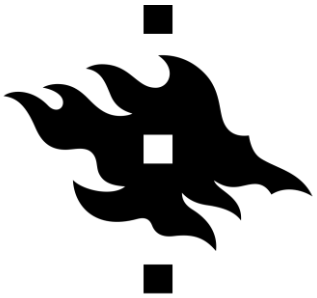


HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

A Critical Assessment of the Strong Authentication System Using Bank Credentials: The Case Study of Finland

Weronika Krupa, Minna Parkkonen, Katja Stempel, Nazli Baglan, Veronica Kontopoulou

Faculty of Social Sciences, University of Helsinki
Master's Programme in Global Politics and Communication

Abstract

The strong authentication system has cemented its grip on Finnish everyday life right before our eyes with little to no public scrutiny. The lack of academic research critically reflecting on the positives and negatives of the implementation of the strong authentication via bank credentials is worrying from the perspectives of equality, privacy and data security. Could the negatives potentially outweigh the positives of this authentication method if we go deep enough into addressing the lack of critical research? This project will address the following research questions: What are the reasons behind the introduction of the strong authentication system in Finland? How does the strong authentication system in Finland translate to the everyday experiences of its residents? What are the positive and negative effects of the implementation of the strong authentication system in Finland?

Keywords: strong authentication, bank credentials, digitisation, eIDAS, PSD2, TUPAS, Finnish Trust Network, inequality, discrimination, data privacy, digital footprint

1.Introduction

Primarily planned as a secondary solution for the digital sector, rapid urbanisation paved the way for the digitisation of the storage and processing of personal data, first, in the form of TUPAS and later, in the digital identity development project and the Finnish Trust Network (FTN).

The shift of service platforms online generated the need for strong authentication which is now a well-established method employed in Finland, specifically via the bank credentials approach. This approach aims to ensure safety, convenience and speed. At the same time, it attributes banks with considerable power while certain groups lacking critical documentation are inevitably left out.

Drawing from relevant first-hand and surveyed experiences, moving to Finland as a non-national has proven to present unreasonable obstacles throughout the process of settling into the country. Despite being a comparatively difficult and long-lasting procedure, obtaining bank credentials is a basic prerequisite for the usage of strong authentication. Meanwhile, being able to access the FTN is of central significance to everyday life. Personal hurdles thus, sparked an interest to critically assess the strong authentication method utilised in Finland.

First, both the technical aspects characterising the strong authentication landscape (2.1.), and the legislative framework in the EU and Finland regulating the process of strong authentication will be presented (2.2.). What follows is a closer examination of the benefits resulting from implementing the FTN in Finland (3.). Thereafter, the next section will present an assessment upon strong authentication practicalities from the perspective of non-EU/EEA residents in Finland, via taking the accessibility merit into consideration (4.1). The analysis will culminate with an exploration of the predicament presented by privacy and safety issues related to the inevitable data accumulation throughout the authentication process (4.2.).

While there is an abundance of literature touching on the technical aspects of strong authentication methods, research drawing from a social science perspective was severely limited - especially in the case of bank credentials. The evident lack of scholarly coverage translated into a thinner academic basis to build this paper's analysis upon. Therefore, this study aims to contribute to the academic research on the wider fields of digitisation, cybersecurity and information society by addressing the gaps mentioned prior.

2. A Synopsis of The Strong Authentication System Using Bank Credentials

2.1 Digitisation: Characterisation of the Strong Authentication System

Strong online authentication via bank credentials, imposed by first TUPAS and then the Finnish Trust Network, is a complex system that allows Finnish citizens to acquire secure authentication and access their online accounts safely (Ubisecure, 2019). This section will serve as a guide for the implementation of strong authentication systems in Finland. This section will illustrate the formats in which strong authentication operates, as well as underline the procedure of obtaining it via bank credentials. The section will

further explain the chronology of implementing TUPAS and the FTN and underline the reasons behind it. An overview of both TUPAS and the FTN will serve as a characterisation of electronic authentication via bank credentials. The objective of this research paper - a critical analysis of the strong authentication system - cannot be achieved without a full comprehension of the practical application of the topic. Hence, this section will be the basis for the future analysis of the strong authentication system in Finland, providing a practical overview of how the system works and allowing the later sections to proceed with their critique.

In a digitalised society, cybersecurity is the core of a safe online presence. Under the threat of cyberattacks and hacking, a simple password may not be enough to secure an online account. When crucial everyday matters such as banking, taxes, bills and work payments operate online, the customer requires something more than password-based protection. On that basis, strong authentication builds upon the simple username/password format and extends it further, therefore enhancing online security (Kerttula, 2015, p. 101). As a two-factor or multi-factor authentication (2FA, MFA), this format can withstand cybersecurity threats and attacks from hackers (hypr.com). From this emerges the Finnish TUPAS system, commonly associated with strong authentication via bank ID. In TUPAS, the customer accesses their online account through multi-layer authentication. In order to receive the TUPAS credentials, the customer needs to visit the bank branch themselves, create a consumer relationship and provide proof of their identity in the form of a passport or an ID card (Suoranta et al., 2015, p. 221). After receiving their credentials and proceeding with the online log-in, the user is redirected to the Operator Authentication service, where they provide information such as the mobile number and a spam prevention code (ibid, pp. 101-102). TUPAS can be used to provide online identification and proceed with internet-based transactions. As explained by Rissanen, TUPAS had actually a bigger share of online transactions in Finland than FINEID - an electronic identity provider (Rissanen, 2010, p. 176). The author further underlines that TUPAS is not a certificate-based system, rather one relying on a "combination of a username and password with one-time transaction authentication numbers (TAN)" (Rissanen, 2010, p. 178). Furthermore, TUPAS does not hold encryption at the message level, so along with its lack of certificate-based authentication format, it has become incompliant with the EU eIDAS regulation and the Finnish national law, which will be addressed in later sections (Signicat, 2019). In the end, TUPAS served as the base for the implementation of online strong authentication systems in Finland for a few years (ibid). It has enabled Finnish citizens to securely operate their online transactions. However, as technology progressed, the security provided by TUPAS became insufficient. Having explained the main factors of the TUPAS authentication system, this section will now proceed into the characterization of its successor - the Finnish Trust Network.

Hämeen-Anttila argues that "the reasons for abandoning TUPAS can be summarised with one word: security" (Hämeen-Anttila, 2019, op-developer). The author explains that the new system - the Finnish Trust Network (first introduced in 2019) - has two operators: the Identification Device Providers e.g. banks, whose role in the system stays the same and Identification Brokers, who now connect applications to the Identification Device Providers (Hämeen-Anttila, 2019, op-developer). Hämeen-Anttila adds that the implementation of the FTN should not only increase online

security, but also significantly decrease bureaucracy (ibid.). Similarly, as explained by the Finnish Transport and Communications Agency (Traficom), this new type of strong authentication should greatly ease the identification process (National Cybersecurity Centre, 2021). Issuing such a form of strong authentication in Finland requires the individual to have a Finnish ID number, and to be registered in the Finnish Population Register (Nordea, 2021). Having obtained this information, the customer must then present their identification document - a passport or an identity card - in order to confirm their identity at the bank of their choice. This means, just as in the case of TUPAS, that establishing a customer relationship with the bank is a crucial step in the process. After completing this procedure and obtaining the bank credentials, "customers can identify themselves for the electronic services of the companies or organisations" which accept this form of strong authentication (Nordea, 2021, p. 1). The process of using this strong authentication in practice is explained step by step by Danske Bank, presenting a scenario in which:

1. The customer presents their Danske Bank credentials;
2. The bank identifies the person and sends an authorisation code to the service provider;
3. The service provider exchanges the code for an ID Token with the bank, allowing the customer to complete their authentication (Danske Bank).

The banks, which in this case, act as the Identification Device Providers, also have a number of obligations to fulfil. Operating under the Traficom regulations, the banks are required to pay the annual fee and to submit written notifications to Traficom (National Cybersecurity Centre, 2021). The responsibility for the Finnish Trust Network lays on the Finnish Ministry of Transport and Communications (also referred later in the next section), along with the Finnish Ministry of Finance and the Digital and Population Data Services Agency which are responsible for subsequently the guideline of the provision of services and the identification in public services such as Suomi.fi (National Cybersecurity Centre, 2021). In the end, the Finnish Trust Network is a new strong authentication system operating in Finland which allows the customer to complete their online authentication safely via bank credentials.

The aim of this section was to introduce the practical meaning behind the strong authentication system in Finland. This section has explained that strong authentication is a 2FA or MFA process which enables customers to identify themselves online, proceed with their transactions and withstand cybersecurity threats (hypr). It has presented the two forms of strong authentication operating in Finland - TUPAS and the Finnish Trust Network. After characterising the nature of TUPAS, this section has established that in light of the rising security threats in the digital sphere, TUPAS was considered insufficient in providing a safe way for electronic identification (Hämeen-Anttila, 2019, op-developer). Consequently, this text has provided an overview of the main features of the Finnish Trust Network, a current strong authentication system provided by Traficom since 2019 (National Cybersecurity Centre, 2021). It has explained how the FTN allows the customer to complete their online identification through bank credentials. Finally, this section presented the strong authentication via bank credentials in the form of the Finnish Trust Network as a two or multi-layer process

that begins with the customer obtaining a Finnish ID number and registering at the bank of their choice and ends with them using the bank credentials to verify their identity online and proceed with everyday transactions.

