CONSUMER ACCEPTANCE AND USAGE OF DIGITAL SIGNATURE TECHNOLOGIES

Jyväskylä University
School of Business and Economics

Master's Thesis

2021

Author: Lassi Lääveri
Subject: Digital Marketing & Corporate Communication
Supervisor: Aijaz A. Shaikh

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

ABSTRACT

Author
Lassi Lääveri

Title
Consumer acceptance and usage of digital signature technologies

Subject	Type of work
Digital Marketing & Corporate Communication	Masters' thesis
Date	Number of pages
22.06.2021	60 + appendices

Abstract

Digital signatures have grown in popularity as a method of signing and collecting signatures on documents. After the movement and contact restrictions posed by the coronavirus pandemic in 2020, the popularity of the technology exploded. Technically speaking, digital signatures are created using asymmetric cryptography. Asymmetric cryptography enables the verification of authentication, integrity of the document and signatory non-repudiation. Digital signatures hold a similar legal status to that of a traditional signature within the European union.

Most of the studies focusing on digital signatures have been focusing on the technical aspects of the phenomenon, while the users' perspective is often neglected. This study is bases on the presumptions provided by technology acceptance studies, in the field of information technology to study the factors affecting user acceptance of digital signature technologies. The unified theory of acceptance and use of technology (UTAUT) is a model that is used to study use behaviour of technologies and information systems. In the model performance expectancy and effort expectancy are two of the constructs that affect behavioural intention. Therefore, it is valuable to study what performance and effort actually mean in the context of digital signatures from the users' point of view. While this study bases on the technology acceptance studies and especially the UTAUT model, it is important to note that the study does not attempt to be an extension to UTAUT or use UTAUT to predict behaviour.

This study identified six different main categories of parameters that the users judge the performance of digital signatures: efficiency, information security, convenience, comparative performance, scalability functions and other factors. The effort and ease is judged basing on service-specific user experience, information availability, comparative ease and contextual factors. The implications of the study for theory and practice as well as limitations and future research suggestions are provided in the discussion chapter

Key words
Digital signatures, user acceptance, UTAUT, consumer acceptance

Place of storage
Jyväskylä University Library

TIIVISTELMÄ

Tekijä
Lassi Lääveri

Työn nimi
Sähköisen allekirjoittamisen kuluttajahyväksyntä ja käyttö

Oppiaine	Työn laji
Digital Marketing & Corporate Communication	Pro gradu -tutkielma
Päivämäärä	Sivumäärä
22.06.2021	60 + liitteet

Tiivistelmä

Sähköinen allekirjoitus on yleistynyt tapana allekirjoittaa ja kerätä allekirjoituksia asiakirjoihin. Vuonna 2020 alkaneen koronaviruspandemian myötä teknologian suosio suorastaan räjähti, kun liikunta- ja tapaamisrajoitukset rajoittivat ihmisten välisiä kontakteja. Teknologisesta näkökulmasta sähköinen allekirjoitus tehdään käyttämällä asymmetrista kryptografiaa, jonka avulla voidaan vahvistaa alkuperäinen todennus, tietojen koskemattomuus sekä allekirjoittajan kiistämättömyys. Sähköisten allekirjoitusten juridinen asema on vastaava kuin perinteisillä allekirjoituksilla Euroopan Unionin alueella.

Suurin osa sähköisiä allekirjoituksia koskevasta tutkimuskirjallisuudesta keskittyy ilmiön teknologisiin osa-alueisiin. Käyttäjänäkökulmaan keskittyvä tutkimus on jäänyt toistaiseksi vähäiseksi. Tämä tutkimus perustaa tutkimusasetelmansa teknologian omaksumistutkimuksien luomien olettamien varaan tutkiessaan sähköisten allekirjoitusteknologioiden käyttäjähyväksyntään liittyviä tekijöitä. Yksi teknologian omaksumis- ja hyväksymistutkimuksessa käytetyistä malleista on niin kutsuttu UTAUT-malli. UTAUT-malli on yhtenäinen teoria teknologian omaksumisesta ja käytöstä. Tähän tutkimukseen valikoituivat UTAUT-mallin tekijöistä teknologian kyvykkyyteen ja suoriutuvuuteen liittyvät odotukset sekä vaivattomuuteen liittyvät odotukset, jotka mallin mukaan vaikuttavat käyttäjän aikomuksiin käyttää jotain teknologiaa, ja siten myös välillisesti todelliseen teknologian käyttöön. Tässä tutkimuksessa selvitetään, mitä kyvykkyys ja vaivattomuus tarkoittavat sähköisten allekirjoitusteknologioiden kontekstissa käyttäjien näkökulmasta. Vaikka tämä tutkimus pohjautuu teknologian omaksumismalleihin, on tärkeää huomioida, että tämän tutkimuksen ei ole tarkoitus käyttää UTAUT-mallia teknologian käytön ennustamiseen.

Tutkimuksen tulosten mukaan käyttäjät arvioivat sähköisten allekirjoitusten kyvykkyyttä tehokkuuden, tietoturvallisuuden, kätevyyden, verrannollisen kyvykkyyden, skaalautuvuustoimintojen, sekä muiden tekijöiden perusteella. Käytön vaivattomuutta puolestaan arvioidaan puolestaan palvelukohtaisen käyttökokemuksen, informaation saatavuuden, kontekstitekijöiden sekä verrannollisen helppouden perusteella.

Asiasanat
Sähköinen allekirjoitus, UTAUT, käyttäjähyväksyntä, kuluttajahyväksyntä

Säilytyspaikka
Jyväskylän yliopiston kirjasto

CONTENTS

LIST OF TABLES AND FIGURES

1 INTRODUCTION

Digital signature technologies have emerged as a digital alternative for traditional handwritten signatures. While the use has increased slowly but steadily until 2020, the COVID-19 pandemic and the rapid shift to remote work and social distancing led to significant increase in digital signing. Visma Solutions, a technology company providing the digital signature service Visma Sign, reported in a press release issued in May of 2020 that within ten weeks the number of digital signatures through Visma Sign had nearly doubled, while the yearly increase before the pandemic had been measured in tens of per cents (Visma Solutions, 2020). Due to the growing popularity of digital signature services, it is important to understand the different factors that are at play when users either adapt or reject the technology.

1.1 Digital signatures

Digital signatures are an emerging technology that provides an alternative to making handwritten signatures. The digital signature technologies in Finland commonly use banking credentials as well as mobile ID technologies to authenticate the signatories. (Vähimaa, 2021.) The terms digital signature and electronic signature are terms that are often used in describing the same phenomenon (DNA Oyj, 2017). In EU-legislation, the term that is used is electronic signatures, while the companies providing means to use these technologies most often refer to them as digital signatures. As it is not necessary to differentiate between electronic signatures and digital signatures for the purposes of this study, the term that will be used is "digital signature".

Legally digital signatures hold the same power as handwritten signatures (EU regulation No 910/2014, 2014). While the law distinguishes between three different levels of electronic signatures (electronic signature, advanced electronic signature, qualified electronic signature), the law also states that electronic signatures legal power can't be denied on the grounds of it not meeting the requirements of qualified signature (EU regulation No 910/2014, 2014). Qualified electronic signatures use qualified certificates, which currently in Finland can only be issued by the digital and population data services agency in form of citizen- and organizational certificates. Therefore, the commercially available digital signature technologies in Finland are typically either basic or advanced electronic signatures.

1.2 Technology acceptance

Technology acceptance is a topic widely studied in information systems studies. The field of technology acceptance studies how and why individuals adopt new information technologies (Venkatesh et al., 2012; Venkatesh et al., 2003). Theoretical models concerning technology acceptance and use have been developed from the fields of psychology and sociology (Venkatesh et al., 2012).

One of the most powerful theoretical models to predict technology acceptance is the unified theory of acceptance and use of technology, also known as the UTAUT model. The UTAUT model consists bases on the assumption that use behaviour of technology is predicted by behavioural intention, which is further affected by performance expectancy, effort expectancy and social norm (Venkatesh et al., 2003.). Use behaviour is also affected by facilitating conditions (Venkatesh et al., 2003). The effects of performance expectancy, effort expectancy, social norm and facilitating conditions are filtered by age, gender, experience and voluntariness of use (Venkatesh et al., 2003).

While UTAUT has been applied in different kinds of settings with different technologies, there has been very little studies on what the different factors, such as performance expectancy and effort expectancy actually mean in specific technological contexts. In other words, studies have used the UTAUT model to measure for example performance expectancy numerically, but there have been very little qualitative studies studying what these different factors consist in the minds of users – what constitutes as performance in a certain technology.

1.3 Research gaps and justification for study

The previous studies on digital signatures are very heavy on the technological point of view, yet light on the users' perspective. As the implementation of the technologies has not been very fast until lately, understanding the different drivers behind the utilisation as well as the underlying definitions of these drivers is important.

While there have been papers discussing digital signature technologies, there is not a huge volume of research on them. The little volume of research on digital signatures focuses heavily on the technological aspects of digital signatures and are mostly from the field of information technology studies. There has been some technology acceptance studies on digital signature technologies, using the technology acceptance model (TAM) such as Aydin et al. (2018) and Haryanto et al. (2020), but the volume of these studies is very limited. These papers have studied the drivers and factors affecting utilisation of digital signature systems quantitatively using surveys to measure factors such as perceived usefulness and perceived ease of use numerically (Aydin et al., 2018). However, questionnaires fail to provide answers to the questions concerning the nature of these factors;

what makes a digital signature service easy to use, or what are the aspects that contribute to the usefulness of these systems.

The UTAUT model is one of the theoretical models used to study technology acceptance. The strength of UTAUT model lies in the fact that it synthesises a number of different technology acceptance models, including the aforementioned technology acceptance model (TAM) (Venkatesh et al., 2003). In the studies resulting in the UTAUT model, performance expectancy was found to be the strongest contributor to behavioural intention (Venkatesh et al., 2003). Another strong contributor to behavioural intention was effort expectancy (Venkatesh et al., 2003). Behavioural intention in turn was a strong predictor of actual use behaviour in several different models (Davis et al., 1989; Venkatesh et al., 2003).

As UTAUT model has established, performance expectancy and effort expectancy are strong factors towards behavioural intention and, through behavioural intention, also usage behaviour. However, there is no scientific information available on what performance and effort actually mean in the case of digital signatures. Therefore, this study aims to find the underlying meanings behind the performance of digital signature technologies as well as effort and ease of using digital signature technologies.

1.4 Research questions

This study will base on the presumption that performance expectancy and effort expectancy affect behavioural intention, which in turn is a strong predictor of use behaviour and look to study what performance and effort actually mean to the users of digital signature technologies. It is important to note that this study does not actually test the UTAUT model to predict usage of the technology, but rather uses the insights it has provided about performance and effort expectancy having strong effects on behavioural intention towards using a technology. Therefore, the research questions are as follows:

RQ 1: On what parameters do users perceive the performance of digital signature technologies after its adoption?
RQ 2: On what parameters do users perceive the ease and effort of using digital signature technologies after its usage?

The study will answer these questions by using qualitative methods. The data will be collected using semi-structured priori-theme interviews. The interview protocol is loosely based on the scales that Venkatesh et al. (2003) used in their study and development of the UTAUT model. The data will be analysed using conventional content analysis.

1.5 Structure of paper

This master's thesis is structured as follows. The second and third chapters provide a theoretical context for the study. In the second chapter the paper discusses digital signatures and the concepts related to that. It is important to understand the basis on which the legitimacy of the technology rests and therefore the first part of the chapter will go through the legislation regulating the technology. The scope of this thesis is limited to Finland, and therefore the laws in this case are set by EU directives and regulations. After introducing the legislation regulating the technology and services, the practical state of digital signatures is addressed. In this part the practicalities of digital signature, such as the signature process, digital authentication and identification are discussed.

The third chapter discusses technology acceptance and introduces the basis on which the research model lies. This chapter discusses the UTAUT model as well as its predecessors. The fourth chapter of this paper will go through the methodology of this study.

The fifth chapter presents the results of this study. The chapter is split into two sections, one for each of the research question, which in turn are split into smaller subsections that go through each of the subcategories of the study. The perceptions of users on factors that contribute to performance of the technology are efficiency, information security, flexibility, comparative performance, scalability functions and other factors. The factors that users perceive to contribute to ease and effort are service-specific user experience, information availability, comparative ease and contextual factors.

The sixth chapter is discussion, which consists of managerial implications, theoretical implications as well as limitations and suggestions for future research. In this chapter the different implications of the results will be discussed as well as presenting the different factors that limit this study. Suggestions for future research are also provided.

2 DIGITAL SIGNATURE TECHNOLOGIES (DST)

Digital signature (also eSignature, electronic signature) is an emerging digital alternative for handwritten signatures. The terminology is somewhat unclear as terms such as "digital signature", "electronic signature" and "eSignature" are used to describe the same phenomenon interchangeably, especially in everyday life.

Gamalielsson et al. (2015, 73) define digital signatures as "an implementation of asymmetric cryptography to ensure the integrity and authenticity of a document". The purpose of a digital signature is similar to that of a traditional handwritten signature, which is to prove the document's origin as well as the integrity of the document (Gamalielsson et al., 2015).

