mathematics

MDPI

Article

eIDAS Interoperability and Cross-Border Compliance Issues

Marko Hölbl *, Boštjan Kežmah and Marko Kompara

Faculty of Electrical Engineering and Computer Science, University of Maribor, 2000 Maribor, Slovenia
* Correspondence: marko.holbl@um.si; Tel.: +386-2-2207361

Abstract: The eIDAS Regulation provides a common foundation for secure electronic interaction between citizens, businesses, and public authorities. We investigated and identified interoperability and cross-border compliance issues in this paper. We have identified the following weaknesses: Organizational independence, remote access to banking services, remote video identification, use of electronic signatures in public administration, commercial access to the eIDAS network, biometric authentication mechanisms, and, finally, some technical issues with the mechanisms used to provide security and authentication in eIDAS nodes.

Keywords: eIDAS; interoperability; cross-border compliance; heterogeneity; European Union

MSC: 94A62

1. Introduction

When new technologies are used for information acquisition, transmission, and collection, there are many data risks. The electronic Identification Authentication and Signature Regulation—Regulation EU No. 910/2014, commonly known as eIDAS, establishes a legal framework for electronic identification in the EU internal market [1]. Its goal is to establish a uniform framework for legally secure electronic collaboration in the EU and to increase the confidence of individuals, legal entities, and public authorities in electronic transactions. The eIDAS Regulation's goal is to make it easier for each EU Member State's natural and/or legal persons to use electronic identity resources at the European level. For this, the eIDAS Regulation aims to make it easier to use electronic authentication channels by establishing the mutual recognition and acceptance of electronic identification systems for use by public authorities in verifying the identity of citizens and legal entities. The ability to create e-signatures remotely, where a trust service provider administers the environment for doing so on behalf of the signatory, is one of the most significant improvements brought about by the eIDAS Regulation. The e-signature service provider must make sure, through the use of the proper mechanisms and procedures, that the signatory has complete control over the use of its data to generate an e-signature and that the specifications for qualified e-signature are met when using the device when we want to create a qualified e-signature. Currently, there is a big push from the EU to update the eIDAS Regulation ("eIDAS 2.0" is being prepared) to, among other things, make it more uniform across the Member States. However, there is very little analysis or comparison of the eIDAS implementations except by EU-related organizations.

In this paper, we aim to identify situations and areas where there are differences between the EU Member States by analyzing eIDAS implementations in a sample of Member States. The goal is to identify weak points in interoperability and cross-border compliance by analyzing the real-world implementations from Italy, Slovenia, Spain, and Switzerland. The identified concerns include privacy/security/trust vulnerabilities, unfair marketplaces, and various verification degrees. These issues should be considered when updating the current eIDAS Regulation since, to the best of our knowledge, they are not addressed by the recently suggested Regulation update (i.e., eIDAS 2.0).

Citation: Hölbl, M.; Kežmah, B.; Kompara, M. eIDAS Interoperability and Cross-Border Compliance Issues. *Mathematics* **2023**, *11*, 430. https://doi.org/10.3390/math11020430

Academic Editor: Todor Tagarev

Received: 3 December 2022
Revised: 6 January 2023
Accepted: 10 January 2023
Published: 13 January 2023

The very broad nature of the proposed research implies some limitations. First and most obvious is the limited selection of Member States that were included in the analysis. Unfortunately, gathering the required data from different countries is very difficult because it requires much knowledge of local e-ID systems and legislation. That is why we employed the help of locals that work in the field of cybersecurity and authentication. The limited number of analyzed Member States reflects the difficulty of finding willing and qualified people to help gather the necessary data. The following limitation is the result, which cannot be considered exhaustive. The list considers problems associated with situations that the authors have been made aware of during previous work or had a hunch that could be problematic from learning how different implementations of eIDAS work. The end goal of the paper is not to provide suggestions or solutions on how to solve these issues. Nonetheless, we do provide some recommendations; however, ultimately, the solution to the majority of the identified issues would be a higher unification of eIDAS services across the EU.

The paper is structured as follows: Section 2 discusses the eIDAS Regulation briefly, followed by an overview of related work in Section 3 and the methodology employed in Section 4. The main contribution and findings regarding the eIDAS implementation issues identified in the research are presented in Section 5. We discuss the findings, provide recommendations in Section 6, and present a conclusion and possible direction for future work in Section 7.

2. The eIDAS Regulation Implementations

The eIDAS Regulation was released on 17 September 2014 and became effective on 1 July 2016. The eIDAS Regulation aims to increase the efficiency of public and private online services and e-commerce in the EU by establishing a common framework for secure electronic interactions between citizens, businesses, and public authorities. The e-signatures Directive has established the legal basis for electronic signatures; services linked to supplementary trust and electronic identification and authentication have not.

The eIDAS regulation was designed to make it possible for citizens, businesses, and public administrations to use electronic identification and trust services (such as electronic signatures, electronic seals, time stamping, registered electronic delivery, and website authentication) to access online services or manage electronic transactions. It was proposed to achieve the following:

- Transparency and accountability: Well-defined minimal obligations for Trust Service Providers (TSP) and liability.
- A guarantee of trustworthiness of the services, together with security requirements for TSPs.
- Technological neutrality: Avoiding requirements that could only be met by a specific technology.
- Market rules and standardization certainty.

A prerequisite for an e-signature is to confirm the authenticity of the signatory's identity (i.e., authentication). The eIDAS Regulation prescribes that a qualified e-signature, which is the equivalent of a handwritten signature, can only be created by means of a qualified electronic certificate, i.e., a means of e-identification with a high level of reliability.

In September 2017, Germany was the first country to have a notified eID scheme with eID means based on its National Identity card and its resident permit for a high assurance level. In 2018, the number of notification processes increased notably, with six Member States notifying eID schemes between September and the end of December 2018 [2]:

- Italy, with its SPID scheme, includes multiple eID means provided by several identity providers for low, substantial, and high assurance levels (depending on the type of eID means used).
- Estonia, with six eID schemes based on the national identity card, the resident permit card, a dedicated card (Digi-ID), the diplomatic card, and the e-resident card, and

a mobile scheme based on a dedicated PKI-enabled SIM (Mobiil-ID), all for a high assurance level.