2.2 An overview of the legislative framework: Finland and the EU

This section will focus on providing an overview on both the strong authentication framework within the European Union (EU) and on the Finnish legislative level. The strong authentication system in Finland defined in the Act on Strong Electronic Identification and Electronic Trust Services 617/2009 (Act 617/2009) is largely based upon the European Union (EU) Regulation No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) enforced on 23 July 2014, which repealed the former directive 1999/93/EC focusing on the electronic signature process only (Ministry of Transport and Communications, 2019). Alongside these legislative items, the newest EU Directive on the Second Payment Services Directive (PSD2) 2015/2366 and specifically, its articles 97 and 98, affects the process of strong authentication, mandating the need for customers to use strong authentication via online payments, and providing added technical requirements in the identification process. On the Finnish level, this has been divided between the Payment Services Act 898/2017 (Act 898/2017) and Payment Institutions Act 890/2017 (Act 890/2017) (FIN-FSA, 2019). Whereas the process defined in the Act 617/2009 and PSD2 differ in terms of their regulatory frameworks in the context of EU and Finland, the role of PSD2 in strong authentication will be explained later in the context of the eIDAS regulation.

Overall, the eIDAS regulation governs the use of strong authentication within the EU. The aim of the regulation is to provide a legal framework to ensure trust and security of using online services by the "citizens, businesses and public authorities" within the Union, thus enhancing both public and private services and their usage (European Parliament, 2014, para 1). The regulation defines parameters on the assurance levels on identification and authentication to be used within member states but grants them the freedom to decide how the access to online services and their final delivery is set out for applicants in their national legislation (para 14).

The eIDAS process is part of the digital agenda defined by the Commission to address the barriers for citizens to access the internal digital market across country borders (ibid., para 3). The regulation itself identifies that currently citizens and businesses lack the ability to identify and authenticate themselves electronically, when especially conducting cross-border activities, due to the incompatibility of the national electronic schemes (eIDs) on recognizing identification attempts from another country's eID scheme (ibid., para 9). Currently, only 15 member states have notified the European Commission that they have the needed eID system in place (see CEF Digital, 2020 for the list). Even when the aim of the eIDAS regulation is not to streamline electronic identification systems across the member states, but rather to ensure that online identification and authentication is possible securely across the EU (European Parliament, 2014, para 12), the lack of recognized eID systems within EU hinders migration across borders and thus identification opportunities on various levels.

However, the EU has aimed to address this issue by introducing a digital identity (ID) "wallet" (Cater, 2021). The adoption of the ID wallet would be used to provide a shared identification platform for both private and public services and form a digital single market that has been lacking. This technical solution will, however, remain as an additional layer on top of the national eID systems, pushing the enforcing role on national governments to define the logistics of the process similar to the eIDAS process currently. The aim of the wallet is identified as market-based to boost economic activities via online providers with increased identification opportunities, but the Commission has emphasised that the users would have heightened possibilities to govern their own data and that the ID would remain optional to give room to those who desire to opt-out. The plan is to launch a test project for the ID in October 2022 EU-wide after all member states have approved the initiative. Finland has aimed to establish itself as a driver for this digital ID wallet, as it has a possibility to "create common European technical architecture and common standards" and "equitable conditions and opportunities for everyone accessing public services" through a digital identity platform (Ministry of Finance, 2021).

Currently in Finland, the process of strong online authentication is divided between two governmental regulators, the Financial Supervisory Authority FIN-FSA ('Finanssivalvonta') and Traficom (Signicat, 2020). Whereas the former regulates the process of payment services initiative under the PSD2 regulation, and thus payment related Act 898/2017 and Act 890/2017, the latter governs authentication on other electronic services and governmental issues under the eIDAS regulation, and thus the Act 617/2009. This separation into two different regulatory frameworks has provided practical problems, when both parties want to keep their issues separate in the somewhat overlapping processes. For citizens and service providers, the issues are often seen as mutual due to their similarity in everyday life, feeding into the complexity of the system (Signicat, 2020). This problem, however, is inherited from the EU level, where the harmonisation of the two regulations has left gaps in national layouts of the processes. In practice, Traficom has reported in 2020 that there has previously not been any impediments on the matter, but due to the insufficiency of using bank coding lists as a sole identification factor set out by FIN-FSA, this will affect processes under Act 898/2017 and Act 890/2017 but also Act 617/2009 in providing new methods for identification by bank services (Traficom: National Cyber Security Centre, 2020).

In Finland, the national regulation on strong online authentication has been modified to complement the eIDAS regulation in 2016 and therefore it can provide a platform for future cross-border authentication activities as outlined above (Juutinen, 2021). The aforementioned Act 617/2009 regulates the requirements for strong authentication - meaning the identification of a natural person electronically - for the service providers, the public and the trust network providers (Finnish Parliament, 2011). In regard to the role of the banks in this process, the Act 617/2009 recognizes the role of bank credentials as a commonly used device for authentication. For example, in 2020, bank credentials were used by 89% of the users, who logged into the governmental services through Suomi.fi service, while only 7% opted for using mobile certificates, provided by Finnish mobile operators (Finnish Parliament, 2011). This highlights the centrality of bank credentials on the national scale. The Act 617/2009 is currently in the process of modification; specifically, statute 6 to include the requirement for

identification and trust services providers to check the personal identity code of an applicant when using strong authentication.

In regard to the regulation on the availability of strong authentication for all citizens, at the current stage, the Finnish identification law does not include a mandate for the right for a citizen to gain access to strong online authentication. As mentioned in the previous section, Finnish legislation entails that a natural person's possibility to obtain strong authentication is tied to having a Finnish personal identity code and without it, strong authentication is not possible (Juutinen, 2021, p. 32). As this process is also tied to access to bank services and credentials, the Act on Credit Institutions, chapter 15, statute 6, further enforces that banks are not obligated to provide these services when a natural person does not possess a Finnish personal identity code or they are not listed in the civil registry, making it harder for non-nationals to use strong authentication as a means for identification.

With the amendments to the Act 617/2009, the problem does not seem to be addressed in legislation, even when recognized by Traficom. As regarded by the EU regulation, legal persons of foreign nationalities in a given country are all subject to the national regulation on strong authentication. Those individuals who do not fill the requirements of the current regulation, like foreign students or immigrants, are hindered in gaining access to the Finnish strong authentication systems (Juutinen, 2021, p. 61). This will be further explored in section 4.1.

In sum, the legal framework on strong authentication in Finland is currently governed by both the EU-wide eIDAS and PSD2 regulations and the national legislative items, meaning the identification related Act 617/2009 in addition to the payment related Act 898/2017 and Act 890/2017, creating a complex legislative environment. Currently, bank credentials are widely recognized in the Finnish legislation, but the equality of access to strong authentication is not mandated as a right for all natural persons, and thus those lacking a Finnish personal identity code are excluded from this identification possibility. All of this constitutes the role of bank credentials used in strong authentication systems in Finland, further explored in section 3.

3. The FTN's benefits put into practice: convenience, enhanced safety, multi-sector applicability - a necessity in everyday life

This section will identify the major benefits of the implementation of strong authentication using bank credentials in the case of Finland. Advantages such as customer convenience, high-security standards and an overall positive reception will be critically assessed with regards to the different fields of its usage. The main difficulty one is faced with when researching this topic is the lack of academic literature given. This section thus draws predominantly from websites, the academic assessment on previous authentication systems, such as TUPAS, which preceded the Finnish Trust Network, as well as a survey (see: Appendix 1) conducted on users' experiences.

As elaborated before, identity authentication is a key element of future society and government. It is therefore one main task for each administration to ensure the framework for a safe and successful implementation of digital authentication into the broader context of eGovernment. Building on a definition provided by the EU, the term 'eGovernment' is defined as a digitised governmental platform that employs "tools and

systems to provide better public services to citizens and businesses" (Lentner & Parycek, 2016, p. 9). To live up to security standards, eGovernment thus most certainly requires strong authentication.

The first major advantage of general strong authentication is the aspect of convenience for its users as well as providers. Strong authentication is used in a variety of contexts, i.e. accessing eGovernment services, logging into the university website, creating a library account or using HSL transport discounts. In 2010, the Finnish government launched the 'patient accessible electronic health records' (PAEHR) comprising a variety of possibilities for patients to digitally access their data, book an appointment with the practitioner or receive and view one's prescription (Erhola et al., 2019, pp. 299f.). The wide range of services all accessible in one place is highly convenient for the patient as it facilitates keeping track of one's health condition and medical records. Evidently, such sensitive data cannot be accessed without any form of identification, wherefore, strong authentication is an inevitable function which must be included in such a service. The study presented by the Finnish Journal of eHealth and eWelfare furthermore shows that the number of Finnish citizens using the services provided in the health sector is steadily increasing with two out of three adults accessing some service offered in 2018 (ibid., p. 306, 308).

A second factor of heightened convenience resulting from the application of the FTN is the possibility of cross-border authentication. ElDAS allows for providers of authentication systems implemented in different states to apply for EU notification. In theory, this means that once affirmatively peer-reviewed by the European Commission, a Finnish citizen using bank credentials to authenticate, can make use of the very same method to prove his or her identity in various other EU member states. Vice versa, an Italian citizen - provided that the Italian system has been approved - can use that method when accessing Finnish e-services (Op developer). This means that providers of authentication services are not forced to spend time and effort on designing individual solutions for each country resulting in a decreased amount of bureaucracy (Op developer).

So far, inter-European authentication applies only to services of the public sector and the expansion of including more member states of the European Union is still an unfinished process (Traficom). Nonetheless, cross-border authentication is more than simply convenient; it is a useful means for enhancing mobility within the EU (Op developer).

An undoubtedly important issue regarding digital services is safety and transparency. As stated in the Nordic Digital Promise, consumers are willing to lightly give away their data to platforms owned by private companies making their lives significantly easier (2018, p. 40). The Finnish Trust Network on the other hand is a system that was brought to life by public institutions which need not equally consider economic aspects as private enterprises do. It can therefore be argued that in a country like Finland, a responsible management of sensitive data is perhaps best ensured by the state's administrative body. Besides economic aspects, the state is furthermore held accountable to a higher extent for the system's impact.