In EU legislation, electronic signature is defined as "data in electronic form which are attached to or logically associated with other electronic data, and which serve as a method of authentication" (EU regulation No 910/2014, 2014, Article 3). However, in some sources, such as the certificate policies of electronic identification service providers Telia Oyj and Elisa Oyj, a distinction is made between the terms "electronic signature" and "digital signature" (Elisa Oyj, 2014; Telia Oyj, 2017). In these documents, electronic signatures are defined as "A computer-readable signature of a person, or its equivalent, such as a digital signature, as evidence of a connection to a specific document or message associated with the signature to a specific person (Elisa Oyj, 2014). In everyday life electronic signature usually refers to digital signature…" (Elisa Oyj, 2014; DNA Oyj, 2017). Digital signatures, on the other hand, are defined as "An electronic signature made with the private key of a document or message signer in accordance with the public key method. In practice an encrypted hash of the message." (Elisa Oyj, 2014; DNA Oyj, 2017). Therefore, digital signatures can be viewed as a subset of electronic signatures that use specifically the public key method. However, as it is not necessary to differentiate between electronic and digital signatures for the purposes of this study, the term digital signature will be used as a reference to both of these definitions. This excludes the legislation chapter, in which the language used will be dictated by the law text.

In a digital signature standard published in the Federal Information Processing Standards Publication (FIPS PUB) by United States department of commerce, digital signatures are defined as "the result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation" (Kerry & Gallagher, 2013, 2).

Digital signatures hold a similar legal status to that of a traditional signature (EU regulation No 910/2014, 2014). While digital signatures have been recognized as a means to sign documents digitally since the 1990's (Brandner et al., 2002; EU directive 1999/93/EC, 2000), the literature about digital signatures consists mostly on either the technological aspects, such as Roy and Karforna (2012),

or implementation in different fields, such as Gamalielsson et al. (2015) and Brandner et al. (2002). In addition to scientific literature, information is available through technical service descriptions of different service providers such as Elisa Oyj (2014 & 2017) and DNA Oyj (2017), as well as governmental entities such as Traficom (2021) and Kerry & Gallagher (2013).

2.1 EU legislation on digital signatures

Due to the nature of electronic signatures as a means to sign documents, it is important to understand the legislation securing its status. Because this study focuses on digital signature technologies used in Finland, the legislation is dictated by the European Union. This chapter introduces the two most important pieces of EU legislation concerning the legal status of electronic signatures, as well as the definitions of different constructs in relation to electronic signatures. Within the European Union, the legal recognition of electronic signatures was first legislated by the EU directive 1999/93/EC (2000). The aims of the directive at the time were to make electronic signatures easier to use and to help them become legally recognised within all EU countries (EU directive 1999/93/EC, 2000). Directive 1999/93/EC was repealed in 2014 upon the introduction of regulation (EU) No 910/2014 (also called the eIDAS Regulation) of the European parliament and of the council. The need to reform the legislation on eSignatures was due to directive 1999/93/EC not delivering "a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions." (EU regulation No 910/2014, 2014).

2.1.1 Article 3: Definitions

Article 3 of eIDAS regulation provides definitions for key concepts around the topic of digital signatures. This subchapter will introduce the most important definitions and concepts that are relevant to understand for the scope of this study.

Electronic signatures are defined in the eIDAS regulation as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". Distinct from electronic signature are advanced electronic signature and qualified electronic signature. **Advanced electronic signature** which is defined as an electronic signature that meets four requirements: (1) "it is uniquely linked to the signatory", (2) "it is capable of identifying the signatory", (3) "it is created using means that the signatory can maintain under his sole control" and that (4) "it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable". **Qualified electronic signature** is defined as an advanced electronic signature that is created by a qualified electronic signature creation device, and

which is based on a qualified certificate for electronic signatures. (EU regulation No 910/2014, Article 3.)

The eIDAS regulation defines **electronic identification** as "the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;" (EU regulation No 910/2014, 2014). **Authentication** is defined as an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed". (EU regulation No 910/2014, Article 3.)

Certificate for electronic signature is defined as "electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person". The former is defined as "a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I" (EU regulation No 910/2014, Article 3). Annex I can be found in the appendices of this paper (Appendix 1).

Electronic signature creation device is defined as "configured software or hardware used to create an electronic signature". Electronic signature creation device also has a more sophisticated category of **qualified electronic signature creation device** which has to meet a number of requirements (EU regulation No 910/2014, 2014).

Trust service is defined as electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification, and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those service. (EU regulation No 910/2014, 2014).

Trust services are also divided into two categories, the first being trust service and the other qualified trust service. The Finnish law 1009/2018 regulates focuses on electronic identification and trust network in Finland. As it relates to electronic signatures, the trust network is a key part in the identifying process of the signatories. The law defines the trust network as the "network of service providers that have filed the notification to Finnish Transport and Communications agency" (SäädK, 1009/2018). In the law, it is stated that a public register of identification service providers and their services is maintained by to Finnish Transport and Communications agency Traficom (SäädK, 1009/2018).

The requirements for qualified trust service providers are provided in article 24. The public list of trust services (trusted list) in Finland is maintained by Traficom and as of May 2021, the only qualified provider with strong identification means available for users in Finland is the Population Register Centre (Traficom, 2021).

2.1.2 Article 8: Assurance levels of electronic identification schemes

eIDAS regulation (2014, Article 3) defines identification schemes as systems for "electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons". These electronic identification schemes are divided into three different categories by their level of assurance: low, substantial and high EU regulation (No 910/2014, 2014). Each of them has their own criteria which they have to meet:

Low: "assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;". (EU regulation No 910/2014, 2014, Article 8)

Substantial: "assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;" (EU regulation No 910/2014, 2014, Article 8).

High: "assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity." (EU regulation No 910/2014, 2014, Article 8).

The public list of trust services (trusted list) includes all of the registered trust services available in Finland, and includes the assurance levels provided by these services. All of the services providing strong identification means to users are labelled as assurance level substantial, with the exception of Finnish population centre, which offers high assurance level through providing citizen- and organisation certificates (Traficom, 2021).

2.1.3 Article 25: Legal effects of electronic signatures

Article 25 of eIDAS regulation is key in ensuring the status as an equal method of signing documents in relation to a handwritten signature: "An electronic sig-

nature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures." … "A qualified electronic signature shall have the equivalent legal effect of a handwritten signature" (EU regulation No 910/2014, 2014). Consistent with the single-market principle of the European Union, it also ensures that an electronic signature "based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States." (EU regulation No 910/2014, 2014).

2.1.4 Article 26: Requirements for advanced electronic signatures

Article 26 of the eIDAS regulation states the requirements for advanced electronic signatures. These are (1) "it is uniquely linked to the signatory"; (2) "it is capable of identifying the signatory"; (3) "it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control" (4) "it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable" (EU regulation No 910/2014, 2014).

2.2 Digital Signature technologies in practice

Digital signature technologies are used for the same purpose as traditional signatures (Gamalielsson et al., 2015; Roy & Karforma, 2012). Typically, digital signature algorithms consist of three different stages: key generation algorithm, signing algorithm and signature verification algorithm (Roy & Karforma, 2012). The key generation algorithm is used to select and output a private key and a public key that corresponds to the private key (Gamalielsson et al., 2015). The private key is chosen by random from a group of probable private keys (Roy & Karforma, 2012). A key is a parameter in cryptography that is used in determining the functional output of a cryptographic algorithm, or to put simply, cipher text (Roy & Karforma, 2012). The signature algorithm uses the message and the private key to generate a digital signature (Roy & Karforma, 2012). Finally, the signature verification algorithm, which is executed at the recipients end, is used to check the authenticity of the document based on the message, public key and the signature (Gamalielsson, 2015). The recipient receives the message along with the signature and the public key that is available in order to verify the authenticity of the message (Roy & Karforma, 2012). This is conducted by comparing the received signature with the calculated signature (Roy & Karforma, 2012).

This method, basing on asymmetric cryptography where the users have a pair of keys, public and private, is also called the public key method (Telia Oyj, 2017; Elisa Oyj, 2014). In the method, each user has two uniquely associated cryptographic keys (Elisa Oyj, 2014). The public key is available in a public repository, while the private key is held by the user of the keys. (Telia Oyj, 2017; Elisa Oyj,

2014; Kerry & Gallagher, 2013). The public key method is based on the public key infrastructure, which is established to issue, maintain and revoke public key certificates (Kerry & Gallagher, 2013).

In the case of digital signatures, the private key is used to calculate a digital signature that can be verified using the corresponding public key (Kerry & Gallagher, 2013). The private key can also be used to open messages encrypted with the public key and vice versa (Elisa Oyj, 2014). The public key, in the case of digital signatures, is used to verify digital signatures that were signed using a private key (Kerry & Gallagher, 2013).

A public key is a cryptographic key used with an asymmetric algorithm and is associated to a distinct private key (Kerry & Gallagher, 2013). According to Kerry & Gallagher (2013), the private key, also called a secret key is used in the public key method to make digital signatures that can be verified with the corresponding public key. They can also be used to open messages that are encrypted using the public key (Telia Oyj, 2017; Elisa Oyj, 2014). In the case of Finnish Mobile Certificate (Mobiilivarmenne), the private key is saved in the users SIM-card (Telia Oyj, 2017; Elisa Oyj, 2014).

According to Kerry & Gallagher (2013), digital signatures using the public key method offer a mechanism for verifying origin authentication, data integrity and signatory non-repudiation when properly implemented. Non-repudiation means that the integrity and authenticity can be proved using a certificate corresponding to the key (DNA Oyj, 2017).

2.2.1 Digital signature levels and authentication

A key feature of digital signature services is authentication. Authentication as an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed (EU regulation No 910/2014, 2014). As discussed in the earlier chapter, there are three levels to digital signatures in the eIDAS regulation which are determined by their authentication methods: simple, advanced and qualified (EU regulation No 910/2014, 2014). In practice, the simple electronic signature can be an tick box labelled as "I accept" on a website (Vähimaa, 2021). The second level of digital signatures is "advanced" and defined in the eIDAS regulation as an electronic signature that meets the following requirements: (1)"it is uniquely linked to the signatory", (2) "it is capable of identifying the signatory", (3) "it is created using means that the signatory can maintain under his sole control" and that (4) "it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"(EU regulation No 910/2014, 2014). In practice this means that the signatory has to be identified using either an identification card, banking ID's or a mobile ID (Vähimaa, 2021). The highest level of qualified digital signature is currently in Finland only possible using organisation cards granted by Digital and Population data services agency (DVV), and are not available for commercial use (Vähimaa, 2021). Therefore, when this study refers to digital signatures with strong authentication, it refers to digital signatures that satisfy the

criteria for Advanced Electronic Signature stated by eIDAS regulation. The term strong authentication refers to authentication that uses strong identification services.

Within Finland, a register of strong identification services providers is maintained by the Finnish transport and communications agency (Traficom, 2020). The register keeps track of the strong identification means available to users, strong identification brokerage to eServices, level of assurance and other details, such as contact details, links documents on identification principles and certificate policies et cetera. Currently the list contains 17 providers, which are mostly banking companies and telecommunications providers, with the exceptions of Finland's Population Register Centre (in Finnish: Väestörekisteri), Idemia Identity & Security France and digital identity and signature service Signicat (Traficom, 2021).

The strong identification methods are available to consumers through banks and telecommunications providers. These means are either mobile certificates (in Finnish: mobiilivarmenne) provided by telecommunications providers or Bank ID's provided by banks (Traficom, 2021). Separate from these are the means provided by the population register centre, which provides citizen certificates and organisation certificates (Traficom, 2021).

In the mobile certificate (also called Mobile ID) service, a person's certificate of identity is attached to a SIM-card used in a mobile device (Elisa Oyj, 2017). The Mobile certificate service is based on X.509 certificates and the public key method, where the private keys related to the certificates are on the SIM-card protected by a PIN-code (Elisa Oyj, 2017; DNA Oyj, 2017). The mobile certificate uses an electronic unique identification number (Sähköinen asiointitunnus, SATU) provided by the digital and population data services agency of Finland (Digi- ja väestötietovirasto, DVV) as the identification data uniquely representing the person (Elisa Oyj, 2017; DNA Oyj, 2017). When applying for a mobile certificate, the initial identification of the applicant is conducted either using a bank ID or in person using a passport or an identity card (Elisa Oyj, 2017; DNA Oyj, 2017).

The Bank ID's as a means for electronic identification is based on the banking credentials that are granted to a person by banks (Danske Bank, 2019; OP-Palvelut Oy, 2020). The initial identification for the banking credentials is conducted using a valid, police issued identification document, an ETA member (or Swiss or Sammarinese) nation issued passport or an identification document that can be used as a travel document (OP-Palvelut Oy, 2020;. Danske Bank, 2019). In case the applicant does not have an acceptable document, the police can also take care of the identification process (OP-Palvelut Oy, 2020;. Danske Bank, 2019).

These providers of strong identification services provide their identification as a service to a number of service providers in different industries that need to identify their customers. These include also many of the digital signature service providers in Finland. They are also very widely adopted among the population of the country.

2.2.2 Digital signatures from the users' point of view

Currently there are several providers of digital signature services available in the Finnish market, both Finland-based and international. While many of them offer a similar product in terms of digital signatures, they services differentiate in other features, such as archiving solutions, available methods of identification and authentication and customisable document templates. Some services also aim to cater to a specific industry, such as real-estate companies. Digital signatures have steadily become more common, and as of May of 2020, 1,5 million users had signed documents using just Visma Sign, which is one of the service providers in Finland (Visma Solutions, 2020).