- Belgium, Croatia, Luxembourg, and Spain notified eID schemes based on their electronic national identity cards for high assurance levels.

In 2019, six more Member States notified their eID schemes for the first time [2]:

- Portugal and the Czech Republic with eID schemes based on the electronic national identity card for a high assurance level.
- The United Kingdom (even though it is not part of the EU anymore) with GOV.UK Verify and eID means issued by private providers (bank, post office, etc.) and appointed by the UK government for low and substantial assurance levels.
- The Netherlands with a business-oriented scheme (for legal persons) for substantial and high assurance levels depending on the identity provider.
- Slovakia with an eID card-based scheme for nationals and foreigners for a high assurance level.
- Latvia with a card-based scheme and a mobile application for substantial and high assurance levels.

Additionally, in 2019, two countries notified a second eID scheme [2]:

- Italy with a scheme based on electronic identity cards for a high assurance level.
- Belgium with the FAS/a digital identity app called Itsme, a solution provided by Belgian Mobile ID based on a smartphone application as eID means, for a high assurance level.

Later in 2020, 2021, and 2022, eight countries notified a second eID scheme, and three countries notified an additional eID scheme [3]:

- Austria with its ID Austria.
- Denmark with NemID.
- France with the eID scheme "FranceConnect+/The Digital Identity La Poste".
- Lithuania with a Lithuanian National Identity card (eID/ATK).
- Malta with Identity Malta.
- The Czech Republic updated its national identification scheme with the Mobile eGovernment Key and mojeID systems.
- The Netherlands added its DigiD solution.
- Portugal with the commercial provider Chave Móvel Digital.

So far, 22 Member States have notified at least one eID scheme. As a result, approximately 81% of EU residents have access to trusted and secure eID schemes. Only seven schemes are entirely mobile. As not all technical nodes that ensure the connection to the eIDAS interoperability framework are fully operational, cross-border access is limited; very few online public services accessible domestically can be reached cross-border via the eIDAS network [4].

As a result of the current shortcomings, a new proposed Regulation [5] was published on 3 June 2021, aiming to amend the eIDAS Regulation by establishing a new framework for the "European Digital Identity" (known as the "EUid" or "eIDAS 2" or "eIDAS 2.0"). This proposal, which is not yet final, seeks to enhance eIDAS and bring about a paradigm shift in the European digital identification of citizens and companies.

Although the European Commission recognized the need to bring the eIDAS framework to the next level and to be able to support the Single Market, there is scarce information on how the proposed changes will influence the harmonization of technical details. For example, there is no immediate vision for addressing authentication security issues already identified by ENISA [2] and how to relate the use of biometrics with the GDPR and the cybersecurity liability of the device providers.

3. Related Work

We could not find much research or comparison of eIDAS implementations across the EU. The EU naturally compiles some more general lists of comparable information between the Member States. This includes a compilation of information regarding the implementation of the Trust Services of the eIDAS Regulation [1], IDAS-Node implementation progress with service providers and identity providers in each country [6,7], the eID-supported public services across the EU [8], and the Member State's strategies for eID [9].

There are case studies of individual countries and their implementations of eIDAS (e.g., [10–12]), but studies addressing a broader scope of Member States are not common. However, there is non-eIDAS-related research on eIDs. Some examples of such studies looking into the security and privacy of eID frameworks include [13–16]. The most relevant research here is [17], which looks at the federated identity architectures used and analyzes the CEF eID protocol, which is the basis of the eIDAS network. They also evaluate the performance of the network. The transactions in the eIDAS network were analyzed in [18]. The eID and Self-Sovereign Identity overview of the existing solutions and current projects developing and implementing the solutions are presented in [19]. Although the paper contains information from around the world, a large portion of the collected data is from Europe (14 countries). The work heavily references the connections to eIDAS and the direction of the upcoming update to the eIDAS Regulation.

F. Roelofs [20] describes authentication systems from seven countries (the Netherlands, Germany, Belgium, Estonia, Luxembourg, Spain, Italy, and Croatia) that had completed eIDAS notification of at least one system by the beginning of 2019. The research included all eID systems from the selected countries, even if they had not been notified. Before the EU is notified of a system, the system is reviewed by the European Commission. If the system meets the quality and security requirements, the EU is then notified of it, at which point all other nodes in the eIDAS network must connect to it (to ensure their services are available through that system), and its usability for users is evaluated in one year. For each system, the author provides the basic information on the system, encryption and PKI, authentication process, and other relevant information. All the systems are compared in their usability, privacy, and security. Usability is divided into sections for the service provider and user. Usability for service providers is evaluated on the use of federation and compatibility with private service providers. Usability for users is evaluated on the available authentication methods, single sign-on, availability of other qualified trust services (e.g., qualified electronic signatures), and the possibility of accessing past authentication information. Privacy is compared based on privacy hotspots (aggregation of data in one place) and the possibility of pseudonyms. Security is compared based on communication security and vulnerability to Man-in-the-browser attacks. The author finishes by providing insights and recommendations based on comparing the different solutions.

4. Methodology

For the eIDAS Regulation to be implemented and used in practice, cross-border interoperability is needed. In the scope of the CyberSec4Europe project, we had the possibility to collect data from some of the partner countries. The aim was to analyze real-world implementations of the chosen use cases. The use cases were selected based on observations and through talks with project partners and other members of the community on what they found lacking in eIDAS implementations through the years since the establishment of eIDAS.