As a result of this accountability, TUPAS was replaced when its lack of data security crystallised, e.g. an individual's personal identity code was passed on without encryption (Op developer). Other methods, such as authentication by voice or by

verifying an email address, have proven to bear a high potential of facilitating identity theft (Pathak et al. and Andrade et al., 2012, p. 2, 71). Although a so-called 'perfect solution' is yet to be found, using bank credentials appears to cause the least of security concerns. The procedure, to which an authentication provider must commit before being allowed to offer their service, is transparently laid out on the Traficom website. Providers are obliged to notify Traficom of their plans, reporting periodically on how they intend to conform to standards of security. Traficom moreover has the authority to prohibit providers from offering their services in case they do not meet requirements (Traficom).

If one agrees with the statement that "political decisions […] influence the direction of technological development" (Nordic Digital Promise, 2018, p. 28), it was momentous that Finnish policy-makers brought to life a strong authentication system available to every resident. FNT represents an alternative to authentication methods that have already proven to be flawed in many regards.

Lastly, it is largely indisputable that any modern society of the 21st century will not be able to avoid technological progress just as little as politics will be able to refrain from promoting eGovernment. The resulting question therefore does not evolve around *if* but *how*. By comparing the usage of the Finnish electronic ID card with the usage of bank credentials, Rissanen finds that more than 99% of online transactions, including the public as well as the private sector, were made using the FTN's preceding system TUPAS (2010, p. 176). He concludes that this clear preference is due to the Finnish singularity of providing one method of authentication for both, eGovernment and eCommerce (ibid., p. 193). The article moreover demonstrates that a clear demand for secure and effective online authentication has already existed for a while now, e.g. for online payments.

By examining the survey conducted for this paper, one can observe that more than 65% of the participants claimed to be either satisfied or very satisfied with the current strong authentication in Finland and 82% acknowledge that life would be harder without having the ability to use it (Survey, 2021). As only 48% of the participants stated to not have experienced any obstacles during the process of obtaining bank credentials, a closer examination of the open comment section clarifies that the procedure demands refinement (ibid.). To ensure the approval of Finnish residents, the challenge at hand lies not with the method itself but with improving the process of accessing it. Evidently, this survey should merely be taken as a starting point as it needs to be expanded for further, more in-depth study. It does nevertheless echo with the findings of a study published recently by Traficom which stresses the fact that the responsible authorities are aware of the FTN's shortcomings (Traficom Study, 2021, p. 3).

This section has highlighted the benefits of the Finnish system of strong authentication using bank credentials ranging from convenience of using a single authentication method and speed to higher standards of security and the already existing usage of the system for various purposes.

4. The Shortcomings of Using Bank Credentials for Strong Authentication

4.1. Inequality and Accessibility Issue: Case of Outsiders

The strong authentication system in Finland holds a significant role in accessing online public services such as Kela, the Tax Office, healthcare services and so on. Public but also private services alike, such as mobile phone subscription providers, might require strong authentication in order to grant access to their online services. Taking into consideration the scale of digitisation in the conduct of daily life in Finnish society, comprehensiveness in terms of granting access to online banking credentials is a crucial aspect to consider when equality is taken into account. This section aims to provide a critical overview of the process of obtaining online banking credentials which is being used for strong authentication, from the perspective of nationals coming outside of the European Economic Area (EEA).

The two most popular (due to their English service for international people) banks in Finland, Nordea and OP, present requirements of obtaining bank credentials to access strong authentication as follows: 1. Finnish personal identity code ('henkilötunnus') with a permanent address in Finland; and 2. an ID document issued by a Finnish authority or by EEA countries, San Marino or Switzerland (Nordea, pp. 2-3).

These requirements raise an issue for the *outsiders* (non-EU/EEA nationals), since the accepted ID document issued by "foreign authority" only refers to authorities from the EEA zone and the two exception countries of San Marino and Switzerland. Furthermore, the prior condition is obtaining the Finnish Personal Identity Code and an 11-character-identifier generally provided to foreigners together with their residence permit result. If not, an application to the Digital and Population Data Services Agency *"DVV"* for registration is needed. However, apart from the long waiting time to get an appointment, DVV states that the processing time of registration of foreigners might take up to 6 weeks after application (DVV, 2020).

In 2014 and 2015, Yle News interviewed two *outsiders* regarding discriminative procedures of banks while granting online access rights. In the interview, a non-EU national who had recently moved to Finland explained that they had to wait over one year just to have their bank account opened. They added how difficult it had been for them to integrate into Finnish society since the strong authentication via banking credentials is so broadly used in the country, but also how they encountered investigative questions about money laundering and drug smuggling during their appointment with the bank (Yle, 2014). Moreover, another interviewee, Andy Allred, who had been working in Finland for many years prior, got rejected when requesting online credentials due to his American passport as the bank did not trust his identity - his ID document was issued neither by a Finnish nor an EU authority (Yle, 2015). On this topic, Yle also interviewed OP (Osuuspankki) Senior Manager, Sirkku Ikäheimo, who addressed the reason behind such implementation. Ikäheimo stated as follows: "The problem is that with other passports we are unable to identify if there is any forgery. There are so many passports in the world we can't be educating our personnel to identify all kinds of passports" (ibid.).

Banks also often refer to Finnish legislation, the Act 617/2009, in justifying their online banking policies. However, the indication of "another state" under Section 17 is often being passed off by banks:

> "…In initial identification that is solely based on a document issued by an authority showing the person's identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification-means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state..." (Act 617/2009, Section 17: 1009/2008).

An important point to mention is, before the legislation reform in 2017, the Ombudsman for Minorities also received complaints from EU/EEA nationals facing obstacles obtaining online banking credentials and National Discrimination Tribunal examined cases (Kortteinen, 2014). According to banks, the risk of money laundering and terrorist financing is higher, in case of non-Finnish government-issued ID documents; however, the Tribunal found such action discriminatory and as having no legal basis (ibid). Thereafter, Finland adopted a new law in January 2017 that guaranteed access rights to EU citizens for online banking credentials (Yle, 2016). One could say that such a response deepened the inequality within minorities, ignoring non-EU nationals in Finland as if they were not susceptible to the same problems as EU residents do.

In this sense, to enhance foreigners' accessibility to strong authentication system, FIN-FSA and the Non-Discrimination Ombudsman collaborated to promote the reform of "Foreigner's ID card", which was adopted in 2017 (K 6/2018 vp). The Foreigner's ID card issued by the Finnish Police, then, appears as the only alternative for non-EU residents in Finland to obtain banking credentials. On the other hand, requirements of obtaining the Foreigner's ID card might be perceived as inconsistent. The reason behind this statement is, Finnish banks seem to assume a trust towards ID documents issued by Finnish authorities. However, the Police issues Foreigner's ID cards on the basis of applicants' passports and residence permit cards (cf. Police of Finland). Therefore, the prerequisite of a Foreigner's ID card is already the non-EU/EEA passport itself, which is found not reliable enough by Finnish banks to grant online banking credentials.

Receiving up-to-date data about recent experiences of non-EU nationals further benefited us to better examine current situations regarding accessibility of strong authentication. Thus, a Google Survey on Finnish strong authentication system (see: Appendix 1) was conducted with 47 anonymous people residing in Helsinki, between the dates 15.10.2021 and 31.10.2021: 20 people reported they are from outside the EU, 14 as Finnish citizens and 13 as non-Finnish EU nationals. Participants were asked about the time period of obtaining bank credentials since the beginning of the application via open-ended questions in order to receive a wider scope of answers. Results varied generously: while some reported 1-2 weeks, 5 answers recorded time lengths expanding from 5 months to over a year. Following the multiple-choice question directed at participants: *"*Do you feel that the adoption of the strong authentication via bank credentials system is discriminatory towards non-Finnish citizens, especially non-EU

nationals?". More than half of participants, 53.2%, found it discriminatory towards non-Finnish nationals.

Participants were also requested to share more details about their experiences on using strong authentication via bank credentials as an optional part of the survey. Several participants mentioned how their stay in Helsinki was limited, therefore not having a Finnish bank account; however starting from January 2022, HSL will be selling student tickets only using their mobile-app which requires strong authentication. Four participants stated their deep frustration withthe process as a whole, underlining the extra cost of 60€ to receive an additional ID card from police, which is issued already based on their passport and having no other use. Another widely common complaint was long waiting times and the complexity of each step, e.g. from DVV registration to bank appointments. Since the system as a whole functions at a slow pace in terms of waiting for appointments and then for processing times already, non-EU/EEA nationals encounter only more difficulties.

A salient point underlying the system complaints of non-EU residents was the non-existence of any other alternative to access strong authentication other than the Finnish ID card reader and *Mobiilivarmenne* options, which both require the aforementioned Foreigner's ID card from the police. Although banks may open a bank account for *outsiders*, they might require monitoring bank transactions before granting online credentials to ensure it is not being used for money laundering purposes, which might take up to several months or over a year. On the contrary, such presumption is simply avoided if the applicant provides a Finnish or EEA ID document. Nonetheless, procedures highly vary between banks, which indicates how the system actually does not have a policy coherence. Considering the criticality of the authentication system in the conduct of everyday life in Finland, authorities should extend their usage of the term "foreigners" to include non-EU nationals.

4.2 Questions of privacy, safety and handling of data

In recent times, privacy and data protection laws have entered the forefront of public discourse, especially regarding (inscrutable) data collection by public offices as well as private corporations. The 21st century has witnessed smartphone technologies become a catalyst in the disintegration of age-old personal information protection practises; having simultaneously opened the pandora box of companies' access rights.

At the core of the aforementioned discussion is the concept of privacy, a term that is yet to receive effective definition, or attention, by scholarship. Alan Westin (1967) complained that "few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists" (Bier, 1980, p. 199). In the context of this research it is helpful to take John Locke's description of privacy as a 'natural right' into account, which he provided in the process of pushing for policies and legislation that protect personal information (Duff, 2004).