Generally, the signature process in digital signature services used in Finland follow roughly the following steps: the party collecting the signatures sends an invitation to sign a document to the signatory. Common mediums for this invitation are email and SMS. Next, the signatory opens the invitation, which he or she has received. To open the document, the user often must provide some form of credentials, such as a password provided by the sender of the invitation. After accessing the document, the signee can observe it.

To proceed to signing the document, the signatory uses a method of identification that depends on the service used and the methods that the sender has chosen to allow. This can be a combination of email and password at lightest, in which case the assurance level of the identification scheme is low, but commonly the services aim to use a method that provides a substantial assurance level such as Mobile Certificate or Bank ID. In Finland, Bank ID's are the most popular means to strong authentication. The strong authentication is the digital equivalent of showing one's identification card. The action of signing itself can be completed by clicking a button or drawing a signature with a computer mouse. Once all the signing parties have signed the document, it is available for archiving. Depending on the service used, the document can be archived in the service and/or downloaded and saved on one's own device. The archiving services are one of the differentiating points of these services as some services offer long term archiving while others do not provide archiving at all. The services typically save identification data, such as ip-addresses and timestamps that can be used afterwards to verify the genuineness of the signature. (Vähimaa, 2021.)

The popularity of digital signing increased rapidly due to the covid-19 pandemic that forced limitations on contacts between people (Visma Solutions, 2020). According to Visma Solutions (2020), the number of signatures made using their service Visma Sign doubled in just ten weeks after the lockdowns brought forward by the pandemic.

The number of studies about the user acceptance of digital signatures is fairly limited. Haryanto, Gandhi and Sucahyo (2020) used an integrated framework technology acceptance model (TAM) and technology-organisation-environment to identify seven driving factors of digital signature utilisation are security protection, internal need, training and education, government policy, vendor support, perceived ease of use and perceived usefulness.

3 TECHNOLOGY ACCEPTANCE, UTAUT MODEL AND RESEARCH FRAMEWORK

Technology acceptance is a one of the mainstream fields of study in information systems research. The field of technology acceptance studies how and why individuals adopt new information technologies (Venkatesh et al., 2012; Venkatesh et al., 2003). Theoretical models concerning technology acceptance and use have been developed from the fields of psychology and sociology (Venkatesh et al., 2012). This study bases its theoretical model on the presumptions set by work of Venkatesh et al. (2003) and their unified theory of acceptance and use of technology (UTAUT) as well as the technology acceptance research before that. In this chapter the models that preceded the UTAUT model will be shortly introduced before moving on to the UTAUT model and two of its main constructs: performance expectancy and effort expectancy as well as the research model of this study (Figure 2).

3.1 Predecessors of UTAUT model

3.1.1 Theory of reasoned action

The theory of reasoned action (TRA) was created by Fishbein and Ajzen in 1975 (Davis et al., 1989). The theory drew from social psychology and was applied to technology acceptance by Davis et al. (1988). TRA is one of the most well-researched intention models and has been successfully applied to explain behaviour in a wide variety of domains (Davis et al., 1989). TRA argues that behavioural intention determines whether a person performs a specified behaviour (Davis et al., 1989). Behavioural intention is defined as "a measure of the strength of one's intention to perform a specified behaviour (Davis et al., 1989, 984). Behavioural intention is determined by attitude and subjective norm towards the specified behaviour (Davis et al., 1989; Venkatesh et al., 2003). The subjective norm refers to the opinions of peers about whether an individual should perform a behaviour (Venkatesh et al., 2003). TRA is credited as one of the first groundbreaking technology acceptance models and was found to perform quite well in predicting behaviour (Sheppard et al., 1988).

3.1.2 Technology acceptance model

The technology acceptance model (TAM) was introduced by Davis and is an adaptation of TRA (Davis et al., 1989). The goal of the model was to provide an explanation of the determinants of computer acceptance with sufficient explanatory power across different technologies and populations (Davis et al., 1989).

TAM shares the constructs of behavioural intention and attitude toward using with TRA but does not include the construct subjective norm (Davis et al., 1989; Venkatesh, 2003). TAM also introduces three new constructs that are not included in TRA: perceived usefulness, perceived ease of use and external variables (Davis et al., 1989). Perceived usefulness is determined by the perceived ease of use and external variables (Davis et al. 1989). Therefore, while also distinct constructs, perceived usefulness and perceived ease of use are also associated (Davis et al., 1989). Perceived usefulness is also affected by external variables, such as design characteristics (Davis et al., 1989).

3.1.3 Motivational model

The motivational model explains the performance of an activity basing on two constructs: intrinsic motivation and extrinsic motivation (Davis et al., 1992). The former construct, extrinsic motivation, can be classified as performance an activity to achieve outcomes of value that are separate from the activity itself. Such valuable outcomes may be improved job performance, bonuses, pay etc. (Davis et al., 1992). The latter construct, intrinsic motivation, can be classified as performing an activity for no other reinforcement other than one's enjoyment (Davis et al., 1992). They applied the motivational model to their user acceptance studies where they studied the effects of perceived usefulness (extrinsic) and enjoyment (intrinsic) on computer usage in workplace.

3.1.4 Theory of planned behaviour

Theory of planned behaviour (TPB) is an intention model that can be considered an extension to TRA (Venkatesh et al., 2003). In addition to the constructs of TRA (Attitude toward behaviour, subjective norm, intention, behaviour), the TPB introduced an additional construct: perceived behavioural control (Ajzen, 1991). Perceived behavioural control refers to the ease or difficulty related to performing a behaviour (Ajzen, 1991). Taylor and Todd (1995b) tested and compared two different versions of TPB (traditional and decomposed) with TAM based on usage of a computing resource centre by business school students. The decomposed TPB differs from the already introduced version so that the constructs of perceived behavioural control, subjective norm and attitude are further broken down into constructs (Taylor & Todd, 1995b). Attitude was broken down into compatibility, ease of use and perceived usefulness (Taylor & Todd, 1995b). The construct of subjective norm is further decomposed into the constructs of peer influence and superiors influence (Taylor & Todd, 1995b). The construct of perceived behavioural control is further decomposed into self-efficacy, resource facilitating conditions and technology facilitating conditions (Taylor & Todd, 1995b). In their study, Taylor and Todd (1995b) found that both versions showed improvement over TAM in explanatory power for the behavioural intention, and therefore actual behaviour.

3.1.5 Combined TAM & TPB

Taylor and Todd (1995a) argued that TAM had two critical shortcomings: it is unclear whether TAM predicts behaviour for inexperienced users and that it is unclear whether the determinants of IT-usage are same for experienced and inexperienced users. In order to study these issues, Taylor and Todd (1995a) used an augmented version of TAM (to which Venkatesh et al. (2003) refer to as "combined TAM & TPB") which took into consideration social influences and behavioural control. Taylor and Todd (1995a) found that the augmented version of TAM can be used to predict behaviour for users with no prior experience with a system, they also found that the amount of experience causes differences in the relative influence of the determinants of usage.

3.1.6 Model of PC Utilization

While lot of the previous theories, such as TAM and its adaptations had leaned on Fishbein's and Ajzen's TRA, Thompson, Higgins and Howell (1991) based their model of PC utilization (MPCU) on a competing theory by Triandis (1971) that argued that behaviour is determined by attitudes, social norms, habits and expected consequences of the behaviour in question (Thompson et al., 1991). In his theory, attitudes refer to what people would like to do, social norms refer to what people think they should do and habits refer to what people usually do (Thompson et al., 1991). Thompson et al. (1991) used Triandis' theory as a base for their model of PC utilization (MPCU) attempting to explain the factors affecting PC usage. Thompson et al. (1991) tested a subset of Triandis' model and focused on the direct effects of social factors, affect, perceived consequences and facilitating conditions on behaviour. Unlike most of the previously discussed theories and models, they decided to exclude behavioural intention because their interest was in actual behaviour (Thompson et al., 1991). According to MPCU, the factors determining the utilisation of PCs are long term consequences, job fit, complexity, affect, social factors and facilitating conditions (Thompson et al., 1991). In their model, the construct of perceived consequences is further broken down into the constructs of complexity, job fit and long-term consequences (Thompson et al., 1991).

3.1.7 Innovation diffusion theory

Innovation diffusion theory (IDT) had been used to study a number of innovations in many different contexts, such as agricultural tools and organisational innovations before making its way to the field of information technology (Venkatesh et al., 2003). In 1991, Moore and Benbasat (1991) adapted it to study individual technology and were able to find support for the validity of the innovation characteristics presented in the theory (Venkatesh et al., 2003). The adaptation of IDT by Moore and Benbasat (1991) focuses on the perceived characteristics of us-

ing an innovation. They argued that the findings of studies focusing on the primary characteristics of innovations had been inconsistent and that perceptions about these characteristics are a stronger predictor of behaviour than the characteristics themselves (Moore & Benbasat, 1991). It is important to note that differing from the original IDT by Rogers, Moore and Benbasat (1995) focused on the perceptions of using an innovation instead of focusing on the perceptions about the innovation itself. For their adaptation of IDT, Moore and Benbasat (1991) chose to include seven different constructs: relative advantage, ease of use, image, visibility, compatibility, results demonstrability and voluntariness of use.

3.1.8 Social cognitive theory

Social cognitive theory (SCT) is a theory on human behaviour and regarded as one of the most powerful theories of its respective field of study (Compeau & Higgins, 1995b; Venkatesh et al., 2003). The theory is based on the premise that environmental influences and personal factors are reciprocally determined (Compeau & Higgins, 1995b). Environmental influences in this case may be social pressures or unique situational characteristics while personal factors can include characteristics such as personality or demographic characteristics (Compeau & Higgins, 1995b). This means that a person influences the environments it chooses to exist in while also being influenced by these environments (Compeau & Higgins, 1995b). Thirdly, cognitive and personal factors influence behaviour while the behaviour also effects said factors (Compeau & Higgins, 1995b).

Compeau and Higgins (1995a) applied social cognitive theory their studies on studying computer skills as well as studying the role of computer self-efficacy (an individual's belief about their ability competently use computers) in determining computer utilisation (Compeau & Higgins, 1995b). Compeau and Higgins (1995a) applied social cognitive theory their studies on studying computer skills as well as studying the role of computer self-efficacy (an individual's belief about their ability competently use computers) in determining computer utilisation (Compeau & Higgins, 1995b). The core constructs of their revised model included nine core constructs: encouragement by others, others use, support, computer self-efficacy, outcome expectations about performance, outcome expectations – personal, affect, anxiety and usage (Compeau & Higgins, 1995b). The study found that self-efficacy had an important role in determining feelings and behaviours. Individuals with high self-efficacy were found to use computers more, enjoyed the computer use more and had less anxiety (Compeau & Higgins, 1995b). The study also found that the outcome expectations had a significant impact on affect and computer use – especially the expectations concerning job performance (Compeau & Higgins, 1995b)

3.2 Unified theory of acceptance and use of technology (UTAUT)

UTAUT was created in 2003 in an effort to integrate the best elements of the previously introduced models and form a unified model (Venkatesh et al., 2003). The need for this unification stemmed from the fragmentation of theory and research on individual acceptance of information technology (Venkatesh et. al, 2003). The model used elements from eight previously constructed theories: TRA, TAM, MM, TPB, MPCU, IDT and SCT (Venkatesh et al. 2003).

The research model (Figure 1) that Venkatesh et al. (2003) created consisted of eight constructs that had been found to be significant determinants of intention or usage in previous studies. These constructs were performance expectancy, effort expectancy, social influence, facilitating conditions, gender, age, experience and voluntariness of use (Venkatesh et al., 2003). In their model, they hypothesised that four of these constructs, (performance expectancy, effort expectancy, social influence and facilitating conditions) have a direct effect on behavioural intention or actual usage, while the four others (gender, age, experience and voluntariness) are acting as moderators, having an effect on these relationships (Venkatesh et al., 2003).

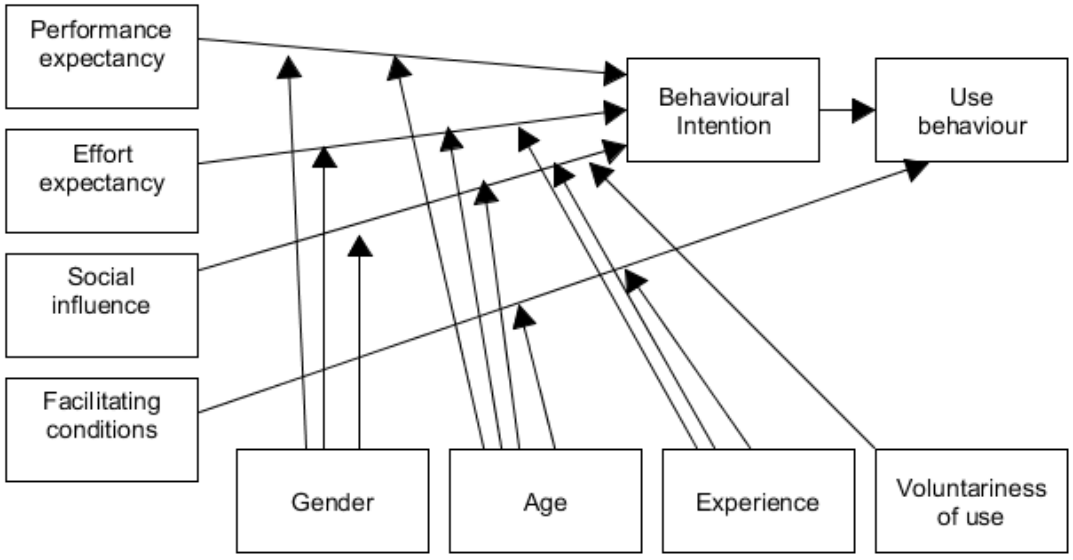

Figure 1 UTAUT model (Venkatesh et al., 2003)

Venkatesh et al. (2003) found strong empirical support for their theory. In the UTAUT model, there are three direct determinants of intention to use: performance expectancy, effort expectancy and social influence (Venkatesh et al., 2003). In addition, there are two direct determinants of usage behaviour: intention to use and facilitating conditions (Venkatesh et al., 2003). In addition to the direct determinants, UTAUT also includes four moderators: experience, voluntariness,

gender and age (Venkatesh et al., 2003). The UTAUT provided a significant improvement to the explanatory power of the previous models that had been created; it was able to explain 70% of variance in usage intention (Venkatesh et al., 2003). The researchers conducting the study were also satisfied with the simplification that was achieved through integrating the original 32 main effects from the eight theories used into four main effects as determinants of intention and behaviour (Venkatesh et al., 2003).

