, like SIEM, which collects logs, will be used in evaluating the threat and improving the response under the reactive group, such as for IM (Wenge et al., 2014).

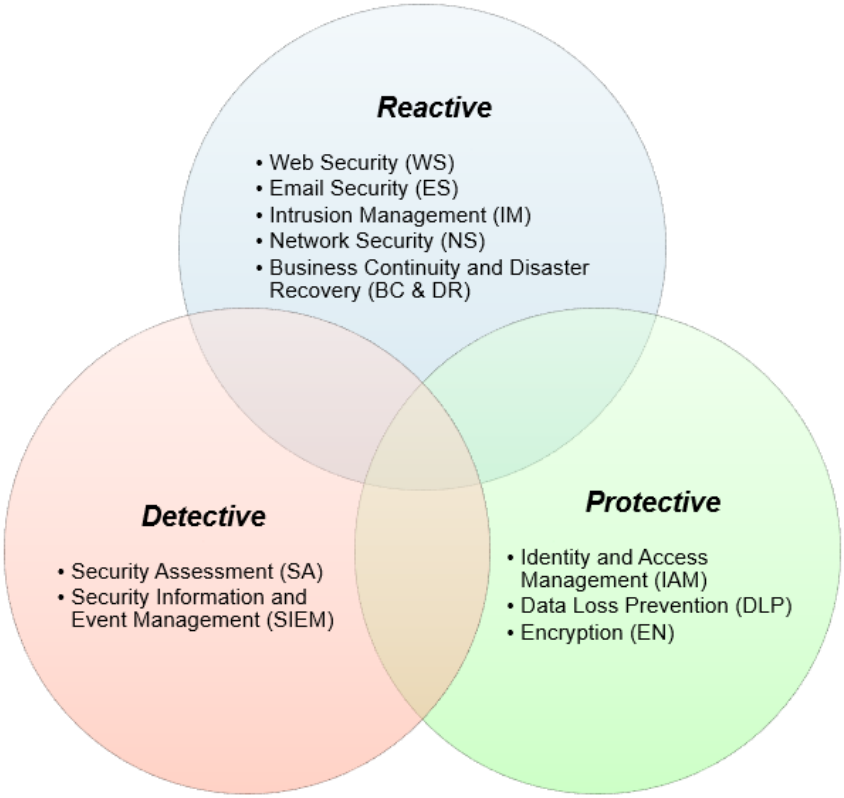

Figure 2.6: Interactions of the different SECaaS Groups and Categories
Adapted from (W. Wang & Yongchareon, 2017)

By design, SECaaS allows users to reduce their costs as they can integrate security measures without investing in on-premise solutions. As the users adopt a pay-per-use model, not only do they reduce their capital costs on hardware but also reduce operational costs by optimising deployments and reducing the total cost of ownership (Chaisiri et al., 2015; Sharma et al., 2013). Moreover, since the SECaaS provider is responsible for managing security, they handle the investment in both hardware and software, offering users flexible and user-friendly solutions instead (Senk, 2013). Additionally, SECaaS providers have deeper expertise in identifying and addressing security threats and are continuously updating their knowledge, offering higher specialisation that often surpasses what a firm could achieve by hiring multiple security experts for separate tasks (Al-Aqrabi et al., 2012; Furfaro et al., 2014; Wenge et al., 2014). Finally, SECaaS can help users in achieving compliance with standards and regulatory requirements for instance abiding by the guidelines put in place by the National Institute of Standards and Technology (NIST) (Furfaro et al., 2014).

On the other hand, the growing popularity of SECaaS makes it an attractive target for malicious attacks (Furfaro et al., 2014; Sharma et al., 2013). As illustrated in Figure 2.6, the interaction between services across different groups significantly expands the attack surface, increasing the risk of intercepted communications. Since SECaaS centralises the management of security processes, including logging, monitoring and threat response, a single breach could compromise all connected services. Therefore, while it offers new opportunities for delivering and managing security, it also becomes an attractive and high-value target for cyberattacks (Boyle & Panko, 2014). Furthermore, as the SECaaS revenue model is based on the services used by the user, it could cannibalise traditional solutions based on licenses, implementation and maintenance fees. As the model starts being adopted, higher competition puts more pressure on profit margins, making it necessary for SECaaS providers to differentiate themselves from others, not just through transparent processes and performance but also reliability (Furfaro et al., 2014; Senk, 2013). Building upon this W. Wang and Yongchareon (2020), highlight that the critical challenge for SECaaS providers is sustaining their reliability and staying ahead of competing as well as non-cloud-based services.

Recent studies have begun to explore how SECaaS can be adapted to emerging technologies in 5G networks. For instance, Chafika et al. (2021) propose a network slicing framework that leverages AI and SECaaS to enable automated and distributed security management across network slices through a closed-loop approach. Similarly, Jamil et al. (2024) introduce a SECaaS layer designed to enhance trust and protect against vulnerabilities when integrating digital twins and blockchain for energy trading in smart grids. Zhang et al. (2024) develop a SECaaS-based defence model that dynamically formulates strategies to safeguard Industrial Internet of Things (IIoT) devices from advanced persistent threats. In addition, Rahmouni et al. (2023) present a solution to improve security Service Level Agreements (SLAs) by using third-party SECaaS providers, enabling mobile and IoT customers to secure cloud service adoption via a centralised platform for discovering providers in multi-cloud environments. Moreover, Ranaweera et al. (2020) propose a SECaaS architecture that utilises the MEC edge platform providing IoT users with security services like intrusion detection and prevention, authentication and secure transmission channels. While these examples reflect a growing interest in adapting SECaaS to newer technologies, such contributions remain relatively focused and do not yet fully address the broader challenges of the next-generation 6G networks.

2.2. Related Theoretical Background

The development of 6G networks introduces a complex evolving landscape, characterised by increased decentralisation, intelligent edge infrastructures, and multi-stakeholder ecosystems. These shifts necessitate a re-examination of foundational concepts such as security provisioning, value creation, and trust, especially as 6G aims to support critical applications at the intersection of physical, digital, and human systems. This section outlines the theoretical foundations relevant to this evolving context, focusing on the roles and interactions of security stakeholders, the mechanisms of value co-creation in service ecosystems, and the complex role of customer trust, functioning both as a precursor to and a result of these interactions.

2.2.1. Value Interactions in 5G Networks

In the mobile telecommunications domain, advancements in information and communication technologies have significantly transformed services and expanded the scope of stakeholder interactions, thereby creating potential opportunities for creating value. The traditional linear model, where value is sequentially created and ultimately captured by just a single company, has given way to a more dynamic view which leads to the co-creation of value by both service providers and users within a broader ecosystem of interdependent actors (Aagaard et al., 2024; Basaure et al., 2024; Yrjölä et al., 2022). This transition is underpinned by the reduction in coordination costs facilitated by digital technologies, which enable service co-production to become more collaborative, participatory and inclusive (Kallinikos et al., 2011).

Academia argues that the conventional model, often employed by legacy fixed network operators to assert control over each stage of the value chain, has become inadequate in today's digitised environment and acknowledges that value emerges through a complex web of interdependent stakeholder relationships (Peppard & Rylander, 2006). Moreover, the rise of the service ecosystem has led to configurations of actors who integrate resources, operate under common institutional frameworks and collaboratively create and share value through service interactions (Vargo & Lusch, 2016). Value creation is often seen as the customer's process of generating "value-in-use," shaped by their experiences and interpretive logic. Co-creation arises through direct interaction between the firm and the customer, where the provider actively contributes to the customer's value realisation (Grönroos & Voima, 2013). To support effective co-creation, actors must be able to exchange and integrate resources in ways that align with the contextual conditions of their specific ecosystem (Lepak et al., 2007).

Whilst 5G is expected to create value through techniques like Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC) and Massive Machine Type Communications (mMTC) as defined in ITU-R (2015), they do not represent the current available services as only eMBB is currently being deployed and URLLC and mMTC are yet to be adopted. Instead, research finds six different types of mobile network services, ranging from centralised public networks to Non-Public Networks (NPNs) consisting of MNOs and different local operators (Aagaard et al., 2024). Moreover, data, algorithms, components and interfaces are also identified to be important factors for 5G value

creation (Iivari et al., 2022; Yrjölä et al., 2021). Table 2.2 summarises how value is co-created and shared among stakeholders in these six deployments currently deployed 5G networks.

Table 2.2: Value Co-creation and Sharing Across 5G Network Configurations

Network Configuration	***Description***	***Value Co-creation***	***Value Sharing***
Public Networks	Network connectivity services provisioned by an MNO for anybody to connect	Bundling of services with connectivity (for e.g. equipment and applications)	Connectivity enables other stakeholders to provide their services to end users
Virtual Public Networks	Network connectivity services provisioned by a Mobile Virtual Network Operator (MVNO), utilising an MNO's infrastructure for anybody to connect	Bundling of services with connectivity (for e.g. equipment and applications)	Provides the MNO an opportunity to capitalise on extra capacity
Neutral Host	Network connectivity services for any customer provisioned either by an MNO or non-MNO firm sharing the deployment costs	Offerings differentiated based on the SLAs and quality of service	Value is shared only among contracted partners
NPN Operated by MNO	MNO offers a private network for local users	Business through contracts between MNOs with specific stakeholders and customers	Value shared among local ecosystem partners
NPN Operated by non-MNO	A private network for local users provisioned by a non-MNO firm	Value created by the local ecosystem stakeholders (independent of the MNO)	Value shared among local ecosystem partners
Public Network Integrated Non-Public Network (PNI-NPN)	A private network hosted on the public MNO network through slicing or virtualisation	Value created by the local ecosystem stakeholders, including connectivity outside the private network	Value shared among local ecosystem partners

Adapted from Aagaard et al. (2024)

2.2.2. Proposed Value Interactions in 6G Networks

As 6G transitions from centralised, technology-driven models toward shared ecosystem approaches for value creation (Yrjölä et al., 2022), it is often viewed as a transformative general-purpose technology that will shape future digital societies (Xiang et al., 2024). Unlike previous mobile generations, 6G is expected to not merely enhance connectivity but shape political, economic, societal, technological, legal and environmental systems (Xiang et al., 2024; Ylianttila et al., 2020). Moreover, it is envisioned that the 6G value proposition will stretch horizontally and vertically in the value network (Xiang et al., 2024), leading to the development of a hybrid oblique (mix of horizontal and vertical) business model centred around the value-sharing economy (Yrjölä et al., 2022).

As discussed in Chapter 2.1.2, 6G networks will embrace novel enabling technologies like immersive communication, integrated AI, hyper-reliable and low-latency performance, massive communication and ubiquitous global connectivity. Therefore, the sources of value creation in 6G networks will extend beyond traditional mobile connectivity to encompass services across healthcare, logistics and agricul-

ture, as well as support for increasingly autonomous systems. As these capabilities evolve, another key source of value creation arises from ensuring privacy, safety and security for both humans and autonomous entities becomes critical (Aagaard et al., 2024).

Furthermore, building upon the ecosystem approach in being adopted in 5G, value in the 6G ecosystem is fundamentally co-created by an array of interconnected stakeholders (Pera et al., 2016; Yrjölä et al., 2020; Yrjölä et al., 2022). This goes beyond simple bilateral exchanges to a dynamic ecosystem of collaboration and resource integration. The complexity of this ecosystem necessitates a shift in managerial focus, from initiating isolated partnerships to orchestrating multifaceted stakeholder interactions. Ultimately, the value realised is subjective and defined by each stakeholder's unique perspective and needs (Pera et al., 2016). To analyse these complex multi-stakeholder ecosystems, the concept of the Value Network Configuration (VNC) offers a valuable lens for mapping both technical and business relationships among actors (Basaure et al., 2024; Casey et al., 2010; Kulkarni et al., 2021).

The VNC approach departs from the traditional linear value chain, which focuses on value-adding activities within a single firm, and instead reflects a networked logic of co-production (Peppard & Rylander, 2006). A value network is defined as a set of interlinked business actors and technical or functional resources that collaborate to create economic value through services and products (Casey et al., 2010). At its core, a VNC diagram distinguishes three fundamental elements: the technical component (such as provisioning of a service), the role or activity (a set of technical grouping of associated technical components) and the stakeholder or actor (such as an MNO). The relationships within a VNC are depicted through two types of interfaces: technical interfaces, shown as dotted arrows, which define the relationships between technical components (e.g. how different parts of the technological infrastructure connect and interact), and business interfaces, represented by continuous-lined arrows, which define the relationships between actors (e.g.including elements such as service/revenue models and contracts) as shown in Figure 2.7

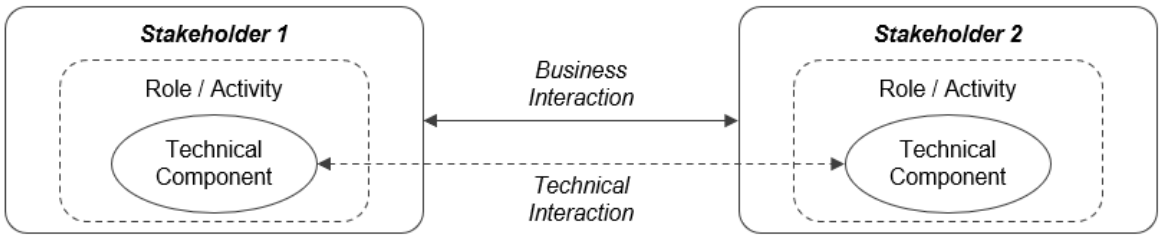

Figure 2.7: Notation for VNC Analysis
Adapted from Basaure et al. (2024)

By separately identifying technical components, performed roles, and the actors responsible for them, VNC diagrams reveal how increased functionality and openness in network architectures give rise to new forms of interaction among both established and emerging stakeholders (Basaure et al., 2024; Kulkarni et al., 2021). This facilitates a more comprehensive understanding of how value is generated not by individual entities in isolation, but through the configuration of the entire actor network. The VNC approach also helps clarify role distribution across key stakeholders in various configurations, thereby addressing ambiguities related to stakeholder responsibilities and interrelations (Kulkarni et al., 2021). The VNC approach has been applied across various contexts, including industrial 5G deployments, network slicing, telehealth, and platform ecosystems (Casey et al., 2010; Kulkarni et al., 2021; Walia et al., 2017, 2019). Recently, it has been used to examine local 6G deployment modes, such as real-time digital twin use cases, enabling comparison of alternative network deployment configurations and exploring the benefits and constraints of each (Basaure et al., 2024).

Despite the growing recognition of 6G as a general-purpose technology transformative ecosystem shaped by multifaceted stakeholder collaboration and advanced technologies, there remains a notable gap in the literature concerning business model innovation for SECaaS models. While existing studies underscore the importance of co-creation and orchestration among diverse actors to generate collective value, specific investigations into how SECaaS providers can strategically align value creation through

integrated stakeholder interactions are scarce. In particular, the complex interplay between telecom operators, security service providers, infrastructure stakeholders, and end users in the 6G ecosystem has yet to be fully explored from a business model perspective. Notably, no existing research has applied the VNC approach to the SECaaS domain, nor has it examined how stakeholder roles and relationships differ across varying degrees of network centralisation and decentralisation.

2.2.3. Role of Customer Trust

Trust is positioned as a foundational element in 6G networks, with early literature highlighting the challenge of embedding end-to-end trust across technological, regulatory, and ethical dimensions in increasingly open and decentralised ecosystems (Latva-aho & Leppänen, 2019; Ylianttila et al., 2020). Moreover, many recognise that current 5G only considers trust in a limited manner (Liyanage et al., 2018; Saad et al., 2021) and with the convergence of digital and physical worlds in 6G, embedding trust-building elements into the network becomes even more crucial (Veith et al., 2023). For instance, to improve the trust between AI, Guo (2020) highlight the need for Explainable Artificial Intelligence (XAI) in the design of 6G networks to support trust building between humans and machines. Literature on trust in cloud computing highlights the complexity of trust assessment due to the diversity of services, stakeholders, and evolving environments (Medeiros et al., 2017). While cloud trust labels have been proposed to enhance customer confidence (van der Werff et al., 2019), these approaches remain underdeveloped in terms of how they would be operationalised within a SECaaS context, particularly across decentralised 6G networks.

Whilst trust has been conceptualised in various ways across disciplines, several characterisations stand out in the context of customer–provider relationships. For instance, Schurr and Ozanne (1985) view trust as the belief that promises will be honoured and obligations fulfilled, while Zucker (1986) frames it as a set of expectations embedded within implicit contracts. In e-commerce, Jarvenpaa et al. (1999) define trust as the willingness to rely on an online party under conditions of vulnerability, and Gefen et al. (2003) argue that trust in business relationships is shaped by perceptions of ability, benevolence, and integrity. Despite the range of interpretations, one of the most widely cited definitions is provided by the Integrative Model of Organisational Trust proposed by Mayer et al. (1995), who define trust as "the willingness of one party (the customer) to be vulnerable to the actions of another party (the service provider) based on the expectation that the other party will perform actions important to the trustor." A key contribution is the emphasis on vulnerability, implying that trust involves a willingness to accept risk based on positive expectations, rather than risk-taking itself (Mayer et al., 1995).

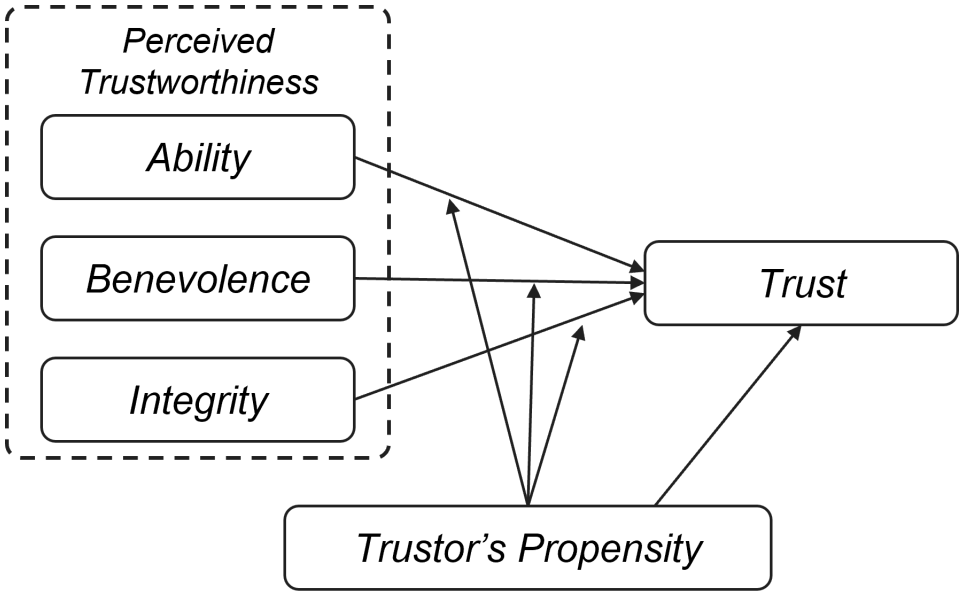

Figure 2.8: Integrative Model of Organisational Trust
Adapted from Mayer et al. (1995)

As shown in Figure 2.8, Mayer et al. (1995) propose two primary categories of antecedents that influence the level of trust a trustor places in a trustee. The first is the trustor's general propensity to trust, often regarded as a stable personality trait shaped by factors such as upbringing, personality, and cultural background. The second category concerns the perceived trustworthiness of the trustee, determined by three core attributes: ability, benevolence, and integrity. Ability refers to the trustee's competence and skills within a given context, acknowledging that expertise in one domain may not translate to another. Benevolence captures the extent to which the trustee is perceived to genuinely care about the trustor's interests beyond self-interest. Integrity involves adherence to principles valued by the trustor, including fairness, honesty, consistency, and alignment between words and actions.

The successful adoption of SECaaS services is highly dependent upon the customer's trust in the service provider (Ngo-Ye et al., 2020; Senk, 2013). Building on this definition, Ngo-Ye et al. (2020) identify customer trust as being influenced by knowledge-based beliefs, institutional beliefs, calculative-based risk beliefs and service-quality-based beliefs of the customer in their theoretical model. The contributing factors shape the customer perceptions of the SECaaS provider, ultimately influencing the adoption of their solutions. Furthermore, they also argue that trust in SECaaS providers includes the customer's beliefs in the provider's ability, benevolence and which reduces the precipitated risk and enhances the likelihood of adoption. Moreover, Senk (2013) conceptualises trust as the inverse of perceived risk, treating it as a reflective construct measured through indicators such as overall trust in adoption and confidence in certified service providers. The study finds trust as a driver for the adoption of the SECaaS solution, demonstrating a significant positive influence on adoption. Furthermore, trust is found to be negatively associated with various perceived risks (like security, social, and strategic risks) highlighting the importance of reducing these risks to foster trust and support SECaaS adoption.

Additionally, customer trust plays a pivotal and reciprocal role in the value co-creation process, functioning both as a key antecedent and an emergent outcome of collaborative interactions between consumers and service providers (Shulga et al., 2021). As a foundational enabler, trust becomes particularly critical in digital environments, such as online banking or virtual co-creation platforms, where heightened uncertainty and perceived risks arise from the lack of physical presence (Marcelo Royo-Vela & Ferrer, 2024). Individuals with a greater disposition to trust are more inclined to form initial confidence in a service provider, thereby increasing their readiness to engage in co-creation activities. This initial trust facilitates the exchange of ideas, joint contributions, and open communication, which are essential for cultivating an effective co-creation environment (Shulga et al., 2021).

Extending this view, Pera et al. (2016) emphasises that trust also enhances resource sharing, mutual value realisation, and collaboration in complex, multi-stakeholder ecosystems, positioning trust as a catalyst for co-innovation and joint value creation. Thus, in addition to its role as a prerequisite, trust also evolves as a result of effective co-creation activities. Ongoing engagement and the integration of customer and provider resources contribute to improved trust and organisational reputation. This cyclical dynamic aligns with the principles of service-dominant logic and social exchange theory, which suggest that repeated service interactions and relational exchanges reinforce mutual value and trust over time (Shulga et al., 2021).

Therefore, whilst existing literature establishes the importance of trust in digital service adoption and co-creation, particularly within cloud computing and SECaaS contexts, no studies have yet examined how customer trust manifests in SECaaS solutions offered across different 6G network deployments. Specifically, how antecedents of trust may vary within centralised, decentralised, and hybrid 6Gs ecosystems remains unexplored. Addressing this gap is essential to understanding how trust can be fostered and operationalised to enable the successful adoption and value creation of SECaaS solutions in 6G network ecosystems.

2.3. Emerging Literature Gap

This study aims to explore the techno-economic value interactions and trust dynamics among stakeholders involved in SECaaS solutions across varying 6G network deployments. Existing literature provides a strong foundation on the technical evolution of both 6G and SECaaS, and offers valuable insights into value creation within multi-stakeholder ecosystems. Prior research also highlights the critical role of customer trust in the adoption of SECaaS offerings, emphasising its reciprocal influence on value co-

creation. However, a clear gap remains in understanding SECaaS business models and trust-building mechanisms vary in different 6G network architectures, particularly in centralised versus decentralised deployments.

Current stakeholder analyses in the 6G literature predominantly focus on infrastructure and platform-layer actors, such as MNOs and infrastructure vendors. While Yrjölä et al. (2023) acknowledge the importance of security and privacy-enhancing services providers in mitigating the growing threat surface of virtualised and cloud-based 6G infrastructures, their treatment of this stakeholder group remains limited. Beyond noting their role in deploying privacy-enhancing technologies, the authors provide little detail regarding the providers' specific responsibilities, whether they develop or manage security solutions in-house, or how they collaborate with other stakeholders within the ecosystem. Consequently, functionalities such as managed detection and response, zero-trust architectures, and unauthorised access control remain insufficiently examined from a stakeholder responsibility perspective. This narrow framing risks overlooking how third-party providers may shape the service layer of 6G networks, particularly in delivering scalable, differentiated, and trust-embedded SECaaS offerings.

Moreover, despite growing recognition of 6G as a complex and dynamic ecosystem that requires coordinated value creation across a diverse set of stakeholders, research on how SECaaS providers can develop viable business models within this landscape remains limited. While existing studies have begun to explore co-creation and stakeholder collaboration in 6G, they often overlook how value is distributed across telecommunications, infrastructure, and security actors. For instance, Aagaard et al. (2024) provide insights into value co-creation and distribution in different 5G network configurations, and Basaure et al. (2024) examine techno-economic stakeholder interactions in the context of digital twins in 6G networks. However, no study to date has applied a Value Network Configuration (VNC) lens to investigate how stakeholder roles and interactions are structured specifically in the context of SECaaS, particularly across varying network architectures. This gap limits current understanding of how trust-centric service models can be effectively leveraged to create and capture value in centralised, decentralised and hybrid NPN deployment scenarios.

Finally, although trust is well established in the literature as a critical enabler of digital service adoption and value co-creation, particularly in SECaaS solutions for cloud computing domains, these insights have not yet been fully extended to the context of future 6G deployments. While Senk (2013) highlight the importance of trust in SECaaS adoption and Ngo-Ye et al. (2020) explore the antecedents of customer trust in SECaaS providers, neither study considers how these factors might evolve in mobile network environments, particularly in relation to decentralised NPNs architectures expected to become more prominent in 6G. Specifically, the extent to which trust dynamics vary across centralised, decentralised, or hybrid NPNs remains unexplored. Addressing this gap is essential for designing and deploying trusted SECaaS solutions that align with the distributed and adaptive characteristics of next-generation mobile networks.

3

Research Methodology

3.1. Research Design

Given the exploratory nature of this study, it adopts the perspective of a firm seeking to position itself as a SECaaS provider within the evolving 6G landscape. To examine how such a firm can navigate this dynamic ecosystem, a qualitative research design is employed to investigate contemporary phenomena such as stakeholder interactions and customer trust dynamics within the broader value co-creation process. To guide this inquiry, the study applies Value Network Analysis, drawing specifically on the Value Network Configuration (VNC) framework introduced in Chapter 2.2. This methodological approach supports the exploration of how value is created, exchanged, and distributed among actors across various deployment architectures.

To map both technical and commercial interactions, the study first identifies the roles and responsibilities of relevant SECaaS stakeholders. This is achieved through interviews with key actors involved in the deployment and management of SECaaS solutions, enabling a nuanced understanding of their positions and the techno-economic interactions shaping future 6G ecosystems. In parallel, the study explores how the antecedents of trust differ across centralised and decentralised network contexts by incorporating elements of trust-building mechanisms grounded in the model of organisational trust proposed by Mayer et al. (1995). Semi-structured interviews are used to capture rich, contextual insights into interpersonal, organisational, and external factors that influence how customer trust is established and maintained

3.2. Data Collection

Given the qualitative and exploratory nature of the research being conducted in an emerging domain where the 6G standard is still under development, the data sources used for this study are primary sources collected through semi-structured interviews. This method employs pre-determined questions designed to address the research question whilst maintaining the flexibility to probe emerging themes during the conversation. Interviews are conducted with key stakeholders, including MNOs, infrastructure providers, and SECaaS vendors, who are expected to play a role in the future 6G ecosystem. These interviews provide direct insights into stakeholder roles, interactions and the underlying trust dynamics across different network deployment scenarios.