Because of the complexities involved (e.g., language barriers and lack of knowledge of legislation specific to individual countries), the effort required would be too considerable without substantive external help. For this reason, we used project partners to help collect information in their respective countries. The project partners were given guided questionnaires that functioned similarly to structured interviews. They could choose to answer the questions themselves or, where they did not know the answers, collect the information from other people. In the end, we managed to collect information for three EU countries

(Italy, Slovenia, and Spain) and one European Economic Area country (Switzerland). The collected data were analyzed together with the compatibility of solutions and policies in different countries. While the sample is not necessarily representative of the EU, the goal of the research was only to show any potential differences in the EU and what consequences those differences could have for the cohesion of the EU's single market.

The goal of the guided questionnaire sent to the partners was mainly to collect information on how eIDAS is implemented and works in their countries. Below we list the questions as they were given to the project partners to collect the answers for their Member States. Based on the answers collected in the last quarter of 2021, we were able to compare Member States and find where interoperability and cross-border problems are (considering the EU's wishes and planned functionality of the eIDs). We will show the main and/or relevant feedback we received through the paper as we address each issue:

1. Is the supervisory body in the Member State providing trust services at the same time?
2. Can you open a banking account in your Member State by solely identifying yourself remotely, using electronic identification? Are there any restrictions on assurance levels or trusted service providers when opening such an account? Are there any further restrictions on banking services with this account (e.g., renting a loan)?
3. Can you get a qualified certificate remotely, e.g., by using remote video identification? Are there any Member State-level rules defining requirements for video identification?
4. Are you familiar with any government-level electronic services that don't require qualified electronic signatures when filing claims, reporting taxes and similar services? Do you have any regulation that specifically defines assurance levels for different procedures, at least for public services?
5. Are businesses able to connect to eIDAS infrastructure? Do you have any laws that specifically allow or prohibit the use of eIDAS infrastructure for businesses? Can companies from other Member State access eIDAS services in your Member State? Are prices for using eIDAS services for companies clear? Can you provide a price list?
6. Are you aware of any trust services based on biometric authentication?
7. Please describe the online (remote) process of trusted service registration and its use (authentication for the use of identity).

5. Investigation of eIDAS Implementation Issues

The current regulation falls short of addressing new market demands due primarily to its inherent limitations to the public sector, the limited possibilities, the complexity for private online providers to connect to the system, its insufficient availability of notified eID solutions in all Member States, and its lack of flexibility to support a variety of use cases. Furthermore, identity solutions fall outside the scope of eIDAS, such as those offered by other identity providers. They cannot respond effectively to new market demands and lack the cross-border outreach to address specific sectoral needs where identification is sensitive and requires a high degree of certainty [17].

5.1. Organizational Independence

In Slovenia, the supervisory body is the same organization that provides trust services. In essence, that means it is supervising itself. Consequently, transparent rules for the certification and supervision processes become even more important as the supervisory body could alter the rules to serve its purpose. The intent was to find out whether there are similar occurrences of organizational independence issues in the selected Member States.

The results show (Table 1) a pattern where supervisory authorities provide trust services simultaneously. This contradicts a host of Standards (International Standard of Auditing 200, IESBA Code, ISO 19011) that define the independence of auditors or other types of professional reviewers. For example, independence is defined for financial auditors in the International Standard of Auditing 200 [10]. A16 defines that in the case of an audit engagement, it is in the public interest and, therefore, required by the IESBA Code that the auditor be independent of the entity subject to the audit. The IESBA Code describes

independence as comprising both independence of mind and independence in appearance. The auditor's independence from the entity safeguards the auditor's ability to form an audit opinion without being affected by influences that might compromise that opinion. Independence enhances the auditor's ability to act with integrity, be objective, and maintain an attitude of professional skepticism [21]. Similarly, according to ISO 19011 [22], auditors should be independent of the activity being audited wherever practicable. They should, in all cases, act in a manner that is free from bias and conflict of interest.

Table 1. Organizational independence for the sampled countries.

Member State	Findings
Italy	The supervisory authority for trust services provides qualified trust services simultaneously. The National Register of the Resident Population, Administrative Procedure Management System, Storage
Slovenia	The supervisory authority is itself providing qualified trust services. The Ministry of Public Administration
Spain	The supervisory authority for trust services provides non-qualified trust services simultaneously. The Ministry of Economic Affairs and Digital Transformation
Switzerland	The system is decentralized, and there is no apparent single, centralized supervisory authority.

Such an arrangement could also affect the competition in the market as the main entity offering trust services and defining legislation or even access to the eIDAS network is competing with other service providers in a closed market.

5.2. Remote Access to the Banking Services

According to the European Commission, eIDAS solutions should lead to efficient and secure digital life using the following technologies [23]:

- eSignature—will help citizens sign legal documents and emails without printing any paper.
- Qualified Web Authentication Certificate—will let citizens know that the websites and apps they like using are trusted and safe.
- eTimestamp—will give citizens proof that they have bought concert tickets.
- eSeal—will guarantee that the football tickets are authentic and are not counterfeit.
- eID—will allow citizens to open a bank account in another country with their national ID card.
- Electronic Registered Delivery Service—will guarantee the protected exchange of data, including proof of sending and receiving the data.

For example, the European Commission envisioned a basic use case for opening a cross-border bank account. An EU citizen is relocated temporarily from Spain to Luxemburg for business reasons [24]. They are opening a bank account in Luxemburg before traveling. The citizen uses their Spanish eID so that the bank in Luxembourg can verify their age and identity. There is no need for them to visit Luxembourg to open a bank account personally. The bank carries out its due diligence by checking the person's financial record based on the data of their eID. The citizen does not have to provide additional information, and the bank can give a green light swiftly.

As local regulation could hinder the envisioned scenarios, we investigated local scenarios in the selected Member States, as presented in Table 2.

Table 2. Organizational independence for the sampled countries.