3.2.1 Performance expectancy

In the UTAUT model, performance expectancy is constructed basing on five root constructs applied from previously introduced theory. These are perceived usefulness (TAM), extrinsic motivation (MM), job-fit (MPCU), relative advantage (IDT) and outcome expectations (SCT) (Venkatesh et al., 2003).

The construct of perceived usefulness stems from the technology acceptance model (TAM) and is defined as "the prospective users subjective probability that using a specific application system will increase his or her job performance within an organisational context" (Davis et al., 1989, 985).

The construct of extrinsic motivation is adopted from the motivational model (MM). Davis et al. (1992, 1112) define extrinsic motivation as "performance of an activity because it is perceived to be instrumental in achieving valued outcomes that are distinct from the activity itself, such as improved job performance, pay or promotions".

The construct of job-fit is adapted from the model of PC utilisation (MPCU) and defined as "the extent to which an individual believes that using can enhance the performance of his or her job" (Thompson et al., 1991, 129)

The construct of relative advantage is adapted from the innovation diffusion theory (IDT) and defined as "the degree to which an innovation is perceived as being better than its precursor" (Moore & Benbasat, 1991, 195).

Venkatesh et al. (2003, 447) used these root constructs to define performance expectancy as "the degree to which an individual believes that using the system will help him or her to attain gains in job performance." In each of the theories that were used in the birthing of UTAUT, construct corresponding with performance expectancy was the strongest predictor of intention (Venkatesh et al., 2003).

As stated, Venkatesh et al. (2003) found that performance expectancy has an effect on behavioural intention which is moderated by gender and age. This moderation works in a manner, which makes this effect stronger for men and younger individuals (Venkatesh et al., 2003).

The different items Venkatesh et al. (2003) used to measure performance expectancy were typically statements that were graded based on level to which the subjects agreed or disagreed with it. In estimating the UTAUT model, the following items were used as scales that were graded on a seven-point scale:

1. I would find this system useful in my job.

2. Using the system enables me to accomplish tasks more quickly.
3. Using the system increases my productivity.
4. If I use the systems, I will increase my chances of getting a raise.

(Venkatesh et al., 2003, 460)

To study what features contribute to the users perceptions about performance of digital signature technologies, the first research question will be "on what parameters do users perceive the performance of digital signature technologies after its adoption?".

While the term "performance expectancy" in UTAUT model is defined as the "degree to which an individual believes that using the system will help him or her to attain gains in job performance" (Venkatesh et al., 2003, 447), this study will extend the definition from job performance to task performance. This is to accommodate the fact that many users use digital signature technologies in non-work situations. The research model is presented in figure 2.

3.2.2 Effort expectancy

In UTAUT model, the construct of effort expectancy is constructed basing on three previous models: perceived ease of use (TAM), complexity (MPCU) and ease of use (IDT) (Venkatesh et al., 2003).

The construct of perceived ease of use is adapted from the technology acceptance model (TAM) and defined as "the degree to which the prospective user expects the target system to be free of effort" (Davis et al. 1989, 985).

The construct of complexity is adapted from the model of PC utilisation and defined as the "the degree to which an innovation is perceived as relatively difficult to understand and use" (Thompson et al., 1991, 128).

The construct of ease of use is adapted from innovation diffusion theory and defined as "the degree to which an innovation is perceived as being difficult to use" (Moore & Benbasat, 1991, 195).

These root constructs were used to create the construct of effort expectancy as "the degree of ease associated with the use of the system (Venkatesh et al., 2003. p. 450). In each of the models the construct corresponding with the UTAUT models ease of use was found significant in both mandatory and voluntary usage contexts (Venkatesh et al., 2003). However, these effects weakened over extended periods of sustained usage (Venkatesh et al., 2003).

Venkatesh et al. (2003) found that effort expectancy has an effect on behavioural intention. This effect is moderated by gender, age and experience (Venkatesh et al., 2003). The effect of effort expectancy on behavioural intention was found to be stronger for women, older workers and those with limited experience (Venkatesh et al., 2003).

The different items Venkatesh et al. (2003) used to measure performance expectancy were typically statements that were graded based on level to which

the subjects agreed or disagreed with it. In estimating the UTAUT model, the following items were used as scales that were graded on a seven point scale:

1. My interaction with the system would be clear and understandable
2. It would be for me to become skilful at using the system
3. It would be easy for me to become skilful at using the system
4. I would find the system easy to use
5. Learning to operate the system is easy for me

(Venkatesh et al., 2003, 460)

To study what features contribute to the users' perceptions about ease and effort related to use of digital signature technologies, the second research question will be "on what parameters do users perceive the ease and effort of using digital signature technologies after its usage? **".** The research model is presented in figure 2.

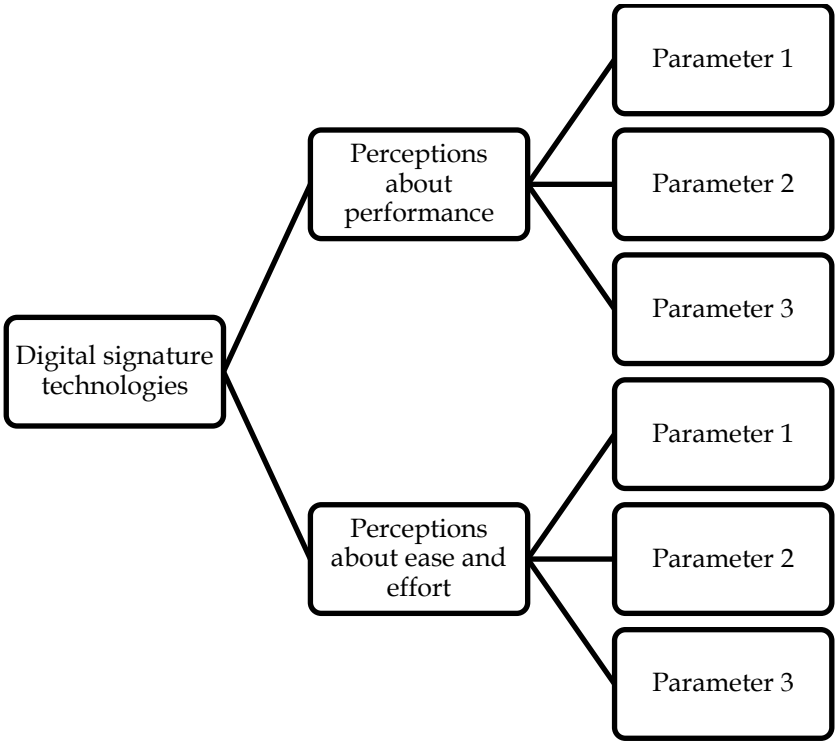

Figure 2 Research model

4 METHODOLOGY

This chapter discusses the methodology used in this research. In the first part I will describe the qualitative methods and especially my chosen mode of qualitative research, which is phenomenological study. After that I will discuss the interview methods and the sampling. Finally, the interview processes and the data analysis are described.

4.1 Qualitative methods

This study uses conventional content analysis which is a qualitative research method. Qualitative methods differ from quantitative methods in the nature of the data, relevance of context, nature and control of potential causes and key research instruments (Belk et al., 2012, 3; Tuomi & Sarajärvi, 2009, 71). While quantitative methods process responses into numeric scores, qualitative methods use richly detailed data, such as visual and verbal recordings (Belk et al., 2012, 3). Context is also more relevant in qualitative research, as the data is often gathered from a very specific setting the data is also assumed to be time-, place, people- and culture specific (Belk et al., 2012, 3). Qualitative research is also naturalistic, meaning that data collection usually takes place in the natural settings where people spend time, such as workplaces or live, instead of controlled settings, such as laboratories (Belk et al., 2012, 4). Lastly, where the quantitative methods aim to minimise the impact of the researcher on the data, in qualitative research is the fact that the researcher and his or her skills are the research instrument (Belk et al., 2012, 4). This means that the researcher has a significant role in building trust or asking questions that may not have been anticipated prior to the interview (Belk et al., 2012).

While quantitative research is best suited to measuring numerically quantifiable variables and relations between them, qualitative research can identify underlying reasons for these relations (Belk et al., 2012, 5). Qualitative research has had a role in marketing research since the 1930's and has since been used widely (Belk et al., 2012, 8). While qualitative researchers faced criticism arguing that scientific knowledge relies on quantitative methods, the criticism has since waned and the top journals have accepted numerous qualitative papers (Belk et al., 2012, 10).

This study will use methods associated to the hermeneutic phenomenological tradition of qualitative research. Phenomenology often focuses on meanings of people's individual experiences in a certain experiential context (Belk et al., 2012, 21; Tuomi & Sarajärvi, 2009, 34). Phenomenological research does not seek to find universal understanding of phenomena, rather seeking for deep understanding on a very specific phenomenon (Belk et. al, 2012, 21). Through gathering

personal perspectives of a phenomenon, phenomenological study can attempt to aggregate individual perspectives or provide a structured way of understanding differences (Belk et al., 2012, 21). Hermeneutic phenomenological research can also be called interpretative because the hermeneutic dimension of phenomenological research is extracted through the necessity for interpretation Tuomi & Sarajärvi, 2009). Because the research questions of this study focus on the experiences of individuals using digital signature services, I have decided that my research methods will follow the phenomenological tradition of qualitative research.

It is important to note that while this study bases on the presumptions established by the quantitatively measured UTAUT model, this study does not aim to predict usage or use the UTAUT model. Instead, through using qualitative methods, the goal is to find aspects specific to digital signature technologies that factor into the perceptions of the interviewees about performance and effort of using the technologies.

4.2 Data collection & sampling

The method chosen for the data collection is semi-structured priori-theme interviews. Theme interviews are closely related to deep interviews and follow certain central themes chosen in advance and related follow-up questions (Tuomi & Sarajärvi, 2009, 75). Theme interviews emphasise the interpretations and meanings that people give to objects and phenomena and how they are constructed (Tuomi & Sarajärvi, 2009, 75). It is not obligatory to ask all informants all off the questions, or to ask them in the same order or form (Tuomi & Sarajärvi, 2009, 75). The questions, however, should aim to find meaningful answers to research questions, and the themes should be based on the context of the research and previous knowledge of the phenomenon in question (Tuomi & Sarajärvi, 2009, 75). Due to the ongoing pandemic, data collection will in most part be conducted via online meetings using tools such as Google Meet, Zoom or Skype. While it does not provide the intimacy of face-to-face interviews, it provides opportunities for interviewing people in a larger geographical area and makes recording the interviews easier. As most of the interviewees, as well as the researcher, are native Finnish speakers, all but one of the interviews will be conducted in Finnish. The one interview that is not conducted in Finnish is conducted in English.

The data used in this research was collected from seven interviews. Because qualitative research does not aim to provide statistical generalisations but rather to describe a phenomenon or understand a certain behaviour, it is important that the informants used for data collection are informed or experienced in the subject of study (Tuomi & Sarajärvi, 2009, 85). Therefore, the sample of informants used in this research is limited to people who have used digital signatures in within the last two years.

It should also be noted that while the sampling successfully was able to reach a variety of experience levels of digital signature users, it is demographically very homogenous, with all of the interviewees being male and in the 25-34 age group (Table 1).

Table 1 The interviewee sample

Interviewee	Gender	Age	Frequency of usage	Purpose of use
P1	Male	25-34	Occasional - less than monthly	Employment contracts
P2	Male	25-34	Monthly	Employment contracts, consent letters, etc.
P3	Male	24-34	Weekly	Work: sales contracts Personal: bank & insurance documents
P4	Male	24-35	Daily	Work: Documents in the bank sector, documents in the real-estate
P5	Male	24-36	Weekly	Work: Contracts, meeting reports Personal: Meeting reports
P6	Male	25-35	Occasional	Employment contracts, consent letters for thesis.
P7	Male	25-34	Occasional	Employment contracts etc.

4.3 Interview protocol

The interview protocol (Appendix 2) for data collection was developed basing on the questionnaire that Venkatesh et al. (2003) used to measure the constructs of performance expectancy and effort expectancy. The questions about performance and effort expectancy included aspects that Venkatesh et al. (2003) included in their scales when measuring these constructs. These scales were presented for each of the respective constructs in chapters 3.2 and 3.3. While Venkatesh et al. (2003) measured these scales quantitatively on a seven-point scale in a questionnaire to develop their model and used statements such as "using the system in my job would increase my productivity", this study looks to find answers to "how" and "why" using a system, in this case a digital signature technology, increases or decreases the interviewees productivity. Being a semi-structured interview, the questions are not limited to those in the interview protocol, and a lot of follow-up questions will be asked in order to gain insights about the interviewee's perceptions.