Information privacy, data accumulation and democratic interests have become heavily interconnected in modern political and social life. As Keller (2019) argues, the anonymity and obscurity once offered by the influx of people into cities are becoming

increasingly irrelevant and digitisation has seen public participation radically transform. What is more, combined with smartphone technology, internet banking has shaken up the entire financial ecosystem and revolutionised the way we conduct our daily lives. Mobile phones' banking apps have essentially become one-stop authentication channels and financial institutions have embraced this shift by making each person's smartphone "the central hub for functionality and security" (Thales Group). Some could argue that this accumulation of data access-power on banking corporations' lap is rather concerning.

Recent years have seen the emergence of several data misuse scandals, including the famous example of Cambridge Analytica, that have raised questions of how individual rights, data collection and privacy are correlated. As a result, liberal democracies recently began to recognise 'information privacy' and 'data protection' as fundamental rights that are heavily intertwined with the concepts of "personal autonomy, dignity and agency" (Keller, 2019, p. 151). It could be argued that liberalism's strict aversion towards protective paternalism is slowly loosening, paving the way for new data protection practises including the European Union's General Data Protection Regulation (GDPR, 2018).

"The prevailing liberal democratic model of information law", Keller (2019, p. 132) argues, "is structured around two key concerns: protecting the state's powers of ultimate access to information, and ensuring that all information remains potentially marketable." States' powers in relation to information access have been integral to their ability to protect themselves as well as the public from harm such as violent threats like terrorism. Liberal market economies, on the other hand, have capitalised on and monetised personal information via acquisition and trade. These data flow transformations have occurred before our very eyes, with the seeming 'consent' and support of the population thanks to promises such as safety and convenience – while some groups, i.e. people from a lower socio-economic background, could simply not afford to protect their privacy in light of these transformations (Franks, 2017; Hess, 2017; Morozov, 2017; Bridges, 2017).

Recent developments have ultimately presented liberalist societies and technologies with a dilemma. Margaret Hu (2017, p. 1830) argues that the individualised 'reasonable expectation of privacy' ought no longer be investigated as a "individual-based tangible harm" issue but rather as an issue of "society-wide intangible harm." For that reason, consolidating our understanding of privacy is in fact crucial to recognising the risks that a compromised information privacy can have on a societal level, and seeing how the free reins of liberalism can jeopardise the very autonomy of the individual that it has historically sworn to defend.

In order for new legislation on data protection to be effective, Information Society academic Alistair Duff insists that the legislation ought to require that personal information is:

1. Fairly and lawfully processed,
2. Processed for limited purposes
3. Adequate, relevant, not excessive
4. Recorded accurately
5. Not kept longer than necessary

6. Processed in accordance with subject's data rights
7. Secure - not transferred to countries lacking protection (Duff, 2004; Relyea, 2001)

These measures are by and large covered in the EU's 2018 GDPR Bill among other declarations such as that each individual has the right to be forgotten (Article 17). Do, however, the aforementioned measures or 'values' agree with the infiltration of the authentication via bank credentials and does the GDPR conflict with the adoption of this authentication method?

According to Juha Mitrunen, head of the Digital Identity Development Project and senior specialist at the Ministry of Finance, the matter is not entirely black or white and the real problem occurs when authentication paves the way for profiling. Bank companies can operate as data owners and processors but only to a limited extent; only within the limits that the GDPR and eIDAS. "For example, a bank holds the data about how much money I have in the bank account today, they also know that it's their bank account. So, they are data owners, and they are data processors, but still they cannot use that data for certain purposes – the GDPR prevents them," Mitrunen said during the interview. (see: Appendix 2)

The Finance Ministry's leading expert argues that the Finnish bank authentication system is safe in regard to privacy due to the following factors: 1. Finnish banks are trustworthy and licensed by the Finnish government itself (hence the name Finnish *Trust* Network), 2. they have to comply with regulations such as GDPR and are being monitored by public bodies and finally, 3. Finnish banks rarely get to even access, let alone combine, information, due to their role as tools of proof rather than authentication. (see: Appendix 2)

Unlike Google Pay and Apple Wallet, Finnish banks receive licences by the Finnish government. The monitoring of compliance with GDPR and eIDAS is jointly carried out by Traficom and the Finnish Ministry of Finance, which mainly focuses on the financial sector. "According to section 42 b, it is the responsibility of the Data Protection Ombudsman to monitor compliance with the provisions of this Act regarding personal data," Traficom added in their email correspondence, referring to the Act on Strong Electronic Identification and Electronic Trust Services (617/2009) (see: Appendix 3).

The Finance Ministry specialist further explained that sophisticated profiling can only occur if the company has access to more detailed information about the user. "Like with Apple and Google and Facebook, they go deeper, they go to the content, they go to actual information," Mitrunen said, adding that "banks only go to the information if it's related to the bank business" (see: Appendix 2).

According to Juha Mitrunen, as private companies, banks may seek to protect their business interests via collected data relating to the finance sector. This is evident in the following extract, which Mitrunen later described as a case of "misbehaviour" (see: Appendix 2) against the GDPR:

> *Juha Mitrunen*: "Now we are talking about banks, I can make a similar example about Apple or mobile operator or Google or whoever but think about this; I'm applying for a loan from the bank. I'm planning to buy a house. At the same time, I'm visiting a website which advises people who have problems with online

> gaming so now my bank knows that I have some problem with online gaming. And I'm applying for a loan from the bank. So […] you don't have to be a rocket scientist [to understand that], I might have problems getting the loan now."
>
> *Veronica Kontopoulou*: "Oh right, so is this actually happening?"
>
> *Juha Mitrunen:* "This is profiling. I can't prove that it is happening. But it is something to think about."

Ultimately, the extent to which banks can actually gather data for profiling purposes remains rather unclear. Originally meant as a secondary channel, the digital Finnish bank authentication system has allowed Finnish banks to accumulate power and essentially become gatekeepers. It is clear, however, that with increased powers, come increased opportunities for data manipulation, such as in the case of profiling, which go strictly against the principles set by the GDPR and eIDAS. In the interim, it could be argued that messages of the sentiment "in the banks we trust" (see: Appendix 2) fail to provide necessary assurance with respect to data safety and privacy.

6. Conclusion

In order to forward digitisation and promote eGovernment in the Information Age, the development and creation of adequate means of strong authentication is key. This research paper introduced and assessed the method of strong authentication via bank credentials used in the case of Finland, that is, the Finnish Trust Network which followed the previous system TUPAS. It has also explained the multi-factor process and presented an overview of both TUPAS and the Finnish Trust Network with the switch backed by reasons related to cybersecurity. This paper also encompasses the strong authentication procedure through simple steps: obtaining the bank credentials, presenting them to the service provider, identifying the credentials by the bank followed by sending an identification code and finally the exchange of the identification code for an ID Token by the service provider.

Similarly, this paper further showcased that the strong authentication process is governed by the eIDAS and PSD2 regulation within the EU, which frame and inform the national legislation in Finland on the issue. The Finnish legislative items, the Act 617/2009, Act 898/2017 and Act 890/2017, have provided the means to govern identification and authentication in Finland via bank credentials, with a future focus on enabling cross-border authentication, but currently, this ability is limited with non-nationals not being granted the same access to authentication methods, fostering, thus, inequality.

Implementing the FTN allows its users to authenticate in a more secure and more convenient way as compared to previous systems. The wide-ranging field of utilisation does not only result in heightened practicality but moreover aids in decreasing bureaucratic burdens enabling even cross-national authentication.

While the shift from TUPAS to the FTN was done on the premise of enhanced security, this research's findings recommend for a better assurance of data security in relation to data storage and processing, such as in the case of profiling. This concern is reflected in the ardent (some could even argue 'blind') trust attributed to Finnish-

government licensed institutions and authorities which is contrasted by the high levels of suspicion towards non-national residents, especially in the case of non-EU/EEA nationals. While public bodies hasten to keep regulations efficient and up-to-date, loopholes susceptible to 'trust' mean that their strict monitoring is as timely and crucial as ever.

Meanwhile, Finland's institutional emphasis on the notion of equality could be practised more competently in regard to non-marginalised understanding of 'trust' towards its residents. Although strong authentication via using bank credentials notably reduces the burden of bureaucracy and thus expedites the daily life of residents, its comprehensiveness on the basis of granting such access is still contested. This paper revealed the need for reconsideration of the current complex, discriminatory and oftentimes incoherent 'regulations' towards non-EU/EEA nationals which are being exercised by banks in the provision of online access codes.

Further research could inspect whether this high level of the aforementioned trust is indeed justifiable, especially considering the low levels of academic scrutiny exercised on this topic. Moreover, there is an evident gap within the field of social sciences that ought to be filled in order to gain further insight into the cultural, political and economic implications the FTN (and comparable authentication methods) have on our society. Only by loosening the current overwhelming emphasis on technical aspects, can a deeper and more comprehensive understanding of the topic as a whole be achieved.

It is evident that society cannot evade the need for digital authentication and even though the Finnish solution might not be flawless, its potential should not be ignored. Hence, continuous improvements of the FTN is an essential task for the future, especially around its shortcomings on safety and equality, as a preferred alternative to the system's total removal or replacement altogether.

References

Andrade, A., Aura, T. & Suoranta, S. (2012). Strong authentication with Mobile Phone. In Freiling, F. C. & Gollmann, D. (Eds.). *Information Security*. Springer, Heidelberg.

Bier, W. C. (1980). *Privacy: A Vanishing Value?.* Fordham University Press, New York.

Bridges, K. (2017). *The Poverty of Privacy Rights*. Stanford University Press, California. 133-178.

Cater, L. (2021). The EU has introduced a new 'digital' ID. Here's what it means for
you. *Politico*, 3 June. Available at: https://www.politico.eu/article/eu-europe-digital-id/ [Accessed: November 2, 2021].

CEF Digital. (2020). *New notified eID schemes in 2020*. Available at: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2020/12/17/New+notified+eID+schemes+in+2020 [Accessed: November 3, 2021].