In addition to interviews, secondary data sources are used to establish a foundational understanding of the domain. These include peer-reviewed academic literature, as well as industry reports and white papers published by research consortiums. Such sources provide context on ongoing developments in 6G, especially with regard to emerging network deployment models (such as different NPNs) and the evolution of SECaaS functionalities. They also offer a conceptual and technical basis for constructing the VNCs used in this study. By triangulating insights from both primary and secondary sources, the research ensures greater depth and credibility in its findings. This is majorly done in Chapter 2.1 of the literature review covering major technical background in SECaaS and 6G networks. However, for the interview process a sampling strategy is prepared in Chapter 3.2.1 to identify the appropriate sample

and interview participants and followed by an interview protocol in Chapter 3.2.2 to ensure a systematic approach and rigour when collecting data.

Rather than viewing participants solely as knowledge holders and the interviews as a means of extracting information, the study adopts a co-creative approach to knowledge generation. Given the exploratory nature of the research, the interviews are framed as collaborative dialogues between the researcher and participants. While the researcher entered the process with a grounding in academic literature, the participants contributed practical, industry-based insights on the feasibility and evolution of SECaaS models within emerging 6G networks. Together, these perspectives were integrated to more effectively explore the research questions and address the identified gaps in the current body of knowledge.

3.2.1. Sampling Strategy

As the unit of analysis in this study is the value network that captures interactions among stakeholders, the sampling strategy is derived accordingly. Given the study's focus on SECaaS solutions within 6G networks, the relevant stakeholders include firms involved in the design, provision, integration and management of security services in mobile network environments. The unit of observation comprises employees from these firms who actively contribute to the development or delivery of SECaaS offerings. Accordingly, the population could be defined as employees from key stakeholder organisations engaged in shaping 6G SECaaS ecosystems. These organisations include Mobile Network Operators (MNOs), infrastructure vendors, security tool providers, and service-oriented security firms, each influencing value creation and trust dynamics across centralised and decentralised 6G deployments. To ensure contextual relevance to the Ensure-6G project, this study focuses on stakeholders operating within the European Union. This regional focus aligns with the EU's strategic ambitions for 6G development and resilient security and privacy solutions.

As the 6G standard is still under development, the availability of individuals with direct experience in 6G-specific deployments is limited. Consequently, the population must be narrowed to employees who are actively engaged in the development of 6G technologies, many of whom occupy technical or research-focused roles, including academics affiliated with stakeholder organisations. These individuals are typically responsible for shaping their organisations' positions in emerging network architectures and can provide insights into expected stakeholder roles and interactions. In contrast, sales and customer-facing specialists are less likely to possess detailed knowledge of 6G-specific functionalities, as no commercial 6G products currently exist. However, since the study seeks to understand how customer trust manifests across different network deployments, it is essential to include participants with experience in selling or integrating SECaaS offerings in today's 5G networks, who suggest that they would have a role to play in offering services in 6G networks as well. Therefore, the ideal sample frame is a combination of technically knowledgeable employees involved in 6G development and commercially oriented employees with experience delivering security services in 5G, who are likely to play equivalent roles in the 6G ecosystem, with the scope limited to the European Union.

Next, a sampling design is implemented to derive a sample from the identified population and sample frame. Given the limited availability of expertise on 6G networks, particularly regarding security solutions and network deployment models, the study adopts judgment sampling, a form of non-probability purposive sampling. Whilst this approach may limit external validity, particularly the generalisability of the findings, it is appropriate due to the scarcity of participants with sufficient knowledge of 6G stakeholder roles and interactions. Although a probability sampling approach could enhance generalisability, it would likely include participants lacking the necessary domain expertise, potentially compromising the internal validity and accuracy of the study's conclusions.

Furthermore, to identify relevant stakeholder organisations within this scope, the study draws on established industry resources such as the Gartner Magic Quadrant, a market research report that highlights market trends and key industry participants (Gartner, Inc., 2025); and the GSMA member directory, which represents the interests of MNOs globally (GSMA, 2024a). Sample elements were contacted through the researcher's professional network. As highlighted by Guest et al. (2006) initial themes are identified from the interviews with as little as six and saturation occurs by twelve interviews. Moreover, in an empirical-based systematic review of the literature in this domain, Hennink and Kaiser (2022) suggest a group of nine to seventeen interviews reached saturation. Thus, in total, ten participants

were interviewed for this study. This was done to ensure the reliability of the data collected but also to address saturation in the data collection process. These participants represent a diverse range of stakeholder domains, including MNOs, security vendors, and SECaaS providers, as outlined in the sampling strategy (see Appendix B.1 for more details).

- 3 employees from different MNOs who also offer SECaaS solutions
- 3 employees from different security tool developers/vendors
- 2 employees from a satellite operator
- 1 employee from a non-MNO based SECaaS provider
- 1 employee from an independent telecom and security consultancy provider

3.2.2. Interview Protocol

To ensure the reliability of the study and explore the elements of the research question in depth, an interview protocol was developed. Furthermore, maintaining detailed documentation of the entire research process (such as forming the codebook) will allow future researchers to trace how the findings were reached. Additionally, this approach allows for a balance between consistency across interviews and flexibility to probe relevant topics that emerge during the conversation. The protocol was designed to capture both technical and commercial perspectives on SECaaS solutions in future 6G network deployments, with particular attention to stakeholder roles, value creation processes, and trust dynamics. Interview questions were aligned with the conceptual focus of the study and structured around key themes such as value network interactions, deployment architectures (centralised vs decentralised), and customer trust in managed security services. Thus the interviews were used to fulfil the following four objectives:

- Explore SECaaS functionalities and deployments in the 6G context.
- Identify key and emerging stakeholders when offering SECaaS solutions in 6G networks.
- Explore how stakeholder roles and interactions vary across network centralised and decentralised deployments when offering SECaaS solutions in 6G networks.
- Explore how antecedents of customer trust in a SECaaS provider vary across network centralised and decentralised deployments when offering SECaaS solutions in 6G networks.

To address the four interview objectives, a set of detailed questions was developed, as presented in Appendix B.2. These questions also served to establish a clear context and scope for the discussions, for example, by inquiring about the interviewee's current and anticipated roles within their firm. This helped to clarify the firm's position within the broader ecosystem. Given the breadth of topics covered, each interview was scheduled for approximately 60 minutes. This duration was considered sufficient to address the four key objectives while remaining a reasonable time commitment for participants. All interviews were recorded and transcribed to ensure transparency, reproducibility and methodological rigour, as recommended by Sekaran and Bougie (2009).

3.3. Data Analysis

To analyse the qualitative data collected through semi-structured interviews, this research applies the six-phase thematic analysis framework developed by Braun and Clarke (2006), illustrated in Figure 3.1. This method offers a flexible yet systematic approach to identifying, interpreting, and reporting patterns, or emerging themes, within the data set. Anchored in a contextualist epistemology, the analysis recognises both the meanings participants attribute to their experiences and the broader organisational and technological settings that shape these meanings. By systematically progressing through the phases of familiarisation, coding, theme development, refinement, and reporting, this approach facilitates a transparent and rigorous exploration of how trust, stakeholder roles, and interactions are conceptualised across different 6G network deployments.

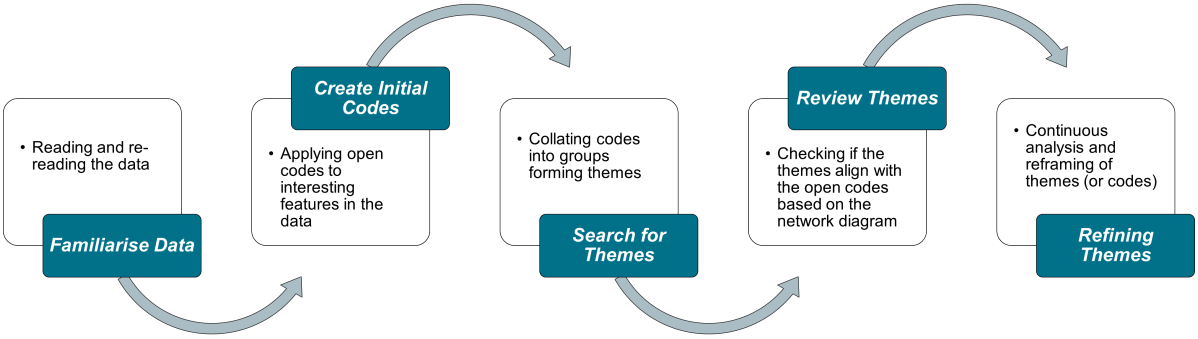

Figure 3.1: Thematic Coding Process
Adapted from Braun and Clarke (2006)

The analysis is conducted using a commonly used software for qualitative analysis, Atlas.Ti, and begins with familiarisation, which involves reading through the interview transcripts to gain a deep understanding of the data. This is followed by data reduction through the coding process, where segments of text are assigned descriptive labels that capture their underlying meaning (Sekaran & Bougie, 2009). To balance structure with flexibility, a middle-ground coding strategy is adopted: an initial set of codes is informed by the research questions, such as focusing on broad categories of trust antecedents discussed with participants. At the same time, the coding scheme remains open to adaptation, allowing new codes to emerge during analysis to ensure the full complexity and nuance of the data are captured.

Next, the open codes are organised into code groups, representing overarching themes, within Atlas.ti. Network diagrams are then created to visually map the relationships between these themes and their associated codes. Given the iterative nature of the thematic analysis, these diagrams are continuously reviewed and refined to ensure the themes remain grounded in the data and contribute meaningfully to answering the main research question. To further support this, themes are categorised according to the sub-research questions they relate to. For example, when participants reflect on what they expect SECaaS to encompass in the context of 6G networks, their responses may include expectations regarding its functionalities or how such services should be deployed. These insights are grouped into themes, such as SECaaS Functionalities and SECaaS Deployment Approaches, which collectively inform the first sub-research question on how SECaaS is conceptualised within 6G network environments.

Furthermore, the interviews were

3.4. Addressing Limitations in Participant Knowledge in 6G

As described in the previous section, participants typically hold either technically specialised roles or commercially oriented responsibilities, but more often not both. Consequently, their insights may be limited to particular aspects of the study, for instance, those in technical roles may provide detailed input on SECaaS functionalities and stakeholder interactions within 6G networks but may lack a nuanced understanding of customer trust dynamics. Conversely, those with commercial roles may offer perspectives on trust and value but be less familiar with technical implementation. It is therefore important to critically reflect on these limitations when analysing the data, recognising that participant perspectives are shaped by their professional focus and may not capture the full complexity of cross-functional dynamics within emerging 6G ecosystems.

To address the limitations stemming from participants' domain-specific expertise, the data analysis applied a critical lens that recognised the partial nature of each perspective. During the theme review and refinement phase, responses were interpreted with careful attention to the participant's role, whether technically or commercially oriented, to avoid overgeneralising insights beyond their scope of expertise. For example, when analysing themes related to customer trust, statements from technical stakeholders were treated with caution and cross-referenced with insights from commercially focused participants wherever possible. If, for instance, a 6G researcher at an MNO identified accountability or transparency as factors fostering trust in the SECaaS provider, this was only reinforced as a broader theme if a sales manager at a SECaaS firm echoed similar views. This approach ensured that the analysis remained

grounded in the context of each participant's expertise while enabling a more balanced and robust interpretation through the triangulation of diverse stakeholder perspectives.

Another potential limitation in the interview process was the varying interpretations of network decentralisation among participants. In this study, decentralisation is defined as the use of Non-Public Networks (NPNs), which operates independently of an MNO-based public network. However, some participants associated 6G with a more utopian vision of decentralisation, imagining highly fragmented networks capable of direct device-to-device communication without reliance on conventional infrastructure such as cell towers. While the researcher acknowledges the validity of this broader vision, efforts were made to steer the conversation towards the more immediate and realistic interpretation of decentralisation aligned with NPN models. This was achieved by asking participants about standalone private networks or by presenting a modified version of Figure 2.3 where necessary to ensure a shared understanding of the concept being discussed.

Furthermore, within the context of this highly explorative study, the interview process was treated as a form of knowledge co-creation. When participants introduced ideas that appeared overly speculative or dystopian, the researcher adjusted the interview protocol (see B) to redirect the conversation towards more grounded discussions relevant to the SECaaS and 6G domains. This was typically done by prompting participants to reflect on developments within their own sector and how they envisioned 6G in that context, rather than discussing hypothetical use cases they were aware of but did not consider feasible. This limitation became apparent following the very first interview, during which the participant described a fragmented vision of 6G and questioned the need for separate security services, suggesting instead that security would be inherently embedded within the product or service itself.

4

Findings and Analysis

4.1. Uncertainty about 6G Networks

In the interviews, many participants noted that while 5G systems are being deployed across Europe, their full potential has yet to be realised. One MNO indicated plans to offer commercial 5G slicing starting in 2026, another participant highlighted low private 5G adoption, and another pointed out that many current 5G deployments do not use 5G-SA systems, but rather combine 5G RAN with legacy 4G/LTE core networks, with complete 5G-SA adoption potentially taking another decade. This technological lag is not fully addressed in the literature but is evident in industry reports. For example, the European Commission reports that 94% of households are covered by 5G, yet coverage using the new 3.6 GHz mid-band, crucial for 5G-SA, remains around 70% (European Commission, 2025). In contrast, GSMA estimates that only 30% of mobile connections in Europe were on 5G networks in 2024, and just 15% of operators had launched 5G-SA networks by the end of that year (GSMA, 2025b). These figures reiterate that, while 5G RAN deployment is advancing, current networks still rely on older core infrastructure. As a result, customers are yet to experience the full technological benefits promised by 5G.

While some academically oriented participants were actively engaged in the development of 6G networks and security technologies, the findings indicate that most industry participants remain primarily focused on the continued deployment and evolution of 5G systems. For many, 6G was viewed as a distant and uncertain prospect. Consequently, participant insights on 6G were often speculative, with limited recognition of the relevance or urgency of complementary SECaaS solutions within future mobile networks. This posed a challenge for the researcher, as discussing security concepts linked to an underlying network architecture that may not materialise for another decade often lacked practical grounding. In some cases, these discussions veered into abstract or dystopian scenarios, such as fully fragmented, decentralised networks and highly ambitious KPIs that may not yield tangible improvements in quality of service. Such narratives risk potentially reinforcing the growing hype around 6G, as academic and industry stakeholders race to define and commercialise a standard still in its early conceptual phase.

> IN2: *"Yeah, I see that it's our ambition actually to start offering 5G slicing commercially as of 2026, so it's not commercially active yet. But indeed it's really our ambition to move in that direction"*
>
> IN3: *"From my understanding, the ambition with 6G is that there is no difference between terrestrial networks (TN) and non-terrestrial networks (NTN) any more and that it's a single standard that will work as one. Again, not the perfect expert here, but that's from what I see, the leap from 5G to 6G that's relevant for SatCom in an NTN framework."*
>
> IN5: *"In terms of use cases for 6G, I don't have like a list of use cases yet because I think the market is still trying to digest 5G. There's a lot to do with 5G nowadays before we jump into 6G [...] My point here is that there are still many, many other locations or use cases that haven't happened yet. So the adoption of 5G, the private 5G, so far has been really weak."*

> IN9: *"5G, for the moment, everything in roaming is based on the 4G and the 2G and 3G number seven diameter signalling. And that will last for, I would assume, a couple of decades [...] If you are looking at your display on your phone at this 5G [symbol], this is only the radio and not core, but that detail is not being known to the customer."*

Moreover, this limited adoption is mirrored in enterprise security practices. Participants noted that only a small number of customers are exploring advanced security approaches such as zero-trust architectures in the context of 5G. Many vendors, particularly those lacking specific expertise in 5G systems, continue to rely on traditional security mechanisms like centralised firewalls and identity management systems. This indicates that, despite 5G's potential to transform network security, its implementation still reflects legacy mindsets, requiring a fundamental shift in how networks are designed and secured. While some participants acknowledged that 5G promotes a secure-by-design approach, which is expected to carry forward into 6G, as also noted by Ylianttila et al. (2020), they emphasised that this remains aspirational. In practice, current deployments do not yet reflect this paradigm.

Furthermore, one participant noted that addressing emerging security threats will require a rethinking of how future 6G networks are deployed, as even in today's networks the security and network layers are often poorly integrated, creating conflicts that could be resolved only through deeper integration from the ground up. The researcher observes that even if established standards and implementation guidance for secure-by-design principles in 6G, network operators and vendors are likely to face significant delays in adapting to them. The researcher speculates, these delays stem not only from the technical and organisational challenges of adopting novel and emerging technologies but also from the high costs of transitioning to fundamentally new security architectures, particularly when capital expenditure is still heavily directed towards rolling out 5G infrastructure and services.

> IN2: *" So that's where we collaborate, for example, today with Security Technology Vendor 1 (STV1) or with STV2 or STV3, who are capable of providing SD-WAN capabilities. I'm not sure if they are capable of doing this on 5G already."*

> IN4: *"And in terms of adoption, I think it's quite low. I've only had a couple of customers who have been trying to implement zero trust, and the rest are still in the more traditional way of working with, like the centralised IDs, centralised firewalls and centralised everything."*

> IN7: *"Unfortunately, the way we've built our networking infrastructures in the past was always that you get two types of infrastructure. You get a connected infrastructure and then you get a secure infrastructure [...] What we see traditionally, I believe, for the last 30 years is that the networking component, the connected space, has won. But with what's happening today with the security landscape is that we are now seeing a shift, a mind shift [...] Are they playing well together today? No, still not. Even now I have a customer where we have solutions, but they decided from a networking point of they want to do their own thing."*

> IN9: *"5G is the first mobile system that is being designed for the security of mind and that has implications. That comes from a security philosophy that everything that is being passed should be confidential and should be protected. And some security individuals believe in security paradigms, without being open to considering how such an ecosystem is working or how it is being operated."*

4.2. SECaaS in the 6G Context

Despite the speculative nature of some discussions, these insights are valuable for understanding evolving perceptions within the industry. Participants revealed that security solutions could vary and include products to managed services based on the customer-specific requirements of the network being deployed. Security products could include firewalls and programmable network switches, whereas managed services include elements like network monitoring using AI and unauthorised access management. Mapping these identified products and services using the grouping framework used in W. Wang and Yongchareon (2017) of reactive, protective, and detective security solutions allows the researcher to better analyse the findings for what the participants expect SECaaS solutions to entail, as shown in Table 4.1.

Table 4.1: SECaaS Functionalities in 6G by Security Group

Group	*SECaaS Feature*	*Description*
Protective	Physical Infrastructure Security	Threat protection of the physical layer of network infrastructure like servers, RAN equipment, etc
	Cryptographic Encryption	Converting data into unreadable code using traditional computer algorithms
	Quantum Encryption	Converting data into unreadable code by leveraging the principles of quantum mechanics
	Firewall Deployment	Implementation of a system that monitors and controls incoming and outgoing network traffic
	Unauthorised Access Management	Implementation of a system that authenticates and authorises users to interact with data based on policies
	Internet Security	Implementation of a system that protects users against web-based traffic and threats
	Update and Maintain Solutions	Continuous improvement and reliability of security systems by regular enhancements
Detective	System Information and Event Management	Implementing a solution that gathers and logs data regarding traffic on the network
	Network Monitoring	Implementation of a system that observes the traffic behaviour of different elements of the network
	Managed Detection and Response	Implementation of a solution that identifies anomalies in the network and raises alerts to the user
Reactive	Security Incident Response	Implementation of a solution that takes action after a cyber threat has occurred
	Network Backup and Recovery	Implementation of systems that allow system and user data to be restored

4.2.1. Protective Features

Protective features refer to the measures implemented proactively to prevent security threats before they occur. These include the products and services designed to deter or block attacks at the outset. Participants highlighted that in the context of 6G networks, physical layer security is a key concern, particularly for stakeholders involved in network operation. This concern was especially prominent among interviewees from firms involved in deploying and provisioning network connectivity, likely because they currently work closely with national governments that impose strict security requirements.

> IN1: *"We need to make sure that our servers are protected and stuff like that [..] that phone towers don't get DDoS'd and stuff like that. [...] If you look at the security part of this, I expect the [6G integrated] satellite network to be safe. That nobody can hijack the satellite, that nobody can make it crash, that nobody can DDoS the satellite."*

> IN3: *"I think one thing where a SatCom company actually has a probably a more than average focus on security is on that physical layer. So when we sell to the government services, that security piece is so important"*

Whilst participants acknowledged that conventional security measures such as preventing internet phishing, encryption and firewall deployment will remain relevant in 6G networks, several also pointed to emerging protective features that will become increasingly important. These include technologies such as quantum encryption, unauthorised access management within network slices, and the adoption of zero-trust architectures. For example, a satellite or mobile network operator integrated into the 6G infrastructure could deploy Quantum Key Distribution (QKD) to ensure physical-layer security when transmitting data. Additionally, zero-trust principles would require network operators to adopt a security-first design approach, where connectivity is granted through strict policy enforcement, thereby

preventing unauthorised access. This would be particularly critical for MNOs offering localised network slices, as maintaining the integrity and confidentiality of these private networks would be paramount.

> IN2:*"I think if you do slicing, for example, I think we are at least responsible for making sure that no one can access the slice, so that the slice itself, for example, is shielded [...] the slices themselves are secure that we don't create backdoors through the slicing as such."*

> IN3: *"There is the big uncertainty whether post-quantum encryption will be sufficient post the quantum computer or something like Quantum Key Distribution (QKD), which QKD today does not exist and also is not really needed, but it is something novel because it gives you physical security. You have guaranteed that there's no eavesdropper with post-quantum encryption [...] And for us, with our doubling into quantum key distribution, is not a telecommunication service, but that's a security service"*

> IN7: *"How can we move the customer today from a typical network infrastructure which has a bit of security on top of it or security point products to move into a more zero trust infrastructure where we by default don't trust and then through policy, enable connectivity."*

An important insight that emerged is that many of the features discussed by participants were focused on preventing security threats before they occur. This emphasis reflects an implicit endorsement of secure-by-design principles for 6G networks, aligning with recent literature (Veith et al., 2023). Interestingly, these findings challenge the categorisation of SECaaS functionalities proposed by W. Wang and Yongchareon (2017), who primarily focus on reactive security measures rather than protective functionalities. Additionally, participants underscored the significance of maintaining and updating security solutions, an aspect notably absent from the framework (W. Wang & Yongchareon, 2017). As networks become increasingly software-based and integrated across industries, the continuous upkeep of security systems becomes essential for ensuring long-term protection. This is particularly relevant in light of evolving regulatory requirements, such as compliance with the NIS2 Directive, which imposes stricter obligations even on legacy systems.

> IN1: *"If I add a security solution, then I also have to maintain, update and upgrade sometimes [...] A drawback of OT devices, so in this case, MRI machines for instance, or cars. A car will keep on driving for the coming 10/15/20 years. So the contract you sign with the security product means that it will have to be a contract for about 10/15/20 years."*

> IN3: *"Say you want this firewall or this type of encryption or something. Rather than that's all on the hardware of everything that you produced, you say, okay, software configuration turned on, and now you pay for it. Or okay, and we can turn it off, and it can evolve or it can be updated over the air."*

4.2.2. Detective Features

Detective features refer to the measures implemented while a security threat is actively occurring. These include products and services designed to log system information, monitor traffic activity, and detect anomalies in real time. Participants identified Security Information and Event Management (SIEM) solutions as a key element in this category, commonly used for network monitoring and log collection. A recurring theme was the emergence of end-to-end services such as extended or managed detection and response, where service providers use the data gathered through monitoring to identify abnormal patterns and take countermeasures against threats. Participants also emphasised that such services enable the application of AI models to improve threat detection, aligning with the findings of Benzaïd et al. (2022).

> IN2: *"One of the cases that we've been looking into for 5G is also the need to monitor the security of these networks [...] That [security contract] is in itself a bundle of services where we actually provide the end-to-end security, including security monitoring [...] including the monitoring of the service, of the firewall."*

> IN4: *"We analyse alerts for them and escalate potential security incidents to our customers. Then they have to verify whether something is going on or if it was just a false positive or a legitimate action [...] So of course in our detections, we are using AI models to train on the*

data of our customers and be able to detect deviations on their normal way of working, and that's something that a lot of security companies have been working on in the past years."

IN8: *"And we're specialising in cybersecurity network monitoring to detect security breaches [...] And the monitoring, the network monitoring tools are very important for 6G because what we're trying to do in 6G is to automate the management of security.*

However, the researcher observes that participants largely discussed these capabilities within the context of centralised network architectures, where system logs and traffic data are collected in a single location. This centralisation enables more streamlined threat detection and simplifies the application of AI tools. Yet, this assumption may not hold as Non-Public Networks (NPNs) become more prominent in future 6G deployments. The decentralised nature of these networks means there may be no single authority with complete visibility over network traffic, raising important questions about how detective features such as Security Information and Event Management (SIEM) and managed detection services can operate effectively. One participant acknowledged this challenge, suggesting that security providers will also need to evolve to address the demands of decentralised environments. As such, new approaches to distributed detection and coordination may be required to ensure effective security monitoring in private and decentralised networks.

IN4: *"But if the whole goal of 6G is decentralised, the way we do security also needs to evolve into that as well because it doesn't make sense if one party just decentralises everything and then we come in and say, yeah, we need everything centralised to provide security it wouldn't make a lot of sense."*

IN7: *"So we need to put that data into a single place to make sense of it, which is the SIEM infrastructure, you know and that's why I believe Infrastructure Provider 1 (IP1) bought Monitoring Software Company 1 (MSC1) recently because they want to get into the SIEM game as well, that overlay network."*

4.2.3. Reactive Features

Finally, the last category of SECaaS solutions discussed by participants includes reactive features, measures taken after a security incident has occurred. Participants noted that firms often offer incident response services, recognising their significant influence on brand reputation. One participant emphasised that transparent communication following an incident can help turn a security breach into an opportunity to demonstrate resilience and accountability. For example, several participants referenced a recent high-profile case involving a cybersecurity firm, where an issue led to a global service outage and even grounded airplanes. This incident was widely cited to illustrate how security providers themselves can also be vulnerable. Interestingly, a participant with direct experience working with the affected firm clarified that the issue was not a security breach, but rather a result of internal oversight. Due to the interconnected nature of their solutions, the failure cascaded across devices. The researcher highlights this example as a powerful illustration of why clear post-incident communication is essential. Another recurring theme was the importance of having robust backup and recovery mechanisms in place to ensure service continuity in the face of unexpected disruptions.