Member State	Findings
Italy	Currently, no matter if you are a resident, a temporary worker, a student, a tourist, or a professional traveling often for business—you have to provide the local branch of an Italian bank with the same set of documents as the Italians do: Identification, such as a valid passport, identity card, or driver's license The Italian tax code called "codice fiscal" and the "Certificato di Attribuzione del Codice Fiscale", which both come with the Italian tax code. Proof of address in Italy, student enrollment in the university program, or residence permit or work contract. The proposals using the system for payments to the Public Administration are similar to pagoPA, which is the national platform. It allows users to choose how to pay taxes and fees to the Public Administration and other participating entities that provide services to citizens.
Slovenia	There were rules from 2018 to 2021 that prohibited the use of eIDAS certificates from the other Member States when accessing the central database of credit information (SISBON), defined in "Rules on the system for the exchange of information on the indebtedness of natural persons (SISBON)—article 18" [25]. That meant that even if the bank allowed remote identifications, there were many restrictions on what services the bank could provide to such customers. This changed in June 2021 with the latest changes to the before-mentioned Regulation, including eIDAS, trusted service providers that are now equal to Slovenian trusted service providers. Electronic identification must meet the requirements for a high assurance level. Regardless of the legal basis, none of the Slovenian banks currently provide a remote onboarding service. The bank would have to be included in the eIDAS network to provide such a service to access the identity attributes provided. Even though the new Electronic Identification and Trust Services Act envisions using the eIDAS network for private entities, this access has yet to find its way into actual use.
Spain	The SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias) authorized the use of video-identification processes by financial entities in 2017 [26].It defines a high assurance level, as required by Law 10/2010 [27], on the prevention of money laundering and financing of terrorism. The process involves the presentation of identity documents and a set of technical and organizational measures.
Switzerland	Previously, a bank account was only possible when a personal identification document and a handwritten signature were provided on-site. As of 1 January 2016, the entire process can be completed electronically: Article 49 (2) of the fully revised FINMA Anti-Money Laundering Ordinance stipulates that a copy of an identification document from a recognized provider of certification services in accordance with the Swiss Electronic Signature Act (ZertES) of 19 December 2003, suffices as authentication [28]. For example, when opening an account at UBS Bank, there are two options available. However, Credit Suisse Bank offers the ability to open an account remotely in full via an app. CIM Bank also allows opening bank accounts online and collaborates with a Swisscom trusted service provider to authenticate signatures.

According to the selected sample (Table 2), there are many different scenarios for opening a bank account. Every Member State has its own solution and its own requirements for the remote opening of a banking account.

When setting up eIDAS, one of the use cases was to enable the remote opening of bank accounts across borders. However, the banking area is heavily regulated, and local legislation hinders the envisioned seamless connection with foreign banks.

5.3. Remote Video Identification

The use of video identification is allowed in some Member States, even for onboarding (i.e., becoming a client) for banking services (Spain).

According to [29], based on the recently approved Order ETD/465/2021, of 6 May 2021, regulating the remote video identification methods for issuing qualified electronic certificates, Spain is currently the EU Member State with the most electronic trust service providers. The new legislation helped increase this number as it allows video identification and therefore makes it more interesting/viable for companies to sell such services.

It is possible to use eIDAS trust services and associated electronic documents as evidence in legal proceedings across the EU Member States, contributing to their general usability within and across borders. While the legal validity of trust services is warranted, courts (or other adjudication bodies) cannot discard them as evidence only because they are electronic but must assess these electronic tools in the same way as they would for their paper equivalent [30]. This leads to the question of how different requirements for video identification might affect the cross-border use of identities and how they could affect the security of identities.

With the digital interoperability of the eIDAS network, borders are fading away. A citizen obtaining an identity in one Member State could use the acquired identity in any other Member State. In marginal scenarios, a citizen of one Member State could obtain a digital identity using remote video identification in another Member State and use that identification later in their own country. Consequently, the questions of regulating requirements for remote video identification are invading the regulation area of the eIDAS network. Table 3 presents the use of video identification in the selected EU Member States.

Table 3. Remote video identification for the sampled countries.

Member State	Findings
Italy	The digital signature can be obtained with Video Recognition or with SPID (Sistema Pubblico di identità Digitale) Online Recognition. It is possible to perform Online Video Recognition from a PC or Smartphone with the support of an operator. Online recognition can be performed via SPID every day, 24 h a day, through a PC or Smartphone.
Slovenia	Slovenia has a Prevention of Money Laundering and Terrorist Financing Act [31]. The intent of the provision is the prevention of money laundering. It is not directly relevant for remote video identification for the issuance of identities, but it is the only Act that defines special requirements for it. Currently, none of the trusted service providers in Slovenia provides remote video identification services that would result in the issuance of electronic identification (either low, substantial, or high assurance levels). Under the Electronic Identification and Trust Services Act [32], electronic identities issued by the Republic of Slovenia can be issued only to Slovenian citizens at least six years old or to foreigners with a domicile or temporary residence in the Republic of Slovenia. There are no other special requirements for any private, trusted service providers.
Spain	Law 6/2020 [33] authorizes other methods for identification, such as identification via videoconference or video-identification with a level of security equal to the physical authentication and evaluated by a conformity assessment body. To determine the conditions and technical requirements, it must refer to those determined at the EU level (e.g., ETSI TS 119 461 V1.1.1(2021-07)). Furthermore, Order ETD/465/2021 [29] applies to qualified public and private providers of trust services established in Spain or with a permanent establishment located in Spain as far as the authority of different Member States does not already supervise their services. It contains specific requirements regarding security aspects, identity documents, facilities, and the remote identification process.
Switzerland	Since the FINMA Circular 2016/7 [34] entered into force, video identification has equal validity to in-person identification, provided the following criteria are met: Identification is made via real-time audio-visual communication between the contracting party and the financial intermediary. The latter must utilize adequate technical equipment to ensure the secure video transmission as well as the reading and decryption of the information stored in the identification document's machine-readable format. Specially trained employees are responsible for identifying the contracting party. The interview must be audio-recorded in its entirety. Different requirements/clarifications need to be met depending on whether the video identification concerns an individual, a legal entity, or more than one contracting party.

Similar to opening a banking account, there are different approaches to remote video identification in the selected Member States. Since every Member State (where video identification is allowed) has its own requirements regarding the security of remote identification, this may lead to different levels of trust in the obtained title and difficulties in cross-border recognition.