Danske Bank. (2019). *Finnish Trust Network - Danske Bank's Identity Provider Business Documentation', in 'Electronic Identification Service Specifications.* Available at: https://danskebank.fi/-/media/pdf/danske-bank/fi/en/yritysasiakkaat/muut/ftn-idp-business-documentation.pdf?rev=a8db10b51a154f038bc4e91d88c80bbe&hash=B9AD31491E9676A2B12C506FC90C9A47 [Accessed: November 2, 2021].

Digital and Population Data Services Agency. (2020). *Processing Times of customers' applications and other requests*. Available at: https://dvv.fi/en/-/delays-in-customer-service-for-individuals [Accessed: October 30, 2021].

Duff, A. S. (2004). The Past, Present, and Future of Information Policy. *Information,*
Communication & Society, 7(1), 69–87. doi:10.1080/1369118042000208906

European Parliament. (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=FI [Accessed: November 3, 2021]

Eranti, V., Koponen, J., Leppänen, J., Lätti, R., Mikkonen, J., Neuvonen, A., & Rantanen, K. (2018). The Nordic Digital Promise: Four theses on a hyperconnected society. *Demos Helsinki*. Available at: https://demoshelsinki.fi/wp-content/uploads/2018/04/the-nordic-digital-promise_web-compressed-double.pdf

FIN-FSA. (2019). *PSD2*. Available at: https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/psd2/ [Accessed: November 3, 2021].

Finnish Ministry of Finance. (2021). *Press Release: Finland and Germany intensify cooperation to promote digital identification.* Available at: https://valtioneuvosto.fi/en/-/10623/finland-and-germany-intensify-cooperation-to-promote-digital-identification [Accessed: November 2, 2021].

Finnish Parliament. (2011). *Hallituksen esitys HE 237/2020 vp*. Available at: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_237+2020.aspx [Accessed: November 3, 2021].

Finnish Transport and Communications Agency 'Traficom'. (2021). *Electronic identification*. Available at: https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification [Accessed: November 3, 2021].

Finnish Transport and Communications Agency 'Traficom'. (2020). *Finnish Transport and Communications Agency survey of 4 August 2020 on the update needs of Regulation 72A/2018 on Electronic Identification and Trust Services and of other technical guidance.* Available at: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/M72B_questionnaire_final_EN.pdf [Accessed: November 2, 2021].

Franks, M. A. (2017). Democratic Surveillance. *Harvard Journal of Law and Technology*, 30(2), 425.

Hess, A. (2017). How Privacy Became a Commodity for the Rich and Powerful. *The New York Times Magazine*. Available at: https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html [Accessed: November 3, 2021].

Hu, M. (2017). Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test. *Washington Law Review*, 1819-1903.

Hypr. Strong Authentication. In *Security Encyclopedia.* Available at: https://www.hypr.com/strong-authentication/ [Accessed: November 2, 2021].

Hämeen-Anttila, P. (2019). *eIDas and Finnish Trust Network bring an end to TUPAS – is your company all set for the change?*. Available at: https://op-developer.fi/articles/more-security-and-less-bureaucracy-in-user-authentication [Accessed: November 3, 2021].

Intersoft Consulting. (2018). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Available at: https://gdpr-info.eu/

Jormanainen, V., Parhiala, K., Niemi, A., Erhola, M., Keskimäki, I., & Kaila, M. (2019). Half of the Finnish population accessed their own data: comprehensive access to personal health information online is a corner-stone of digital revolution in Finnish health and social care. *Finnish Journal of eHealth and eWelfare*, 11(4), 298-310. doi: https://doi.org/10.23996/fjhw.83323

Juutinen, J. P. (2021). Sähköisen tunnistamisen markkinat. *Traficomin tutkimuksia ja selvityksiä*, 2/2021.

Lentner, G. M. & Parycek, P. (2016). Electronic identity (eID) and electronic signature
(eSig) for eGovernment services – a comparative legal study. *Transforming Government: People, Process and Policy*, 10(1), 8-25.

Keller, P. (2019). The reconstruction of privacy through law: a strategy of diminishing
expectations. *International Data Privacy Law*, 9(3), 132–152. Available at: https://doi-org.libproxy.helsinki.fi/10.1093/idpl/ipz012

Kerttula, E. (2015). A novel federated strong mobile signature service—The Finnish case. *Journal of Network and Computer Applications*, Vol. 56, 101-114. doi: https://doi.org/10.1016/j.jnca.2015.06.007.

Kortteinen, J. (2014). National Discrimination Tribunal prohibited ethnic discrimination in the provision of banking services. *Ministry of the Interior in Finland*. Available at: https://intermin.fi/en/-/national-discrimination-tribunal-prohibited-ethnic-discrimination-in-the-provision-of-banking-services

Krupa, W., Parkkonen, M., Stempel, K., Baglan, N., & Kontopoulou, V. (2021). Finnish strong authentication system. *Google Forms*. Available at: https://docs.google.com/forms/d/13ztTxK_9JriYf0gD2_4a_czHINCnzIFvqD0nPXEafiw/edit#responses

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review*, 95(1), 53-125.

Ministry of Transport and Communications in Finland. (2019) *Act on Strong Electronic Identification and Electronic Trust Services 617/2009.* Available at: https://www.finlex.fi/en/laki/kaannokset/2009/en20090617.pdf

Morozov, E. (2017). We All Have the "right to disconnect" – But only Some of us can
Afford It. *The Guardian*, 19 February. Available at: https://www.theguardian.com/commentisfree/2017/feb/19/right-to-disconnect-digital-gig-economy-evgeny-morozov

Nordea. *Identification principles for services using strong electronic identification*.
Available at: https://www.nordea.fi/Images/147-231054/identification-principles-for-services-using-strong-electronic-identification.pdf [Accessed: October 28, 2021].

OP-Pohjola Group. *Accepted personal ID documents*. Available at: https://www.op.fi/accepted-personal-iddocuments [Accessed: October 28, 2021].

Pathak, M., Portelo, J., Raj, B., & Trancoso, I. (2012). Privacy-Preserving Speaker Authentication. In Freiling, F. C. & Gollmann, D. (Eds.). *Information Security*. Springer, Heidelberg.

Pimiä, K. (2018). *The report of the non-discrimination ombudsman to the parliament*: *K 6/2018 vp. Finland*. Available at: https://rm.coe.int/fin-the-report-of-the-non-discrimination-ombudsman-to-the-parliament/16808b7cd2

Police of Finland. *How to apply for an identity card.* Available at: https://poliisi.fi/en/how-to-apply-for-an-identity-card

Relyea, H. C. (2001). Information policy: legislating personal privacy protection: the
federal response. *Journal of Academic Librarianship*, 2(1), 36–51.

Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. *IDIS* 3, 175–194. Springer International Publishing. doi: https://doi.org/10.1007/s12394-010-0049-8

Signicat AS. (2019). *7 things you need to know about TUPAS being replaced with Finnish Trust Network*. Available at: https://www.signicat.com/blog/7-things-you-need-to-know-about-tupas-being-replaced-with-finnish-trust-network [Accessed: November 3, 2021].

Signicat AS. (2020). *Sähköinen tunnistus – onko vahva tunnistaminen PSD2-yhteensopiva*?. Available at: https://www.signicat.com/fi/blogi/sähköinen-tunnistus-onko-vahva-tunnistaminen-psd2-yhteensopiva [Accessed: November 3, 2021].

Stenius, P. (2019). What is the Finnish Trust Network (FTN)?. *Ubisecure*. Available at: https://www.ubisecure.com/authentication/finnish-trust-network-ftn/ [Accessed November 2, 2021].

Suoranta, S., Haataja, L., & Aura, T. (2015). Electronic Citizen Identities and Strong
Authentication. In Buchegger S., Dam M. (Eds.). *'Secure IT Systems' Lecture Notes in Computer Science,* vol. 9417, 213-231. Springer International Publishing. doi: https://doi.org/10.1007/978-3-319-26502-5_16

Thales Group. *Mobile authentication solutions: For a frictionless digital banking*
experience. Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/sdk [Accessed: November 1, 2021].

Yle. (2014). Foreigners' banking still problematic. *Yle News*. Available at: https://yle.fi/uutiset/osasto/news/foreigners_banking_still_problematic/7613539 [Accessed October: 30, 2021].

Yle. (2015). Banks under pressure to offer online banking to foreigners. *Yle News*.

Available at: https://yle.fi/uutiset/osasto/news/banks_under_pressure_to_offer_online_banking_to_foreigners/7804023 [Accessed: October 30, 2021].

Yle. & Wall, D. (2016). Online banking access soon guaranteed for EU citizens. *Yle News.* Available at: https://yle.fi/uutiset/osasto/news/online_banking_access_soon_guaranteed_for_eu_citizens/9373490 [Accessed: October 31, 2021].