IN1: *"Looking at what you can do with 5G and 6G later on with OT devices, smart cars, smart everything. The security is on the device [...] and in the physical hardware that's necessary for the network recovery itself"*

IN3: *"This cybersecurity company had this outage and global airports and aeroplanes were down, their share price dropped like 40% in a day [...] they had a gigantic hit to their brand.*

IN4: *"Another team within our firm helps customers when they have had an incident like a security incident and security incidents have a really big mental impact on people [...] Nowadays everyone can have an incident and we're seeing this pretty much everywhere, and to me, that's more of a personal opinion, but it really comes down to how they handled the incident and how they communicated to the outside world."*

IN9: *"I would say the huge problem with MNO2, that they have to replace all the SIM cards of the customers because of a security breach. Of course, this is a huge brand damage to MNO2, but they can also turn it to their advantage because they are showing nowadays*

> *that they are ready to act if they have a problem and that they are doing their best to secure the customers again."*

While the discussion on reactive features was not as extensive, the researcher highlights their critical role in the broader security ecosystem. Any actor, whether a customer, MNO or a security provider, could eventually face a security threat, making incident response capabilities essential. Furthermore, the researcher observes that insights gained from previous incidents play a vital role in shaping future protective strategies. This supports W. Wang and Yongchareon (2020) finding that these categories are not strictly separate but rather interconnected, with functionality often flowing from one phase of the security lifecycle to the next. However, this should imply that elements such as intrusion management and network security should be considered protective, rather than reactive, contradicting the original categorisation in W. Wang and Yongchareon (2017).

> IN7: *"OK, so that impact [regarding grounding of aeroplanes due to a cybersecurity issue] there was not a security breach, that impact there was only bad due diligence because they needed to push a patch through which wasn't good, or well checked [...] Yeah, they messed up. Is that a policy change they can affect that will make it better in future? Absolutely. They went and fixed that little loop"*

4.2.4. SECaaS Deployment Modes

When analysing the role of SECaaS in 6G networks, it is essential to consider how these services would be deployed within the network. Whilst 6G visions anticipate more decentralised deployments, they simultaneously embrace trends like cloudification and softwarisation, which lean towards centralised architectures. Reflecting this tension, participants discussed three distinct SECaaS deployment models. Some argued that the network itself should not be trusted with ensuring security and that its core responsibility should be limited to providing connectivity between endpoints. As a result, they proposed that security solutions be embedded within user devices, such as having zero-trust architecture components in the SIM card by default or deployed at the edge, in the context of NPNs. The researcher observes that this approach aligns with the notion of embedded trustworthy security into products and services by default in future networks (Latva-aho & Leppänen, 2019).

> IN1: *"Looking at what you can do with 5G and 6G later on with OT devices, smart cars, smart everything. The security is on the device, it's not on the network and it shouldn't be. The network is there to facilitate communication, and that's it."*

> IN7: *"We don't trust the network enough to say we'll make sure that the network can actually secure you. We literally go and move that security back to the laptop or to the user or on the device itself [...]. We actually do have a SIM card-relevant option, which means in future any SIM card could actually already have a Zero Trust component built into it by default."*

However, an important insight emerged regarding the feasibility of this model, particularly for resource-constrained devices. One participant noted that many IoT devices are unlikely to support security-intensive functions, as they often rely on older communication standards such as 3G, 4G, or even 5G, and lack the computational capacity to run advanced on-device security mechanisms. This makes backwards compatibility in 6G particularly difficult from a security standpoint, as these generations do not adopt a secure-by-design approach, leading to a potential security threat as older generation devices communicate on 6G networks. This insight echoes the findings of Nguyen et al. (2021), who argue that while backwards compatibility is essential for 6G, it remains a significant challenge. Additionally, another participant highlighted that even more advanced systems, such as connected and autonomous vehicles, typically lag behind the standardisation process. For instance, Release 19 of the 5G standard, expected to be finalised by the end of 2025 (3GPP, 2023), may not be implemented in vehicles until as late as 2030. The researcher, therefore, speculates that, although decentralised device-level security may conceptually be attractive, its practical implementation is constrained by technical limitations, economic considerations and long product development cycles across the wider ecosystem.

> IN3: *"So today is the cars that come out of the factory, they are 3GPP Release 17 compliant, we think that by the end of this decade, by 2030, it will be Release 19 for which we hope then that the complete Satcom piece can work."*

> IN9: *"Number seven signalling [a 2G/3G protocol] is old and insecure, so you need a lot of protection. You may make it more secure by tunnelling it over and a more secure thing like diameter [a 4G protocol] or even 5G, but that's not part of the ecosystem today."*

On the other hand, some participants emphasised that with the growing adoption of cloud-based applications and Software Defined Networks (SDNs), security solutions should be implemented within the central cloud plane. These participants argued that, from a security perspective, the cloud and the edge should not be treated as separate domains, rather, the edge should be viewed as an extension of the centralised policies and solutions deployed in the cloud. This perspective supports the emergence of integrated security frameworks such as Secure Access Service Edge (SASE), which enable firms to combine network and security services through a single solution. Furthermore, the interviews revealed that these participants anticipated future networks to adopt a centralised approach which would also enhance the ability of security providers to apply AI techniques more effectively to aggregated data, thereby improving threat detection and response capabilities.

> IN2: *"So it's a fully centralised cloud-based protection where you have very "dumb" edges, which are basically just routing all the traffic to the cloud and then everything is managed in the cloud. I think the trend is moving much more towards centralised cloud-based security, with SASE and SSE being the buzzwords. That's also mainly driven by the fact that there isn't that much physical protection any more. If your servers and applications are in the public cloud, [...] and if most employees are working from home at least a few days a week, maintaining a local physical infrastructure doesn't make that much sense any more."*

> IN5: *"There shouldn't be a real distinction between the edge and cloud. It's like an extension of what you have in the cloud, but on-prem, at the edge. So all the security, all the governance, models, compliance, whatever you want to call it. Whatever you do in the cloud, at the edge should be the same [...] So there is no cloud and edge from a security perspective, there is a cloud and edge from a physical point of view. But security-wise, is that there is no distinction, or there shouldn't be a distinction."*

> IN7: *"Now if all data flows through one central location, that means that you can apply AI technology on top of that. So you end up with one data lake, and I believe that that's going to be the future. It's not necessarily how we secure things or basically what technologies we have, it's literally do we have visibility in the data and all data flows, and can we make sense of it with AI. The answer is most probably going to be in future, yes and yes."*

However, this approach to security implementation presents challenges when applied to emerging decentralised deployment models, particularly in the case of Standalone Non-Public Network (S-NPN) that operate independently from central public infrastructure. The researcher notes that this model also tends to overlook the importance of deploying certain security services closer to the user or at the edge, where immediate protection is needed. Additionally, centralising security functions could concentrate power in the hands of a few firms that control access to network traffic, raising concerns around transparency and market dominance. While this model may enhance the performance of AI-driven threat detection by enabling more efficient data aggregation, it also introduces significant risks. A centralised architecture could become a high-value target for adversaries, with a successful attack potentially compromising the entire network. Furthermore, one participant described how their zero-trust solutions would decrypt customer data and apply AI models for threat detection. However, they noted that many clients remain uncomfortable with this approach and deliberately restrict certain sensitive data from passing through such systems. The researcher believes this is a reflection of deeper privacy concerns where centralised security services that process potentially sensitive data could themselves become prime targets and pose a severe security risk, if compromised.

> IN6: *"So if you compromise the switch in a centralised way, perhaps it's harder to compromise the centralised point, but if you compromise it, you compromise it entirely."*

> IN7: *"SaaS technologies, for instance, some SaaS applications do not like the fact that we actually decrypt their data [...] So yes, I do see that on a daily basis with every single customer we speak to, they have little pockets of data that they feel okay outside for technology, and that's fine if they believe that's secure enough, but that's a decision they have to make"*

Finally, many participants advocated for a hybrid or middle-ground approach, which involves implementing certain security functions on the device or near the edge, while others are maintained at the central network or cloud layer. This strategy was seen as a practical way to address the resource limitations of devices, whilst still leveraging the advantages of centralised security. Participants highlighted that such an approach allows firms to tailor and deploy security measures according to specific use case requirements. Moreover, they argued that this model offers a more balanced and optimised security architecture, combining the strengths of both decentralised and centralised deployments, and thereby avoiding the limitations associated with relying solely on one or the other.

> IN6: *"I think it's going to be like a middle ground type of solution where some security services or some security defences will run on top of these programmable units, these programmable units are quite constrained [...] so for sure there will be security aspects that you won't be able to run on that. So there will be defences that we have more on the network, defences that we have more on the cloud, and together we'll have a stronger toolbox."*

> IN10: *"It turns on security will be adapted and deployed on the road. Come back to your concept of security as a service [...] we have to seek some dynamic orchestration in order to activate [security] in the right place the right security and commit that we deliver, clearly, this is a solution when we are in some specific area on-premise in the border of the network or potentially over a short part of the cloud"*

Moreover, participants discussed how this hybrid approach of deploying appropriate security solutions where needed, not only ensures localised protection but also contributes to a broader, more integrated security posture. The researcher notes that this is particularly important, as companies often secure their own systems in isolation. However, these components must also communicate securely with one another, which requires an additional layer of overarching security. Participants expressed concern that a failure in one part of the system could easily cascade across other domains, amplifying the potential impact and reinforcing the need for coordinated, network-wide security measures. The researcher further emphasises that this highlights the importance of developing improved stakeholder collaboration frameworks, or introducing common platforms within the 6G standard, perhaps like interoperable APIs, to facilitate seamless and secure coordination across actors.

> IN7: *"What you've said there is very true that the device manufacturers look at their own security, but when they look at it, they only look at their own security environment. But for total security to have good security, you have to look at the entire spectrum. You can't just look at one thing [...] So if we can get them to send the data into one single location and then from there work in, let's call it the secure net, where we combine the data there."*

> IN8: *"Yeah, there are aspects as they are local to a domain, for instance, RAN or core or IoT network. But you also have to look at the overall picture because there can be cascading effects, for instance, if the there's a problem in the RAN, this will have an effect on the on the core as well, So you have to be able to do this correlation of events that's in different domains. That's why it's necessary to have a more global picture, since you have several stakeholders inter-operating, this is also an aspect that you have to consider.*

To reiterate an insight shared by one participant, MNOs could adopt this hybrid approach by implementing centralised security mechanisms alongside localised, user specific solutions at the edge, allowing them to benefit from faster performance and context aware protection. Building on this, the researcher proposes that SECaaS providers do not need to deploy their services solely through or at the central core network. Instead, deployment at the local core or on premise may be more effective, as these solutions can be tailored to specific customer requirements, while the internal core network security would continue to be managed by the MNOs.

> IN9: *"Internally in a network operator, there are special functions that are looking after the security of the network itself, and it can be distributed, and according to the technology, the security architecture, you should have protection wherever the application is. So if you have local computing with a home network very close to the customer because of computing advantages, low latency, high throughput, et cetera, then the security function should be local there instead of, then it is a less stringent application and it happening in a data centre."*

4.3. Stakeholders in 6G SECaaS

To understand the techno-economic interactions, it is essential to identify the stakeholders involved in deploying SECaaS solutions within 6G networks. Participants outlined a diverse range of stakeholders depending on the specific use case in 6G. Whilst traditional actors such as MNOs and Infrastructure Providerss (InPs) were frequently mentioned, participants also identified several emerging stakeholders expected to gain relevance in 6G environments. For example, one participant highlighted the growing influence of major technology companies in the security domain, particularly due to the increasing adoption of Software Defined Network (SDN). Another participant pointed to chipset manufacturers as critical stakeholders in use cases such as direct-to-device satellite connectivity, operating alongside the public network provided by MNOs. The researcher also notes that this also suggests the need for satellite operators as stakeholders in mobile networks, who are traditionally never seen as a relevant actor in previous generations. Additionally, the rise of local operators, such as Mobile Virtual Network Operators (MVNOs), was noted, with participants suggesting they could leverage Network Function Virtualisation (NFV) to offer localised virtual networks tailored to specific user needs.

> IN2: *"The over-the-top solutions are no longer provided by the service provider but by players like Technology Provider 1 (TP1) and such, and I think we are not there yet in the enterprise market and IT market, but it's a risk that or a risk from our perspective that it's moving that direction [...] But today if you look, for example, at the security contract that we've won, it does include a lot of those big security players like Technology Provider 2 (TP2). They are a very huge component in that frame contract."*
>
> IN3: *"The MVNO context is pretty cool, I mean I can start a company tomorrow that basically sells E-SIMs and by leasing somebody else's hardware, where doing that from a physical point of view will probably be multiple and multiple of years. That's an example, but this virtualisation happens everywhere. So you have this concept in telecommunications called NFV or network function virtualisation. So I'm installing my network, and basically if it's virtualised, the economics or the business model can be interesting."*

When it comes to deploying, integrating, and managing security solutions in 6G networks, nearly all participants acknowledged a persistent ambiguity and fragmentation of responsibilities. They identified a wide range of potential actors, such as MNOs, specialised security firms, customers, infrastructure providers, and user equipment manufacturers, without a clear consensus on who holds ultimate accountability. The researcher speculates that this stems from the overlapping and context-dependent nature of stakeholder roles. In many cases, responsibilities are secondary or shared, depending on the network architecture being deployed. For instance, an MNO might not only provide NPN connectivity but also offer SECaaS solutions as an additional service layer to the customer.

> IN4: *"I believe that the main responsibility will still be on the internet service providers, right, Mobile Network Operator 1 (MNO1) and all those big players. But of course, security companies will need to find a way of monitoring independently because usually, you want to have a third party that doesn't have a conflict of interest."*
>
> IN7: *"The Chief Information Security Officer (CISO) signs a document that says I will fairly manage my clients' information [...] So who is responsible? Ultimately, it's the CISO. It's the business that manages their data. They have to have the controls in place to make sure."*
>
> IN8: *"Mostly will be the equipment manufacturer, yes, but also it could also be companies like involved in the cybersecurity, development of cybersecurity tools, but mostly it would be equipment manufacturer that provides the solutions to the operator, but also sometimes the operators also where we get involved in developing their own solutions for cybersecurity, for instance, Mobile Network Operator 1 (MNO1) has its own unit dedicated to cybersecurity."*
>
> IN10: *"I think as operators we don't take this type of action because it will expose our certification. We are not mature enough to go this way, sharing the signature could expose a lot of issues, and we can do it in a reserve, but in real life, I don't know if we have anything for five to eight years."*

Whilst some participants suggested drawing a parallel with the shared responsibility model commonly used in cloud computing, others acknowledged that this model remains underdeveloped within the

mobile networking domain. This ambiguity suggests that future 6G ecosystems may evolve toward a similar shared framework for security responsibility. However, such a shift would require a comprehensive mapping of use cases and clearly defined stakeholder roles within the standard. Although the cloud model could, in theory, be adapted directly, the researcher notes a key limitation: end users of cloud-based security services are often unaware of the underlying platform provider, a point also raised by the participant offering cloud-based SaaS security tools. In contrast, within mobile networks, the network provider (often the MNO) typically offers bundled add-on services, potentially to create added value for the end user. This reflects findings by Bouwman et al. (2008), who highlights service bundling as a strategy to retain customers.

> IN1: *"So Cloud Service Provider 1 (CSP1) simply says we are responsible for the security of the cloud [...] You as a customer are responsible for the security in the cloud. [...] We see something similar in networks."*

> IN2: *"Tricky as in it's very important to be very clear in these responsibilities and actually you could you could make a parallel with the hyper-scaler. So with the clouds, the thing they propagate is the shared responsibility model, where the responsibility depends on the model that you choose. [...] In the networks, in the 5G discussion, I notice it's not yet as clearly defined as it is in the hyper-scaler world or in the public cloud world. "*

In this context, what is needed in 6G is a clear demarcation of responsibilities across the network, particularly regarding who is accountable for which aspects of security. One participant noted that misconceptions about security responsibilities in mobile networks often lead to a false sense of security during deployment. Another participant pointed out that even in Standalone Non-Public Networks (S-NPNs) deployments, which are frequently presented as fully isolated from public networks, potential backdoors may still exist, contributing further to this misplaced sense of security.

> IN2: *"The blue one [S-NPN network diagram] has a false sense of security, it's represented here as it is always represented with a sort of secured network boundary with a firewall. [...] If in that factory there's a vending machine and this vending machine is somehow connected to this network, but also has a connection with the manufacturer, which is maybe not secured somehow, then already you're not secure any more."*

> IN6: *"I think that there are lots of misconceptions around who is responsible for what [...] I think that whatever model you go for, it should be clear who is responsible. I don't think it's problematic if you say I'm not in charge of security, as long as you say it because otherwise, you create a false sense of security.*

Building on this, by using the framework proposed by Yrjölä et al. (2023), the interviews revealed that most identified stakeholders aligned with the twenty stakeholder groups previously outlined. However, through a SECaaS-specific lens, the researcher proposes a revised classification to better reflect the distinct responsibilities in 6G network security deployments. Stakeholders are therefore regrouped into four overarching categories: (i) Infrastructure Providers, (ii) Telecommunications Providers, (iii) Security Providers, and (iv) Target Consumers, as summarised in Table 4.2. Unlike the broader grouping of all security and privacy-enhancing actors into a single category in Yrjölä et al. (2023), this model distinguishes between three types of Security Providers based on their core functions and placement within the security service offering.

Table 4.2: Identified Stakeholders in 6G SECaaS

Infrastructure Providers	***Telecommunications Providers***	***Security Providers***	***Target Customers***
• Network Hardware Providers • Cloud and Technology Providers • Satellite Operators	• Mobile Network Operators • Local Network Operators • Fixed Network Operators • Roaming Hub Operators	• Security Technology Vendors • MNO SECaaS Providers • Non-MNO SECaaS Providers	• Commercial Enterprises • Mobility Customers • Industrial Customers • Governmental Customers

4.3.1. Infrastructure Providers

Infrastructure Providers form the foundation of connectivity by supplying or provisioning the physical and digital components required for network functionality. This group includes network hardware vendors, cloud and technology providers, and satellite operators, the latter two identified as emerging stakeholders in the context of 6G, where ubiquitous global connectivity and Software Defined Network (SDN) are expected to become standard. Whilst these providers may not directly offer SECaaS solutions, their role is increasingly strategic, as the infrastructure layer significantly influences how securely services can be delivered. Several participants noted that infrastructure providers typically bring domain-specific expertise: some focus on access point hardware such as RAN equipment, while others specialise in core components like network switches and routers. Similarly, cloud providers enable the back-end environments that SaaS-based security vendors depend on to build and deploy their services. This growing influence over the technical foundation of security provision suggests that the responsibilities of infrastructure providers may expand in future 6G ecosystems, further blurring the lines between connectivity and security services.

> IN1: *"We use Cloud Computing Platform 1 (CCP1) for our SaaS services, we don't build our own cloud. So we have our software running, but it's running on CCP1."*
>
> IN5: *"I mean how these work, is that there is someone providing the technology for instance, Infrastructure Provider 1 (IP1), IP2 or IP3 as well and there are many others and these ones they provide like the physical and software, but the physical infrastructure and the network."*
>
> IN7: *" If you have an Infrastructure Provider 1 (IP1) network and you are going to deploy, I'm just using names here but you're going to be deploying let's say, an Infrastructure Provider 2 (IP2) Wi-Fi on top of that, you already have two different configuration points. Now the one thing that we have created was lines of business or basically little containers where we work within every network vendor has a speciality."*

Beyond their core role in provisioning network hardware, infrastructure providers may also take on responsibilities related to the integration and management of connectivity and managed security services. Participants highlighted that large firms, particularly those with vertically integrated structures, often bundle complementary services, such as managed connectivity, private network configurations, or continuous security monitoring, alongside their infrastructure offerings. For example, a satellite operator might not only deploy and maintain orbital infrastructure but also deliver end-to-end connectivity services through its network.

> IN3: *"Well, I mean it's the core of our [satellite] business. So a big chunk of our business is what we call our networks business. So it's providing not just the internet but also just basically private connectivity services to multiple sectors. So it's the government sector, the mobility sector and enterprise and cloud."*
>
> IN5: *"Yeah, could be that that depends on the size of the company. But that could be perfectly just for example, Information Technology Company 1 (ITC1). They also have their own 5G technology, and they can also provide all these managed services."*

4.3.2. Telecommunications Providers

Telecommunications providers are primarily responsible for configuring and operating networks using infrastructure supplied by infrastructure providers. As infrastructure components are often sourced from multiple vendors, these actors play an integrative role, configuring and assembling these components into coherent systems that deliver connectivity to end users. This group includes Mobile Network Operators (MNOs), who typically own and operate the core and access networks, and Fixed Network Operators, who manage physical infrastructure such as fibre connections between different network segments. It also includes Local Network Operators, such as Mobile Virtual Network Operators (MVNOs), who may lease access to existing infrastructure while offering regional or specialised services. These configurations are further supported by Roaming Hub Providers, who facilitate inter-network interoperability, ensuring service continuity across geographical and organisational boundaries.

> IN1: *"The reason 5G rolled out in Europe is not because security was present, it's because people wanted a quicker internet connection. That's it. So Mobile Network Operator 1 (MNO1), MNO2 and all those providers started building networks that were capable of that."*
>
> IN9: *"So if you are going somewhere on a tropical island somewhere in the ocean then you can still use your mobile phone. The operator there may be a very small operator, and you are possibly the only client at that moment in time of the home operator in the Netherlands that is travelling there and those roaming hub providers are actually in the middle of that in that ecosystem"*

In addition to their core responsibility of provisioning network connectivity, some telecommunications providers, particularly those embedded within larger corporate groups, are increasingly diversifying their service portfolios to include cloud, ICT, and enterprise-level solutions, potentially extending into SECaaS. This finding aligns with Moussaoui et al. (2022), who suggests that telecom operators must develop new revenue-generating business models beyond basic connectivity to monetise 5G and, by extension, 6G networks. These expanded roles are sometimes facilitated through subsidiaries or distinct legal entities operating under the same brand umbrella. As these organisational boundaries become more fluid, the researcher notes that the responsibilities of telecommunications providers become more complex in future 6G ecosystems, increasingly blurring the line between connectivity provision and the delivery of integrated security services. Alongside their external offerings, MNOs remain responsible for securing internal network operations, including the protection of signalling traffic and ensuring compliance with industry and regulatory security standards.

> IN2: *"So in itself, as the group we provide all sorts of telecommunication systems in Belgium with a focus, of course, on fibre and currently the 5G network of MNO1. There's also a subsidiary of MNO1, which is responsible for inter-company or international traffic, so it's a large player. MNO1 has also acquired Cloud Communications Service Provider 1 (CCSP1) and Communication Service Provider (CSP1), which are also internationally active, so there's the focus is on Belgium, but there's an increasing amount of international solutions provided as well [...] And focusing on the enterprise market there, there's also from an IT perspective there, IT services being provided in Belgium, Luxembourg and the Netherlands. So it's a broad range of services being provided too."*
>
> IN9: *"There are a lot of security things inside such a mobile operator. If you are not roaming, so if you are just in the Netherlands and you have contact with a mobile operator here in the Netherlands, then all the signalling actions are internally managed, and there are no other operators involved. But still, security requirements are coming in 5G, making it a far more secure system than before."*

4.3.3. Security Technology Vendors

Security technology vendors, positioned within the broader category of security providers, are primarily responsible for the development and delivery of security tools, platforms, and software. The participants identified that their core contribution to the ecosystem lies in creating the technological building blocks necessary for secure communication and data protection, rather than in directly deploying or managing these solutions. Typically, their products are distributed through strategic partners or cloud marketplaces. However, the researcher notes that in some cases, vendors may also take on a sec-

ondary role in integration or management, particularly when their offerings are embedded into larger, bundled solutions. Therefore, while their primary responsibility remains the enablement of secure services, their involvement potentially extends into supporting other stakeholders in implementing and operating these tools within complex service environments.

> IN1: *"Our firm is a security vendor, essentially so we build security software that we sell to our customers through partners, through ourselves and through Cloud Computing Platform (CCP1) marketplace. So we have a lot of partners [...] So for instance, we have Mobile Network Operator 1 (MNO1) as our customer, but also as our partner. So MNO1 also sells a service to others with our software, but also uses our software in their own data centres"*

> IN7: *"Do we give managed tools? Yes, we can give them the tools, but we're not a provider of that service. We're a provider of the solution. How they deploy that solution, I mean if they decide to open up all the ports and just make everything available to the whole world, yeah, we're not responsible."*

4.3.4. SECaaS Providers

Another stakeholder within the group of security providers is SECaaS providers who are identified as intermediaries between security technology vendors and end customers by integrating and managing a variety of security tools into cohesive service offerings. Unlike vendors who focus on developing security solutions, SECaaS providers configure, deploy and operate these solutions as managed services tailored to customer needs. Essentially, a parallel could be drawn to telecommunication providers as to how they must collaborate with security technology vendors and configure these tools into a bundled service for the customer.

> IN5: *"I've had experience working with MNO1, and they use technology providers like Security Technology Vendor 1 (STV1) or whatever they use. They have the people and they offer the service through a third party like another company, perhaps an MNO like Mobile Network Operator 1 (MNO1), in the end is delivering or offering security-as-a-service solutions to other companies using STV1, using STV2 or even a combination of them."*

> IN6: *"So basically you pick Mobile Network Operator 1 (MNO1) and what MNO1 does is to manage devices of certain companies that you have. MNO1 doesn't do business by selling you the Infrastructure Provider 1 (IP1) switch or router, but they know very well how to manage the IP1 type of firewall."*

Furthermore, participants noted that SECaaS providers may either operate as specialised, independent firms or be affiliated with an MNO. In both cases, they serve as the primary customer-facing stakeholders responsible for deploying security solutions and delivering them as managed services. As these providers must collaborate closely with security technology vendors to integrate various tools into a unified offering, the researcher proposes that SECaaS providers also hold a secondary responsibility in the provisioning of security tools. This involves working in coordination with vendors to ensure seamless integration and effective delivery. By distinguishing three distinct stakeholder types under the broader category of security providers—security technology vendors, SECaaS providers, and internal security units within operators—this research builds on the framework proposed by Yrjölä et al. (2022), who treated these actors as a single, consolidated group of security and privacy-enhancing service providers.