5.4. The Use of Electronic Signatures in Public Administration

It is no secret that many businesses have little understanding of the eIDAS assurance level requirements when doing business with their customers. eIDAS provides different assurance levels and different kinds of electronic signatures. Every assurance level and every type of electronic signature brings additional costs and complexity to the information system and user experience. Businesses are, therefore, reluctant to use higher assurance levels than necessary.

Since eIDAS was targeted primarily at the public sector, we were interested to understand whether the assurance levels and the kind of signatures used in the public sector could be comparable across the Member States.

It was investigated whether public services do not require qualified electronic signatures when filing claims (e.g., reporting taxes and similar services) and if any local Regulation specifically defines assurance levels for different procedures, at least for public services. A summary is given in Table 4.

Table 4. The use of electronic signatures in public administration for the sampled countries.

Member State	Findings
Italy	Authentication is always required. If an electronic signature is unavailable, proof of identity must be exhibited with a photocopy of an identity card or electronic signature.
Slovenia	There is no requirement for a qualified electronic signature when filing tax-related claims electronically anymore. Clicking a button in the web application suffices but logging into the web application still requires a high assurance level. The Electronic Identification and Trust Services Act [32], Article 15, provides provisions for defining the required assurance level based on technical and legal risk analysis. Further requirements should be defined in the subordinate Regulation that does not yet exist at this time.
Spain	Article 10 of Law 39/2015 [35] allows various options, so it can be said that in Spain, the electronic signature has not been imposed in general, except in the cases specifically envisaged in Article 11 (Administrative Procedure). Electronic signatures are mandatory only in the National Security Scheme, especially Annex II, Section 5.7.4., for information systems of security category high level in the dimensions of integrity and authenticity.
Switzerland	Government-level electronic services do not require any qualified electronic signature. The Federal Act on the Electronic Patient Record stipulates how the Electronic Patient Record (EPR) should be organized and made secure from a technical point of view. Each EPR provider is assessed, certified, and inspected regularly. SwissID will be used during the login as a means of patient verification. In this specific example, SwissID can be obtained only via in-person verification.

Similar to what was shown in previous analyses, there is much heterogeneity. Even though different assurance levels and kinds of signatures are defined in eIDAS, there is little convergence in understanding what levels should be used in specific use cases. The government may decide not to recognize an electronic signature as equal to a handwritten signature by law. If the government is not promoting using the highest assurance levels and qualified electronic signatures with its services, these levels of security have little penetration in the commercial market. Commercial services that require higher assurance levels (e.g., banking and insurance), either by the law or because they are not prepared to take the risk of lower assurance levels, are left alone to promote the use of higher assurance level technologies with the citizens.

5.5. Commercial Access to the eIDAS Network

Since the commercial market needs access to the identities and electronic signatures of the citizens, the next aspect we investigated was the proliferation of the public eIDAS network in the private sector.

Namely, the private sector can also benefit from digital identity, improving the user experience and managing customers' personal data. Since eIDAS does not have a condition

that the eIDAS network must be accessible to private entities, this is left to the regulation of the Member States. Table 5 provides a summary.

Table 5. Commercial access to the eIDAS network for the sampled countries.

Member State	Findings
Italy	The Italian SPID also allows access to public services of the European Union Member States and companies or traders who have chosen it as an identification tool [36,37]. Companies from the other Member States can also access eIDAS services.
Slovenia	Slovenia has an Electronic Identification and Trust Services Act. This Act allows organizations to provide electronic services to use electronic identities issued by the government. Executive Regulation does not yet exist; therefore, further technical and other requirements and/or pricing are still unknown.
Spain	The Royal Decree 203/2021 [38] regulates the Electronic Identification Interoperability Node of the Kingdom of Spain, which is only aimed at public sector entities. Therefore, it seems that it would not be possible for private entities to connect to the Spanish node (except when the private entities act on behalf of a Public Administration). A different case would be the use of the middleware approach, but it would only be valid for those means of electronic identification that have implemented it.
Switzerland	According to Zertes [28], the equivalent eIDAS Regulation in Switzerland, companies can also use certification services for electronic signatures. Presently, Swisscom Trust Services is the only Trust Service Provider offering qualified electronic signatures that comply with the European Regulation on electronic identification and trust services for electronic transactions (eIDAS) and the Swiss law on the use of certification services with electronic signatures (also known as ZertES). No pricing list is available. Under Art 3(2), when a foreign provider has already obtained recognition from a foreign recognition body, the Swiss recognition body may recognize it if it is proved that: • The recognition was granted in accordance with foreign law. • The rules of foreign law applicable to the granting of recognition are equivalent to those of Swiss law. • The foreign recognition body possesses qualifications equivalent to those which are required of a Swiss recognition body. • The foreign recognition body guarantees its cooperation with the Swiss recognition body for the supervision of the provider in Switzerland.

The results show that some Member States do not allow access to the public sector (Spain), access is envisioned but not implemented (Slovenia), or access is allowed even for foreign businesses (Italy and Switzerland).

This result is interesting because it shows that inter-government competition is already starting to build. With some governments providing access to foreign entities, the competition between local regulations will also begin to build. Companies will have the option to choose an eIDAS network entry point and consequently control their costs. That will pressure the public providers to stay competitive or local nodes may start to lose interest. This may also have a negative impact. Suppose there is too much open competition between trusted service providers in the different Member States. In that case, that may have a direct effect on the security of the network in the different Member States. Security incurs costs. Local providers will have a competitive advantage if security requirements in some Member States are lower than in others.