The questionnaire consists of four sections. The first section is the background questions, where the experience of the interviewee on the topic is

mapped, as well as the general impressions about using the technologies. In this section the users are also asked to reminisce the process that they have gone through in using the technology to bring the topic into their mind before going deeper into the questions about performance and ease and effort. The second section consists of questions about performance expectancy and the third section consists of questions about effort expectancy. In addition to the questions in the protocol, the answers may be followed up with questions about the previous answer, such as "why is this important" etc. After the third section, the interviewees are asked whether they have anything to add to the previous topics that have been discussed that they may feel that have not yet been discussed. In addition to the question sections, the interview will be started by going through the interviewees' rights to anonymity and the topics of the interview.

4.4 Data analysis

According to Belk et al. (2012, 138), the essence of data analysis in qualitative research consists of looking for patterns. These patterns can be seen due to the nature of the research questions while other may arise from familiar theoretical frameworks (Belk et al., 2012, 138). The method of data analysis used in this study is conventional content analysis.

Conventional content analysis is a method used to describe a phenomenon (Hsieh & Shannon, 2005). According to Belk et al., (2012, 139) coding refers to discerning small elements in data that can retain meaning if lifted out of context. Codes are concepts that vary in concreteness, abstractness and their emic/etic nature (Belk et al., 2012, 139). "Emic" means that the language used is drawn from the people studied, while etic means that it is not necessarily drawn from the people studied, but otherwise seem appropriate (Belk et al., 2012, 140).

Coding can be described as reducing data into meaningful segments and assigning names for them (Belk et al., 2012, 141) In essence codes have five main purposes: (1) they are internal notes, (2) they parse together what the researcher thinks the material is about, (3) they help in describing the text, (4) they act as a testing instrument for parsing material and (5) they can be used to find and check certain parts if the text (Tuomi & Sarajärvi, 2009, 92). The codes are intended to illustrate what is meant by identifying meaningful units of data and they can be assigned to individual words, sentences, paragraphs or any portion of text varying in length (Belk et al., 2012, 141). The coding process leaves out the uninteresting parts of the materials and separates the coded parts from the rest of the materials (Tuomi & Sarajärvi, 2009, 92).

In conventional content analysis the coding process begins with obtaining a sense of the whole material, in this case the transcribed interviews, and highlighting exact phrases from the data that captures key thoughts or concepts (Hsieh & Shannon, 2005). In essence this means getting rid of everything that is not relevant to the research (Tuomi & Sarajärvi, 2009, 109). The researcher then

makes notes about the impressions that the material has brought up and looks for similarities in these codes (Hsieh & Shannon, 2005; Tuomi & Sarajärvi, 2009, 110). As this process moves forward, these similar codes can be assigned into meaningful clusters that form subcategories (Hsieh & Shannon, 2005; Tuomi & Sarajärvi, 2009, 110). These clusters form a basis for the framework of the research (Tuomi & Sarajärvi, 2009, 110). These subcategories will then be further abstracted into a smaller number of categories as many times as possible, forming a hierarchical structure (Hsieh & Shannon, 2005; Tuomi & Sarajärvi, 2009, 112). An example of the abstracting process can be seen in table 2.

Table 2 An example of abstracting the data

Quote	Code	Subcategory	Main category	Unifying category
P: "Step-by-step guides to signing make use easy"	Step-by-step guide	Usage guides	Information availability	Users' perceptions about factors contributing to ease and effort of digital signature technologies

5 RESULTS

5.1 Digital signature users' perceptions on performance of digital signature services

The first research question sought to examine the different aspects that users perceive to affect the performance of digital signing. The sentiments about the performance of the technology were overall very positive. Through content analysis, five main themes were extracted from the interviews: efficiency, information security, convenience, comparative performance, scalability functions. In addition to five main themes, a category of "other factors" was formed to accommodate topics that were discussed but did not fit other categories nor were not prevalent enough to justify their own main themes. The main and subcategories are presented in table 3.

Table 3 The main categories and subcategories of digital signature users' perceptions o performance of digital signatures

Digital signature users' perceptions on performance of digital signature services	**Efficiency of digital signatures**	Saving time
		Saving effort
		Job performance
	Information security of digital signatures	Sense of Security
		Certainty of identity
		Authentication
	Convenience of digital signatures	Non-site-specificity
		No need for tools
		Document management
		Cross device access
	Comparative performance	Performance in comparison to alternative methods
	Scalability functions	Acceptance in government institutions
		Integration with other systems
	Other factors	Sustainability
		Pandemic

5.1.1 Efficiency

The first main theme of users' perceptions on performance of digital signatures is efficiency. This main theme is further divided into saving time, saving effort and job performance. The subcategories of efficiency of digital signatures and examples of statements matching them are presented in table 4.

Table 4 The subcategories of efficiency of digital signatures

Main category	**Subcategory**	**Example**
Efficiency of digital signatures	Saving time	*The key benefit is time efficiency. There are only a certain number of hours in a day. (P4)*
	Saving effort	*With digital signature, when I've needed to sign a contract I can take care of it right away without looking at a calendar and booking a meeting.* (P1)
	Job performance	*Digital signatures help me save time and therefore take care of more customers and improves results.* (P4)

The first subcategory of efficiency is saving effort. This subcategory included a number of ways that the interviewees felt that the technology had helped them in avoiding effort.

> *If I have a stack of documents that I need to sign, I can just use my mobile device and computer to sign instead of having to print a paper, sign it and scan it. (P7)*

> *In my former job we didn't have a digital signature service in use. I would send a contract to a customer who then printed it, signed it, scanned it and emailed it back. After that, since I didn't have a printer available, I would travel to my university, print the document, sign it, scan it, then email it from my university mail to my job mail and then send the final copy to the customer. It was very slow and arduous. (P3)*

In the first example, the interviewee discusses the saved effort in comparison to the alternative method of signing documents remotely without using a digital signature service. The second example is a fairly extreme example of the effort

required to sign documents remotely without a digital signature service. The sequence of printing, signing, scanning and mailing the document was brought up in multiple interviews as the alternative solution to signing documents remotely. This particular example also overlaps with the other main theme of comparative performance which is to be discussed later.

> *With digital signature, when I've needed to sign a contract I can take care of it right away without looking at a calendar and booking a meeting.* (P1)

> *I don't need to book a meeting with customer just for a signature. I can, for example, send the documents the night before for tomorrows transaction. Then the customer of course needs to take care of the rest.* (P4)

> *It is customer friendly that the customer doesn't need to travel from who-knows-where just to sign a paper.* (P4)

In these two examples the interviewees discuss how digital signature has eliminated the need to book appointments just for signing a document. In the third document the interviewee also brings up the effort saving for the other party.

> *I had to move forward quickly with my research and other things, so it was essentials that I didn't need to spend weeks on hunting down signatures and collect a stack of papers (*P6)

In this example the interviewee discusses how digital signature helped him avoid the effort of collecting physical signatures for consent letters in his research work from his interviewees, whom he had interviewed remotely.

The second subcategory of efficiency is saving time. Quickness was also one of the key benefits of digital signatures for the interviewees.

> *I only have a certain number of hours in a day. It helps save time when I don't need to invite customers over for signing and back office can just send the papers for digital signing and once they are signed they are sent for me* (P4)

> *The whole process is faster in comparison to for example mailing a document. If the document is going abroad the process can take more than a week* (P2).

In these examples the interviewees bring up the timesaving aspect of digital signatures. The first example discusses saving time in work context while the second example is more general.

The third and final subcategory of efficiency is job performance. While it is closely related to both timesaving and effort saving, it was a topic that many interviewees discussed.

> *Digital signatures help me save time and therefore take care of more customers and improves results.* (P4)

> *I would say that digital signatures increase productivity because you can do it quickly in between tasks and then have more time for other things* (P2)

In these examples the interviewees state that digital signatures help them be more productive. In the first example the interviewee sees a direct cause-effect relation between using digital signatures and improving job results. The second example takes the view that digital signing is handy because it can be done between other tasks. However, there were also some sceptical viewpoints towards improvement of job performance

> *I don't know if it truly increases my productivity if I use the saved time in rolling my fingers, but at least I can pretend to be more productive. (*P5)

> *Saying that I'm more productive because of digital signing is a rather extreme statement because in the end it is just a small moment, a drop in a bucket of my time. (*P1)

While both of these examples do take the saved effort and time into account, they downplay the improvements in their productivity and job performance. In their opinion the increases are rather small.

5.1.2 Information security

The second main theme of users' perceptions on performance of digital signatures is information security. The subcategories that the category of information security was divided into consisted of authentication, certainty of identity and sense of security. The subcategories of information security of digital signatures and examples of statements matching them are presented in table 5.

Table 5 The subcategories of information security of digital signatures

Main category	Subcategory	Example
Information security of digital signatures	Authentication	*When you think about digital signatures in professional use, strong authentication is the only option. (P5)*
	Sense of Security	*In Adobe Sign there was nothing that would express that it was a valid signature by a specific person or anything that specifies the signatory. Therefore, I did not find it trustworthy (P6)*
	Certainty of identity	*Knowing who the signatory is, is everything when it comes to signatures in general. You should be able to be sure that the signature is from that person who you have wanted it from. (P6)*

The most prevalent of the topics was authentication. The topic of strong authentication also overlaps with both other subcategories under the information security theme. Most of the interviewees had used digital signing methods that used a strong authentication method (Bank ID's or Mobile ID's). The users that had used digital signatures with strong authentication, especially those that used the technology professionally, were adamant that it is an essential part of the technology. Strong authentication was favoured over other means of authentication:

> *When you think about digital signatures in professional use, strong authentication is the only option. (P5)*

> *Strong authentication is the only way I would like to sign digitally when handling my personal information. (P7)*

In both of these examples the interviewees express that they would not like to use any other authentication method but the strong authentication. The strengths of strong authentication were it's security, proving power of the identity and it's ease:

> *I feel that strong authentication is the safest and the easiest method. I could feel that other means would require more technical understanding and pose problems. Strong authentication is very straightforward. (P1)*

> *Strong authentication is simple and easy because you can use mobile applications of banks for it. (P7)*

In both of these examples the ease of strong authentication is brought forward as a benefit. One of them specifies that it is the mobile applications of banks that make the use easy.

> *I feel that I'm the only one that has access to my banking credentials. It is more likely that somebody else has access to the alternative methods. (P1)*

In this example the interviewee expresses that strong authentication with banking credentials provides a sense of security that the lighter authentication methods cannot provide. The topic of strong authentication overlaps with both of the other subcategories under the information security theme.

The second subcategory of information security theme was sense of security. It is worth noting that the other subcategory, strong authentication, is present in this subcategory also. Digital signatures in general were considered secure and competent in providing legal protection:

> *Digital signatures provide verification of the identity of the signatory, and it is better for the legal protection of the parties. It is a lot easier to confirm afterwards than a written signature with pen.* (P5)

In this example the interviewee states that digital signature provides legal protection because it ensures the identity of the signatory. The example also brings up that digital signatures have a better proving power than a traditional signature. This example also brings up the other subcategory of certainty of identity. Another aspect that the interviewees felt to increase the sense of security were the stamps that specified the signing methods

> *The authentication stamp verifies the identification method and maybe the social security number while anybody can fake a written signature* (P5)

> *In Adobe Sign there was nothing that would express that it was a valid signature by a specific person or anything that specifies the signatory. Therefore, I did not find it trustworthy* (P6)

These examples discuss the different tokens of reliability that are visible to the user. In the first example the interviewee states that the authentication stamp increases the perceived reliability of the service while in the second example the absence of it decreased the trustworthiness and sense of security.

The final subcategory in information security is certainty of identity. One of the key benefits of digital signatures for the interviewees was knowing that the signatory is, indeed, who they say they are.

> *Knowing who the signatory is, is everything when it comes to signatures in general. You should be able to be sure that the signature is from that person who you have wanted it from.* (P6)

In this example the interviewee stresses the importance of knowing that the person who signs the document is the person who you want to sign it.

5.1.3 Convenience

The third main category of digital signatures users' perceptions about the performance of the technology is convenience. This main category is further divided into four subcategories: non-site-specificity, tool redundancy, document management and cross-device access. The subcategories of convenience of digital signatures and examples of statements matching them are presented in table 6.

Table 6 The subcategories of convenience of digital signatures

Main category	Subcategory	Example
Convenience of digital signatures	Non-site-specificity	*It was easy because I could sign a contract when the other party was in Oulu and I was in Spain. We didn't even need to be in the same country.* (P7)
	Tool redundancy	*If you're travelling or just don't have access to a printer, it is impossible to sign a document normally. With these technologies it is super easy. You can just sign it basically everywhere you like. It doesn't matter where you are. I think this is the biggest advantage for me.* (P2)
	Document management	*It is easy to look at the documents afterwards and send the documents in digital format to for example a company bookkeeper. And again, you don't need to take photos, email or scan documents because they are ready. The whole archiving process is easy because it leaves out the scanning.* (P4)
	Cross device access	*I can check up on the status of the signing request using my phone if I do not for some reason have access to my computer (*P3)

Non-site-specificity means that the signatory or the collector of signatures does not need to be in a specific location to complete the signing. Tool redundancy means that no extra tools, such as a printer or a scanner are required to complete the task. Document management refers to the ease of saving, archiving and finding the required documents. Cross device access means that the technology and service are accessible using different devices. These subcategories were often overlapping with each other.