> IN2: *"I work in the security practice which focuses on providing security services. So we're not focused on the internal security of MNO1 as such, but we're focusing on providing security services to our customers [...] With a focus on the services that we as spokespeople provide on top of mainly security solutions, which are provided by vendors like Technology Provider 1 (TP1), Security Technology Vendor 1 (STV1) and others."*

> IN4: *"Managing the experience of our customers based on the service that we provide, which is not related to 6G but is a security service, so monitoring service [...] We do offer network monitoring as part of our service. I do imagine that as companies adopt these new technologies, we as security companies will also have to adopt the security monitoring of our stack."*

4.3.5. Target Customers

Customers are a central stakeholder in any business ecosystem. Several participants highlighted that security solutions are typically offered as an additional service layered on top of connectivity services. Based on this, the researcher identifies the customers of telecommunications providers as the primary target group for SECaaS providers. The interviews revealed that large commercial enterprises with distributed sites and multiple users, such as supermarket chains or universities, are key customers in this context. Furthermore, some participants also identified industrial manufacturing customers as an emerging segment, as they are increasingly adopting mobile networks to support smart automation and operational technology devices. The researcher observes that such organisations, due to their widespread operations and diverse user base, face an inherently larger attack surface. As a result, they are well-positioned to benefit from adopting solutions such as zero-trust architectures and managed detection services for their network slices, delivered alongside their connectivity services.

> IN2: *"It could be any enterprise actually [...] especially in the relational 5G/6G and slicing and such is like customers who are very distributed, like multi-sites. One of our customers is a Belgian supermarket [...] it's those larger companies or those very distributed companies, like building companies, as well, they're also very distributed."*

> IN7: *"Recently I spoke to a university in the Netherlands, and that university said to us, they've got a zero trust plan that needs to be finalised within the next ten years. That's a long time, and I said to them, what if we could start a proof of value and have you transitioned with every single user, including 60,000 odd students, within about three months?"*

> IN8: *"Well, all the industry. All industries are adopting more and more mobile networks in their application because it's easier to deploy mobile networks than wired networks, so that in big industrial sites, for instance. So it's becoming more and more important now."*

Furthermore, as 6G will bring global ubiquitous connectivity, participants identified mobile customers who are not connected to a fixed fibre connection, which not only includes smartphones but also aeroplanes, ships and vehicles. The researcher notes that this will serve security issues for customers like those driving an autonomous car. Whilst, Yrjölä et al. (2022) identifies human users as individual users, based on the interviews, the researcher proposes another set of target customers called mobility customers, which are those who are not connected to a fixed connection.

> IN1: *"At any given moment in time, there are people in aeroplanes. Currently, they're all dependent on either a very bad Wi-Fi network that the plane provides or they don't have the internet at all."*

> IN3: *"Mobility think of everything that moves, and we can't put a fibre cable to it. So think of an aeroplane. Think of a ship. Think of a car."*

Lastly, some participants identified governmental agencies as a critical target customer group, not only for securing communication within federal or central government bodies, but also for supporting defence and emergency response applications. The researcher notes that participants emphasised how these customers typically impose exceptionally stringent security requirements, often necessitating that certain security features be embedded by default within the connectivity offering. While governments may not directly engage with localised SECaaS providers, the researcher speculates that they could still benefit from isolated and localised network deployments due to heightened security concerns. This implies that trusted MNOs and infrastructure providers may need to adapt their strategies by deploying secure, localised network infrastructures to accommodate such specialised use cases.

> IN2: *"So that's of course and in another context, for example, we have now won SECaaS contract or Security-as-a-Service contract with the federal government."*

> IN3: *"So government think of basically the military, supporting military, but can also be crew welfare on ships. It could also be the civil government. So basically, think of emergency relief after a Hurricane comes in, this is usually paid for by the government."*

4.3.6. Stakeholder Roles

In identifying the stakeholders and roles, the interview process revealed both the primary responsibilities and the potential secondary or shared responsibilities of different actors involved in deploying SECaaS solutions within 6G networks. Using these insights, the researcher proposes two overarching role categories: provisioning, which refers to the development and delivery of the product or service; and management, which involves the integration and operational deployment of the solution. These roles are relevant across three key layers of the deployment of SECaaS solutions in the 6G network: the infrastructure, the network connectivity, and the security services built over the network.

Building on the discussion in the previous chapters, the researcher proposes a categorisation of stakeholder roles as follows. As discussed in Chapter 4.3.1, infrastructure providers are primarily responsible for provisioning the physical infrastructure, while also holding a shared responsibility for its management when required. Chapter 4.3.2 highlights that telecommunications providers primarily provision the network connectivity layer, while also sharing responsibility for managing both the infrastructure and connectivity. Chapter 4.3.3 shows that security technology vendors are mainly involved in provisioning security solutions, whereas Chapter 4.3.4 outlines how these solutions are typically managed and integrated by SECaaS providers. However, due to the need for close collaboration, both security technology vendors and SECaaSs providers are proposed to share secondary responsibilities in both provisioning and management.These relationships are summarised in Table 4.3, which illustrates the primary responsibilities (marked with an X) and potential secondary or shared responsibilities (marked with an O) for each of the four stakeholder groups across the three functional layers.

Note, the researcher does not include target customers in Table 4.3 despite identifying them as key stakeholders. Whilst some participants acknowledged the importance of collaboration with customers in the context of SECaaS, most viewed customers primarily as end users of the product or service, with limited responsibility for deploying the network or managing additional services. This perspective contrasts with the findings of Yrjölä et al. (2022), who emphasise the growing relevance of user empowerment and co-creation in 6G ecosystems. The researcher speculates that this disconnect may stem from the legacy of conventional mobile communication systems that historically offered little space for customer involvement in network management. Whilst one could argue that customers might hold shared, secondary responsibilities, such as managing aspects of security in collaboration with SECaaS providers, this would require end-user companies to employ technically proficient personnel, such as experienced Chief Information and Security Officers (CISOs). However, this would undermine one of the core drivers behind adopting SECaaS, the ability for small and medium-sized enterprises, which often lack in-house expertise, to outsource security management to specialised providers.

Table 4.3: Stakeholder Roles Across Provisioning and Management of the Network and Security

Stakeholder Role		***Infrastructure Provider***	***Telecom Provider***	***Security Technology Vendor***	***SECaaS Provider***
Provisioning	Infrastructure	X			
	Connectivity		X		
	Security			X	O
Management	Infrastructure	O	O		
	Connectivity		O		
	Security			O	X

Legend: X = Primary Responsibility, O = Secondary/Shared Responsibility

4.4. Value Interactions in 6G SECaaS

Following the mapping of primary and secondary responsibilities across stakeholders, the researcher shifts focus to how these actors interact in the deployment of SECaaS solutions, particularly across different network configurations. Rather than functioning in isolation, participants consistently described

SECaaS providers as intermediaries who bridge the gap between end users, security technology vendors and telecommunication providers. Importantly, participants emphasised that the value created by SECaaS providers does not stem from developing security products themselves, but from their ability to integrate specialised security solutions into an integrated and locally adapted service for the end user. This integration is driven by domain-specific expertise, a strong contextual understanding of customer environments and the ability to coordinate and manage complex relationships across multiple partners.

> IN2: *"So most of our customers prefer they have a local partner that they can go to for solving their issues [...] But also to be this middle man in getting the support in, in making sure that the configuration is correct. So, fortunately, the complexity is still high enough to allow us to add value on top of the solutions that are provided."*

> IN4: *"It adds value because each company will focus on their expertise like my team is monitoring team, so we will not offer a firewall because we just don't have that expertise like we can integrate the firewall into our service, but we will not offer like a product or a firewall [...] Then you cooperate with them to provide the complete package. Because you will not find one company that they are expert on absolutely everything."*

> IN6: *"I think that we as the man in the middle can provide something a bit more customised that may not be needed in many cases [...] But it's also true that, in my opinion, there could be opportunities to enhance some of these programmes that already come from these manufacturers."*

> IN7:*"What becomes quite important and is critical in this game is to have a really educated partner that has the same business acumen to go and build out, not just to make money out of every customer, but to really go out there and sell managed services [...] I really believe in this, it's one thing for us to sell a solution to a customer. It's the second thing for a customer to understand that this is good for them. But ultimately, what they need is they need a really good partner in between, they need that part of the infrastructure."*

4.4.1. Value Network Configuration for Centralised Deployment

Building on the stakeholder roles outlined in Table 4.3, a Value Network Configuration (VNC) can be constructed to represent the value exchanges between actors. This section first considers a public network deployment, as it represents the most centralised and conventionally widespread network model. The technical interactions are derived from stakeholder responsibilities, followed by the associated business interactions between these actors. For instance, participants identified infrastructure providers as primarily responsible for provisioning network hardware, which is then sold to the MNO. The MNO, in turn, is primarily responsible for configuring and offering connectivity using this infrastructure. These interactions reflect both technical exchanges, such as the provisioning of the hardware, and economic exchanges, such as purchase agreements between the infrastructure provider and the MNO. The MNO is also responsible for deploying the core network and the local area network. The researcher notes this is not necessarily a localised customer-specific network, but rather the general network setup provided to the public as described in Lam et al. (2022).

In a centralised deployment where the MNO is responsible for delivering end-to-end services, participants described how the MNO acts as an intermediary, procuring various security tools, from hardware like firewalls to software such as endpoint threat detection software, from security technology vendors. These tools are then integrated at the end user's premises to provide a consolidated security service, thereby creating value for the customer, as discussed earlier. Whilst the security technology vendor retains primary responsibility for provisioning these tools, the MNO effectively takes on the role of the SECaaS provider in this deployment model. Although participants noted that it is often a legally distinct subsidiary of the MNO that delivers these services, this separation is typically driven by legal constraints or organisational strategies to distinguish security from core networking operations. However, the researcher argues that from the customer's perspective, both connectivity and security are delivered as an integrated service and should therefore be represented under a unified actor, the MNO.

> IN1: *"Mobile Network Operator 1 (MNO1) does not operate as the builder of the network, the maintainer of the network and the mobile phone provider. Those are two separate entities. MNO1 Mobile simply has a contract with MNO1, the network provider."*

> IN2: *"Our main business was staging, setting up and implementing physical hardware, so we received a firewall, we installed it, we staged it. We went physically to the customer, we put it in the rack, and that was our business [...] if you look at endpoint security, also we had to go on site or be remote, but we had to install all sorts of software on the server."*
>
> IN6: *"So I think that MNO1, being let's say a man in the middle, between the final company and the one selling you the firewall and everything, given our experience on the topic many times, we try to find opportunities to enhance those services."*

As with infrastructure providers, the MNO and security technology vendors engage in both technical and economic interactions. In a centralised deployment, the MNO is responsible for configuring and managing individual security tools into an integrated service, based on the provisioning by the security technology vendors. This forms the basis of their technical interactions. In return, security technology vendors typically enter commercial agreements through Service Level Agreements (SLAs), representing the economic exchanges in the VNC.

Furthermore, the researcher argues that the MNO also holds shared secondary responsibilities with both security technology vendors and infrastructure providers, as outlined in Chapter 4.3.6. These shared responsibilities may involve collaborative integration and maintenance of either the network hardware or the security tools provided by vendors. For example, a security technology vendor may commercially offer a physical firewall to the MNO for deployment at the user's premises, and support configuration through a custom operating system tailored to the user's specific requirements. As end users are identified primarily as consumers of these services, they maintain a technical interaction with the MNO by connecting their devices to the network and accessing the SECaaS solution. Additionally, there is a business interaction through a commercial agreement between the MNO and the end user for using the connectivity and security services. Based on these interactions, the VNC shown in Figure 4.1 maps the stakeholder interactions in a centralised 6G deployment.

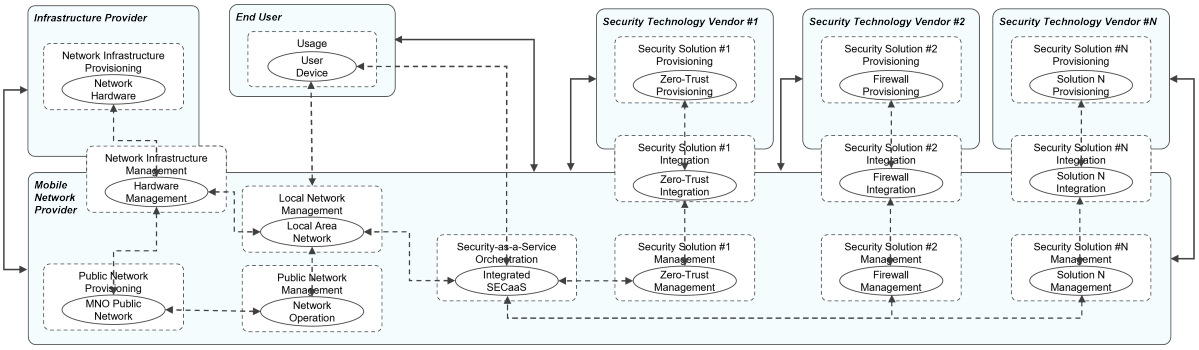

Figure 4.1: Value Network Configuration for Centralised Public Network

In a centralised public network, where the MNO assumes responsibility for end-to-end service delivery, the researcher argues that MNOs are uniquely positioned to create added value for end users by integrating tailored security solutions into their connectivity offerings. This bundling not only enhances the perceived value of the underlying network but also streamlines service management for customers. Participants particularly highlighted that large enterprises favour this one-stop-shop model, as it simplifies procurement and reduces coordination overhead. Critically, the researcher notes that this integrated approach reflects a strategic shift by MNOs to expand their role beyond traditional connectivity provision. This may explain the observed trend of MNOs investing in dedicated security subsidiaries, such as the identified MNO-based SECaaS providers or potentially acquiring established SECaaS firms, enabling them to consolidate expertise and control over the service stack while capturing a greater share of the value chain. However, this consolidation also raises questions about market competition and vendor lock-in, particularly for enterprise customers seeking flexibility in choosing security providers.

4.4.2. Value Network Configuration for Hybrid Deployment

Contrary to a centralised public network, 6G is expected to rely more heavily on Non-Public Networks (NPNs), which involve decentralised approaches to network deployment. Here, the MNO takes on the

role of deploying the network and providing connectivity services, for instance, by enabling network slicing to support a localised customer-specific network. In this type of deployment, the MNO remains responsible for configuring and deploying the network hardware, based on the provisioning of these components from the infrastructure providers. As a result, the technical and business interactions between these two stakeholders remain the same as in public networks. However, in this context, the user contracts the MNO solely for connectivity services, so the techno-economic interactions are limited to delivering connectivity and establishing the necessary commercial agreements for that service.

The researcher notes that in such a network deployment, the customer could contract a separate SECaaS provider that is not affiliated with the MNO, as identified in the interviews. This non-MNO based SECaaS provider becomes responsible for integrating various security tools provisioned by security technology vendors. Whilst the technical interactions between the security technology vendors and the SECaaS provider remain consistent with those in a centralised public network, the change in the actor responsible for configuring and managing the service results in a shift in the business interactions. In this model, the MNO maintains business interactions only with the infrastructure provider and the end user, whereas the SECaaS provider engages directly with both the security technology vendors and the end user. Moreover, since the user is still connected through the MNO's network, the SECaaS provider must also coordinate with the MNO to facilitate data exchange. This creates an additional layer of techno-economic interaction between the SECaaS provider and the MNO, ensuring the secure transmission of relevant data to and from the user. Based on these insights, the VNC for a hybrid network deployment can be constructed, reflecting the dynamics of a Non-Public Network (NPN) that still relies on the MNO's network, as illustrated in Figure 4.2.

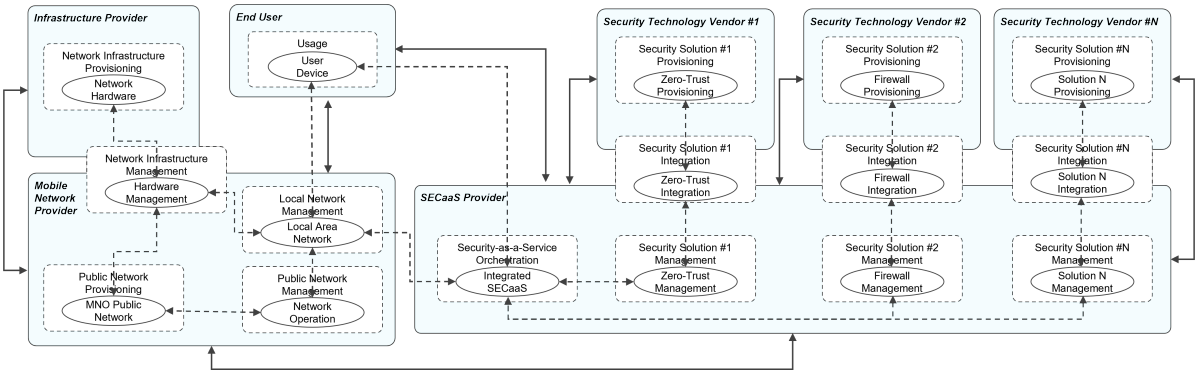

Figure 4.2: Value Network Configuration for Hybrid Non-Public Network Deployment

As the SECaaS provider offers customer-specific security solutions, the researcher argues that these solutions only need to operate within the local network, building on the findings on SECaaS deployment modes in Chapter 4.2.4. Furthermore, while this network deployment offers end users greater flexibility to choose a trusted or previously engaged SECaaS provider, it also introduces the complexity of managing multiple vendor relationships, as connectivity and security services are procured separately. Nonetheless, the researcher speculates that this hybrid approach is likely to be attractive, especially during the rollout of upgraded 6G networks, as it enables continuity of security services through trusted providers. However, this also implies that the MNO and the SECaaS provider must coordinate effectively, which may require standardisation efforts to ensure interoperability and data exchange. This becomes especially challenging in Non-Public Networks (NPNs), where participants emphasised the importance of isolating network slices by design to prevent external backdoor access. Thus, the researcher proposes that the 6G standard should include frameworks enabling secured collaboration with trusted external SECaaS providers within these otherwise isolated network environments.

4.4.3. Value Network Configuration for Decentralised Deployment

Lastly, the researcher considers the most decentralised form of network deployment, a Standalone Non-Public Network (S-NPN), which operates in complete isolation from the public network. These deployments are often designed to meet the most stringent security requirements, such as those needed for government or military communications. In this setup, a local network operator assumes primary

responsibility for provisioning, integrating, and managing the infrastructure directly for the customer, functioning independently of the MNO's public network. As a result, the role of the MNO is minimally restricted to only deploying the public network, and most of the value is created through localised collaboration between the network operator and the SECaaS provider. As with previous deployment models, the technical interactions, such as provisioning and managing the network, remain broadly consistent. However, the business interactions shift significantly, as the actors responsible for deploying the network and delivering the service change.

For example, in this network deployment, the local network provider collaborates closely with both the infrastructure provider and the SECaaS provider to configure and deploy the network, ensuring that security services reach the users. As such, these actors share business relationships primarily with the local network provider. Furthermore, unlike previous deployments where the MNO managed maintenance, here the local network operator and the infrastructure provider share secondary responsibility for maintaining the network hardware. Using these insights, the VNC for a decentralised standalone network can be seen in Figure 4.3, showing the significantly more complex stakeholder interaction.

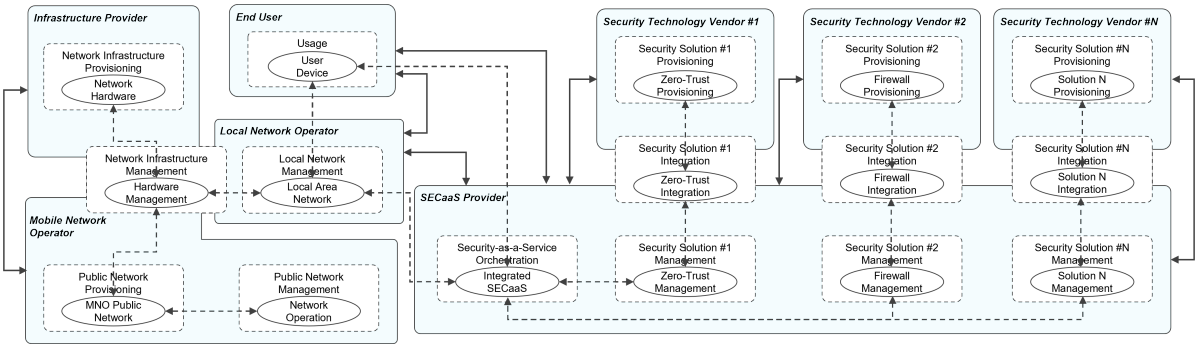

Figure 4.3: Value Network Configuration for a Decentralised Standalone Network

Whilst this network deployment offers the end user the greatest flexibility to select their network connectivity and security service providers, it also significantly increases the complexity of stakeholder management within the ecosystem. The researcher notes that such a network grants the user full control over their data and security services, as the entire network can be deployed on their own premises using local infrastructure. However, the researcher speculates that practical use cases requiring this level of control and isolation are limited, primarily because this approach is likely the most costly to implement. The need to duplicate network hardware and security tools to ensure secure local communications may restrict such deployments mainly to confidential government communication channels that can justify the associated expenses for enhanced security.

4.5. Trust Dynamics Across 6G SECaaS

Multiple participants emphasised that customer trust in a SECaaS provider is a fundamental prerequisite, often considered a baseline requirement before technical capabilities or financial terms are even evaluated. Notably, this view was not limited to SECaaS providers and security technology vendors, but was also echoed by infrastructure providers and MNOs, underscoring the widespread recognition of trust as a critical factor. The researcher notes that this emphasis likely stems from the inherently collaborative nature of the 6G ecosystem, where stakeholders do not operate in isolation. Instead, delivering integrated security services depends on close cooperation, making trust a shared concern across all parties involved. Furthermore, this insight into the significance of customer trust in a SECaaS provider aligns with the findings of Ngo-Ye et al. (2020) and Senk (2013) who identify customer trust as a key factor influencing adoption of SECaaS solutions.

> IN1: *"What can you do for me? What does it cost and stuff like that? But that's only after that trust barrier has been bested first. Do I trust you enough to even look at your software?"*

> IN4: *"In the security sphere, I think trust is really important for your providers because, if you don't trust your provider as a company, you will not trust them with your security."*

> IN5: *"Let's say you have a shortlist of two or three partners, security partners. As a customer, you say, maybe one of these three guys can do the work. You have to trust all of them first, that's like the minimum base."*

Furthermore, participants suggested that trust in a SECaaS provider facilitates deeper collaboration, which in turn reinforces and expands that trust over time. The researcher notes that many participants have already built business strategies around this dynamic, leading to what can be described as a "land and expand" approach. In this model, initial trust enables closer engagement, which not only allows providers to deliver additional services, thereby increasing revenue, but also helps customers build a stronger understanding of their own security needs. This improved literacy enables them to monitor their networks more effectively and respond to potential vulnerabilities. Moreover, this reciprocal relationship between trust and collaboration aligns with the findings of Shulga et al. (2021), who highlights the reciprocal nature of customer trust through value co-creation in service providers.

> IN4: *"If you're doing a really good job in one service and the customer is really happy and they have a big trust relationship with you, then you can also help them with a different service that you offer and then that helps both the customer because they get more security maturity and it also helps you because you get more revenue as a company."*

> IN6: *"I mean, perhaps there's also that you are already collaborating with MNO1 and other things. So it's like okay if they have access to my network, sometimes it's a bit like if they already control the this [specific] managed services for the networking, why not just also, instead of involving another company for doing endpoint detection or endpoint analysis, why don't you just go with the same?"*

> IN7: *"I believe in showing them what could be possible. And together we work on finding a solution for them, and what we do typically is what we call a "land and expand". Basically, give them a part of the solution and inevitably at some point they go yeah, but now I need to also protect my data, do we expand?"*

4.5.1. Antecedents of Trust in the SECaaS Provider

During the interviews, participants identified several factors that influence customer trust in a SECaaS provider. Based on the thematic coding, the researcher categorises these into three broad groups, as shown in Table 4.4: relational factors, organisational factors, and external factors. Relational factors include those antecedents that participants discussed, such as personal interactions, physical proximity, customer intimacy, collaboration, and contextual understanding. These elements typically emerge from direct engagement with customers at an individual level, rather than through broader firm-level. Moreover, on top of the individual-level factors, many participants highlighted the role the organisation itself plays in fostering trust, forming the basis for the second category: organisational factors. These include antecedents such as perceived reputation, firm capability, accountability, organisational size, and a proven track record of reliable service. Lastly, the third category comprises external factors, which refer to influences beyond the firm's direct control. These include geopolitical associations or national affiliations, having either regulatory or industry certifications, and the credibility derived from partnerships with reputable third-party firms.

Table 4.4: Identified Antecedents of Customer Trust in a SECaaS Provider

Category	***Antecedent***	***Description***
Relational Factors	Collaboration Efforts	Trust arising from ongoing co-creation of solutions with customers
	Personal Interactions	Trust built through direct, interpersonal contact and familiarity with customers
	Proximity and Intimacy	Trust built through geographic and contextual closeness to the customer
	Service Experience	Trust fostered through providing solutions that meet the customer's quality requirements
	Understanding Customer Context	Trust reinforced by recognising the specific customer business and requirements

Category	Antecedent	Description
Organisational Factors	Perceived Reputation	Trust influenced by how the provider's brand image in the market, often beyond actual capability
	Firm Accountability	Trust built when providers take responsibility and openly address security incidents
	Firm Capability	Trust fostered by demonstrating proven expertise and domain knowledge to customers
	Firm Size	Trust influenced by larger firms seen as more capable but potentially lacking intimacy
	History of Reliability	Trust fostered through a credible track record and long-term collaborative relationships
	Transparency	Trust built when providers openly share their technologies and processes
External Factors	Compliance and Certifications	Trust established by meeting recognised security standards and regulatory requirements
	Third-Party Credibility	Trust enhanced through associations with credible external partners and reputable customers
	Geopolitical Influence	Trust influenced by the provider's national origin and perceived associations

4.5.1.1. Relational Factors

A recurring theme across the interviews was the importance of proximity to the end user. Multiple participants described the security services market as a "people business," emphasising that trust is often built through direct personal relationships and contextual understanding. Although this form of trust may be difficult to define or measure, it plays a critical role in shaping how security services are delivered and perceived. Notably, many participants also highlighted that collaborating and partnering with end users helped foster deeper trust. This insight aligns with the findings of Marcelo Royo-Vela and Ferrer (2024), who argue that co-creation with customers strengthens trust by reinforcing mutual engagement and shared value.

> IN2: *"One thing that our customers in general very much like is that you proactively think along and that you are like a partner to them [...] making sure that they trust you almost on a personal level [...] In Belgium, proximity and personal contact are very important in this context, much more than it is in the Netherlands. "*

> IN3: *"So it's still about, it's a lot about people. And yeah, you can put a new name over it, but because we're quite a small industry, it's still actually a lot about people. And that trust feeling, which is reasonably not super easy to quantify, still has quite some value"*

> IN7: *"When I went into a customer space, I listened to their story. I love to do whiteboards with them, and then I say to them, just imagine we had the end goal and it looked like this, would that be amazing, or would that be interesting if they saw the end goal?"*

Furthermore, participants emphasised that trust is strongly shaped by the customer's experience with the service, particularly in how the provider responds to security incidents. While effective security may go unnoticed, any visible failures or poorly managed incidents can significantly erode trust. Trust is also reinforced when providers demonstrate a clear understanding of the customer's specific context, including their industry, operational environment, and business needs. The researcher suggests that such contextual understanding is particularly relevant for SECaaS providers in 6G use cases, where priorities may vary across industries, for instance, the manufacturing sector may emphasise business continuity, whereas the financial sector could focus on the protection of sensitive customer data.