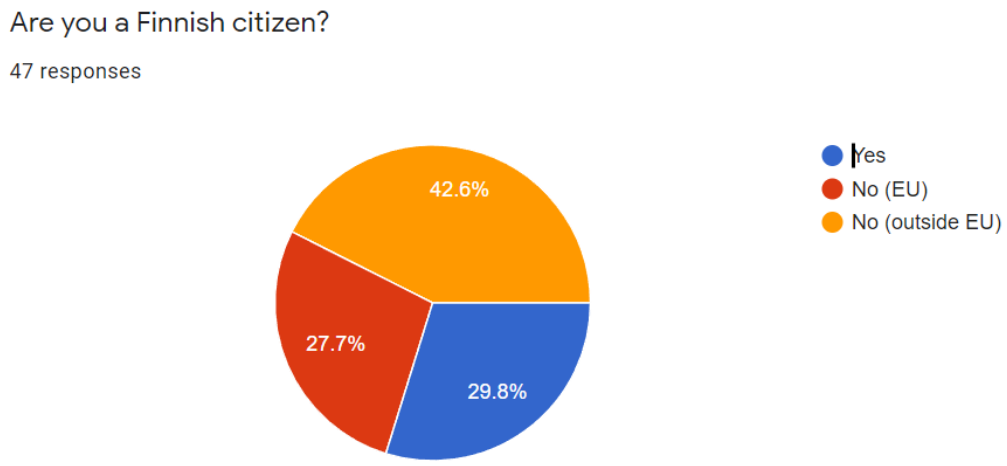
APPENDICES:

APPENDIX 1, Poll

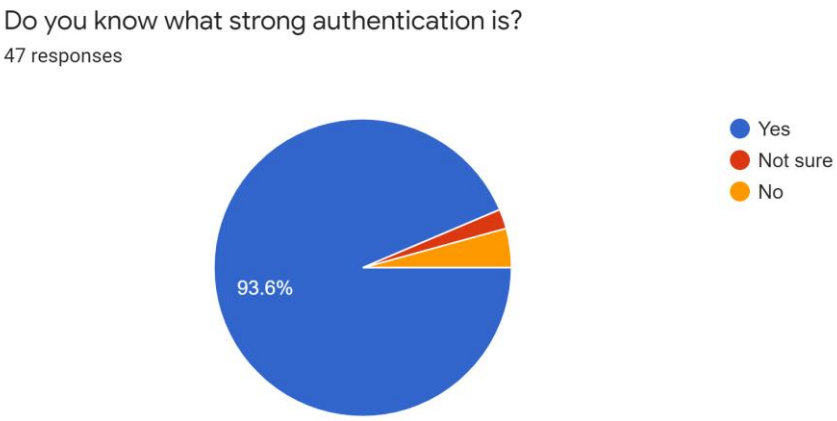
This paper has based its examination on an online study performed through Google Forms to which 47 participants residing in Finland responded. The participants answered

several questions regarding the strong authentication systems in Finland. Below you will find the data gathered during the study.

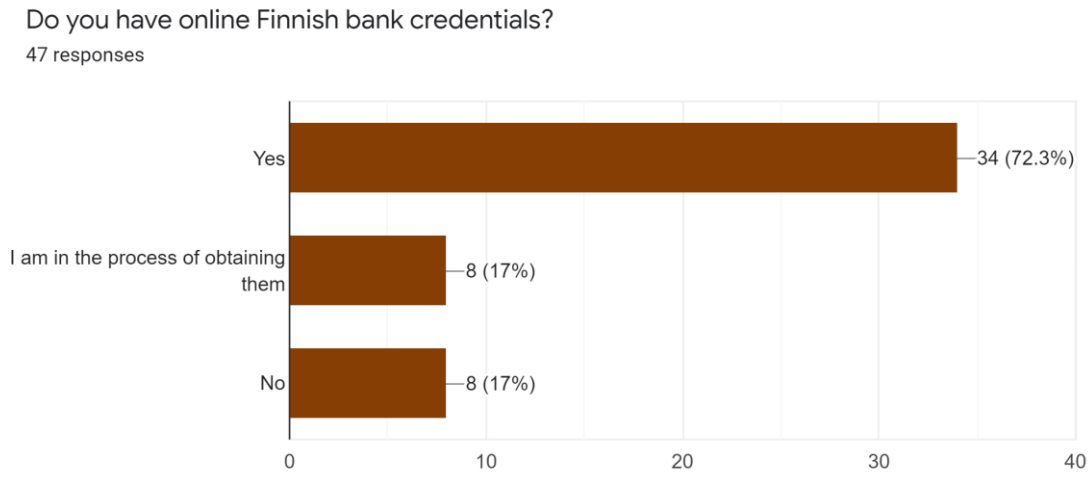
Q1: Are you a Finnish citizen?



Q2: Do you know what strong authentication is?



Q3: Do you have online Finnish bank credentials?



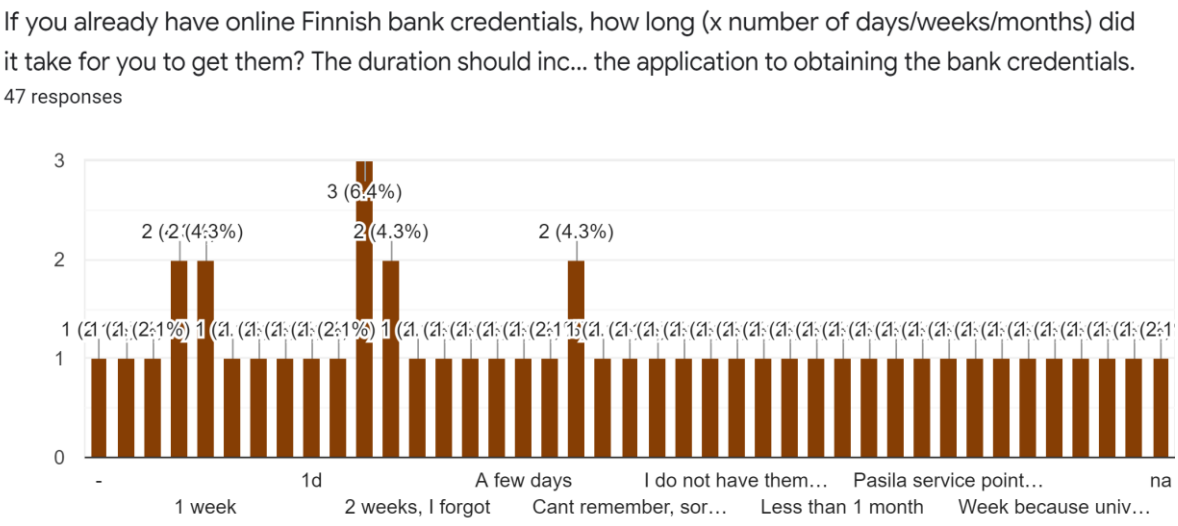
Q4: If you already have online Finnish bank credentials, how long (x number of days/weeks/months) did it take for you to get them? The duration should include the entire process from beginning the application to obtaining the bank credentials.

This question was open, and the answers are the following:

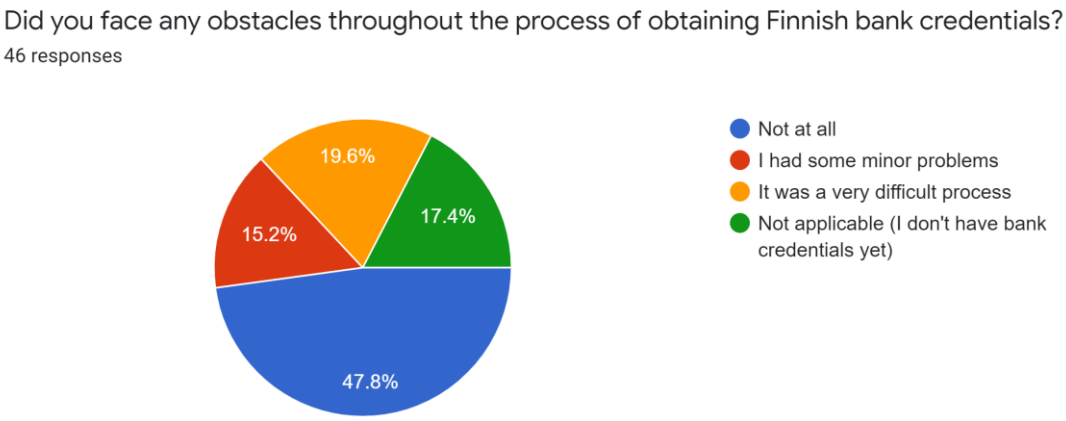
- 2 months (3 responses)
- 1 week (2 responses)
- About a week (2 responses)

- 1 month (2 responses)
- 2 weeks (2 responses)
- 12 months (1 response)
- Less than 1 month (1 response)
- Not applicable (8 responses)
- 1 day (1 response)
- Cannot remember (6 responses)
- 5 months (1 response)
- 5 days (1 response)
- Haven't yet obtained but have spent over 7 months waiting (1 response)
- Three months (1 response)
- '1st bank 1 day, 2nd bank 3 months' (1 response)
- More than 1 year (1 response)
- Do not have them yet, waiting for over 2 months (1 response)
- 'Pasila service point for applying and ID card is so hard to book, next available time is two months later, no info about the processing time after applying. after getting the ID card, still need to visit the bank' (1 response)
- A few days (1 response)
- A week (3 responses)
- 10 days (1 response)
- Several days (1 response)
- Do not know (1 response)
- 'So as someone from outside EU to get banking codes(online banking) OP asked me to apply for Finnish ID card from Police (in 2016). So after I had the ID it took me less than a week to get them. ID process was long.' (1 response)

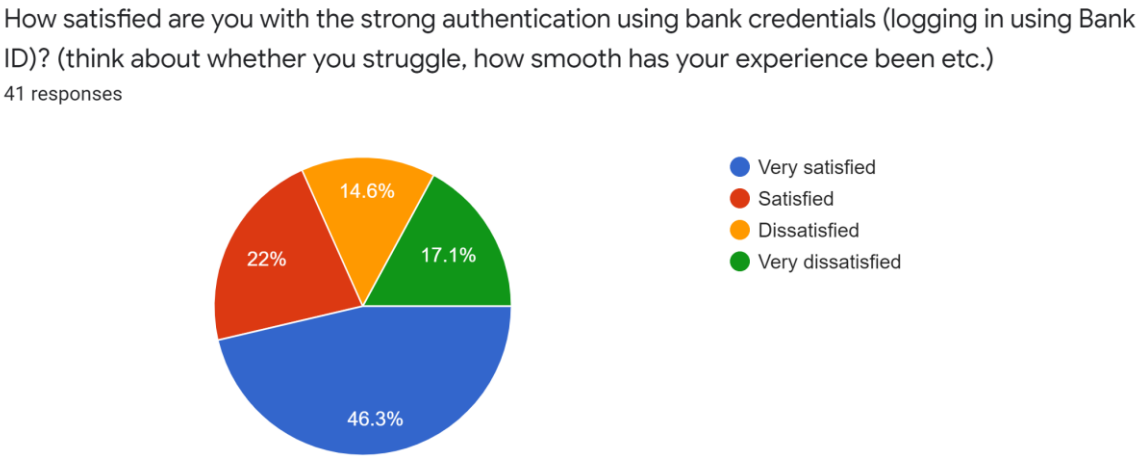
- ‘I didn't have them for a whole year because I didn't have a Finnish ID card and you need that first in order to get them. Finally, after a year I scheduled a Finnish ID card appointment which was a 3 month wait, then I needed to schedule an appointment with my bank which was another 3 month wait. After I had the appointment with my bank and could show the Finnish ID then it went quickly and I got the online Finnish banking credentials in the next few days.’ (1 response)
- 1,5 months (1 response)
- 2 weeks (1 response)