> *If you're travelling or just don't have access to a printer, it is impossible to sign a document normally. With these technologies it is super easy. You can just sign it basically everywhere you like. It doesn't matter where you are. I think this is the biggest advantage for me.* (P2)

> *Because I can't print at home I would need to travel to the office to do the things I can do anywhere with a digital signature service. All of the documents are on my computer, our companys cloud or the cloud service of the digital signature service provider. I can access these anywhere and they don't get lost* (P3)

> *It was easy because I could sign a contract when the other party was in Oulu and I was in Spain. We didn't even need to be in the same country.* (P7)

These three examples include three of the four subcategories of flexibility. In the first example the interviewee discusses the advantages of non-site-specificity when there is no access to a printer, which also fits under tool redundancy. In the second example the interviewee sees discusses the ease of document management and non-site specificity. The third example discusses the benefits of non-site-specificity and brings up how the parties can be even in different countries.

> *I can check up on the status of the signing request using my phone if I don't for some reason have access to my computer (*P3)

In this example the interviewee brings up the benefits of being able to use the digital signature service with his mobile device when he doesn't have access to his computer.

> *The document stays in digital format through the whole time, which is a lot more comfortable (*P7)

> *It is easy to look at the documents afterwards and send the documents in digital format to for example a company bookkeeper. And again you don't need to take photos, email or scan documents because they are ready. The whole archiving process is easy because it leaves out the scanning.* (P4)

These examples discuss how the document management is easier because the documents are in digital format through the process. The benefits are from being able to archive them without using tools (tool redundancy) and also being able to search for old documents.

5.1.4 Comparative performance

The fourth main category of digital signatures users' perceptions on performance of the technology is the comparative performance of digital signatures. The comparative performance refers to the fact that the performance of digital signatures was often compared to either traditional signatures with pen and paper or an

alternative mode of signing documents remotely. The subcategory of comparative performance of digital signatures and an example of a statement matching it is presented in table 7.

Table 7 The subcategories of comparative performance of digital signatures

Main category	Subcategory	Example
Comparative performance of digital signatures	Performance in comparison to alternative methods	*The authentication stamp verifies the identification method and possibly includes the social security number of the signatory, while anybody can fake a written signature.* (P5)

This category also overlaps all of the other categories because the aspects in these categories were often compared to these alternatives.

> *The authentication stamp verifies the identification method and possibly includes the social security number of the signatory, while anybody can fake a written signature.* (P5)

> *I don't need to be in a certain place at a certain time for signing which leaves time for other things in life, such as work or leisure.* (P1)

> *Digital signing is faster, and I think more convenient for everyone.* (P2)

These three are all comparing digital signature to alternative methods. Each of these examples also overlap at least one other main category: the first example overlaps the information security category. The second example overlaps both the flexibility (non-site-specificity) and efficiency (saving time) categories.

5.1.5 Scalability functions

The fifth main category of digital signatures users' perceptions on usefulness of the technology. It is split into subcategories of acceptance in government institutions and integration with other systems. The subcategories of scalability functions of digital signatures and examples of statements matching them are presented in table 8.

Table 8 The subcategories of scalability functions of digital signatures

Main category	Subcategory	Example
Scalability functions of digital signatures	Acceptance in government institutions	*For some reason the national land survey of Finland doesn't accept digital signatures, but apart from them basically every other institution accepts digital signatures.* (P4)
	Integration with other systems	*It would be useful to integrate digital signature technology to for example a contract management system, so you could have people sign documents there instead of moving the documents back and forth between systems.* (P5)

> *For some reason the national land survey of Finland doesn't accept digital signatures, but apart from them basically every other institution accepts digital signatures.* (P4)

In this example the interviewee discusses the limitations on the acceptance of digital signature in national institutions. According to the interviewee, digital signatures are widely accepted in Finland apart from one exception in the national land survey. Acceptance in important entities is vital in for the usefulness of digital signatures.

> *Being able to integrate digital signature services into other information systems would be beneficial. Currently most of the services are so-called standalone systems, to which you upload .pdf files or papers that have been taken from another system. It would be useful to integrate digital signature technology to for example a contract management system, so you could have people sign documents there instead of moving the documents back and forth between systems.* (P5)

In this example the interviewee discusses how being able to integrate digital signature technology to other information systems would be beneficial. This would

make processes more streamlined when it would eliminate the need to move documents manually between different systems.

5.1.6 Other factors

The final main category of digital signature users' perceptions on performance of digital signatures is labelled as other factors. This main category includes subcategories that were discussed in interviews but did not fit under other main categories or were not very prevalent while worth discussing. The subcategories of other factors and examples of statements matching them are presented in table 9.

Table 9 The subcategories of other factors

Main category	Subcategory	Example
Other factors	Sustainability	*Digital signing saves paper because when you're just signing it, you are usually just printing, signing, scanning and the sending it back. Then you have just used the paper for two minutes and it's just stupid to use it.* (P2)
	Pandemic	*During this time of global pandemic and movement restrictions, I couldn't have collected the signatures physically.* (P6)

These subcategories under other factors are sustainability and pandemic.

> *Using paper is not necessary, signing paper documents wastes paper. […] It is environmentally and globally important to, whatever the industry, to minimize excess production and consumption to mitigate global warming.* (P6)

> *Digital signing saves paper because when you're just signing it, you are usually just printing, signing, scanning and the sending it back. Then you have just used the paper for two minutes and it's just stupid to use it.* (P2)

In these two examples the interviewees bring up saving paper as a benefit of digital signatures. While saving resources and sustainability were not prevalent topics throughout the interviews, they were brought up as benefits of the technology.

> *It has been beneficial to not have to physically travel to a certain location to sign papers during these difficult times* (P1)

> *It has been very handy especially now during corona time because people have not had to come here and they can take care of business anywhere in the world* (P4).

> *During this time of global pandemic and movement restrictions, I couldn't have collected the signatures physically.* (P6)

As this study was conducted in midst of the corona pandemic, the pandemic was often mentioned in the interviews. The interviewees felt that digital signatures had been useful for them to operate during the limitations of contact and movement that many countries had exercised.

5.2 Digital signature users' perceptions on ease and effort related to using digital signature services

The second research question sought to investigate the different aspects that users perceive to affect the effort of digital signing. Again, the overall perceptions about the effort related to digital signing was positive. From the data, four main categories rose: service specific user experience, information availability, contextual factors and comparative ease. The main and subcategories are presented in table 10.

Table 10 The main and subcategories of digital signature users' perceptions on ease and effort of using digital signatures

Main category	**Subcategory**
Service-specific user experience	User interface
	User path
	Service outages
	Other features
	Document management
	Authentication
	Spam-filters
	Cross-device usage
Information availability	Usage guides
	Information about authentication methods
	Information about service providers
Contextual factors	Other party
Comparative ease	Non-site-specificity
	Process efficiency

5.2.1 Service specific user experience

The interviewees had used a variety of different digital signature services. In addition to a variety of different services, they had also used them in different roles. Some had used them for signing documents, some had used them for collecting signatures and some had used them for both. This diversity in experiences lead to a number of the features affecting the ease of using digital signature technologies specific to whatever service they had used. From the material, the service specific user experience category was divided into eight subcategories: user path, user interface, cross-device usage, spam filters, authentication, document management, service outages and other features. In general, all of these can be seen to contribute to at least one of the root constructs of effort expectancy. The subcategories of service specific user experience and examples of statements matching them are presented in table 11.

Table 11 The subcategories of service specific user experience

Main category	Subcategory	Example
Service-specific user experience	User path	*In my experience this is an extremely good service which does not require too much trying from the service providers. All you need is clear paths to the document, how to sign it and how to save it. This had been implemented well in the service I used, and I am happy.* (P1)
	User interface	*The functions were well defined and at no point was there a feeling that I couldn't find something I needed.* (P6)
	Cross-device usage	*It is easy because internet is present practically everywhere and I can access the service with my phone or computer in any place if I just remember my login credentials to the service.* (P3)
	Spam-filters	*Sometimes the signing requests get caught in the spam filters in Gmail. If the customer doesn't realise to look from there it causes extra work* (P5)
	Service outages	*The service being down so that I can't log in causes problems* (P3)
	Authentication	*Digital signing with strong authentication is easier than creating user credentials for light authentication or traditional signatures* (P7)
	Document management	*Digitally signed documents are easy to archive digitally* (P4)
	Other features	*Sometimes I've misspelled an email address and the service doesn't notify me that "the email you've given doesn't exist"* (P5)

User path refers to the sequence of actions that the user has to go through in order to accomplish their task, which in this case is signing documents or requesting digital signatures from other parties.

> *In my experience this is an extremely good service which does not require too much trying from the service providers. All you need is clear paths to the document, how to sign it and how to save it. This had been implemented well in the service I used and I am happy.* (P1)

> *It is easy because you get a direct link, you just click it, then you log in using your bank ID's which is easy if you use a mobile authentication app. After that you can see all the papers there, you can open a .pdf and download it for yourself so that they are saved for you. That way you have them in digital format instead of who-knows what box that you have to look for.* (P4)

> *Last time I used it with [name] it was really easy because I just received an email from him when he was collecting a signature from me. So I opened the document and it just basically showed me the spot where I could sign. Then I clicked on it and put my name there. Then it automatically put it there and I just clicked save and it was saved.* (P2)

These examples illustrate some of the aspects in the use path that the users feel making signing digitally easy. In the first example the interviewee states that the digital signature service should focus on the user paths. He states that the three most important user paths to the signer are path to the document, to the signature and to saving the document. The second example discusses the same topic as well as the easiness of authentication with banking ID's, and also the ease of opening, saving and archiving the documents in digital form, bringing up also the subcategory of document management. The third example discusses the overall easiness of the process from clicking the link on the email to signing. These examples also overlap with the subcategory of user interface. Other examples of user interface focused more on the outlook of the service.

> *There is a big button "new signature request" that you click and then you can fill the necessary information and upload the document.* (P3)

> *The so-called layout on the [service name] pageand their landing page was very clear.* (P6)

> *The functions were well defined and at no point was there a feeling that I couldn't find something I needed.* (P6)

> *The user interface was so functional that it did not require any thinking from me.* (P1)

These examples emphasise the benefits of clarity in the user interface. The first interviewee appreciates big buttons with clear calls to action. The second interviewee found the layout on the page and well defined features in the service to ease his use and navigation . The third example says that the functional interface eliminates the need for him to think about the process.

Cross-device usage refers to the ability to use the digital signature service with different devices.

> *It is easy because internet is present practically everywhere and I can access the service with my phone or computer in any place if I just remember my login credentials to the service.* (P3)

> *If get an invitation, I can take care of the signature right then and there on my computer or my mobile device* (P7)

In these examples the interviewees describe the benefits of cross device usage. They find it beneficial to be able to use it on their mobile devices as well as computer because they can take care of the signatures without being bound to a time- or location. Some of the interviewees working professionally with digital signature technologies brought up spam filters of email services occasionally blocking the signing requests.

> *Sometimes the signing requests get caught in the spam filters in Gmail. If the customer doesn't realise to look from there it causes extra work […] These extra explanations may appear as unprofessionalism to the customer.* (P5)

> *Depending on the mailing service that the other party uses, the invitations may end up in junk mail or some "others" folder. Therefore I have to send another email from my personal email saying "Hi, the invitation is there, remember to check", because I can't trust the delivery of the invitation.* (P3)

In these examples the interviewees state that the issues with the spam filters depend on the mailing system that the other party uses. This issue may cause extra work such as writing extra emails or making extra phone calls. The first example also says that these issues may affect the reputation of themselves or their company. Another issue causing effort that was raised is service outages.

> *The service being down so that I can't log in causes problems. […] It causes me the effort that if I have promised to send the contract within an hour and the service is down, I am not a man of my word. […] And of course it is awkward to have to call and tell that the service is down.* (P3)

In this example the interviewee states that he feels that the service outages may even harm his honour because he can't keep his word. He also states that the outages cause extra work. These issues, however are rare occurrences:

> *If I've sent 40 contracts, then maybe with one customer I've had these issues. These are single occurrences* (P3)

There were also other miscellaneous system specific features that either depleted the ease of use or enhanced it.

> *When you log in, you can easily see the status of all of the contracts awaiting signatures or already signed documents* (P3)

> *If I have to send multiple documents and get interrupted, I cant check up on what documents I've already sent of these many papers. Then I might send some document multiple times or not send one of the papers at all.* (P4)

> *Sometimes I've misspelled an email address and the service doesn't notify me that "the email you've given doesn't exist"* (P5)

The service specificity of these examples is present in the first two examples: the first finds it useful that he can check up on the status of his sent signing request, while the second example states that not being able to check what documents have been sent depletes the ease of use. The third example raises the issue that the system doesn't give feedback on human errors, such as wrong email addresses.

5.2.2 Information availability

The second main category of digital signature users' perceptions about ease and effort of digital signatures is information availability. The main category of information availability consists of three subcategories: usage guides, information about authentication methods and information about service providers. The subcategories of information availability and examples of statements matching them are presented in table 12.