> IN2: *"When it comes to trust, you have to show that you understand the business that customers are in. That you know what is important to them [...] we know what you are, what's important to you. We know what direction you're heading in and based on your context, we advise you to. So basically it's all about contextualization."*

> IN4: *"So it's if a customer loses trust in their partner, it's because something bad has happened. Most of the time, like either customer service or a product failure."*

IN7: *"I need to understand and also respect the fact that they come from 30 years of traditional networking. What I have to be very careful of is not to paint a doomsday scenario for them to use to get into your cells. We all have problems [...] first of all, it's a customer with a problem."*

4.5.1.2. Organisational Factors

Beyond trust developed through relational interactions, participants reported that the perceived reputation or brand image of a security provider plays a significant role in shaping customer trust. They emphasised that, in addition to the technical capability and accountability demonstrated by a SECaaS provider when responding to threats, the way the brand is perceived in the market can strongly influence a customer's willingness to trust them. Whilst the participants did not express this, the researcher suggests that there may be interrelationships between perceived reputation and other factors such as capability and accountability. For example, consistently taking proactive responsibility during security incidents could enhance a provider's reputation and, in turn, foster greater customer trust.

IN3:*"Yeah. I mean reputation, right? [...] But perception is important, so no matter what the actual security improvement is, the perception of security in a commercial business will actually help or destroy your value proposition here."*

IN5: *"That gives a good image that you are responsible. You take your own accountability for what happened, and you did something with it. And to me, that's really important to keep your trust or even increase the trust that your company and your customers have in you."*

IN6:*"Rather you trust MNO1 because MNO1 has a reputation [..] I mean, you're really accountable. I mean, you know that you cannot do it wrongly because you have a huge business, and you know that one case that goes wrong could destroy your reputation [...] Yeah, reputation, previous collaborations. All this can help build our trust."*

IN9:*"And when you are a customer of MNO1, for instance, it's a big brand because you know that they have a workforce going after your problem. And you are if you are looking into the details as a customer, then you are looking at statistics of consumer organisations, how their service is being awarded and what kind of problems such customers have, et cetera, and that gives the trust."*

Participants also discussed firm size as a factor influencing customer trust, though with contrasting views. Some suggested that larger companies may inspire greater trust due to their stronger brand reputation, often supported by certifications and partnerships, and their broader industry experience, which can signal higher capability. Conversely, others argued that larger firms may suffer from increased bureaucracy, lack of transparency and reduced customer intimacy, potentially undermining trust. The researcher finds this contrast particularly insightful, as it not only suggests that trust antecedents can interact and influence one another but also highlights how firms might adapt structurally to balance these tensions. For instance, large multinational companies could adopt more flexible or decentralised service models to maintain a strong local presence and customer proximity, thereby preserving trust through intimacy and responsiveness.

IN1:*"People have an inherent distrust of large corporations. I don't know why. It's a simple matter of fact, I don't trust MNO2. I don't trust MNO3. I don't trust them because they're grey boxes [...] So saying you are MNO2 used to mean that you can trust us and stuff like that. By now saying you are MNO2 means you are way too expensive and are not trustworthy any more."*

IN5:*"And that's why in many cases you go to MNO1, you go to MNO2, you go to any of these big players because you can technically trust them rather than contracting something with a smaller player."*

IN6:*"MNO1 is well organised, you know that perhaps MNO1 also has some certifications that others cannot achieve because of how big they are."*

IN8: *"Well, the problem with Security Technology Vendor 2 (STV2) and those types of [large] companies is that they're not very transparent, so you actually don't know what the software is doing. So this can be a problem for some companies or some users [...] because some*

> *customers, for instance, like Infrastructure Provider 1 (IP1), they're very keen on knowing what the third-party provider is doing [...] trust can be provided by making things more transparent."*

Another key theme highlighted by participants was the importance of a service provider's history of delivering reliable services. A credible track record was seen as a strong contributor to building customer trust. Participants emphasised that the duration of collaboration plays a crucial role in this regard, with long-term relationships fostering deeper trust over time. Such enduring partnerships not only strengthen confidence in the provider but also enable them to develop domain-specific expertise. The researcher further speculates that these long-standing relationships may enhance the provider's technical capability and positively influence their perceived reputation in the market.

> IN1:*"One, of course, is a track record. People distrust something, especially on a security level, if you have been hacked, because why would they trust you? You can't even protect your own, right?"*

> IN3: *"The Dutch Ministry of Defence is a long-time serving customer of our company. I don't know exactly how long, I think more than 15 years, maybe even more than 20 years, they've been a customer year on year. When they have a complaint, we answer, and it's not that we leave the phone ringing because there is a long relation."*

> IN7:*"What we have done as a business very successfully is, we figure out what's the best way to migrate a customer from today to tomorrow. OK, so we have a very good plan for that. I believe that is the magic. That's the secret sauce. That's the magic we bring to the table. It's not our technology, but what we've learned in the last 15 to 20 years."*

The researcher notes that the identified organisational factors partially align with existing literature on the antecedents of customer trust in a SECaaS provider. For example, in their model, Ngo-Ye et al. (2020) identify familiarity with the service provider, provider reputation, and service quality as key antecedents of trust. However, their conceptualisation does not account for factors such as firm size, historical reliability, or the potentially growing importance of transparency, all of which were highlighted by participants as crucial in fostering trust in a SECaaS provider.

4.5.1.3. External Factors

Many participants reported that holding certifications for regulatory compliance was a crucial baseline for fostering customer trust. In addition to certifications, another theme was associations with external partners whose credibility would contribute to the service providers' trust. This could either be by being associated with a credible partner or by providing services to customers who expect stringent processes when it comes to security, for instance, government customers. The researcher notes that these certifications are often region-specific and subject to continuous revision in response to evolving threats, requiring multinational SECaaS providers to regularly adapt their services to remain compliant. Nonetheless, compliance with such regulations helps ensure a minimum standard of security, which in turn reassures customers that the provider adheres to recognised rules and best practices.

> IN3:*"So for example, we got very close to Technology Company 1 (TC1) with one of the aspects saying hey, a TC1 end-to-end secure means more than our brand of secure. So that was definitely the viewpoint."*

> IN4:*"But with the whole NIS2, with DORA, there are a lot of regulations coming up this year, and all those are raising the minimum standard of security. So it is a good thing in general"*

> IN5:*"If I'm already providing services to, for instance, the Ministry of Defence or whatever. I mean that shows. You have built some trust in the market already."*

> IN10: *"Then of course, as operators, we will be in the position to manage it [security technologies] and achieve a high level of certification [...] If we discuss with EUCS the new cloud certification scheme. It corresponds to the sovereignty level, High+, in which some customers may be looking for the partner you use and the technology you will use. Then, based on this scheme, for the high trust level."*

An important external factor consistently highlighted by participants as influencing customer trust is the geopolitical context in which a security provider operates. Several participants noted that associations with certain countries can significantly affect perceived trustworthiness, regardless of the provider's actual technical capabilities or service performance. These concerns often stem from fears of surveillance, hidden backdoors, or broader national security agendas. The researcher observes that such perceptions lie entirely outside the control of the SECaaS provider; merely operating in a geography considered politically sensitive may negatively influence customer trust.

> IN1:*"The other thing is currently nationality, unfortunately, starts playing a role as well. So people distrust Security Service Provider 3 (SSP3). SSP3 is an anti-malware provider that has Russian ties. Does that mean that their software is wrong? No. Do people trust it? Absolutely not."*
>
> IN3: *"What's happening geopolitically, that for example in telecom hardware in the West, they're not accepting any Chinese manufacturers. So, because of the thought that there could be a loophole for eavesdropping or whatever, cars in the US are not allowed to be sold with Chinese chipsets. For example, car OEMs are having a China strategy and a non-China strategy because of the geopolitics."*
>
> IN5:*"In Europe, for instance, you could not go and say I'm using a Chinese provider for security services. Even if you are the best in the market, you know that your team is the best and qualified people. People will not trust you. The customer will be like, yeah, thank you, but you can't. I'm not going to let you use that technology because of political reasons"*
>
> IN10: *"Some of our customers in France for instance request us in 5G and 6G that we demonstrate that there is no Chinese company contributing to the production line"*

Despite its relevance, particularly in light of recent developments in the 5G RAN domain, where certain firms were banned from supplying components in Europe (Zhang, 2024), this antecedent remains largely unexamined in existing literature on trust in SECaaS providers. Whilst it may be argued that little can be done when a provider is perceived as geopolitically untrustworthy, the researcher speculates that future 6G standards could incorporate frameworks allowing customers to independently assess a SECaaS provider's trustworthiness, regardless of their geographic origin. In the meantime, this uncertainty implies that SECaaS providers must adapt their business strategies based on the regulatory and political sensitivities of the customer's country, something one participant noted is already happening within the automotive sector.

4.5.2. Variation in Antecedents of Customer Trust

When discussing how decentralisation influences the antecedents of customer trust, many participants observed that end users and enterprise customers typically lack deep knowledge of network technologies and architectures, whether centralised or decentralised. As a result, trust in SECaaS providers was seen to depend less on the deployment model itself. One participant illustrated this disconnect by noting that users are often unaware of how network routing works, pointing out that even a simple video call might see data travel halfway around the world before reaching its destination.

> IN5: *"There are many other companies, smaller companies or medium-sized companies they don't have the expertise, they don't have the knowledge, they don't have resources maybe, and for these companies is more difficult, even if they want, it is more difficult to understand all the threats, all the risks associated to the security."*
>
> IN6: *"I think it always depends on the understanding of the final customer, who is your final customer? Is it really someone who understands technology? What are we assuming? Most people don't understand the implications of this."*
>
> IN8: *"The more technical users will have a different view of trust and less technical ones [...] Depends on the customer and like I said, the more technical the customers with more technical knowledge might be more interested in what exactly the AI is being used for and less technical customers will not be interested or will not be aware."*

4.5.2.1. No Direct Influence of Decentralisation on Trust

The researcher notes that, as participants argued, network decentralisation does not directly influence the identified antecedents of customer trust in a SECaaS provider. Instead, the researcher speculates that participants viewed trust as being primarily shaped by organisational factors, such as perceived brand reputation. Although decentralisation may redistribute security responsibilities across the network, participants emphasised that customers continue to expect consistent and reliable security services in 6G, regardless of how the network is structured. One participant observed that while centralised networks may introduce a single point of failure, they are not necessarily a better option, just as decentralised networks are not without their own limitations. This suggests that neither approach offers a perfect solution when it comes to security.

Furthermore, participants explained that although technology evolves to respond to new threats, such changes do not fundamentally reshape how trust is formed. Therefore, the researcher suggests that as decentralised networks develop, new local connectivity and security service providers may emerge with expertise in such environments. However, trust in these providers will likely continue to depend on familiar factors, including perceived capability, brand reputation, and a strong record of reliable service, rather than on their use of decentralised infrastructure.

> IN1: *"It has more to do so the network becoming decentralised means that, for instance, my car becomes the 6G tower for that neighbourhood or something like that. So they have capability broadcast and receive at the same time. At that point, I would expect the car manufacturer to have that properly taken care of, right? If you look at zero trust and zero trust network access and stuff like that, I expect the provider to take care of that."*

> IN5:*"But I don't expect like a change of how things are or the expectations people could have regarding how to make things secure in the cloud, but also at the edge. What I would expect is that technology will evolve. There will be new risks, and there will be new potential challenges, whatever they are, the technology will also evolve and that will be the change. But I don't think that from a mentality standpoint like this is important or this is not important. I think that's not happening any more"*

> IN6: *"I mean, if you trust MNO1, you would probably trust them regardless of whether they do it more centralised or more decentralised, right? [...] There's no perfect solution. I mean what is better in terms of security, centralised or decentralised? [...] So if you compromise a switch in a centralised way perhaps it's harder to compromise the centralised point, but if you compromise it, you compromise it entirely. Which would you prefer?"*

> IN9: *"Why would decentralisation make a difference? [...] Well security as a service is what you are talking about, I would say it is a difficult use case because what I described before is that customers are not security aware, so they are not willing to invest in security."*

4.5.2.2. Potential Indirect Influence of Decentralisation on Trust

Whilst the researcher acknowledges the view that decentralisation may not directly influence the antecedents of trust, some participants suggested that it could still shape certain factors that contribute to customer trust. For example, the emergence of localised SECaaS providers in decentralised networks may elevate the importance of relational trust. Participants noted that large multinational firms might need to adapt their products and services, as the trust built around their centralised models may not carry over in these new environments. In contrast, localised providers may gain trust by working more closely with end users, demonstrating an understanding of their specific business contexts, and fostering stronger personal relationships. These factors could allow local actors to build and sustain trust more effectively than larger, less agile firms operating from a centralised position.

> IN2: *"Indeed the risk is that most of the securities provided by these over the top players like Technology Provider 1 (TP1) and that your added value is less visible and that at some point they say why do we still need MNO1? It's working perfectly without a partner."*

> IN4: *"I think it will change a lot because of course, all these big parties, they are now offering this big, centralised way of managing security and it will need to change [...] But yeah, if it changes a lot, if it's a whole, completely different new product that they have to sell then their trust doesn't necessarily mean much."*

> IN5: *"But obviously there are always maybe a smaller customers or specific customers and they prefer to work with someone local and there is always room for smaller providers, local providers doing something very specific."*

Another potential indirect influence of network decentralisation identified by participants was the possibility for customers to gain greater control over their data and operations. For instance, one participant described how storing data on the customer's premises enables better protection, as it ensures the data remains within the customer's control. This approach was already being adopted by a SECaaS provider today. Such practices could enhance the overall service experience, helping localised providers build stronger relational trust with their customers. Moreover, another participant highlighted a recent product launch that allows government users to manage and control the network independently, without oversight from the infrastructure provider. This shift of security control back to the customer is especially valuable in high-security contexts, such as confidential government use cases, and was framed as a key selling point. The researcher speculates that similarly, SECaaS providers could explore easy to use services that offer customers greater control over security functions, which may further strengthen trust through improved service experience and perceived quality.

> IN3: *"It's a very successful product because we allow, on the one hand, yeah, it's this kind of we give them control because we allow them to kind of play with the payload, so to say. So we reserve power and frequencies for them [...] But this decentralised feature of that product makes it how to say it, secure in their hands."*

> IN4: *"The data, so the logs themselves stay at the customer site so then the customer has full responsibility of their own data and then we just get access to it. We read it, we apply our intelligence, and we trigger alarms based on this. So in this aspect like the data itself is at the customer's environment and they are responsible for it."*

> IN8: *"Oh, it can be a marketing idea to tell the customer that we don't, we don't get your private data because it's located in your own system. So that will make them more confident than he can trust the operator."*

5

Conclusion

Having conducted the interviews, analysed the data, and discussed the findings, this section presents the conclusion of the thesis. It begins by addressing the main research question and answering the sub-research questions, outlining the academic and practical contributions, such as those made to the Ensure-6G project, in Section 5.1. This is followed by the study's limitations in Section 5.2, and recommendations and suggestions for future research in Section 5.3. Finally, Section 5.4 reflects on the alignment between this thesis and the Management of Technology programme.

5.1. Research Summary

In this section, the main research question is answered, for which the subsequent sub-questions need to be answered based on the data analysis discussion. Furthermore, based on these, this section also addresses the academic and practical contributions, especially the contributions to the Ensure-6G project by discussing potential SECaaS business models.

5.1.1. Answering the Research Question

This study aimed to explore the techno-economic interactions between stakeholders and the trust dynamics associated with Security-as-a-Service (SECaaS) solutions across varying 6G network deployments. In line with this objective, the main research question guiding this study was:

"How does network decentralisation in 6G deployments influence techno-economic interactions and customer trust in SECaaS providers?"

To answer the main research question, four sub-research questions were formulated, which are addressed separately, thereby providing an answer to the main research question.

Sub-Research Question 1

What constitutes SECaaS in the context of 6G networks?

As SECaaS has primarily been conceptualised within the domain of cloud computing, its application in mobile communication environments, particularly in decentralised 6G networks, requires adaptation to ensure its relevance and effectiveness. Based on the interviews conducted in this study, SECaaS in 6G refers to a business model in which an external firm is contracted to provide security services on top of existing connectivity services, often encompassing a range of functionalities tailored to the customer's needs. These functionalities can be categorised into three groups, depending on the stage of threat response: protective, detective and reactive. Protective features aim to prevent attacks through tools like encryption, firewalls, and access management. Detective functionalities, such as system monitoring and Managed Detection and Response (MDR), allow for the identification of anomalies during an attack. Reactive features enable organisations to mitigate and recover from incidents through incident response and backup systems.

Furthermore, while different deployment modes for security solutions are possible, the researcher pro-

poses that these services will likely operate in a hybrid configuration spanning both the edge (or user device) and core network (or cloud) layers. For instance, firewalls and unauthorised access controls are expected to be deployed closer to the user, enabling rapid local response and enforcement. Conversely, functions such as network monitoring and MDR are better suited for centralised execution in the core or cloud, where broader network visibility and processing capabilities are available. This hybrid approach allows for appropriate security solutions to be implemented at the right place in 6G networks, balancing local customisation with central oversight to ensure comprehensive and adaptable security.

Thus, answering the sub-research question, SECaaS in the context of 6G networks comprises a set of protective, detective, and reactive security services tailored to enterprise needs and delivered by an external provider on top of the connectivity services. These services follow a hybrid deployment model, strategically distributed across edge and core network layers.

Sub-Research Question 2

Who are the key stakeholders involved in deploying SECaaS solutions in 6G networks?

Having established an understanding of SECaaS within the 6G networks, this study identifies the key stakeholders involved in deploying these solutions. Figure 5.1 illustrates these stakeholders, grouped into four categories: infrastructure providers, responsible for delivering the physical and digital components of the network; telecommunications providers, who configure this infrastructure to establish the network and ensure connectivity; security providers, tasked with developing and implementing security solutions across the network; and target customers, the end users who consume both the network connectivity and security services.

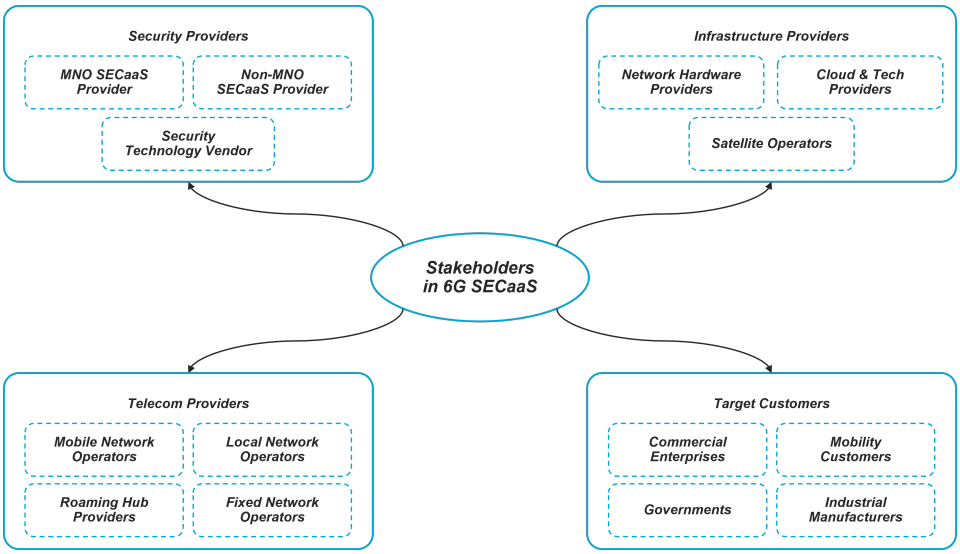

Figure 5.1: Stakeholders in deploying SECaaS in 6G

Infrastructure providers are responsible for delivering the physical and digital components of the network, including hardware, transmission infrastructure and cloud-based platforms. In the context of 6G, this category expands beyond traditional network hardware vendors to include satellite operators and cloud and technology providers, reflecting the increasing convergence of Terrestrial Network (TN) and Non Terrestrial Network (NTN). These emerging actors play a foundational role in enabling global, flexible connectivity, particularly as Software Defined Network (SDN), Network Function Virtualisation (NFV), and network slicing reshape how networks are built and operated. Telecommunications providers, most notably the Mobile Network Operator (MNO), build on this infrastructure by configuring and operating the network to ensure connectivity services are delivered. Their responsibilities include managing access and core network functions, as well as potentially bundling additional services into their offerings.

Security providers are divided into two distinct but interdependent groups. First, security technology vendors develop the tools and frameworks necessary for safeguarding the network, such as firewalls,

threat detection software and zero-trust architecture components. Second, SECaaS providers integrate these technologies into managed service offerings tailored to the needs of individual customers. These providers may be affiliated with MNOs or operate independently, and are increasingly responsible for deploying and managing security capabilities either remotely or at the customer premises. Lastly, target customers, such as enterprises, critical infrastructure operators, or local governments, are consumers of these services. They define the requirements for performance, flexibility and compliance that shape how network and security services are deployed and managed.

In summary, the deployment of SECaaS in 6G involves a diverse set of stakeholders, each with clearly defined technical responsibilities. These stakeholders operate across infrastructure, telecommunications and security domains, including both established and emerging actors. Their collaboration is essential to ensure the successful delivery of secure and reliable communication services in future 6G networks.

Sub-Research Question 3

How does network decentralisation influence techno-economic interactions between SECaaS stakeholders in 6G deployments?

The Value Network Configuration (VNC) analysis reveals that techno-economic interactions in 6G networks differ depending on the degree of centralisation. In centralised public networks, the MNO acts as the dominant stakeholder, delivering both connectivity and bundled security services under a single contract. This creates a tightly integrated value structure with minimal stakeholder complexity, reduced transaction costs, and centralised technical and economic control. The customer engages primarily with the MNO, who assumes end-to-end responsibility for service quality, infrastructure, and security provisioning.

In more decentralised settings, these responsibilities are distributed across multiple actors. In a hybrid deployment such as Non-Public Networks (NPNs) utilising network slicing, the MNO still manages the network infrastructure, but security services are delivered by a separate SECaaS provider, requiring shared governance and increased coordination. In fully decentralised Standalone Non-Public Networks (S-NPNs), the end user independently engages both network and security providers, fragmenting technical and financial interactions. Although this model offers high customisability and control, it introduces greater complexity in managing stakeholder incentives, service quality and trust relationships across decentralised interfaces.

Thus, in summary, network decentralisation reshapes techno-economic interactions by distributing roles and responsibilities across multiple independent stakeholders, increasing coordination complexity but allowing for greater customisability. As 6G networks shift away from centralised MNO-led deployments, SECaaS providers must adapt to operate within fragmented ecosystems that demand increased collaboration with the ecosystem stakeholders.

Sub-Research Question 4

How does network decentralisation influence the antecedents of customer trust in SECaaS providers?

Network decentralisation in 6G deployments does not fundamentally alter the identified antecedents of customer trust, which remain broadly categorised as relational, organisational and external. However, decentralisation can indirectly shape the conditions under which these factors influence customer trust. In particular, it enables greater localisation, user control and service transparency, factors that strengthen relational trust. Within decentralised deployments, SECaaS providers are better positioned to engage directly with end users, tailor services to specific business needs and establish closer proximity and intimacy. These dynamics enhance trust-building mechanisms grounded in interpersonal relationships and contextual understanding. By contrast, centralised models tend to reinforce organisational antecedents, such as brand reputation, perceived capability and a track record of reliable service, which are often supported by firm size and established governance frameworks.

Firm size, however, emerged as a nuanced factor. While larger providers may foster trust through their extensive experience and perceived competence, they may also be seen as rigid or impersonal, lacking the flexibility and closeness often attributed to smaller local providers operating in decentralised environments. External antecedents, such as regulatory certifications or geopolitical associations, remain

largely unexplored in the SECaaS context but appear unaffected by network architecture, as they are shaped by broader legal and political factors. In summary, network decentralisation does not directly redefine the antecedents of customer trust in SECaaS providers. Instead, it influences the environment in which trust is developed, particularly by reinforcing relational antecedents through increased localisation, contextual responsiveness and direct user engagement. These evolving dynamics highlight the need for SECaaS providers to adapt their trust-building strategies to different deployment contexts while maintaining a consistent baseline of service quality and accountability.

5.1.2. Academic and Managerial Relevance

This thesis offers both academic and practical contributions to the study of SECaaS within the context of 6G network ecosystems. From an academic perspective, it advances the conceptual understanding of the SECaaS model in mobile communication networks by framing it as a set of externally sourced protective, detective, and reactive security solutions delivered through a hybrid deployment model, with certain functions operating at the edge and others at the central plane of the network. This distinction reflects the evolving architecture of 6G and provides a foundation for further exploration of how SECaaS can be integrated into future mobile network infrastructures. Moreover, by identifying emerging and previously unexplored functionalities, such as the ongoing maintenance of security tools and the potential adoption of quantum encryption as a security service, this research expands the understanding of how 6G networks may reshape the SECaaS model.

Additionally, the study identifies two major stakeholder groups in the 6G security domain and proposes their respective responsibilities. Security technology vendors are primarily responsible for developing and provisioning security tools, whereas SECaaS providers act as the customer-facing entities that integrate these tools into cohesive, tailored security services. The findings suggest that SECaaS providers play a key role in co-creating value within the network ecosystem by enhancing the managed service experience and adapting solutions to meet specific end-user needs.

Furthermore, by applying the VNC methodology across different 6G network deployments, the study maps the techno-economic interactions between key stakeholders. In centralised public networks, MNOs often also assume the role of SECaaS providers, delivering integrated bundles of connectivity and security services to customers. In contrast, decentralised 6G networks lead to more fragmented and distributed value creation, identifying the emergence of localised network operators and SECaaS providers, highlighting the increased need for effective coordination and management among multiple independent stakeholders.

Additionally, this study advances the existing literature on the antecedents of customer trust in SECaaS providers by identifying previously unexplored factors, such as geopolitical influences and the role of regulatory certifications. Furthermore, by examining how network decentralisation interacts with these antecedents, the research suggests that decentralisation does not directly affect trust factors rooted in organisational or external domains. However, it may indirectly shape relational trust by fostering greater customer intimacy, proximity, and contextual understanding. This is particularly relevant as decentralised networks create opportunities for smaller, local SECaaS providers to tailor their services more effectively to individual customer needs.