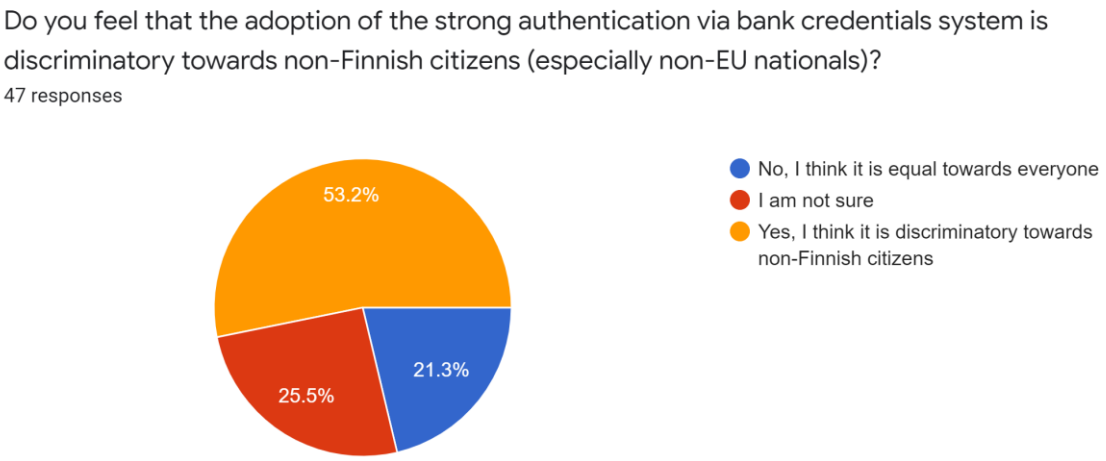
Q5: Did you face any obstacles throughout the process of obtaining Finnish bank credentials?



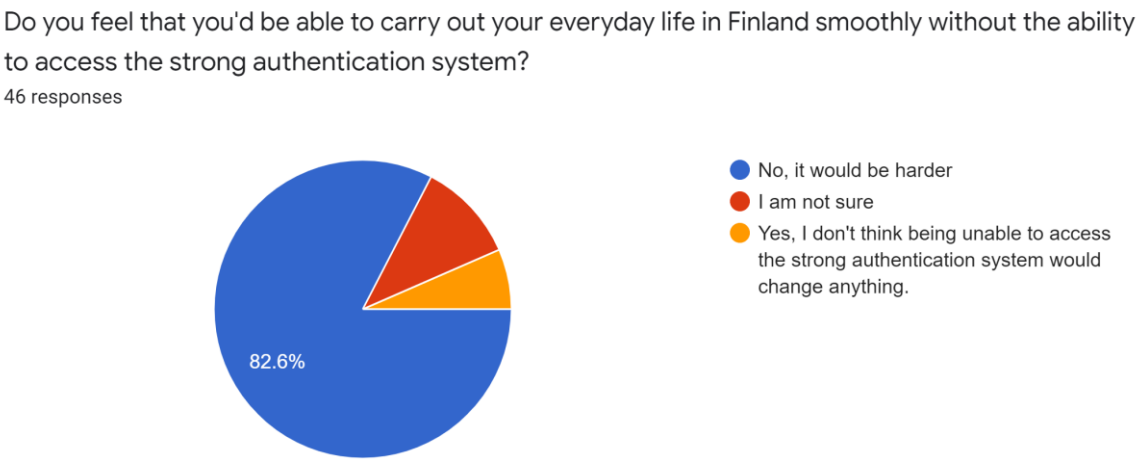
Q6: How satisfied are you with the strong authentication using bank credentials (logging in using Bank ID)? (think about whether you struggle, how smooth has your experience been etc.)



Q7: Do you feel that the adoption of the strong authentication via bank credentials system is discriminatory towards non-Finnish citizens (especially non-EU nationals)?



Q8: Do you feel that you'd be able to carry out your everyday life in Finland smoothly without the ability to access the strong authentication system?



At the end, the participants had the option to leave their own feedback on the Finnish strong authentication system. The study was conducted among a random group of participants, who accessed the form through various social media channels. The study took place from October 15th 2021 to October 31st 2021.

Link to the study:

https://docs.google.com/forms/d/e/1FAIpQLSdUD_6FM9VZS3r55UhkAUtZWMiIf1fGtUQz0nvGyl6sp6I2Kg/viewform?usp=sf_link

APPENDIX 2, Interview

Below you will find extracts from the interview with Juha Mitrunen, head of the Digital identity development project and senior specialist at the Ministry of Finance (The Public Sector ICT Department). The interview took place via a phone call on Wednesday, November the 3rd, 2021.

2:21 Juha Mitrunen: […] The main point is that no one, not even our banks, which we trust, should profile a person, the person when he is using the identification. Profiling is the main problem here. So, whoever, whether it is the government itself, bank, mobile operator or Google or Apple, whoever is providing our tools or means to identify ourselves, digitally should not be able to profile us, like where we or with whom we dealt digitally. So basically, every time you make a transaction, digitally … It doesn't mean that somebody is inside the transaction in that somebody knows what you are doing, how much money you are transferring, or are you looking at some adult movie or whatever, it doesn't mean that - it just means that you are dealing with these parties. So that's already profiling.

4:13 Veronica Kontopoulou: So, are you saying that data is being stored, but they are not allowed to, to use that data for marketing purposes or profiling people?

4:28 Juha Mitrunen: They should not but unfortunately, in a way… think about this: now we are talking about banks, I can make a similar example about Apple or mobile operator or Google or whoever. But think about this; I'm applying for a loan from the bank. I'm planning to buy a house. At the same time, I'm visiting a website which advises people who have problems with online gaming so now my bank knows that I have some problem with online gaming. And I'm applying for a loan from the bank. So […] you don't have to be a rocket scientist [to understand that], I might have problems getting the loan now.

5:28 Veronica Kontopoulou: Oh right, so is this actually happening?

5:31 Juha Mitrunen: This is profiling. I can't prove that is happening. But, it is something to think about.

5:41 Veronica Kontopoulou: […] I was also wondering, because during my research, I read a bit more on the GDPR, the EU Bill on data protection, and I was wondering does the GDPR conflict with the digital identity development project and using bank accounts for authentication purposes?

6:18 Juha Mitrunen: Not necessarily quite. As I said, we basically trust our banks and we audit via Traficom in the way we audit banks in that search we check what they do and then GDPR is like protecting - well, that example what I explained to you was already misbehaviour against GDPR. So, profiling is already something which you should not do. And GDPR is describing these kinds of instances like for data owners, data processors […] they have certain access to data, they are processing the data, or they even own the data. For example, bank holds the data about how much money I have in the bank account today, they also know that it's their bank account. So, they are data owners, and they are data processors, but still they cannot use that data for certain purposes – the GDPR prevents them.

(Mitrunen explaining the setting up on the digital identity project)

9:34 Juha Mitrunen: Nowadays [digital identification] has turned out to be the actual channel and the physical channel is secondary. And that has changed the situation so earlier for example, the government was able to think this way that okay, basically we deal physically with citizens but then we'll open this digital channel as an optional channel for those who want to use the digital sector. Nowadays, it has done so that in many cases, a person doesn't have any more physical channel at all. My mother, 80 years old, she doesn't even she can do things anymore. There is only the digital channel.

10:34 Veronica Kontopoulou: This is another thing we have been looking into like the inequality that comes because of this move to the to this kind of system…

10:41 Juha Mitrunen: Yes, and it was almost radical in the earlier explanation why we accepted banks and mobile operators as gatekeepers to the services because we were thinking that it's a side channel. Now when it's a main channel, and we still have these gatekeepers between us, and my mother, it means it means basically, that the responsibility of banks and mobile operators is getting much bigger because earlier, they were only serving those who were their customers. So they were able to say that I sell this, I serve this one, I don't serve this one. Because it's a private company and they can select which customers they serve, and which not. What government cannot, we must turn everybody, someone doesn't speak Finnish or doesn't speak at all or cannot see-is blind, or eighty years old, it doesn't matter. We have to be able to deal with everybody. And that is the biggest problem with the private companies. They can cover that say 90% of our citizen customers, but who is covering the rest? So, that was the original problem. And then we started to think that we have to do something of our own which

we offer to citizens. And we were never trying to push banks away or mobile operators away, we were thinking that we offer this next to that, so that people have options. […] the whole concept is changing so that it's not any more identification or authentication. It's more like proving something. Like prove that you are a student or that you are over 18 years old. In a way it's not that you are logging in. It's proof, proving something. And it's not authentication anymore at all.

14:55 Veronica Kontopoulou: But going back to the whole data like privacy aspect of things, does this mean that each time you prove - is that how they end up building that sort of profile about you like, each time you prove, for example, that you're a student or each time you prove that you are an EU citizen or something like that, does this mean that they slowly build up a profile about you and they are able to keep that data that information to form this profile about you?