Table 12 The subcategories of information availability

Main category	Subcategory	Example
Information availability	Usage guides	*The guide has to give very step-by-step instructions. That's how it works the best and is easy.* (P6)
	Information about authentication methods	*For many contracts the nature of them is the same. The software should tell which kind of security level is appropriate for what kind of software. For example, "if you're renting an apartment, use this, if you are using this at work use this". More explanations on the security level needed for different types of contracts (P2)*
	Information about service providers	*I found it difficult to find an appropriate service provider for my needs.* (P6)

One of the most important aspects of information availability enhancing the ease of use of digital signatures is usage guides.

> *The guide has to give very step-by-step instructions. That's how it works the best and is easy.* (P6)
>
> *Apparently the service I used was pretty good because it had so clear instructions.* (P7)
>
> *There was clear guide telling how to add document, add signatories, do you want to attach social security numbers.* (P5)

In the first example the interviewee states that he would hope for clear step-by-step instructions because it makes the use easy. The second example states his

satisfaction with the clear instructions provided by the services. The third interviewee specifies the steps that he had instructions for. On the other hand, the absence of these instructions was perceived as depleting the ease of use

> *In the beginning you have the options, but you don't really know which option you need to take and there was no explanation* (P2)

The second subcategory of information availability is information about authentication methods. One of the interviewees had experienced difficulties in finding appropriate information about different means of authentication.

> *I would like to know how the authentication system works and how it verifies the identity of the other party* (P6)

> *For many contracts the nature of them is the same. The software should tell which kind of security level is appropriate for what kind of software. For example, "if you're renting an apartment, use this, if you are using this at work use this". More explanations on the security level needed for different types of contracts* (P2)

In these examples the interviewees discuss the lack of available information about authentication methods. The first interviewee felt that he would've liked more information about how the authentication works. The second interviewee would've liked to have more information available about what types of security levels are appropriate for what kind of contracts. It should be noted that both of these interviewees used a digital signature service that did not have an option to use strong authentication with bank ID's or mobile ID's.

The last subcategory of information availability is information about service providers. When the service used is not dictated by a workplace, an interviewee found it difficult to find an appropriate service provider.

> *I found it difficult to find an appropriate service provider for my needs. […] It would be beneficial to have a clear market leader for digital signatures so choosing the service would be easier.* (P6)

This interviewee had found finding an appropriate service provider difficult because there was no clear market leader in the field.

As is present from these results, The interviewees found it important that there is enough information available about the intricacies of digital signature technologies. Clear instructions and usage guides about digital signature services as well as the different authentication methods could prove useful to mitigate user confusion and frustration. The availability of information can also be seen as a means to affect perceived ease (TAM), complexity (MPCU) and ease of use (IDT), which are root constructs of effort expectancy.

5.2.3 Comparative ease

As was the case in the perceptions about performance, a lot of the perceptions about ease and effort were discussed comparatively to alternative methods. These were either signing traditionally in same location on a paper or signing remotely using a printer and a scanner. Therefore, the third main category of ease and effort in relation to digital signatures is comparative ease. This main category is further divided into subcategories of and ease of process and non-site-specificity. The subcategories of comparative ease and examples of statements matching them are presented in table 13.

Table 13 The subcategories of comparative ease

Main category	Subcategory	Example
Comparative ease	Non-site-specificity	*It was easy, fast. I didn't need to move anywhere or go anywhere to sign a paper.* (P2)
	Process ease	*In the old days we would make the contracts using a contract generator. This contract would be sent to our sales manager, who would then print it, sign it on paper, then scan it, and send it to me. After that I would send this document to the customer, who would again print it, sign it, scan it and send it to me.* (P5)

The subcategory of process ease refers to the ease of the process of signing a document.

> *Digital signing makes working remotely easier. This is because there is no need for printers or scanners.* (P3)

> *If you don't have a printer, you can't design and sign contracts normally. With these technologies it is super easy* (P2)

> *In the old days we would make the contracts using a contract generator. This contract would be sent to our sales manager, who would then print it, sign it on paper, then scan it, and send it to me. After that I would send this document to the customer, who would again print it, sign it, scan it and send it to me.* (P5)

In these examples the interviewees discuss how not needing additional tools such as printers or scanners makes the signing process easier. The first interviewee brings up how digital signing is easier than alternative means of signing contracts when remote working, which at the time of conducting this research was very common due to a global pandemic. The second interviewee brings up not having

access to these additional tools needed for the traditional process without digital signatures. The last interviewee describes how the process of signing sales contracts remotely before digital signatures. Digital signatures eliminate a number of steps from this process.

The other subcategory of comparative ease is non-site-specificity. Interviewees found that digital signing is easier than alternative methods when the signatories are in different locations.

> *It was easy, fast. I didn't need to move anywhere or go anywhere to sign a paper.* (P2)

> *The ease stems from not having to go anywhere. Or then somebody scans a paper for you that you sign it and scan it, when you could just do everything on your smart device* (P4)

These two examples by interviewees state that digital signing is easier than alternatives because they don't have to go anywhere to sign it. The second example includes both of the subcategories of comparative ease while also overlapping with cross-device-access.

5.2.4 Contextual factors

The final main category of digital signature users' perceptions about ease and effort of digital signatures is contextual factors. This main category only has a single subcategory which is other party. The subcategory and an example of a statement matching it is presented in table 14.

Table 14 The subcategories of contextual factors

Main category	Subcategory	Example
Contextual factors	Other party	*Sometimes it poses challenges if the person I send the contract to hasn't used digital signature systems before. Sometimes they don't know what to do even when the instructions are clear. (*P5)

The term contextual factors in this case refers to the ease of digital signing varying in each case depending on the other party. These factors can be capabilities and proficiencies of the other party, but also their behaviour.

> *Sometimes the customers sign a single paper when they have received 15 papers and then I have to remind them to sign the rest of the papers. This results in wasted time and effort.* (P4)

> *Sometimes it poses challenges if the person I send the contract to hasn't used digital signature systems before. Sometimes they don't know what to do even when the instructions are clear. […] Sometimes they ask questions about how to sign the document which causes extra work*

> *[…] Problems in using the system may cause some trust issues towards these services, but usually its nothing major.* (P5)

In these two examples professional users describe how the inexperience of customers in using these services may sometimes cause extra work and effort. The second interviewee raises a concern that these problems may cause decreased trust towards digital signature services but also downplays this concern.

> *I've noticed that when some customers realise how easy signing digitally is, they sign documents containing hundreds of pages within minutes. Then you can just directly assume that they have not read the contract but just signed the contract without going through it. […] It would be important and beneficial for their own legal security that they would read the contract and not just sign it. For us at the bank it legally thinking doesn't matter when the signatory has signed the document with strong authentication. The contract stands and its clear, but when thinking about the customers interests, it would be better that they read the contract. […] It is not the same as going through the document with the customer face-to-face and telling them "make sure to read this part".* (P4)

In this example an interviewee working in the bank sector discusses how he has noticed that sometimes the customers don't read the contracts that they are sent before signing. While he says that it is not legally a concern to him as a representative of the bank, he raises concern about the customers own interests. This example also overlaps the comparative ease main category when he compares signing the contracts digitally with signing them face-to-face with the customers.

6 DISCUSSION

This study sought to research the factors that affect the users' perceptions on the performance and effort of digital signature technologies. This was done using qualitative methods and basing on the presumptions created by years of technology study synthesised by the creators of the UTAUT model. However, the study should not be seen as an extension to technology acceptance models or as a model to predict user acceptance in digital signatures, but rather an individual study providing insights to what aspects users perceive to affect their views on performance and effort of using digital signature technologies. As a result, this study was able to provide a hierarchal structure (Table 15) of the different themes that the interviewees discussed about their perceptions on performance and effort of using digital signatures. In this chapter the results of this study will be discussed.

The first research question was "on what parameters do users perceive the performance of digital signature technologies after its adoption?". As an answer to the research question, the users' perceptions the performance consist of efficiency, information security, convenience, comparative performance, scalability functions and other factors.

The second research question was "on what parameters do users perceive the ease and effort of using digital signature technologies after its usage?". To answer the question, the users' perceptions about factors contributing to ease and effort of using digital signatures consisted of service-specific user experience, information availability comparative ease and contextual factors.

This chapter will provide theoretical and managerial implications based on the results of the study and discuss the limitations and suggestions for future research.

Table 15 Digital signature users' perceptions on performance and effort of using digital signature technologies

Digital signature users' perceptions on performance of digital signature services	Efficiency of digital signatures	Saving time
		Saving effort
		Job performance
	Information security of digital signatures	Sense of Security
		Certainty of identity
		Authentication
	Convenience of digital signatures	Non-site-specificity
		Tool redundancy
		Document management
		Cross device access
	Comparative performance	Performance in comparison to alternative methods
	Scalability functions	Acceptance in government institutions
		Integration with other systems
	Other factors	Sustainability
		Pandemic
Users′ perceptions about factors contributing to ease and effort of digital signature technologies	Service-specific user experience	User interface
		User path
		Service outages
		Document management
		Authetication
		Spam-filters
		Cross-device usage
		Other features
	Information availability	Usage guides
		Information about authentication methods
		Information about service providers
	Contextual factors	Other party
	Comparative ease	Non-site-specificity
		Process efficiency

6.1 Theoretical implications

In general, most of the findings of this study were consistent with the framework that the UTAUT model presents. For example, the different aspects brought forward in the categories "efficiency" and "convenience" of users' perceptions on digital signature technologies are matching to the definitions of the root constructs of performance expectancy, which was the basis for the research question. These root constructs were perceived usefulness (TAM), extrinsic motivation (MM), relative advantage (IDT) and job fit (MPCU)

The information security category was an item that did not directly fit under the root constructs that make up the performance expectancy construct of UTAUT. However, due to the perceptions of the professional users stating that they would only view digital signature competent if it has strong authentication, it can be seen being tied to the job fit construct of model of PC utilisation (MPCU).

Comparative performance can be seen as consistent with the root construct relative advantage of performance expectancy in the UTAUT model, which is adapted to UTAUT from IDT.

The perceptions about different aspects contributing to the ease and effort of using digital signature technologies were also generally consistent with the root constructs of effort expectancy in UTAUT model. These were perceived ease of use (TAM), complexity (MPCU) and ease of use (IDT). An interesting nuance about the subcategory of comparative ease is that it is more consistent with the "relative advantage" root construct of performance expectancy, rather than any of the root constructs of effort expectancy.

6.2 Managerial implications

6.2.1 Performance of digital signature technologies

The main theme of performance of digital signature technologies consisted of six main categories. These are information efficiency of digital signatures, information security of digital signatures, convenience of digital signatures, comparative performance of digital signatures, document management and other factors. In many ways, these categories were overlapping with each other.

The most prevalent main category of this theme was the efficiency. The main category of convenience was also very closely related to efficiency. Generally speaking, the results of this study suggest that users would find adopting digital signatures for signing and collecting signatures beneficial for their performance of tasks, either personal or work related. The overall satisfaction and opinion concerning the efficiency and convenience of digital signing was present in

all the interviewees, no matter whether they had used the technology as a customer of a company using digital signing or as a collector of signatures. Therefore, organisations should consider providing an option of signing digitally when collecting documents that require signatures from people. Moreover, as the different aspects of efficiency and convenience were expressed in comparison to traditional signing with pen and paper or signing remotely without using a digital signing technology, it is possible that frustration related to the inefficiency and inconvenience of travelling to a certain location just to sign a paper or having to print, sign scan and email signed documents may increase among those who have experienced the efficiency and convenience of using digital signature technologies.

Another very prevalent topic discussed in the theme of performance of digital signature technologies was information security. The interviewees expressed that in their opinion digital signature technologies outperform alternative signing methods. This sentiment was especially strong among those who had used digital signature technologies that provided the option of strong authentication. At the time of conducting this study, strong authentication means are not particularly common outside the Nordic states of Finland, Sweden, Denmark and Norway. Those that had used a service that did not provide strong methods of authentication had experienced some confusion on the different security levels that the service had provided. Therefore, it would be beneficial to develop a global standard of strong authentication methods.

There were also discussions about the scalability functions of digital signatures. For the dissemination of the technology to wider popular use, it is essential that government functions accept the technology as a means to sign documents. It was revealed that the Finnish land survey currently doesn't accept digital signatures that do not satisfy the criteria of qualified electronic signature laid down in eIDAS. Apart from those specific exceptions the users did not express that they had encountered non-acceptance of digital signatures. Moreover, not accepting digital signatures on grounds that a digital signature doesn't meet requirements of qualified electronic signatures is against Article 25 of eIDAS regulation.

Integration of digital signatures into other digital services, such as CRM-systems was also discussed. This would enable more dynamic processes, when documents could be signed from different information systems instead of moving documents between systems. Moreover, this would solve the shortcoming that another interviewee discussed about not being able to go through documents with customers before signing, if signing documents digitally could be integrated into online meeting services.

6.2.2 Ease and effort of using digital signature technologies

The four main categories of the users' perceptions about ease and effort of using digital signature technologies after using them were service-specific user experience, information availability, comparative ease and contextual factors. Due to

the interviewees using various different digital signature service providers, a lot of their perceptions about ease and effort were specific to a certain service. In general, clear user paths and user interfaces were found to decrease the degree of difficulty of using the service. User path refers to the sequence of actions that a user has to take in order to complete his goal; in this case signing a document or inviting others to sign a document. Features that the interviewees brought up in discussing user paths were email invitations with links directly to the document, simple functions to sign and save documents, option to use strong authentication, and limited number of different options.