From a managerial perspective, this study aids in identifying the key stakeholders involved in SECaaS solutions within mobile communications. For prospective firms seeking to adopt the SECaaS business model, it enables the mapping and categorisation of stakeholders using a power–interest matrix tailored to specific network deployments. By clarifying how SECaaS providers create value within the network, through offering a managed service rather than a security product, the findings guide security firms in identifying opportunities to enhance their service offerings. This strategic insight also supports informed partnership decisions, such as mergers or acquisitions, for example, an MNO acquiring or partnering with a local SECaaS provider to consolidate and maximise value creation.

Finally, by identifying the antecedents of customer trust, this study provides practical guidance for managers of SECaaS firms, particularly small and local providers, on how to build and maintain trust in emerging 6G environments by leveraging relational factors such as proximity, customer intimacy, and contextual awareness. For managers of large multinational SECaaS firms, the findings highlight the importance of adapting novel organisational structures to preserve brand reputation whilst fostering

stronger customer engagement. Balancing operational scale with responsiveness may be essential for sustaining trust in decentralised and dynamic 6G ecosystems. Moreover, regardless of firm size, the study underscores the importance of holding relevant regulatory certifications and compliance credentials, as these not only assure a minimum standard of security but also instil customer confidence and strengthen trust in the SECaaS provider.

5.1.3. Contributions to 6G SECaaS Business Model through Ensure-6G

Ensure-6G is a multidisciplinary European-funded project involving academic and industry partners, with the overarching aim of developing resilient 6G telecommunication infrastructure. The primary objective is to design, implement, validate and prototype novel security and privacy solutions that enable prevention, detection, response, and mitigation against both physical and cyber-attacks in 6G networks (Ensure-6G, 2024). TU Delft leads Work Package 4, which focuses on developing and evaluating a business model framework to understand the relationship between trust and business models in the context of data security in 6G. A key deliverable of this work package is to integrate dimensions of centralisation and trust into this framework, supporting firms in identifying economically viable ways to offer SECaaS solutions in the evolving 6G ecosystem.

Given that the 6G landscape is still evolving, with emerging use cases, shifting stakeholder roles, and the formation of new ecosystems, this thesis contributes to the Ensure-6G initiative by offering a foundational understanding of what SECaaS may entail within future mobile networks. As highlighted through the interviews, traditional mobile networks often approached security as an add-on. However, beginning with 5G and becoming more pronounced in 6G, there is a clear shift towards security-by-default or security-by-design principles to address increasingly complex and distributed threat environments, particularly with the rise of AI-driven attack vectors. This security-first approach requires not only a rethinking of how network infrastructure is configured and deployed but also how complementary security tools and services are offered and integrated to ensure an end-to-end secure network architecture.

Specifically, this study identifies relevant SECaaS functionalities and deployment modes, maps key and emerging stakeholders, proposes primary and shared responsibilities, and explores how value is co-created in the ecosystem through stakeholder interactions. In doing so, this study contributes to conceptualising the configuration of SECaaS offerings within a dynamic, multi-actor environment of 6G networks. As business models are defined by how value is created, captured, and delivered, the findings highlight that, while value creation in current 5G networks remains concentrated around the telecommunications provider, SECaaS providers in 6G can co-create value by integrating diverse security tools into a managed service tailored to enterprise needs. This positioning enables SECaaS firms to play a strategic role within the broader ecosystem to ensure security requirements are met for the customer.

With 6G expected to increasingly adopt decentralised architectures, such as Non-Public Networks (NPNs), the study speculates that SECaaS providers could establish a differentiated business model by supporting customers during the transition from centralised to decentralised network environments. In doing so, they could offer services that help adapt and integrate existing 5G-based security tools to function within decentralised 6G deployments. This shift may also allow SECaaS firms to operate independently of traditional MNOs, enabling new market opportunities and positioning them as key enablers of secure and flexible network configurations in the emerging 6G era.

Lastly, customer trust is recognised as a pivotal factor in the adoption and success of the SECaaS business model. This thesis identifies emerging antecedents of trust in SECaaS providers, including geopolitical influences and the presence of regulatory certifications. By examining how these trust factors vary across different decentralised network deployments, the study suggests that decentralisation indirectly strengthens relational trust through improved contextual understanding, proximity, and customer intimacy. By integrating the VNC perspective with trust dynamics, this research provides novel insights into how SECaaS providers can adapt their business models to align with the decentralising nature of future 6G network architectures.

5.2. Limitations of the Study

A key limitation of this study lies in the disconnect between academic projections of 6G and the current pace of industry adoption. Several participants highlighted that 5G systems are still in the process of being rolled out, with some operators deploying 5G only at the RAN level, while core networks continue to rely on older generations. This raised concerns about the relevance and timing of 6G discussions, as the full realisation of 5G is expected to take years and remain in operation for decades, illustrated by the fact that MNOs are expected to phase out 2G networks, introduced in the early 1990s (3GPP, 2025), by the end of the decade (GSMA, 2024b). As a result, some participants viewed 6G as a distant and uncertain prospect, limiting their engagement with the topic and affecting the depth of insights provided.

This limitation is particularly significant as it meant that participants often speculated about what SECaaS might look like in future 6G deployments and use cases, rather than drawing on concrete or current experiences. This speculative nature is further compounded by the ongoing evolution of 5G networks themselves. For instance, 3GPP is still finalising components of 5G in Release 19, expected by the end of 2025 (3GPP, 2023). As a result, while interviewees referred to 6G scenarios, many of their observations may, in fact, reflect expectations or plans related to advanced 5G capabilities. One participant, for example, noted that their organisation had not yet commercially launched network slicing but expected to do so only by 2026. This raises the possibility that discussions about future security services, such as security of these slices, were unintentionally centred on unrealised 5G features rather than distinct 6G innovations. While the researcher acknowledges this overlap, these insights may nonetheless provide a useful indication of how SECaaS capabilities and needs could evolve and transition into 6G environments. However, the extent to which current expectations can be directly carried forward into 6G may require further research.

Furthermore, the study's techno-economic approach revealed a fragmented understanding across participants. Those with academic or technical expertise in 6G development often lacked business insight into how service models like SECaaS would be deployed in practice. Conversely, customer-facing professionals in MNOs, SECaaS providers or security vendors typically possessed commercial and operational knowledge but lacked awareness of 6G's technical potential. This division made it difficult for any single participant to offer a complete view across both technological and economic dimensions.

Moreover, many industry participants possessed deep expertise in specific domains, such as mobile roaming, satellite connectivity, or SaaS-based security solutions, which limited their ability to consider the broader ecosystem transformations envisioned in academia. Some even questioned the need for 6G, perceiving it as a marginal performance enhancement (e.g., higher speeds or lower latency) rather than a foundation for new value propositions. This scepticism reduced the perceived relevance of developing new SECaaS models, potentially underestimating the strategic implications of future network architectures. Their responses were therefore shaped by domain-specific knowledge and often speculative expectations of what 6G might entail.

Additionally, since the 6G standard is still under development, key concepts such as SECaaS and decentralisation may have been interpreted differently by participants, leading to varied descriptions of similar use cases. Although interviewer prompting was intentionally limited to encourage natural responses, this contributed to inconsistencies in how certain themes were articulated across interviews. Moreover, while this study primarily views the end user as the recipient of connectivity and security services, it is possible that, in future deployments, end users may take on a more active role in managing these services through shared responsibility models, a dimension that was not fully explored. These limitations are acknowledged within the context of the study's exploratory nature, which was necessary given the evolving state of 6G technologies and standards.

5.3. Recommendations and Future Research

Based on this study's findings, firms aiming to deliver SECaaS in 6G environments should prioritise flexibility in their business models to accommodate both centralised and decentralised networks. As decentralisation reshapes control over infrastructure and data, SECaaS providers will need to define their roles and responsibilities within more collaborative ecosystems clearly. Developing modular service frameworks and establishing transparent SLAs are crucial for building trust and ensuring value co-creation with stakeholders such as mobile network operators, infrastructure providers and end users.

Secondly, as highlighted in the interviews, the antecedents of customer trust in SECaaS providers may be interrelated. For instance, a firm's willingness to take accountability could influence how its brand reputation is perceived. Future research could explore these interrelationships more deeply to better understand how different antecedents reinforce one another. Additionally, quantitative studies are recommended to statistically validate the relative importance of the three categories of trust antecedents in shaping customer trust. Collaborating with industry partners could further support the development of standardised, trust-enabling frameworks necessary to scale SECaaS offerings across diverse 6G deployments. This is particularly relevant as networks become more fragmented, such as in cases where an external SECaaS provider must operate within an MNO-led NPN environment.

Future research should examine the longitudinal development of trust in SECaaS relationships over time, particularly in contexts where the boundaries between infrastructure ownership and service delivery are increasingly blurred. Additionally, further explorative studies are needed to compare stakeholder configurations and requirements across vertical industries (e.g. healthcare, mobility, or manufacturing) to understand how sector-specific security and privacy demands shape techno-economic interactions. Moreover, by adopting a design science research approach, scholars can support the development of a business model tool tailored to the unique characteristics of 6G networks. This tool could incorporate dimensions such as network decentralisation and customer trust to potentially empirically evaluate their influence on the viability and scalability of SECaaS offerings.

As the race to define and commercialise 6G accelerates, there is a growing risk of repeating the missteps observed during previous generational shifts. Notably, the 5G standard itself is still evolving and has yet to achieve its full potential in terms of widespread deployment, industrial adoption, and realisation of its more advanced capabilities. Yet, the push toward 6G threatens to overshadow these ongoing developments, diverting attention and resources from fully capitalising on existing infrastructure. Similar to how EDGE was introduced before GSM reached full maturity (Ansari & Garud, 2009), prematurely promoting 6G capabilities without technological readiness could undermine trust in the ecosystem and create unrealistic expectations, especially in security-related services like SECaaS.

Given the current uncertainty in 6G networks from participants, it is possible that over-promising and contributing to the hype on dystopian decentralised architectures, AI-native networks, or ultra-high performance may lead to industry fatigue, misaligned investments and regulatory backlash. To mitigate these risks, academic and industry stakeholders must adopt a more transparent and measured communication strategy that reflects realistic expectations. Additionally, embedding 6G development in iterative, cross-sector pilot initiatives that test security and trust mechanisms in real-world conditions can help ensure that new standards are grounded in practical and economically viable outcomes.

Finally, based on the interviews, the research finds that network decentralisation does not have a major direct influence on the antecedents of customer trust in a SECaaS provider. Instead, its influence appears to be indirect, primarily affecting relational factors such as proximity, customer intimacy, and contextual understanding. This finding contrasts with the researcher's initial expectations. At the outset of the study, it was anticipated that decentralisation would influence customer trust more significantly, both by enabling improved network security and local customisation, and by raising concerns around service provisioning and maintaining consistent quality. Future research could examine whether this finding remains valid at a later stage, for instance, once the 6G standard has been finalised and is in the early phases of deployment. At that point, both industry stakeholders and customers may have greater contextual awareness and technical understanding of decentralised networks, which could reshape how trust is formed.

5.4. Relevance to Management of Technology

This thesis explores how Security-as-a-Service (SECaaS) can be designed and deployed as a strategic offering in the context of emerging 6G networks. It first characterises SECaaS by identifying its key functionalities and deployment configurations, thus contributing to the development of the service model. Building on this foundation, the study maps the stakeholder landscape involved in SECaaS deployments, proposing both primary and shared responsibilities across telecom, security, and infrastructure providers. It further examines the techno-economic interactions among these actors to understand how value is co-created for end users in centralised and decentralised network deployments. Through

qualitative research grounded in interview data, the study also analyses how these deployment architectures influence customer trust in SECaaS providers. By linking network architecture to stakeholder dynamics, trust formation, and value creation, the research integrates perspectives from technology strategy, customer relationship management and innovation management.

This work aligns closely with the Management of Technology programme by reporting on a scientific study in a technological context that is both forward-looking and strategically relevant. It frames technology, such as the SECaaS service model in 6G networks, not merely as a security solution but as a strategic corporate resource that firms must manage to foster value creation and trust in increasingly decentralised network ecosystems. The research applies scientific methods taught in the Research Methods course, such as adopting semi-structured qualitative interviews as well as open and axial coding to systematically analyse the characteristics of SECaaS, its stakeholders and the influence on customer trust across 6G deployments. In doing so, it shows how firms can use emerging technologies to create competitive services and improve outcomes like providing more customised solutions and greater control to the user. The thesis also integrates insights from Technology Dynamics and Technology, Strategy and Entrepreneurship. In line with Technology Dynamics, it treats SECaaS as a non-linear innovation shaped by actor networks and institutions, examining how telecom operators, infrastructure providers and security firms co-shape service trajectories and trust. This reflects the course's emphasis on system- and organisational-level antecedents of change. Finally, it draws on Technology, Strategy and Entrepreneurship by exploring how firms position SECaaS in 6G ecosystems, analysing value creation, collaboration strategies, and technology adoption under uncertainty, key aspects of innovation strategy and industry transformation.

References

3GPP. (2022, August). 5g system overview. https://www.3gpp.org/technologies/5g-system-overview

3GPP. (2023, November). 3gpp release 18. https://www.3gpp.org/technologies/rel-18

3GPP. (2025). Gsm specifications (by series). https://www.3gpp.org/specifications-technologies/specifications-by-series/gsm-specifications

5G-ACIA. (2019). 5g non-public networks for industrial scenarios. *Tech. Rep.* https://5g-acia.org/media/2021/04/WP_5G_NPN_2019_01.pdf

Aagaard, A., Ahokangas, P., Iivari, M., Atkova, I., Yrjölä, S., & Matinmikko-Blue, M. (2024). Value creation and services in mobile communications. In P. Ahokangas & A. Aagaard (Eds.), *The changing world of mobile communications: 5g, 6g and the future of digital services* (pp. 113–136). Springer International Publishing. https://doi.org/10.1007/978-3-031-33191-6_5

Access, E. U. T. R. (2015). Requirements for support of radio resource management (3gpp ts 36.133 version 12.6. 0 release 12). *ETSI TS*, *136*(133), V11.

Agiwal, M., Kwon, H., Park, S., & Jin, H. (2021). A survey on 4g-5g dual connectivity: Road to 5g implementation. *IEEE Access*, *9*, 16193–16210. https://doi.org/10.1109/ACCESS.2021.3052462

Al-Aqrabi, H., Liu, L., Xu, J., Hill, R., Antonopoulos, N., & Zhan, Y. (2012). Investigation of it security and compliance challenges in security-as-a-service for cloud computing. *2012 IEEE 15th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops*, 124–129. https://doi.org/10.1109/ISORCW.2012.31

Ansari, S., & Garud, R. (2009). Inter-generational transitions in socio-technical systems: The case of mobile communications. *Research Policy*, *38*(2), 382–392. https://doi.org/https://doi.org/10.1016/j.respol.2008.11.009

Basaure, A., Yrjölä, S., Matinmikko-Blue, M., Ahokangas, P., & Jurva, R. (2024). Value network configurations for local 6g deployments. *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 1073–1078. https://doi.org/10.1109/EuCNC/6GSummit60053.2024.10597027

Benzaïd, C., & Taleb, T. (2020). Ai for beyond 5g networks: A cyber-security defense or offense enabler? *IEEE Network*, *34*(6), 140–147. https://doi.org/10.1109/MNET.011.2000088

Benzaïd, C., Taleb, T., & Farooqi, M. Z. (2021). Trust in 5g and beyond networks. *IEEE Network*, *35*(3), 212–222. https://doi.org/10.1109/MNET.011.2000508

Benzaïd, C., Taleb, T., & Song, J. (2022). Ai-based autonomic and scalable security management architecture for secure network slicing in b5g. *IEEE Network*, *36*(6), 165–174. https://doi.org/10.1109/MNET.104.2100495

Bouwman, H., Faber, E., Fielt, E., Haaker, T., & De Reuver, M. (2008). Stof model: Critical design issues and critical success factors. In H. Bouwman, H. De Vos, & T. Haaker (Eds.), *Mobile service innovation and business models* (pp. 71–88). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-79238-3_3

Boyle, R. J., & Panko, R. R. (2014). *Corporate computer security* (4th). Prentice Hall Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Campoy, D., Vilà, I., Pérez-Romero, J., & Sallent, O. (2025). Digital twin as a service for 6g radio access networks: Functional model and key challenges. *2025 31st International Conference on Telecommunications (ICT)*, 1–7. https://doi.org/10.1109/ICT65093.2025.11046305

Casey, T., Smura, T., & Sorri, A. (2010). Value network configurations in wireless local area access. *2010 9th Conference of Telecommunication, Media and Internet*, 1–9. https://doi.org/10.1109/CTTE.2010.5557719

Chafika, B., Taleb, T., Phan, C.-T., Tselios, C., & Tsolis, G. (2021). Distributed ai-based security for massive numbers of network slices in 5g & beyond mobile systems. *2021 Joint European*

Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 401–406. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482418

Chaisiri, S., Ko, R. K. L., & Niyato, D. (2015). A joint optimization approach to security-as-a-service allocation and cyber insurance management. *2015 IEEE Trustcom/BigDataSE/ISPA*, *1*, 426–433. https://doi.org/10.1109/Trustcom.2015.403

Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6g wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open Journal of the Communications Society*, *1*, 957–975. https://doi.org/10.1109/OJCOMS.2020.3010270

Christopoulou, M., Koufos, I., Xilouris, G., & Dimitriou, N. (2025). 5g/6g architecture evolution for xr and metaverse: Feasibility study, security, and privacy challenges for smart culture applications. *IEEE Access*, *13*, 103077–103094. https://doi.org/10.1109/ACCESS.2025.3578595

Cloud Security Alliance. (2019). Security-as-a-service working group charter. https://cloudsecurityalliance.org/artifacts/secaas-working-group-charter

de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The digital platform: A research agenda. *Journal of Information Technology*, *33*(2), 124–135. https://doi.org/10.1057/s41265-016-0033-3

Ensure-6G. (2024). About ensure 6g. https://ensure-6g.eu/about/

Ericsson. (2025, June). *Ericsson mobility report* (tech. rep.). Ericsson. https://www.ericsson.com/49e9b6/assets/local/reports-papers/mobility-report/documents/2025/ericsson-mobility-report-june-2025.pdf

European Commission. (2025). 5g observatory. https://ec.europa.eu/newsroom/dae/redirection/document/116970

European Science-Media Hub. (2021). 5g knowledge map. https://map.sciencemediahub.eu/5g#p=16

Frank, H., Colman-Meixner, C., Assis, K. D. R., Yan, S., & Simeonidou, D. (2022). Techno-economic analysis of 5g non-public network architectures. *IEEE Access*, *10*, 70204–70218. https://doi.org/10.1109/ACCESS.2022.3187727

Furfaro, A., Garro, A., & Tundis, A. (2014). Towards security as a service (secaas): On the modeling of security services for cloud computing. *2014 International Carnahan Conference on Security Technology (ICCST)*, 1–6. https://doi.org/10.1109/CCST.2014.6986995

Gartner, Inc. (2025). Magic quadrant research methodology. https://www.gartner.com/en/research/magic-quadrant

Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and tam in online shopping: An integrated model. *MIS Quarterly*, *27*, 51–90. https://doi.org/10.2307/30036519

Grönroos, C., & Voima, P. (2013). Critical service logic: Making sense of value creation and co-creation. *Journal of the Academy of Marketing Science*, *41*, 133–150. https://doi.org/10.1007/s11747-012-0308-3

GSMA. (2024a). Our members - gsma membership. https://www.gsma.com/get-involved/gsma-membership/our-members/

GSMA. (2024b). Technology upgrades and legacy network sunsets on the rise. https://www.gsma.com/connectivity-for-good/spectrum/technology-upgrades-and-legacy-network-sunsets-on-the-rise/

GSMA. (2025a, April). *The mobile economy 2025* (tech. rep.). GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/04/030325-The-Mobile-Economy-2025.pdf

GSMA. (2025b, January). *The mobile economy europe 2025* (tech. rep.). GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/01/0125-Mobile-Economy-Europe-2025-web.pdf

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Guo, W. (2020). Explainable artificial intelligence for 6g: Improving trust between human and machine. *IEEE Communications Magazine*, *58*(6), 39–45. https://doi.org/10.1109/MCOM.001.2000050

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science Medicine*, *292*, 114523. https://doi.org/https://doi.org/10.1016/j.socscimed.2021.114523

Hussain, M., & Abdulsalam, H. (2011). Secaas: Security as a service for cloud-based applications. *Proceedings of the Second Kuwait Conference on E-Services and e-Systems*. https://doi.org/10.1145/2107556.2107564

Iivari, M., Ahokangas, P., Matinmikko-Blue, M., & Yrjölä, S. (2022). Opening closed business ecosystem boundaries with digital platforms: Empirical case of a port. In *Emerging ecosystem-centric business models for sustainable value creation* (pp. 67–96). IGI Global.

International Telecommunication Union (ITU). (2015). *Imt vision – framework and overall objectives of the future development of imt for 2020 and beyond* (tech. rep. No. M.2370-0). ITU Radiocommunication Sector (ITU-R). https://www.itu.int/dms_pub/itu-r/opb/rep/r-rep-m.2370-2015-pdf-e.pdf

ITU-R. (2015). *Imt vision–framework and overall objectives of the future development of imt for 2020 and beyond* (Recommendation ITU-R M.2083-0 No. 2083). International Telecommunication Union. https://www.itu.int/rec/R-REC-M.2083

Jamil, H., Jian, Y., Jamil, F., Hijjawi, M., & Muthanna, A. (2024). Digital twin-driven architecture for aiot-based energy service provision and optimal energy trading between smart nanogrids. *Energy and Buildings*, *319*, 114463. https://doi.org/https://doi.org/10.1016/j.enbuild.2024.114463

Jarvenpaa, S., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: A cross-cultural validation. *J. Computer-Mediated Communication*, *5*. https://doi.org/10.1111/j.1083-6101.1999.tb00337.x

Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6g: A comprehensive survey. *IEEE Open Journal of the Communications Society*, *2*, 334–366. https://doi.org/10.1109/OJCOMS.2021.3057679

Kallinikos, J., et al. (2011). Bureaucracy under siege: On information, collaboration and networks. *Managing modernity: Beyond bureaucracy*, 130–153. http://eprints.lse.ac.uk/id/eprint/54863

Kavaiya, S., Chauhan, N., & Dalal, P. (2024). *Enhancing physical layer security over 6g wireless networks via quantum key deployment*. IGI Global. https://doi.org/10.4018/979-8-3693-9220-1.ch009

Krasniqi, F., Gavrilovska, L., & Maraj, A. (2019). The analysis of key performance indicators (kpi) in 4g/lte networks. In V. Poulkov (Ed.), *Future access enablers for ubiquitous and intelligent infrastructures* (pp. 285–296). Springer International Publishing.

Kulkarni, V., Walia, J., Hämmäinen, H., Yrjölä, S., Matinmikko-Blue, M., & Jurva, R. (2021). Local 5g services on campus premises: Scenarios for a make 5g or buy 5g decision. *Digital Policy, Regulation and Governance*, *23*(4), 337–354. https://doi.org/10.1108/DPRG-12-2020-0178

Lam, C. F., Yin, S., & Zhang, T. (2022). Chapter 8 - converged fiber-wireless networks. In C. F. Lam, S. Yin, & T. Zhang (Eds.), *Advanced fiber access networks* (pp. 253–277). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-323-85499-3.00002-3

Latva-aho, M., & Leppänen, K. (2019). *Key drivers and research challenges for 6g ubiquitous wireless intelligence* (M. Latva-aho & K. Leppänen, Eds.; Vol. 1). University of Oulu. http://urn.fi/urn:isbn:9789526223544

Lee, Y. C., Kim, Y., Han, H., & Kang, S. (2015). Fine-grained, adaptive resource sharing for real pay-per-use pricing in clouds. *2015 International Conference on Cloud and Autonomic Computing*, 236–243. https://doi.org/10.1109/ICCAC.2015.36

Lepak, D. P., Smith, K. G., & Taylor, M. S. (2007). Value creation and value capture: A multilevel perspective. *Academy of management review*, *32*(1), 180–194.

Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y.-J. A. (2019). The roadmap to 6g: Ai empowered wireless networks. *IEEE Communications Magazine*, *57*(8), 84–90. https://doi.org/10.1109/MCOM.2019.1900271

Liu, G., Huang, Y., Chen, Z., Liu, L., Wang, Q., & Li, N. (2020). 5g deployment: Standalone vs. non-standalone from the operator perspective. *IEEE Communications Magazine*, *58*(11), 83–89. https://doi.org/10.1109/MCOM.001.2000230

Liyanage, M., Ahmad, I., Abro, A., Gurtov, A., & Ylianttila, M. (2018, April). *A comprehensive guide to 5g security*. Wiley Online Library.

Marcelo Royo-Vela, M. F., & Ferrer, A. (2024). The role of value co-creation in building trust and reputation in the digital banking era. *Cogent Business & Management*, *11*(1), 2375405. https://doi.org/10.1080/23311975.2024.2375405

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.2307/258792

Medeiros, N., Ivaki, N. R., Costa, P. N. D., & Vieira, M. P. A. (2017). Towards an approach for trustworthiness assessment of software as a service. *2017 IEEE International Conference on Edge Computing (EDGE)*, 220–223. https://doi.org/10.1109/IEEE.EDGE.2017.39

Moussaoui, M., Bertin, E., & Crespi, N. (2022). Telecom business models for beyond 5g and 6g networks: Towards disaggregation? *2022 1st International Conference on 6G Networking (6GNet)*, 1–8. https://doi.org/10.1109/6GNet54646.2022.9830514

Ngo-Ye, T., Nazareth, D., & Choi, J. (2020). Trust in security as a service: A theoretical model. *Information Systems*, *21*, 64–74. https://doi.org/10.48009/2_iis_2020_64-74

Nguyen, V.-L., Lin, P.-C., Cheng, B.-C., Hwang, R.-H., & Lin, Y.-D. (2021). Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, *23*(4), 2384–2428. https://doi.org/10.1109/COMST.2021.3108618

Peppard, J., & Rylander, A. (2006). From value chain to value network:: Insights for mobile operators. *European Management Journal*, *24*(2), 128–141. https://doi.org/https://doi.org/10.1016/j.emj.2006.03.003

Pera, R., Occhiocupo, N., & Clarke, J. (2016). Motives and resources for value co-creation in a multi-stakeholder ecosystem: A managerial perspective. *Journal of Business Research*, *69*(10), 4033–4041. https://doi.org/10.1016/j.jbusres.2016.03.047

Pi, Z., & Khan, F. (2011). An introduction to millimeter-wave mobile broadband systems. *IEEE Communications Magazine*, *49*(6), 101–107. https://doi.org/10.1109/MCOM.2011.5783993

Porambage, P., Christopoulou, M., Han, B., Asif Habibi, M., Bogucka, H., & Kryszkiewicz, P. (2025). Security, privacy, and trust for open radio access networks in 6g. *IEEE Open Journal of the Communications Society*, *6*, 332–361. https://doi.org/10.1109/OJCOMS.2024.3519725

Qiao, X., Huang, Y., Dustdar, S., & Chen, J. (2020). 6g vision: An ai-driven decentralized network and service architecture. *IEEE Internet Computing*, *24*(4), 33–40. https://doi.org/10.1109/MIC.2020.2987738

Rahmouni, A., Oukid, S., & Ghebghoub, Y. (2023). Upgrade secsla using security as a service based on knowledge graph. In K. Arai (Ed.), *Proceedings of the future technologies conference (ftc) 2022, volume 2* (pp. 486–498). Springer International Publishing.