5.6. Biometrics as Authentication Mechanism—BYOAD

In the private sector, especially in banking and the general public identity providers (e.g., Google, Microsoft), we see a rise in the use of biometrics. Unfortunately, such use of biometrics is currently "a grey area". The use cases are based mainly on the biometric capabilities of current mobile devices. That means the service providers are not processing biometric data and are consequently not under the GDPR requirements. There is no certification scheme in place, and there are no specific requirements for using such devices. Even though these devices have a direct impact on the security of the service for the end-user, the banks do not have contracts with "biometric security device providers", e.g., Apple, Samsung, etc., even though that was the case as long as the banks were buying

authentication solutions on the market to meet their needs and the needs of their customers. Consequently, the user is left to their own mobile device selection, and the security of the service will vary depending on the selected device. We propose the term "Bring Your Own Authentication Device—BYOAD" for this kind of authentication. Since the use of biometrics is limited according to the GDPR, we were interested in how this affects the security services provided according to eIDAS. This is again summarized in Table 6.

Table 6. Biometrics as an authentication mechanism for the sampled countries.

Member State	Findings
Italy	Italy currently does not have a trusted service provider that uses biometrics as an authentication mechanism to access/use identity.
Slovenia	Slovenia currently does have a trusted service provider that uses biometrics as an authentication mechanism to access/use identity.
Spain	We are not aware of any current cases in Spain. However, biometrics are used to verify the identity of the person requesting a qualified certificate (this would also be an example of biometric authentication), in accordance with the provisions of Article 7.2 of Law 6/2020 and the Order ETD/465/2021, of 6 May, regulating the methods of remote identification by video for the issuance of qualified electronic certificates.
Switzerland	The SwissID App allows the use of Touch ID on Apple devices.

The results show the differentiation of the authentication market. Even though banks have high authentication security requirements and offer mobile banking solutions based on biometric solutions provided by modern mobile devices, this technology has not met broad recognition in the authentication mechanisms offered in eIDAS services. Switzerland is the only country included in the research that supports biometric authentication in eIDAS services.

5.7. Technical Authentication and Onboarding Security Requirements

While the eIDAS Regulation provides a common set of requirements, it does not necessarily identify how these requirements may be met following existing technology and organizational arrangements. Standards provide generally accepted means to meet requirements with existing technology whilst, if necessary, the market can develop alternative solutions as new technology emerges to feed further into the standardization life cycle. In the specific context of a Qualified electronic Signature Creation Device (QSCD), however, the security evaluation and certification process must be carried out in accordance with the list of Standards established by means of the implementing Act referred to in Article 30.3 of the eIDAS, i.e., Commission Implementing Decision (EU) 2016/6503, unless there are no "applicable" Standards mentioned in the implementing Act, or when a referred security evaluation process is ongoing [30].

The main policy standard, ETSI EN 319 401 V2.3.1 (2021-05), has little detailed technical guidance on the use of authentication as it primarily references ISO/IEC 27002:2013.

According to ETSI TS 119 432 V1.2.1 (2020-10) (4.4.1.2), the SSASC (Server Signing Application Service Component) uses a remote SCDev (Signature Creation Device) to generate, maintain, and use the signing keys under the control of their authorized signers. The authorized signer controls the signing key remotely with a certain level of confidence, eventually by means of the Signature Activation Module (SAM). The SAM is a software component using the Signature Activation Data (SAD) to authenticate the signer and gain its authorization to activate its signing key to sign the DTBSR (Data to Be Signed Representation). This process ensures confidence that the signing keys are under the control of the signer.

The signing operation is performed with a Signature Activation Protocol (SAP) that requires that SAD be available in the local environment. The SAD brings three elements together:

- Signer authentication.
- A signing key.
- The data to be signed (DTBSR).

The signature operation requires authorization to ensure that the signees/signing parties have sole control of their signing keys. This is performed by a SAM. Both the SAM and the Cryptographic Module must be in a tamper-protected environment. Verification of SAD means that the SAM verifies the binding between the three SAD elements while ensuring that the signer is authenticated.

Signee authentication is one of the elements included under SAD. The SAM may carry out signee authentication in one of three ways:

- Directly, where the SAM verifies the signee's authentication factor(s).
- Indirectly, where an external authentication service (e.g., one that is part of the TW4S or delegated party) verifies the signer's authentication factor(s) and issues an assertion that the signer has been authenticated. The SAM then verifies the assertion.
- Through a combination of two direct or indirect schemes, where the SAM performs part of the signer authentication directly, and another part is performed indirectly by the SAM.

The SAM verifies the SAD to be able to authorize the requested signature operation. The SAM can delegate signer authentication to an external party. According to its environment, when the SAM does not perform signee authentication directly, it must assume that part, if not all, of the authentication, has taken place and then rely on the provided assertion. This means that in the Protection Profile (PP) signer authentication, the signer has been authenticated using one of the three methods listed above.

With EN 419 241-2, the SAM module is the Protection Profile's target of evaluation. Both the target of evaluation and Cryptographic Module, certified according to EN 419 221-5, are required to obtain a Qualified electronic Signature Creation Device (QSCD).

As ENISA emphasizes [30], at the time of writing the Commission Implementing Decision 2016/650, there were no available Standards for signing devices operated by a trust service provider in a secure environment that aimed to meet the requirements in Regulation (EU) 910/2014 Annex II for qualified signature/seal creation devices. However, two major CEN (European Committee for Standardization) Standards (CEN EN 419 241-2 (Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing dated 2018-05-11) and CEN EN 419 221-5:2018 (Protection Profiles for TSP Cryptographic Modules—Part 5—Cryptographic Module for Trust Services)) published by the CEN TC224 cover the following use cases relating to the identified gap:

- Trust service providers managing signature creation data on behalf of the user to support the creation of qualified electronic signatures/seals.
- Trust service providers are creating qualified electronic signatures/seals on their own behalf.

Since the last ENISA research in 2018, the CEN Standards have been upgraded to newer versions. ETSI TS 119 431-1 V1.2.1 (2021-05) [39] clearly defines the scope of remote signing Standards. According to the ETSI TS 119 432 V1.2.1 (2020-10) [40], there are two models of SSASC activation. With the SCAL1 model, when the signer authentication succeeds, the corresponding signing key may be used for signature operations on behalf of the signer within a certain time frame and/or a certain amount of signature operations, thus allowing the management of bulk/batch signature operations. Once the SAM module has verified signature activation data (SAD), it then authorizes the Cryptographic Module's signing key to produce a digital signature value.