15:28 Juha Mitrunen: The opposite, they cannot do it, they cannot do it at all. And because of that, they never get that information. So in a way, if you have an identification system, if you perform, if you are providing just a log-in, or service or identification service all these happens after that so that the bank doesn't know whether I am a student or not. Because first I log in, and then I brought some other mechanism using some other mechanism that I'm a student. So that's not a problem if you are in the identification business. Profiling only occurs when you know more with whom you are dealing, like with Apple and Google and Facebook, they go deeper, they go to the content. They go to actual information. And banks only go to the information if it's related to the bank business.

17:05 Veronica Kontopoulou: So basically, what you're saying is that companies like Google and Apple are able to do more of that profiling of putting like one and two together and build this image about you based on the content that you put out, and all the data, the digital footprint that you leave behind, whereas banks are just like the middleman and are not really able to, like they are just able to check that this is indeed you, but not build up. It's more information.

17:37 Juha Mitrunen: That's - what you explain is black and white. If it's related to the financial business, banks are acting like Google or Facebook. Because they have products and business reasons, they have a business to protect.

18.00 Veronica Kontopoulou: Like in the example you mentioned before with gambling.

18:05 Juha Mitrunen: Yes, or they don't want German bank to grant the favour.

18:12 Veronica Kontopoulou: And in practice, you're saying that they have the power to do that. The GDPR doesn't prevent them from doing that.

18:19 Juha Mitrunen: Yeah, or they don't want that Apple Pay comes to or Google Pay to enter the payment business. It's financial business. So, they don't want that Facebook is the Bank of Finland. So it's that's simple. And in that sense, we have a mutual interest in that case because this government doesn't want to either that that that Apple or Google is like, like our bank. So we go through all our banks, but we cannot go through Apple.

19:05 Veronica: And for that reason, you would say that it's not good to connect your bank details to the Google Pay app or the Apple wallet for iPhone users?

19:16 Juha Mitrunen: Yeah, yeah, there you are in the deep in the in the problem that that when you put something in the Google wallet or Apple wallet; Is it any more your information or is it shared information with Apple and Google? That's the question. Google or Apple are giving that wallet free of charge to you, and say that you can use this, this is very secure and very safe and very easy to use. but you share this information with me. This is the main problem. Many people accept that.

20:10 Veronica Kontopoulou: So have I understood correctly that basically, the authentication via banks is not that dangerous, because there's people or governments, our public offices, agents, regulating them, and they have to abide by bills such as the GDPR?

20:49 Juha Mitrunen: Yes and the eIDAS which is the European Union, permission, regulation, about identification and many other things.

21:08 Veronica Kontopoulou: ..Whereas companies like big giant tech companies like Google and Apple, have more power and they don't necessarily abide by GDPR

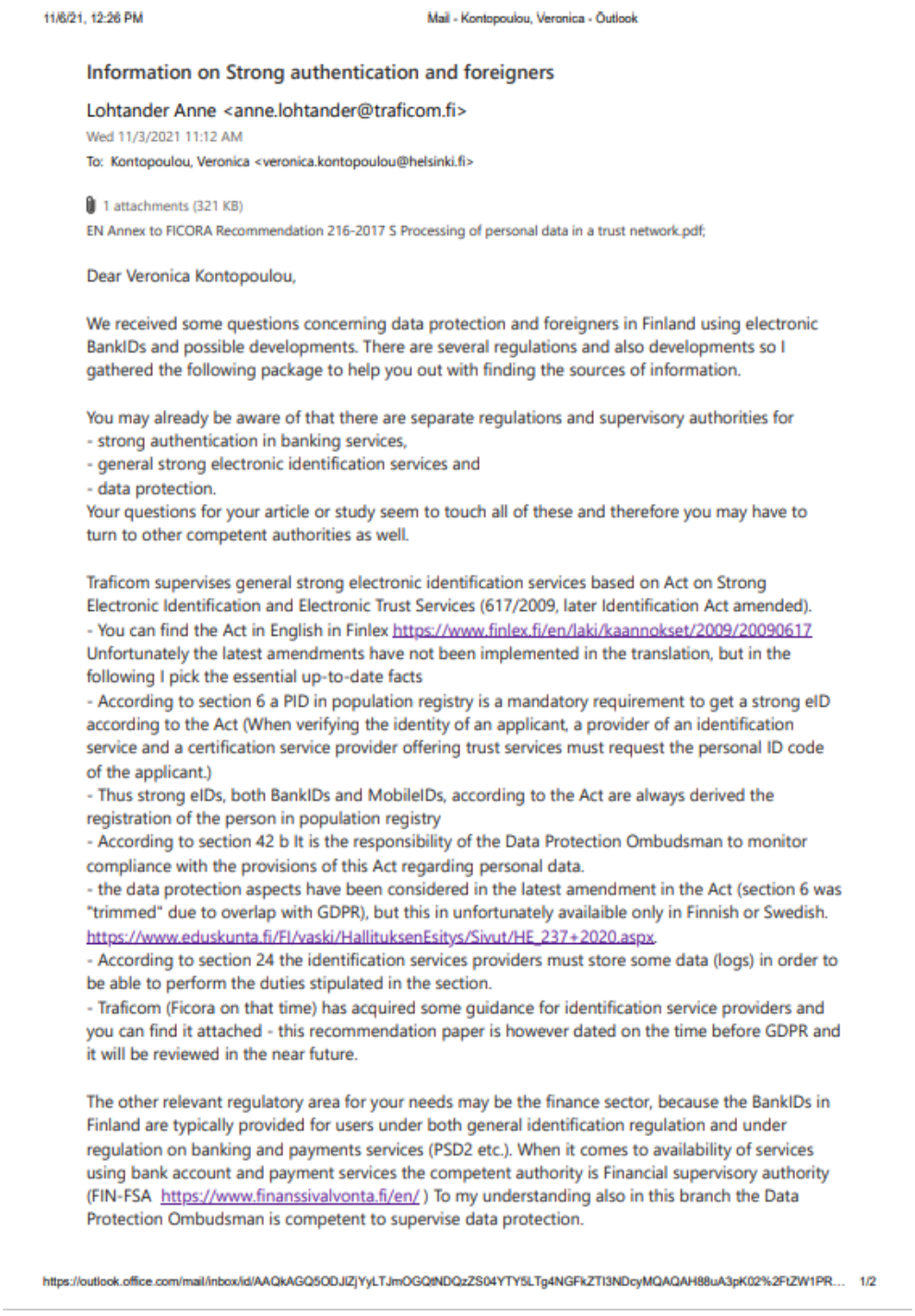
21:20 Juha Mitrunen: We can say to the bank that you have a bank license from the Finnish government, but we cannot say to Apple that you have a license from Finnish government. So that's the difference.

21:34: Veronica Kontopoulou: and which are the bodies that do the regulating? Is it the finance ministry, is it Traficom?

21:52 Juha Mitrunen: at the moment, it's LVM. So, it's basically the Liikenne ja Viestintä-ministeriö - it’s the traffic ministry. So Traficom. But related to the financial segment, it’s the Ministry of Finance where I am and, you could say this way that it's shared, that it's there is some things which are done by Traficom, and then there are some things which are done in the Ministry of Finance, so it is a shared task.

APPENDIX 3, Email Correspondence

We requested an interview with a Finnish Transport and Communications Agency representative, however, our request was met with an email reply instead. Below you will find a segment of our email correspondence with Traficom.



Information on Strong authentication and foreigners

Lohtander Anne <anne.lohtander@traficom.fi>
Wed 11/3/2021 11:12 AM
To: Kontopoulou, Veronica <veronica.kontopoulou@helsinki.fi>

1 attachments (321 KB)
EN Annex to FICORA Recommendation 216-2017 S Processing of personal data in a trust network.pdf;

Dear Veronica Kontopoulou,

We received some questions concerning data protection and foreigners in Finland using electronic BankIDs and possible developments. There are several regulations and also developments so I gathered the following package to help you out with finding the sources of information.

You may already be aware of that there are separate regulations and supervisory authorities for
- strong authentication in banking services,
- general strong electronic identification services and
- data protection.
Your questions for your article or study seem to touch all of these and therefore you may have to turn to other competent authorities as well.

Traficom supervises general strong electronic identification services based on Act on Strong Electronic Identification and Electronic Trust Services (617/2009, later Identification Act amended).
- You can find the Act in English in Finlex https://www.finlex.fi/en/laki/kaannokset/2009/20090617 Unfortunately the latest amendments have not been implemented in the translation, but in the following I pick the essential up-to-date facts
- According to section 6 a PID in population registry is a mandatory requirement to get a strong eID according to the Act (When verifying the identity of an applicant, a provider of an identification service and a certification service provider offering trust services must request the personal ID code of the applicant.)
- Thus strong eIDs, both BankIDs and MobileIDs, according to the Act are always derived the registration of the person in population registry
- According to section 42 b It is the responsibility of the Data Protection Ombudsman to monitor compliance with the provisions of this Act regarding personal data.
- the data protection aspects have been considered in the latest amendment in the Act (section 6 was "trimmed" due to overlap with GDPR), but this in unfortunately availaible only in Finnish or Swedish. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_237+2020.aspx.
- According to section 24 the identification services providers must store some data (logs) in order to be able to perform the duties stipulated in the section.
- Traficom (Ficora on that time) has acquired some guidance for identification service providers and you can find it attached - this recommendation paper is however dated on the time before GDPR and it will be reviewed in the near future.

The other relevant regulatory area for your needs may be the finance sector, because the BankIDs in Finland are typically provided for users under both general identification regulation and under regulation on banking and payments services (PSD2 etc.). When it comes to availability of services using bank account and payment services the competent authority is Financial supervisory authority (FIN-FSA https://www.finanssivalvonta.fi/en/) To my understanding also in this branch the Data Protection Ombudsman is competent to supervise data protection.