Ranaweera, P., Imrith, V. N., Liyanag, M., & Jurcut, A. D. (2020). Security as a service platform leveraging multi-access edge computing infrastructure provisions. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 1–6. https://doi.org/10.1109/ICC40277.2020.9148660

Saad, S. B., Ksentini, A., & Brik, B. (2021). A trust architecture for the sla management in 5g networks. *ICC 2021-IEEE International Conference on Communications*, 1–6.

Schurr, P. H., & Ozanne, J. L. (1985). Influences on exchange processes: Buyers' preconceptions of a seller's trustworthiness and bargaining toughness. *Journal of Consumer Research*, *11*(4), 939–953. Retrieved July 9, 2025, from http://www.jstor.org/stable/2489219

Sekaran, U., & Bougie, J. (2009). *Research methods for business: A skill building approach (5th edition)* [Pagination: 488]. Wiley Publishers.

Senk, C. (2013). Adoption of security as a service. *Journal of Internet Services and Applications*, *4*(1), 11. https://doi.org/10.1186/1869-0238-4-11

Sharma, D., Dhote, C., & Potey, M. (2013). Security-as-a-service from clouds: A comprehensive analysis. *International Journal of Computer Applications*, *67*(3), 15–18. https://doi.org/10.5120/11374-6642

Shulga, L. V., Busser, J. A., Bai, B., & Kim, H. ((2021). The reciprocal role of trust in customer value co-creation. *Journal of Hospitality & Tourism Research*, *45*(4), 672–696. https://doi.org/10.1177/1096348020967068

Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). Ai and 6g security: Opportunities and challenges. *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 616–621. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482503

van der Werff, L., Fox, G., Masevic, I., Emeakaroha, V., Morrison, J., & Lynn, T. (2019). Building consumer trust in the cloud: An experimental analysis of the cloud trust label approach. *Journal of Cloud Computing*, *8*. https://doi.org/10.1186/s13677-019-0129-8

Vargo, S., & Lusch, R. (2016). Institutions and axioms: An extension and update of service-dominant logic. *Journal of the Academy of Marketing Science*, *44*. https://doi.org/10.1007/s11747-015-0456-3

Veith, B., Krummacker, D., & Schotten, H. D. (2023). The road to trustworthy 6g: A survey on trust anchor technologies. *IEEE Open Journal of the Communications Society*, *4*, 581–595. https://doi.org/10.1109/OJCOMS.2023.3244274

Walia, J. S., Hämmäinen, H., & Flinck, H. (2017). Future scenarios and value network configurations for industrial 5g. *2017 8th International Conference on the Network of the Future (NOF)*, 79–84. https://doi.org/10.1109/NOF.2017.8251224

Walia, J. S., Hämmäinen, H., Kilkki, K., & Yrjölä, S. (2019). 5g network slicing strategies for a smart factory. *Computers in Industry*, *111*, 108–120. https://doi.org/https://doi.org/10.1016/j.compind.2019.07.006

Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, *6*(3), 281–291. https://doi.org/https://doi.org/10.1016/j.dcan.2020.07.003

Wang, W., & Yongchareon, S. (2020). Security-as-a-service: A literature review. *International Journal of Web Information Systems*, *16*(5), 493–517. https://doi.org/10.1108/IJWIS-06-2020-0031

Wang, W., & Yongchareon, S. (2017). A survey on security as a service. *Web Information Systems Engineering – WISE 2017*, 303–310. https://doi.org/10.1007/978-3-319-68786-5_24

Wenge, O., Lampe, U., Rensing, C., & Steinmetz, R. (2014). Security information and event monitoring as a service: A survey on current concerns and solutions. *PIK - Praxis der Informationsverarbeitung und Kommunikation*, *37*(2), 163–170. https://doi.org/doi:10.1515/pik-2014-0009

Xiang, P., Wei, M., Liu, H., Wu, L., & Qi, J. (2024). How does technological value drive 6g development? explanation from a systematic framework. *Telecommunications Policy*, *48*(7), 102790. https://doi.org/https://doi.org/10.1016/j.telpol.2024.102790

Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T. H., Liu, F., Hewa, T., Liyanage, M., Ijaz, A., Partala, J., Abbas, R., Hecker, A., Jayousi, S., Martinelli, A., Caputo, S., Bechtold, J., Morales, I., … Röning, J. (2020). 6g white paper: Research challenges for trust, security and privacy. https://arxiv.org/abs/2004.11665

Yrjölä, S., Ahokangas, P., & Matinmikko-Blue, M. (2020). *White paper on business of 6g* (White paper). University of Oulu. http://urn.fi/urn:isbn:9789526226767

Yrjölä, S., Ahokangas, P., & Matinmikko-Blue, M. (2021). Platform-based business models in future mobile operator business. *Journal of Business Models*, *9*(4), 67–93. https://doi.org/https://doi.org/10.5278/jbm.v9i4.6222

Yrjölä, S., Ahokangas, P., & Matinmikko-Blue, M. (2022). Value creation and capture from technology innovation in the 6g era. *IEEE Access*, *10*, 16299–16319. https://doi.org/10.1109/ACCESS.2022.3149590

Yrjölä, S., Matinmikko-Blue, M., & Ahokangas, P. (2023). Developing 6g visions with stakeholder analysis of 6g ecosystem. *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 705–710. https://doi.org/10.1109/EuCNC/6GSummit58263.2023.10188379

Zhang, Z. (2024). Technology and geopolitics: The social construction of huawei's 5g controversy in europe. *Global Media and Communication*, *20*(2), 217–235. https://doi.org/10.1177/17427665241251448

Zhang, Z., Ding, C., Li, Y., Yu, J., & Li, J. (2024). Secaas-based partially observable defense model for iiot against advanced persistent threats. *IEEE Transactions on Services Computing*, *17*(6), 4267–4280. https://doi.org/10.1109/TSC.2024.3422870

Zucker, L. (1986). "production of trust: Institutional sources of economic structure, 1840-1920". *Research in Organizational Behavior*, *8*, 53–111.

A

Appendix A: Data Analysis

A.1. Use of AI in this Thesis

This thesis makes use of AI tools to support various aspects of the research process. For example, the free version of ChatGPT 4.0 was used to generate the cover page, support brainstorming ideas, debug LaTeX code, and improve the clarity and academic tone of draft paragraphs. In these instances, paragraphs initially written by the researcher were refined by ChatGPT to enhance grammatical coherence and academic style. Additionally, NotebookLM was employed during the literature review to assist in quickly understanding and assessing the relevance of academic papers. This tool enabled more efficient screening of literature and helped ensure that appropriate sources were selected. To verify its accuracy, key claims generated by the AI were cross-checked by manually reviewing portions of the papers.

Furthermore, Atlas.ti was used to support the analysis of interview transcripts. Although the platform offers an AI-assisted coding function powered by OpenAI, this feature was not utilised. There were two main reasons for this decision. First, prior experience with the tool showed that it often produced overly abstract or generalised coding themes, which risked missing specific details critical to the analysis. Second, the use of this tool raised concerns around participant privacy, as it remains unclear to the researcher how interview data might be processed or stored by OpenAI.

A.2. Coding Themes and Groundedness

Thematic coding was used to form themes based on the open codes. Below is the summary of the codes that were used for forming themes, followed by the network diagrams that were used to refine the themes further

Table A.1: Open Codes and Groundedness for SQ1: SECaaS in 6G Context

Sub-Question	*Theme*	*Open Code*	*Groundedness*
SQ1: SECaaS in 6G Context	5G & 6G Expectations	5G Still Being Adopted	7
		Integrated 6G Networks	3
		Connectivity Offering Secure by Default	4
		Network Security by Default	5
		Uncertain of 6G Usecases	2
		Sub-Total	**21**
	SECaaS Deployment	Cloud Driven Centralised Security	13
		Decentralised Security on Device	6
		Hybrid Security on Device & Network	13
		Sub-Total	**32**
	SECaaS Features	Cryptographic Encryption	9
		Firewall Deployment	7
		Information and Events Management	4
		Internet Security	4
		Managed Detection & Response	13
		Network Backup & Recovery	2
		Network Monitoring	11
		Physical Infrastructure Security	13
		Quantum Encryption	4
		Security Incident Response	6
		Unauthorised Access Management	10
		Update & Maintain Solutions	6
		Sub-Total	**89**
	Grand Total		**142**

Table A.2: Open Codes and Groundedness for SQ2: Key Stakeholders in 6G SECaaS

Sub-Question	*Theme*	*Open Code*	*Groundedness*
SQ2: Key Stakeholders in 6G SECaaS	6G SECaaS Stakeholders	Customers	18
		Infrastructure Providers	20
		Security Providers	29
		Telecom Providers	18
		Sub-Total	**85**
	Grand Total		**85**

Table A.3: Open Codes and Groundedness for SQ3: Techno-Economic Interactions

Sub-Question	*Theme*	*Open Code*	*Groundedness*
SQ3: Techno-Economic Interactions	Stakeholder Analysis	Additional Roles and Responsibilities	3
		Different Legal Entities	3
		Security Responsibility Unclear	6
		Shared Responsibility for Security	3
		Sub-Total	**15**
	Stakeholder Roles	SECaaS Provider's Role	12
		Telecom Provider's Role	5
		Infrastructure Provider's Role	10
		Security Vendor's Role	2
		Sub-Total	**29**
	Value Creation for SECaaS	Added Value From Enhanced Service	3
		Added Value from Expertise	4
		Established Firms Struggle to Adapt	2
		Local Integrators Provide Support	6
		Value Added Through Collaboration	4
		Sub-Total	**19**
	Grand Total		**63**

Table A.4: Open Codes and Groundedness for SQ4: Antecedents of Trust

Sub-Question	*Theme*	*Open Code*	*Groundedness*
SQ4: Antecedents of Trust	Role of Trust in SECaaS	Trust Enables Collaboration	7
		Trust Prerequisite for Security Services	7
		Sub-Total	**14**
	Trust Factors - External	Certification Influences Trust	9
		Geopolitical Influence on Trust	8
		Third Party Credibility Influences Trust	8
		Sub-Total	**25**
	Trust Factors - Organisational	Accountability Influences Trust	5
		Firm Capability Influences Trust	12
		Firm Size Influences Trust	7
		History of Reliability Influences Trust	11
		Perceived Reputation Influences Trust	12
		Transparency Influences Trust	8
		Sub-Total	**55**
	Trust Factors - Relational	Collaboration Influences Trust	8
		Personal Interactions Influence Trust	9
		Proximity & Intimacy Influence Trust	8
		Service Experience Influences Trust	5
		Understanding Customer Context Influences Trust	5
		Sub-Total	**35**
	Variation in Trust Factors	Customers Lack Awareness	10
		Decentralisation Does Not Influence Trust	13
		Decentralisation Influences Trust	8
		Sub-Total	**31**
	Grand Total		**160**