In the SCAL2 model version, the signing keys are used with a high confidence level under the signer's sole control. The authorized signer's use of its key for signing is enforced by the Signature Activation Module (SAM) by means of Signature Activation Data (SAD) provided, by the signer, using the Signature Activation Protocol (SAP) in order to enable the use of the corresponding signing key.

From the perspective of the signer, the keys are only as secure as the authentication procedure provided by the SAM.

SCAL2 refers to a substantial assurance level that does not require a physical presentation of the user. To some extent, this might downgrade the assurance level provided when the supporting certificate is a qualified certificate (or is issued under ETSI EN 319 411-1). Whomever the TSP (Trust Service Provider) that performs the task is, it is crucial that the signer's information (identity data, signature validation data (SVD, or public key), certificate and eID means, and related signer authentication reference) is consistent and belongs to the very same person. Otherwise, one faces the risk that the SSASC lets a pretender sign in place of the person registered by the TSP having issued the certificate [30].

The downgrade of the assurance level results from signing data with a qualified digital signature, even though the assurance levels to use the service and assurance level provided by the service (provider) may differ. The definitions of assurance levels according to eIDAS are:

- The low assurance level requires the electronic identification scheme to use at least one authentication factor, including username and password.
- The substantial assurance level requires the electronic identification scheme to use at least two authentication factors from different categories (possession, knowledge, or inherent). In total, there are three different factors for authentication: Something you are (inherent), something you have (possession), and something you know (knowledge). Two-factor authentication necessitates two different authentication factors: Something you have (e.g., a mobile device) and something you know (e.g., a PIN code). The user should be in control of or possess the authentication factors, and the authentication process shall include dynamic authentication. An example of a substantial assurance level is the use of one-time passwords that are distributed by text messages to mobile phones.
- The high assurance level requires a substantial assurance level and additional means to protect the electronic identification scheme against duplication and tampering. A high assurance level states the following requirements: Multi-factor authentication, private data/keys stored on tamper-resistant hardware tokens, and cryptographic protection of personally identifying information. An example of a high assurance level is a PKI-based authentication scheme with a hardware authentication token, such as a PKI (Public Key Infrastructure) certificate stored on a smart card plus a PIN.

As ENISA already points out [30], the (Q)TSP issuing the certificate will produce a certificate with a high assurance level to a particular user B. User B is expected to be the owner of the signing key residing in the device operated by the QTSP managing the key on behalf of user B. Still, EN 419 241-1 does not require the (Q)TSP to enroll its user with a physical presentation (or equivalent). The fact that the levels are not the same, with "substantial (SCAL2)" on the one hand and "face-to-face based substantial (eIDAS Art.24.1)" on the other hand, can be exploited by user A. User A can impersonate user B to receive an authentication means from the TSP managing the key and, in this way, would be able to create a Qualified Electronic Signature (QES) in the name of user B (having requested the certificate with a face-to-face level).

Creating advanced electronic signatures (AdES) requires the guarantee of the sole control of the signature creation data by the signatory or the control of the seal creation data by the creator of a seal (Articles 26 (c) and 36 (c) of eIDAS). When a TSP creates signatures on behalf of users, this is likely to be covered by a sound implementation of Article 19. However, this is not necessarily verified proactively by means of supervision because "signature creation" per se is not a qualified trust service (it is a "simple" trust service). In addition, even when the TSP is a QTSP operating a QSCD, the QSCD certification does not necessarily imply that AdES will be created (indeed, Annex II only talks about "electronic signatures" and not specifically "advanced" electronic signatures). The verification that "the electronic signature creation data used for electronic signature creation can be protected reliably by the legitimate signatory against use by others" is warranted through QSCD

certification. The difference between an electronic seal and an electronic signature does not affect the QSCD directly; rather, it affects the entity managing the device that may apply stricter policies when a QSCD is used to create electronic signatures. In the end, the QSCD must ensure that the electronic signature creation data used for electronic signature creation can be protected reliably by the legitimate signatory against the use or misuse by a third party, independently of the service (creation of seals or creation of signature) available [30].

To understand how successful Regulations and related Standards provide authentication security to end-users, we investigated the selected services in the sampled Member States, shown in Table 7.

Table 7. Technical authentication for end-users.

Member State	Findings
Italy	In Italy, the onboarding is harmonized between providers to such a level that the recognition methods of the identity can be depicted for all available providers. After the registration, further authentication is left to the trusted service provider. In a publicly available identity provider registry [41], there is a very descriptive table of OTP mechanisms used by trusted service providers. Trusted service providers also offer OTP (One-Time Password) SMS codes.
Slovenia	SI-PASS is a service from the Government-based trusted service provider (SI-TRUST) that works using an SMS during multi-factor authentication and provides the user with a high assurance level and the possibility to create a qualified electronic signature in the cloud. When accessing the service, the user enters a username (email address) and password in the first step. In the second step, the user enters his mobile phone number. After receiving an SMS message, the user enters the one-time password from the SMS message into the web form. The second example is SI-TRUST user registration (the basis for the SMS-PASS service). The user must enter the following information: Email, password, security question (the suggested question is "what is your tax number"), security answer, Security code for the CAPTCHA, and Checkmark to accept terms of use. Note that the tax number is not a private number in many cases. For example, this information is published automatically for a natural person with VAT business registration. Users who want to register for a new identity use the qualified certificate to open the form (not necessarily stored on a certified hardware device—QSCD). After registering and requesting a new SMS-PASS identification, the user receives a new one-time password via snail mail to his home address. After finishing the registration, the user obtains a full identity with a high assurance level and access to the qualified certificate on a certified hardware device (QSCD) in the cloud.
Spain	According to Law 6/2020 [33] and the Order ETD/465/2021 of 6 May [29], regulating the methods of remote identification by video for the issuance of qualified electronic certificates, video identification has been regulated, and it is now possible to obtain electronic certificates in a completely remote process. In addition, there are other examples of remote identification offered by private trust services in Spain, such as the Identity validation of an ID card: Information regarding the document that needs to be validated is sent to the trust service. The trust service sends a link to the person to attach or capture their documents. Once the documentation is received, the trust service provider extracts the data and confirms their validity. The trust service generates a certificate with all the data from the process and the results from the validations and, if required, might maintain custody over the evidence. The public sector uses the Cl@ve service. Cl@ve is not a trusted service but a method for electronic identification and electronic signature based on electronic certificates managed by the Public Administration to access public services. When registering in Cl@ve, the following options are available: Registering via physical visit at a Register Office or online (Via electronic certificate or DNIe) is possible. Without any prior electronic identification means. However, while the first two options correspond to a high assurance level, online registration without prior electronic identification means will correspond to a "Basic" assurance level. Therefore, accessing certain services or using Cl@ve Firma (electronic signature) will not be possible.
Switzerland	SwissID offers remote registration only for certain acts. For the rest, in-person identification is mandatory. First, the user needs to download the free app. Then the user creates an account by filling out a form. There are specific requirements for the password. After the user submits all the information, a verification code is sent to their email. Then, an SMS code confirmation is sent as SwissID uses two-factor authentication. The user is thus required in this step to enter their mobile number. Once this is confirmed, the user needs to insert their PIN. A PIN confirmation then appears. The user can then activate the two-factor authentication. This is not mandatory. If a touch ID is available on the user's smartphone, there is also the option to use a Touch ID instead of a PIN. The user must then verify their identity by scanning an identity document and recording their face on a video. Specific procedures are in place if the user forgets their email or password. After 5 wrong inputs, the account is blocked.