While there were not many aspects that the interviewees told to affect their degree of effort negatively, service outages were one of them. Outages in the service may prevent users from logging into the service and sending or signing documents. An outage at the wrong time was told to even affect one's self-image as a man-of-word if they cannot send a document after promising to do so, due to outage. Professional users had encountered difficulties with email services marking their signing invitations as spam. This on the other hand caused extra labour when they had to communicate with the customer about finding the invitation. On the other hand, these issues were suggested to even cause loss of trust in digital signature technologies and appear as unprofessionalism on behalf of the inviting party.

Cross device usage was a feature that many of the interviewees found highly beneficial. This was something that was discussed in both of the aspects of this study. Being able to use the service with a mobile device as well as a computer was told to enhance the ease of using digital signatures. The reason for this was not being tied to a time or a place and being able to use the service "on-the-go". The use of smartphones has increased rapidly in the last decade and it is the device of choice for many people for reading emails, for example. Therefore, it is easy to assume that being able to sign a document with the same device that you receive the invitation to would enhance the ease of use and decrease the required efforts. Mobile experience is therefore an aspect that digital signature service providers should look to enhance.

Information availability was a key aspect of the interviewees' perceptions about the ease and effort of using digital signatures. Usage guides were brought up as a key feature in enhancing the ease of using digital signature services. Many interviewees expressed that they would like clear step-by-step instructions about using digital signatures. Moreover, the unavailability of information or insufficient information was seen as the biggest single factor affecting the ease of use negatively. This suggests that the service providers should allocate resources in developing informational materials about how to use their services.

The second subcategory of information availability was information about authentication methods. While strong authentication has been discussed in previous chapters, in this case the information authentication was brought up by users using a digital signature service that did not have strong authentication

methods available. Instead, the service had different security levels. The interviewees found that the information about these security levels was insufficient and it caused some confusion. A practical suggestion from one of the interviewees was to have a clear guide that tells what kind of security levels are appropriate for what kind of contracts. This seems like an appropriate measure to take in order to avoid confusion among users.

As was the case with the perceptions about performance, perceptions about ease were often discussed in comparison to either traditional signing or remote signing without a digital signature service. Digital signing was deemed easy because the interviewees didn't need additional tools and steps to complete the signing process. Again, the arduous process of printing, signing, scanning and mailing was brought up as a point of comparison, to which digital signing provided an efficient alternative. Comparative ease is a point of strength for digital signature technologies that the service providers could leverage when marketing and communicating the benefits of their products as it is something that many will relate to.

The final main category of users' perceptions about ease and effort of digital signature technologies is contextual factors. Contextual factors refer to the skills and capabilities of the other party involved in the signing process. These contextual factors possibly could be affected with enhancing the information availability for the signatories. This way the digital signature services could enhance the user experience of the signatories through mitigating confusion and the user experience of the signature collectors through mitigating issues with the signatory.

6.3 Limitations & future research suggestions

This research has a number of limitations. First of all, the sample size of this qualitative study is fairly small and therefore it does not aim to provide generalisable information. The data consists of personal experiences of digital signature users and they cannot be seen as representative of the experiences of the wider community.

Secondly, the sample is very homogenous, with all of the interviewees being males between the ages of 25-34. The young age of the users may very well have caused an emphasis on the positive experiences and perceived ease of using the technologies as the younger generations typically are more tech-savvy than their elders. There is no indication that the perceptions of performance and effort are dependent on gender, but it cannot be ruled out either and therefore it should be noted that all of the interviewees were male.

Thirdly, all but one of the interviewees were Finnish and had previous experience of using strong authentication methods, such as mobile and banking ID's. As these strong authentication technologies are not as common outside of the Nordics and Finland, it should be noted that results are in parts very specific

to Finland. All but one of the interviews was conducted in Finnish language and then translated into English for the appropriate parts.

As this study focused on people who already had experience in using digital signature technologies, it would be beneficial to study how the perceptions about the performance and ease and effort of using the technology differ when there is no previous experience in using these technologies. Due to the sample consisting of only young adult males, conducting this same study with females or different age groups would provide valuable insight to the way different demographic groups perceive the performance of digital signature technologies. Because this study did not focus on just the signing party or the party collecting the signatures, it would be beneficial to conduct this same study focusing on just the other user group.

While this study was based on the performance expectancy and effort expectancy factors of the UTAUT model, it would be beneficial to study the parameters by which the users perceive social influence and facilitating conditions in the context of digital signatures. Moreover, using qualitative methods to study the underlying factors that cannot be reached through mere questionnaires could prove beneficial when studying different factors that affect technology acceptance.

7 REFERENCES

Ajzen, I. 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes 50 (2), 179-211.

Aydin, S., Handan, Ç. A. M. & Alipour, N. 2018. Analyzing the factors affecting the use of digital signature system with the technology acceptance model. Journal of Economics Bibliography 5 (4), 238-252.

Belk, R., Fischer, E. & Kozinets, R. V. 2012. Qualitative consumer and marketing research. New York: Sage.

Brandner, R., Van der Haak, M., Hartmann, M., Haux, R. & Schmücker, P. 2002. Electronic signature for medical documents–integration and evaluation of a Public Key Infrastructure in Hospitals. Methods of Information in Medicine 41 (4), 321-330.

Compeau, D. R. & Higgins, C. A. 1995a. Application of social cognitive theory to training for computer skills. Information Systems Research 6 (2), 118-143.

Compeau, D. R. & Higgins, C. A. 1995b. Computer self-efficacy: Development of a measure and initial test. MIS Quarterly 19 (2), 189-211.

Danske Bank. 2019 Danske Bankin tunnistusvälineen tunnistusperiaatteet [online]. [cited 20.1.2021]. Available in www-form at: <URL: https://www.danskebank.fi/PDF/fi/Henkiloasiakkaat/Verkkopalvelut/Tunnistusperiaatteet.pdf >.

Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. 1989. User acceptance of computer technology: a comparison of two theoretical models. Management Science 35 (8), 982-1003.

Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. 1992. Extrinsic and intrinsic motivation to use computers in the workplace 1. Journal of Applied Social Psychology 22 (14), 1111-1132.

Deltagon Group Oy. 2020. Digitaalinen allekirjoitus nopeaan sähköiseen asiointiin [online]. [cited 20.1.2021]. Available in www-form at: <URL: https://cdn2.hubspot.net/hubfs/2789488/deltagon-files/Deltagon-sec-Signed-esite.pdf >.

DNA Oyj. 2017. DNA Oyj:n varmennuskäytäntö mobiilivarmenteita varten [online]. [cited 20.1.2021]. Available in www-form at: <URL: https://www.dna.fi/documents/753910/853444/Mobiilivarmenne_varmennuska%CC%88yta%CC%88nto%CC%88_v11.pdf/3d79a977-39ea-ab0c-7d89-72d1145bc550 >.

Elisa Oyj 2014. Elisa Varmenne, varmennuskäytäntö [online]. [cited 20.1.2021]. Available in www-form at: <URL: https://elisa.fi/attachment/content/ELISA-Oyj-Varmennuskaytanto-Asiointivarmenne-1_2.pdf >.

Elisa Oyj. 2017. Tunnistusperiaatteet – Elisa Mobiilivarmenne [online]. [cited 20.1.2021]. Available in www-form at: <URL: https://elisa.fi/attachment/content/Tunnistusperiaatteet-Mobiilivarmenne.pdf >.

EU directive 1999/93/EC. 2000. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013 , 19/01/2000 P. 0012 – 0020. [online]. [cited 13.1.2021]. Available in www-form at: < URL: https://eur-lex.europa.eu/legal-content/EN-FI/TXT/?from=EN&uri=CELEX%3A31999L0093 >.

EU Regulation No 910/2014 of the European Parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union | L 257/73. [online]. [cited 13.1.2021]. Available in www-form at: < URL: https://eur-lex.europa.eu/legal-content/EN-FI/TXT/?from=EN&uri=CELEX%3A32014R0910 >.

Gamalielsson, J., Jakobsson, F., Lundell, B., Feist, J., Gustavsson, T. & Landqvist, F. 2015. On the availability and effectiveness of open source software for digital signing of PDF documents. Open Source Systems: Adoption And Impact AICT-451, 71-80.

Haryanto, B., Gandhi, A. & Sucahyo, Y. G. 2020. The Determinant Factors in Utilizing Electronic Signature Using the TAM and TOE Framework. In 2020 Fifth International Conference on Informatics and Computing (ICIC) (pp. 1-8). IEEE.

Hsieh, H.-F. & Shannon, S. E. 2005. Three Approaches to Qualitative Content Analysis. Qualitative Health Research 15 (9), 1277–1288.

Moore, G. C. & Benbasat, I. 1991. Development of an instrument to measure the perceptions of adopting an information technology innovation. Information Systems Research 2 (3), 192-222.

Kerry, C. F. & Gallagher, P. D. 2013. Digital signature standard (DSS). FIPS PUB 186-4.

OP-Palvelut Oy. 2020. Tunnistusvälineen tunnistusperiaatteet [online]. [cited 20.1.2021]. Available in www-form at: <URL: https://www.op.fi/tac?did=Hesah0000000671&cs=354d4cd8a8485bb25b04d3c60039d45118c1a307806e583c36cad40e4876c325 >.

Roy, A. & Karforma, S. 2012. A Survey on digital signatures and its applications. Journal of Computer and Information Technology 3 (1), 45-69.

Sheppard, B. H., Hartwick, J. & Warshaw, P. R. 1988. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. Journal of Consumer Research 15 (3), 325-343.

Suomen Säädöskokoelma. 2018. SäädK 1009/2018. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta. Helsinki: Oikeusministeriö.

Taylor, S. & Todd, P. 1995a. Assessing IT usage: The role of prior experience. MIS Quarterly 19 (4), 561-570.

Taylor, S. & Todd, P. A. 1995b. Understanding information technology usage: A test of competing models. Information Systems Research 6 (2), 144-176.

Thompson, R. L., Higgins, C. A. & Howell, J. M. 1991. Personal computing: toward a conceptual model of utilization. MIS Quarterly 15 (1), 125-143.

Telia Oyj. 2017. Telia mobiiliasiointivarmenne varmennuskäytäntö. Versio 2.2 [online]. [cited 20.1.2021]. Available in www-form at: <URL: https://support.trust.telia.com/repository/Telia_Mobiiliasiointivarmenne_CPS_v2.2.pdf >.

Traficom. 2021. Vahvan sähköisen tunnistuspalvelun tarjoajat, Diaarinumero 783/620/2017. [online]. [cited 22.5.2021]. Available in www-form at: <URL: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen >.

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi (5. edition). Helsinki: Tammi.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. 2003. User acceptance of information technology: Toward a unified view. MIS Quarterly 27 (3), 425-478.

Venkatesh, V., Thong, J. Y. & Xu, X. 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Quarterly 36 (1), 157–178.

Etätyö johti digiloikkaan – alueelliset erot sähköisten prosessien käytössä valtavat [online]. [cited 25.1.2021]. Visma Solutions Oy. Available in www-form at: <URL: https://vismasolutions.com/ajankohtaista/etatyo-johti-digiloikkaan/ >.

Vähimaa, A. 2021. Näin toimii sähköinen allekirjoitus [online]. [cited 1.4.2021] Kauppalehti. Available in www-form at: <URL: https://www.kauppalehti.fi/uutiset/nain-toimii-sahkoinen-allekirjoitus-testissa-6-ratkaisua/5572c4d8-cacb-495a-8da7-bf2de6fa1294 >.

APPENDIX 1 - EU REGULATION NO 910/2014, ANNEX I

(1) "an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;"

(2) "a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and: | — | for a legal person: the name and, where applicable, registration number as stated in the official records, | — | for a natural person: the person's name;"

(3) "at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;"

(4) "electronic signature validation data that corresponds to the electronic signature creation data;"

(5) "details of the beginning and end of the certificate's period of validity;"

(6) "the certificate identity code, which must be unique for the qualified trust service provider;"

(7) "the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;"

(8) "the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;"

(9) "the location of the services that can be used to enquire about the validity status of the qualified certificate;"

(10) "where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing."

(EU regulation No 910/2014, 2014).

APPENDIX 2 Interview protocol

Interview

Pre-interview

- Introduction to the research topic, and the process
- Explaining the subjects right to anonymity
- Disclose how interview and personal data is handled
- Request permission for recording

Background questions

- Since when have you been using digital signature technologies?
- For what purpose have you been using digital signature technologies
- Did you use the technology to collect signatures or sign documents?
- What is the frequency of using these technologies? Daily, monthy weekly?
- Do you think the benefits of using these technologies outpaced the efforts and the cost involved in procuring and using this technology? If yes, how?
- On a scale of 1-5, how convenient do you find the technology
- Would you recommend others to use this technology? Why?
- Describe the process of using the technology.

Performance expectancy

- Did you find these technologies useful for accomplishing your daily or necessary goals/job tasks? Why, in your opinion, was it / wasn't it useful?
- Do you think using these technologies help you accomplishing your tasks more quickly or efficiently? If yes, how?
- Do these technologies help you be more productive / efficient? If yes, how?

Effort expectancy

- Do you find these technologies easy/difficult to use? If yes, how?
- Was learning to use these technologies easy for you?
- Could the using these technologies somehow be made easier?

Other factors

- Is there something you would like to say about digital signing that was not discussed in the interview?