A.3. Identified SECaaS Features

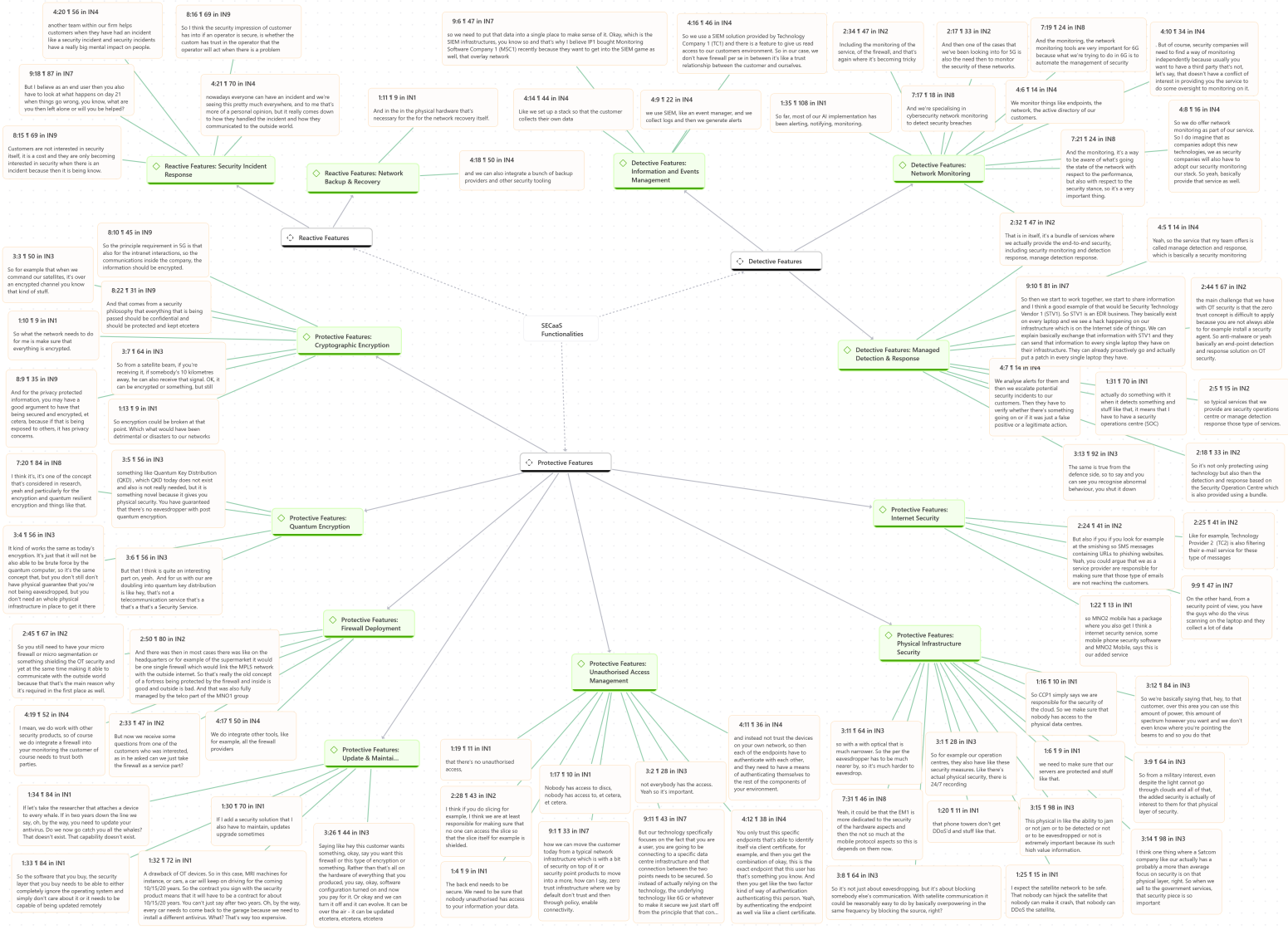

Figure A.1: Identified Features of SECaaS Solutions

A.4. Stakeholders in 6G SECaaS

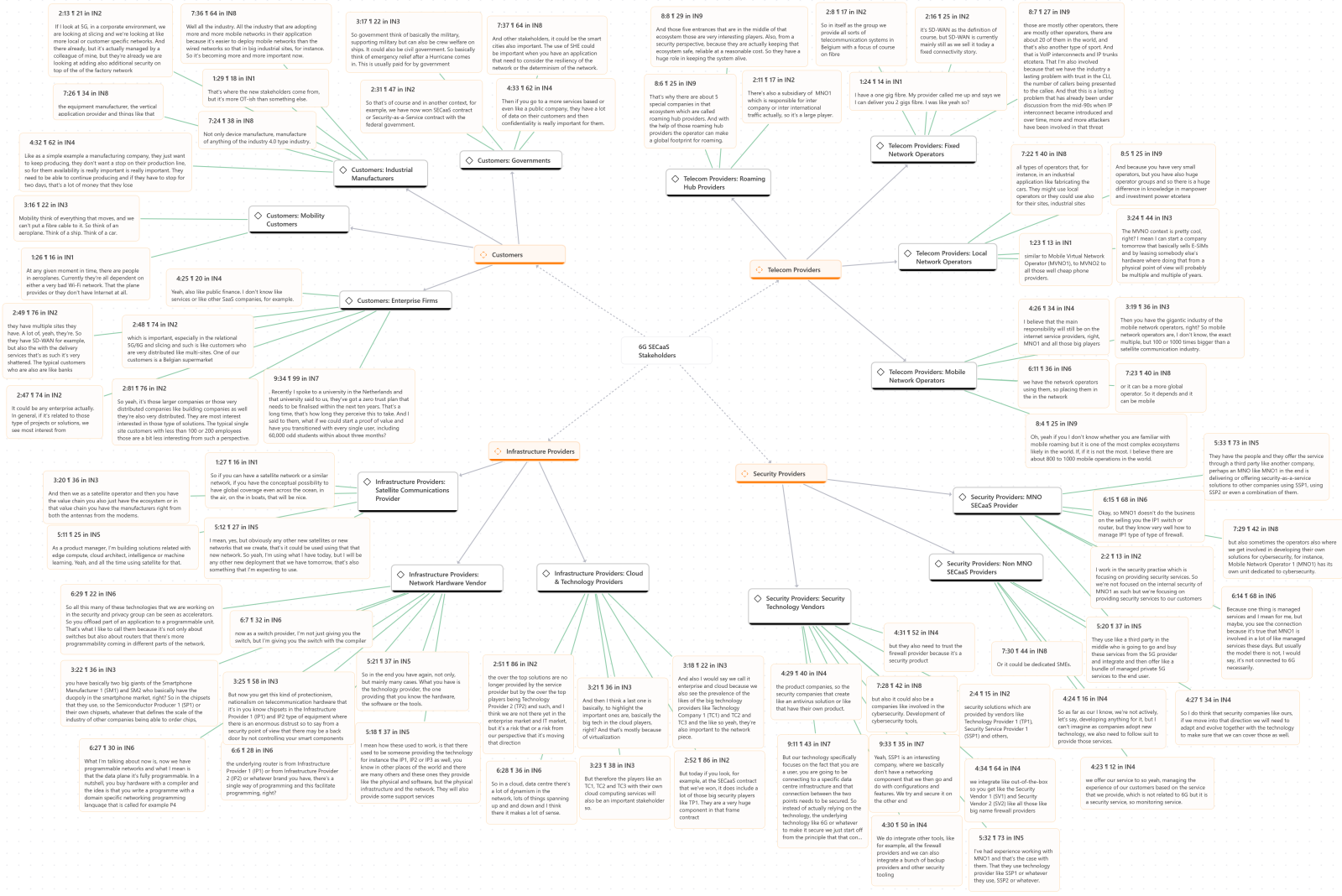

Figure A.2: Identified Stakeholders in 6G SECaaS

A.4.1. Role of Trust in Security Providers

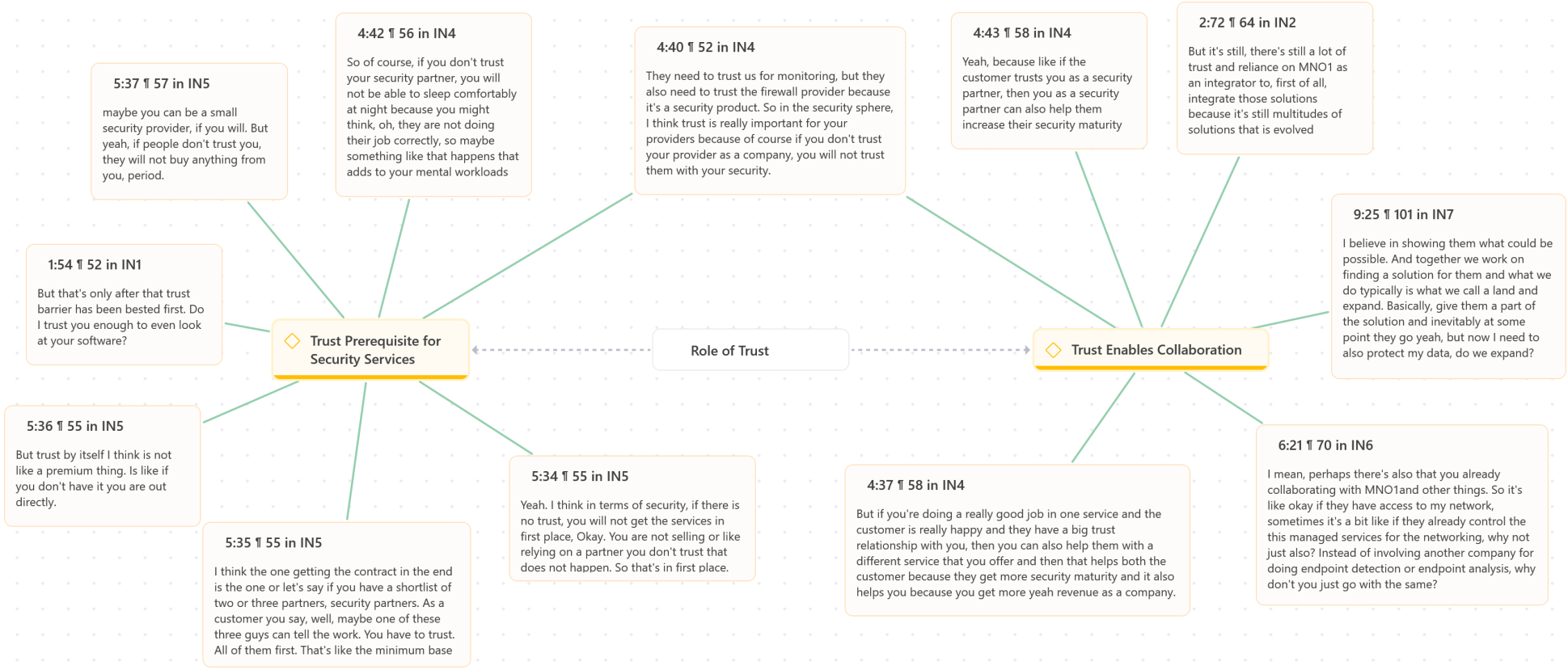

Figure A.3: Role of Trust in Security Providers

A.4.2. External Factors Influencing Customer Trust

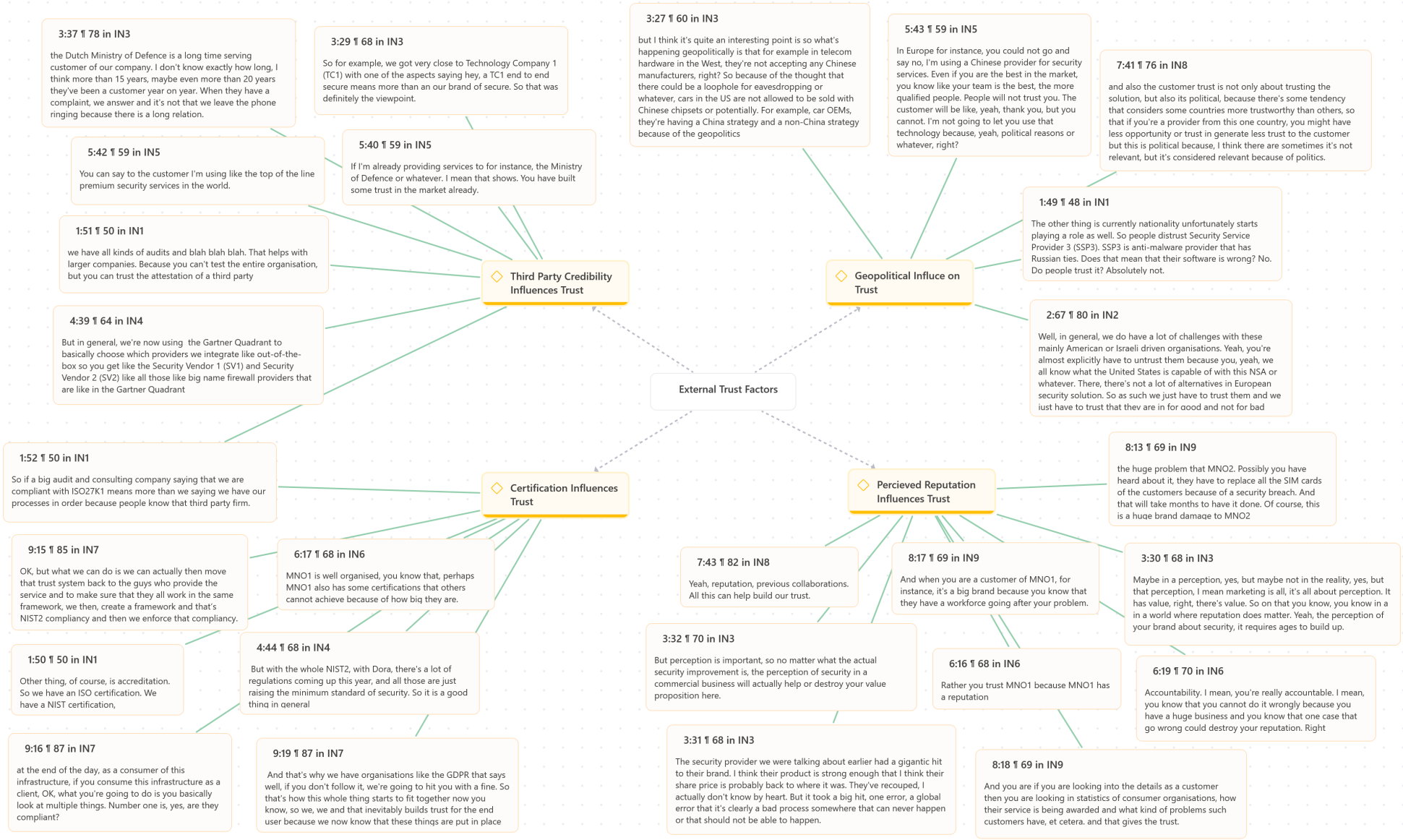

Figure A.4: External Factors Influencing Customer Trust

A.4.3. Organisational Factors Influencing Customer Trust

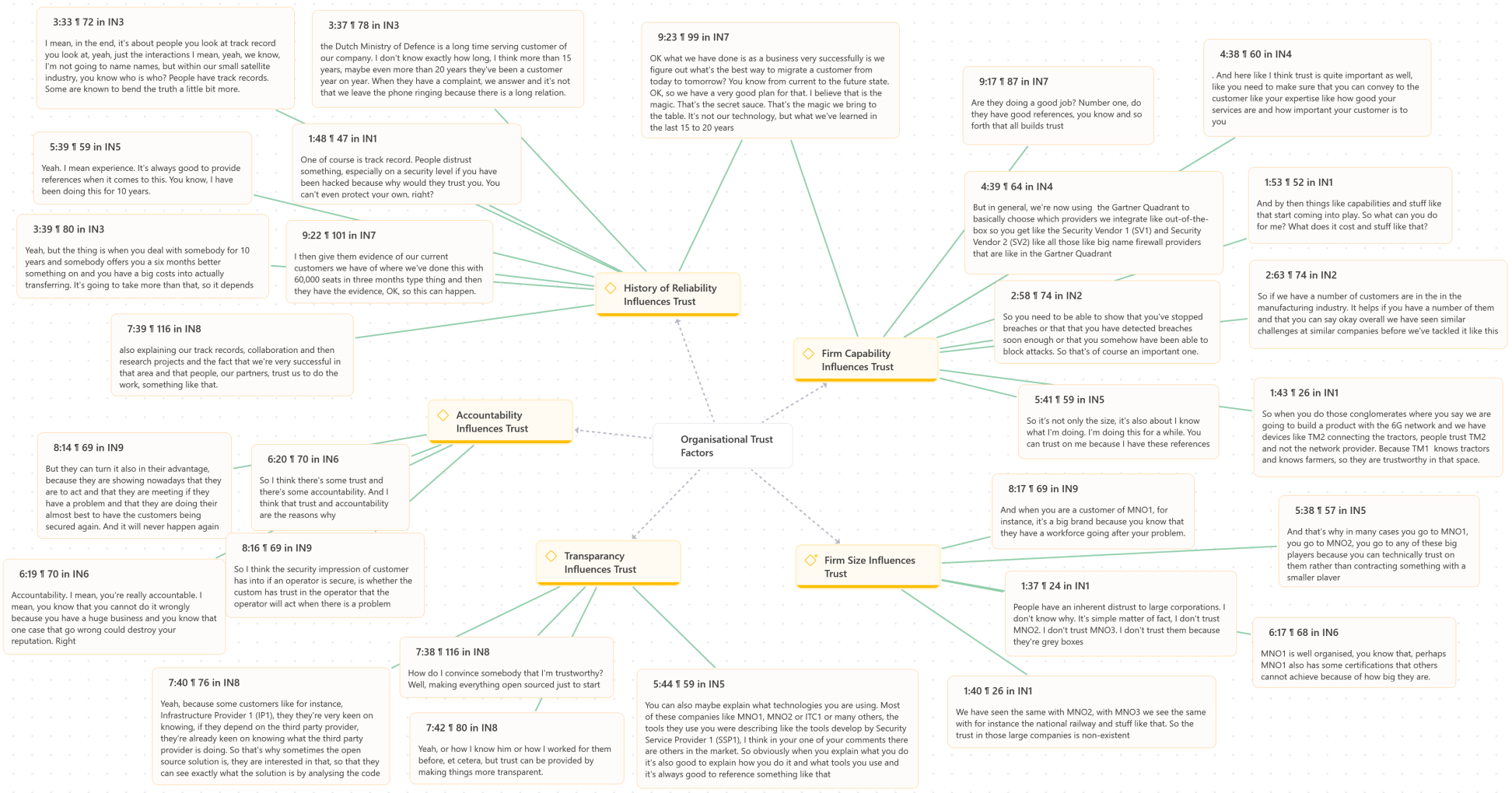

Figure A.5: Organisational Factors Influencing Customer Trust

A.4.4. Relational Factors Influencing Customer Trust

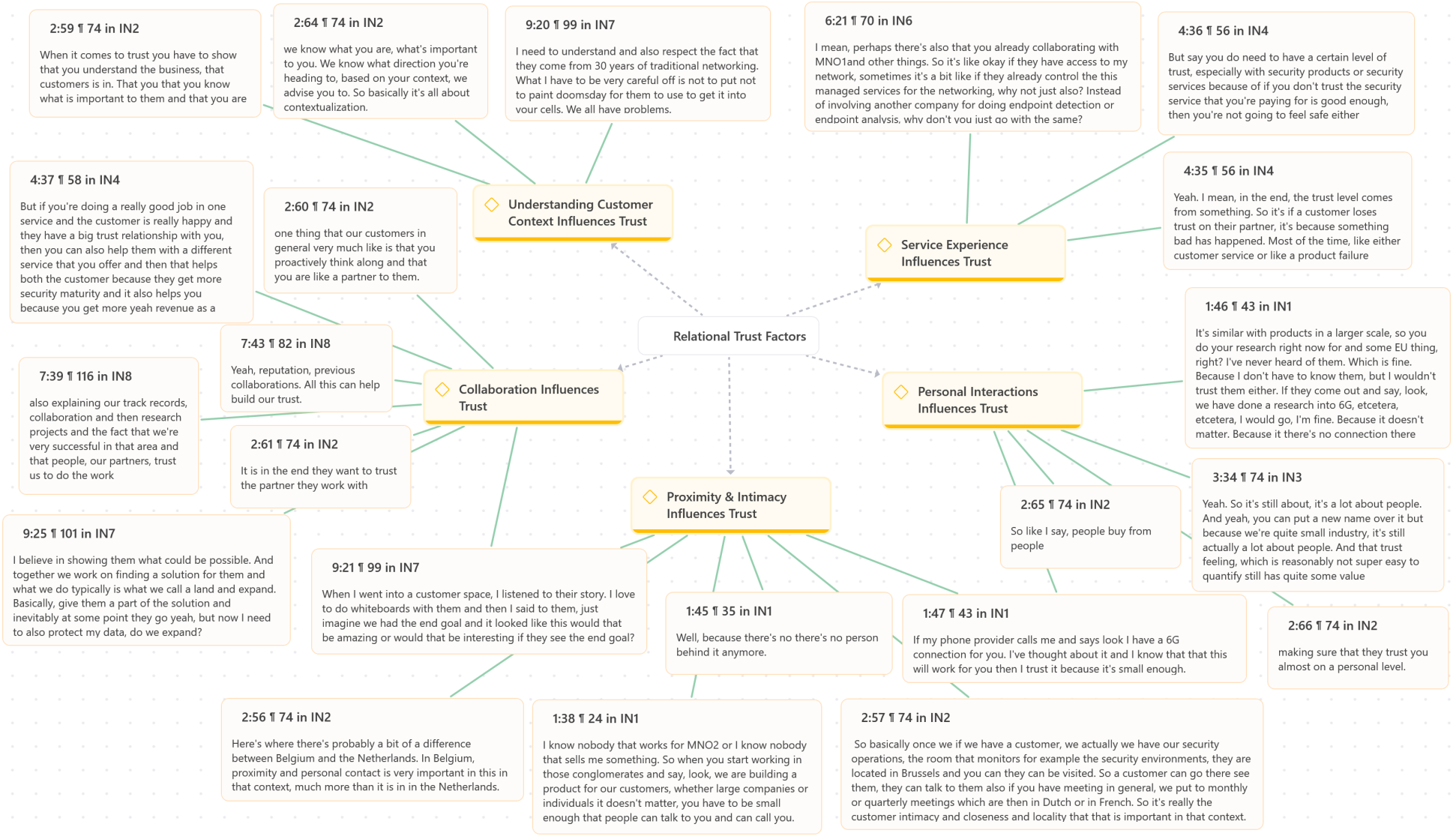

Figure A.6: Relational Factors Influencing Customer Trust

A.4.5. Variation in Factors Influencing Customer Trust

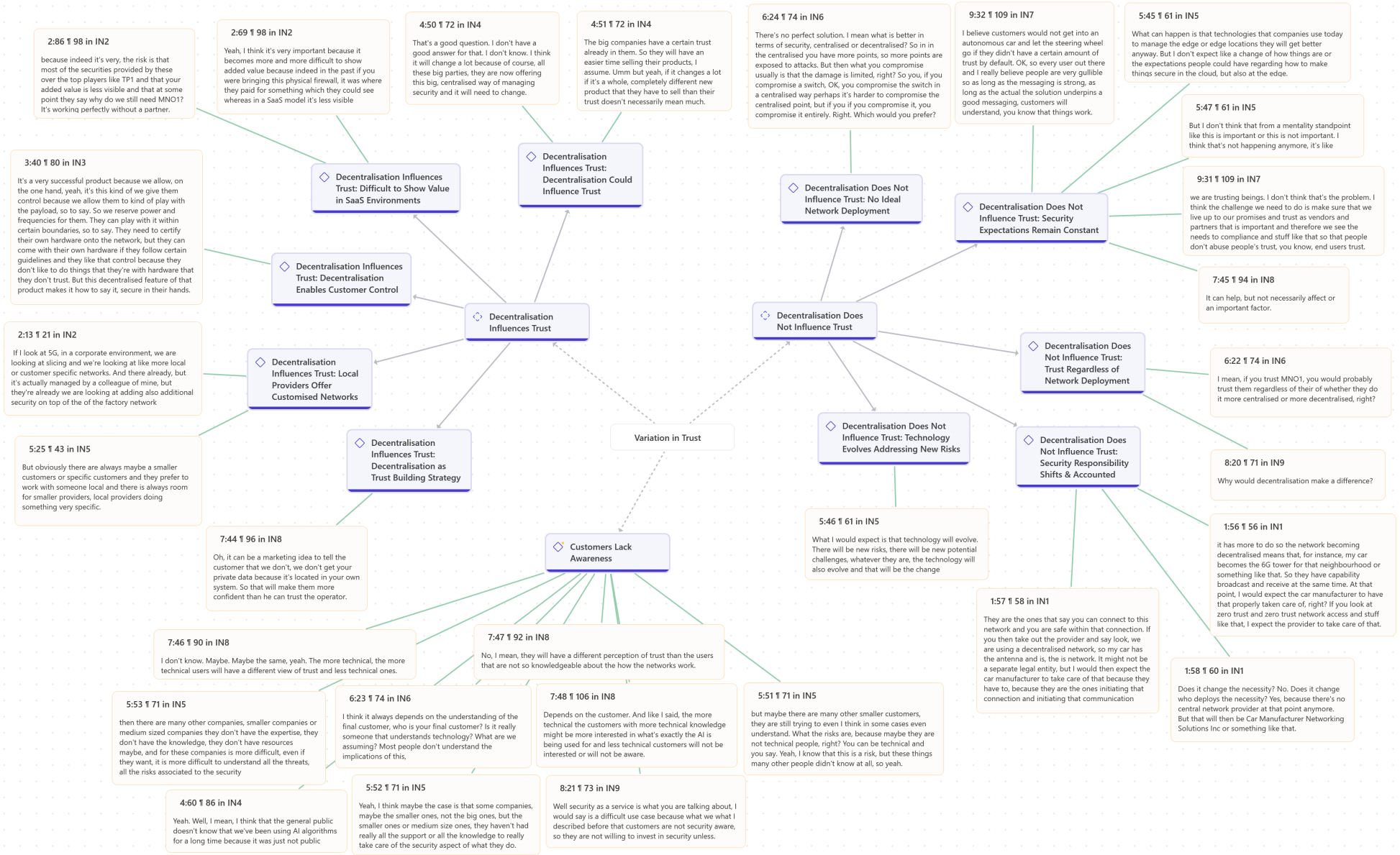

Figure A.7: Variation in Factors Influencing Customer Trust

A.5. Value Network Diagrams

A.5.1. VNC for Centralised Public Networks

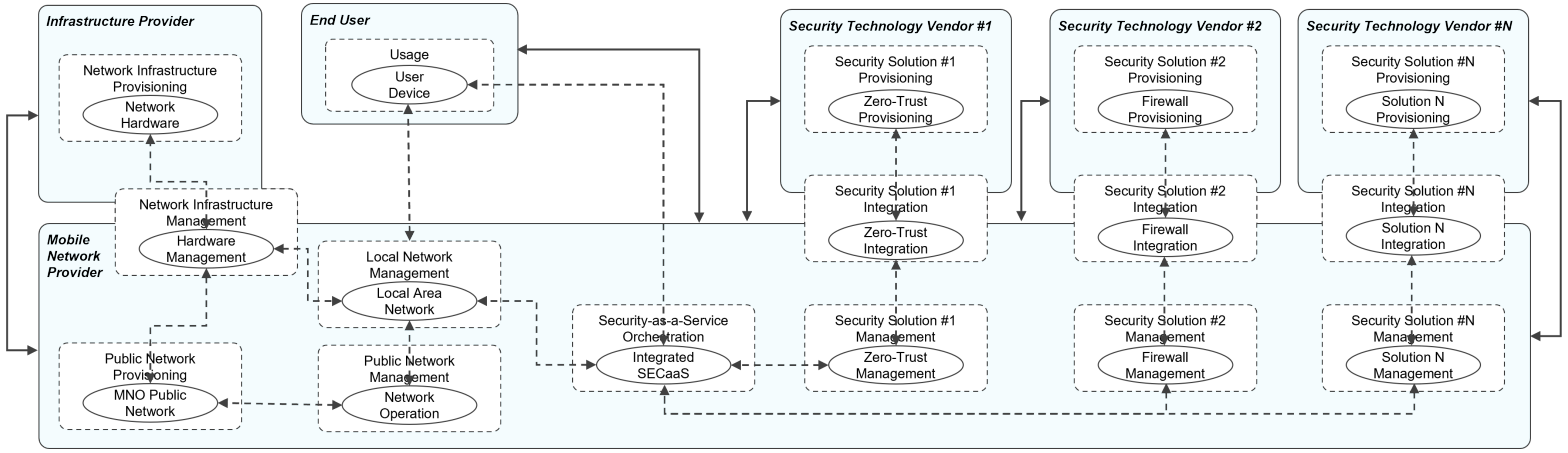

Figure A.8: VNC for Centralised Public Networks

A.5.2. VNC for Non-Public Networks Sharing Public RAN

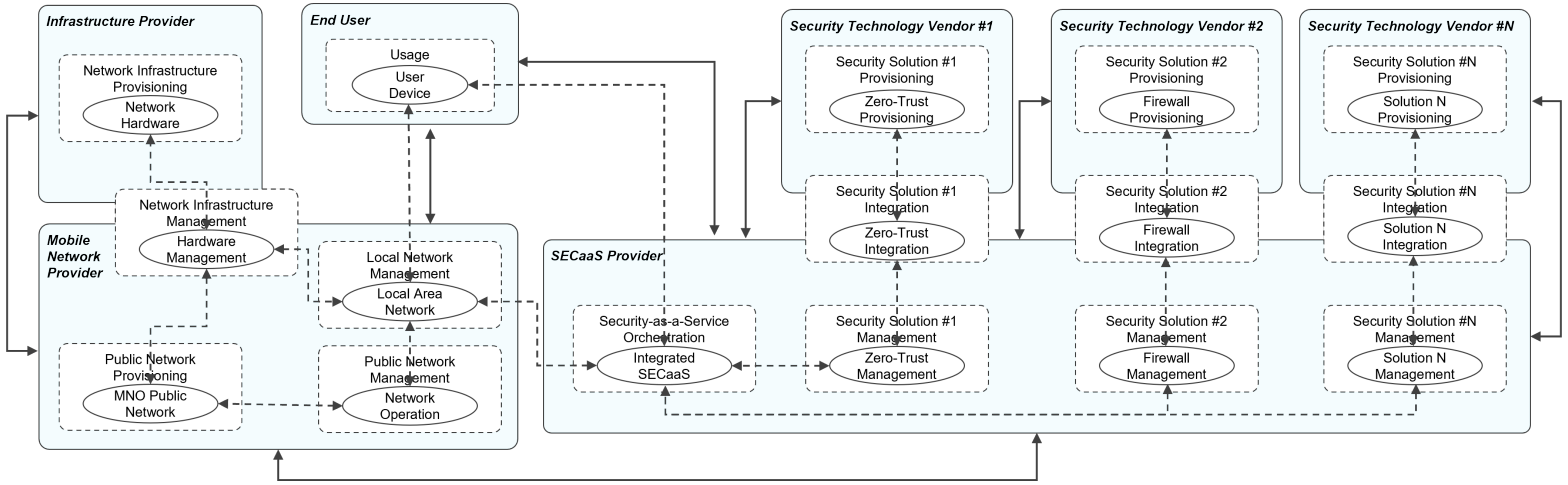

Figure A.9: VNC for Non-Public Networks Sharing Public RAN

A.5.3. VNC for Standalone Non-Public Networks

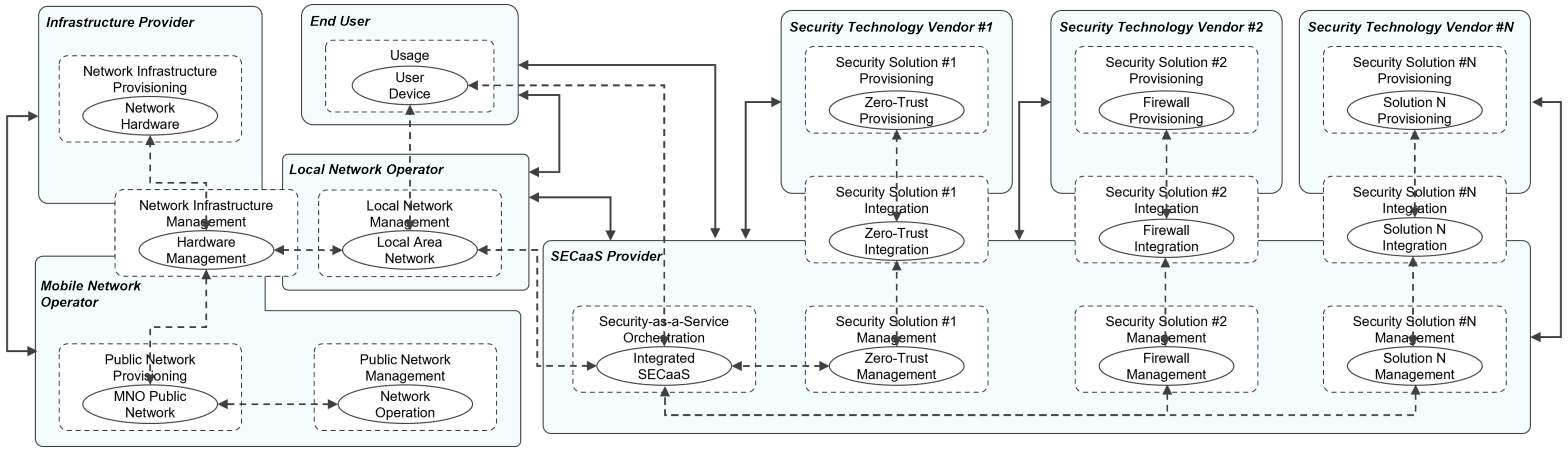

Figure A.10: VNC for Standalone Non-Public Networks

B

Appendix B: Interview Protocol

B.1. List of Interviewees

Initials	*Company Type*	*Role*	*Expertise*
Interviewee Number 1 [IN1]	Security Technology Vendor	Senior Sales Engineer	Technical specialist in selling cloud-based security solutions to enterprise firms
Interviewee Number 2 [IN2]	Mobile Network Operator (offering SECaaS)	Senior Product Manager	Managing the security solutions portfolio offered by the MNO to enterprise firms
Interviewee Number 3 [IN3]	Satellite Communications Provider	Senior Manager	Product definition of future products and business development
Interviewee Number 4 [IN4]	Non-MNO based SECaaS Provider	Security Operations Manager	Managing customer experience in offering security monitoring services to SME enterprise firms
Interviewee Number 5 [IN5]	Satellite Communications Provider	Senior Product Manager	Providing edge and cloud connectivity solutions using satellite connectivity
Interviewee Number 6 [IN6]	Mobile Network Operator (offering SECaaS)	Senior Research Scientist	Further research on the intersection of security, networking and systems
Interviewee Number 7 [IN7]	Security Technology Vendor	Senior Systems Engineer	Integrating zero-trust solutions for public sector customers including telecoms
Interviewee Number 8 [IN8]	Security Technology Vendor	Chief Executive Officer	Developing tools for testing and monitoring networks, applications and services
Interviewee Number 9 [IN9]	Telecom Consultancy Provider	Independent Consultant	Contributed to standardisation efforts and drafting security guidelines in 5G networks
Interviewee Number 10 [IN10]	Mobile Network Operator (offering SECaaS)	Department Head	Research on end-to-end security for products and systems at the MNO

Table B.1: List of Interviewees

B.2. Interview Questions

Sr. No.	*Objective*	*Sub-theme*	*Interview Question*
1	Introduction	Interviewee profile	Strictly for administrative purposes, could you please tell me your name and a brief description of your role at your firm?
2	Introduction	Role definition	Can you briefly tell me what role your firm plays in providing network connectivity today?
3	Introduction	Current Scope	Does your firm also offer any managed services along with offering network connectivity?
4	Introduction	Future role scope	What role would you expect your companies like your firm to play in deploying 6G networks? What use cases would your firm cater to?
5	Introduction	Central vs local deployment	(selecting one of the use cases for example) In your view, would this use case rely on a central or local network deployment? How would it be different and why would it benefit from this deployment?
6	Stakeholder roles and interactions	Stakeholder identification	(selecting one of the use cases for example) When delivering this use case would it require close collaboration with other stakeholders? If so, who do you envision these to be?
7	Stakeholder roles and interactions	Security lead	(selecting one of the use cases for example) In deploying such 6G networks, in your view who would be responsible for integrating and managing security services?
8	Stakeholder roles and interactions	Emerging stakeholders	Transitioning from 5G to 6G, do you envision new and emerging stakeholders in deploying networks, (particularly considering network security)? If so who are they and what will they be responsible for?
9	Stakeholder roles and interactions	Central vs local stakeholders	Do you envision these security services being integrated and managed centrally or at the edge closer to the end user? (use an infographic of the network if needed)
10	Stakeholder roles and interactions	Technical roles	Assuming network security is managed by a specialised provider for this 6G use case, which elements do you expect them to be responsible for? What would their technical roles be?
11	Identify customers of SECaaS	Customer segments	Assume your firm offers managed security services in 6G, who are the main customer segments that your solution would target? Can you give me some examples?
12	Identify customers of SECaaS	Emerging customers	Are you seeing new types of customers emerge due to shifts in 6G or edge computing trends?
13	Identify customers of SECaaS	Customer expectations	Do customer expectations for network security vary between centralised vs decentralised deployments?
14	Customer trust as value driver	Importance of trust	Assume your firm offers managed network and security services in 6G along with an external partner, how important would you say is customer trust in the service provider for you when creating value for the customer? Why?
15	Customer trust as value driver	Importance of trust	Do you think if you were to collaborate with a highly trusted security service provider you can create greater value for the customer? If so, why?
16	Customer trust as value driver	Value cocreation	How would your company approach co-creating value with partners when offering integrated services (e.g., connectivity and security services)?

Sr. No.	*Objective*	*Sub-theme*	*Interview Question*
17	Customer trust as value driver	Trust in collaboration	In what ways can customer trust enable new kinds of collaborations between your firm and other players (e.g., cybersecurity firms, cloud providers)?
18	Antecedents of trust	Partner company's POV on SECaaS	Assume your firm offers managed security services in 6G, what factors would influence your trust in that security service provider?
19	Antecedents of trust	SECaaS' POV	Assume your firm offers managed security services in 6G, what factors do you believe influence customer trust in your security service offering?
20	Antecedents of trust	Segment-based factors	Do you think customers would express different trust concerns based on their industry, regulatory environment, or network setup? If so, how would they be different?
21	Antecedents of trust	Company's POV	What factors or signals do your customers typically rely on to evaluate your trustworthiness as a (security) service provider?
22	Antecedents of trust	Central vs local difference	How would you expect these factors to vary when the network is centrally or decentrally deployed? Why?

Table B.2: List of interview questions

Appendix C: Informed Consent Form

C.1. Informed Consent Form

As this thesis involves interviewing human participants, HREC approval was granted to ensure the research was carried out whilst minimising the potential risks of participating in the interviews. Following is the informed consent form used to clearly communicate these risks to the participants and explain how they would be mitigated.

Opening Statement

You are being invited to participate in a research study titled Trusting Security-as-a-Service in 6G Ecosystems: Exploring Customer Trust and Value Co-Creation in Security Services Across Different 6G Network Deployments. This study is being conducted by Rohit Pandit from the TU Delft as part of the Master programme in Management of Technology.

The purpose of this research study is to explore the factors influencing customer trust in Security-as-a-Service (SECaaS) and how this trust impacts value co-creation in 6G mobile communication network ecosystems. It also examines how these factors vary between centralised and decentralised network deployments and will take you approximately 60 minutes to complete. The data will be used to map relevant stakeholders for SECaaS providers to identify their customers in central and local 6G networks. Furthermore, key factors influencing customer trust in the value co-creation of the ecosystem will be identified and compared for both central and local 6G networks. Finally the findings from the data will be used in the master thesis which will be made publicly available on the TU Delft repository. Additionally, these findings could be utilised for future academic research in this domain.

We will be asking you questions on which stakeholders interactions when offering (or using) security services, how these interactions vary across different network deployments and the factors influence trust in them.

To ensure that we minimise any risk when storing and using the data, any data that is collected will be done in a password protected environment using TU Delft's institutional storage. Moreover, unauthorised access to all personal and interview data will be prevented via access control. This data will only be accessible to the TU Delft research team consisting of the responsible researcher and the responsible researcher's graduation committee. As with any online activity there may pose a risk of a potential breach, however to the best of our ability we will ensure your data remains strictly confidential.

To help with the data analysis of this study, we will record the interview via MS Teams to generate a written transcript of the interview. As we will also be collecting your name, associated company and role, strictly for administrative purposes, this interview is not anonymous. After the interview, a copy of the interview transcript will be shared with you to verify and confirm if the data can be used for the analysis in this study.

Furthermore, all data included in the final thesis will be anonymised and aggregated to ensure confidentiality. The thesis will be publicly published on the TU Delft repository. An anonymised interview

transcript will be kept at TU Delft for future research and education activities. All personal data will be deleted at the end of the research project dated 01st Sept, 2025.

Your participation in this study is entirely voluntary and you can withdraw at any time. You are free to omit any questions. For any questions, feel free to contact the responsible researcher, Rohit Pandit and/or the responsible researcher's supervisor, Mark de Reuver.

PLEASE TICK THE APPROPRIATE BOX	Yes	No
I agree that my responses, views or other input can be quoted anonymously in research outputs	☐	☐
I agree that an anonymised version of the interview transcripts can be kept at TU Delft for future academic research and education purposes in this domain	☐	☐

Signatures

I, as a participant, have read and understood this information, and I consent to participate in this study along with the data being processed as described above.

Name of participant	**Signature**	**Date**

I, as researcher, have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

Rohit Pandit	**Signature**	**Date**