According to the findings, the Member States use and implement authentication systems in the eIDAS network differently. Some employ technological methods with doubtful security features, such as SMS OTP codes. Some Member States are even using outdated security questions.

5.8. SMS as the Second Factor in Multi-Factor Authentication

In 2016, NIST (the National Institute of Standards and Technology in the United States of America) published a draft for their upcoming NIST Special Publication 800-63 (part B) on Digital Identity Guidelines [42]. In it, they recommended the deprecation of SMS as an out-of-band second authentication factor, where out-of-band authentication establishes a separate (second) communication channel that is used to supply an out-of-band secret, which is then returned by way of the primary communication channel for authentication (essentially, a method for delivering a one-time use code for multi-factor authentication). This proposed recommendation caused a big stir in the media, and they posted a blog post [43] documenting their reasons for the decision. They noted that SMS communication is not all mobile phone-based anymore. A message can easily change between SMS, MMS, or data message to another internet service (e.g., a WhatsApp message). For this reason, they recommended verifying that the phone number was attached to a mobile phone before allowing SMS as an out-of-band second authentication factor. Secondly, NIST expressed their skepticism about using SMS as a secure channel because attacks against it that could be performed on a large scale were becoming more successful and efficient.

With these reasons and the fact that, considering how old this technology already was, the security of SMS will most likely not improve with time, NIST suggested deprecating the use of SMS as a second factor. By marking it as deprecated, they wanted to signal that, while it was still completely acceptable to use SMS as a second factor, its usefulness was decreasing, and using it would likely not satisfy future security standards and requirements. They suggested that developers in the future consider using other methods before choosing SMS as the second factor. Deprecating out-of-bound authentication with SMS does not mean that multi-factor authentication is less valid. In fact, NIST has emphasized that using SMS messages is still much more secure than only using a single-factor authentication.

Ultimately, the NIST recommendation to deprecate SMS as a second factor was removed and is no longer present in the final version of the Digital Identity Guidelines [44], published in 2017. However, the recommendations maintain that the possession of a mobile device should be authenticated by a SIM card, and methods should not be used that do not prove possession of a specific device (e.g., voice-over-IP (VOIP)). The most significant reason for the recommendation's removal is likely the media outcry at the recommendation and lobbying by interested organizations [45].

Since then, the attacks against SMS have become even more successful. There are possibilities for attackers to trick carriers into rerouting a phone number to a new device they control. The attack is called a SIM swap. ENISA has recently published a news item [42,45] describing such an attack. Among other potential ways to exploit it, they mention the possibility of bypassing two-factor authentication.

Another major problem is the traditional phone networks, which have their fair share of problems that allow malicious entities to listen to calls, intercept text messages and see your phone's location. One attack that showed such vulnerabilities was the SS7 attack (SS7 stands for the Signalling System No.7 protocol) [46]. The attack allows access to SMS messages, rendering the second factor in the two-factor authentication useless. Other examples of attacks and exploitation of the systems (and social engineering attacks), with similar consequences for the security of two-factor authentication with SMS, can be found in [47,48].

As a result of such attacks and vulnerabilities, the calls to stop using SMS-enabled two-factor authentication have become louder. Authentication services using SMS messages provide authentication for many service providers with essential services (e.g., e-governance). Attackers compromising such services by gaining access could have devastating consequences for individuals. Considering the stakes at play, it is better not to trade ease of use for actual security. This is especially true because alternatives exist and steering away from using SMS-based two-factor authentication would also improve users' trust in the system.

We would, therefore, suggest that SMS is no longer an appropriate technology to be used for the high level of assurance, and any service using it should move on to better alternatives.

Given all the shortcomings of using SMS as the second factor, there are good reasons why it is hard to replace. They revolve primarily around its simplicity to use and deploy. Still, there is also the fact that users have grown familiar with it because it is one of the oldest second factors deployed en masse. That said, the most obvious replacement for out-of-bound authentication with SMS messages is to use authentication apps (e.g., Google Authenticator, Microsoft Authenticator, or Authy) as the out-of-bound verifier. Apps generate random codes that are used as the second factor. The codes change very quickly and are tied to the app. The attackers cannot access them unless they steal the device itself. This is not a severe issue because (in addition to also working against SMS authentication and any other mobile-based two-factor authentication) the attack is much more noticeable (eavesdropping is very hard to detect, especially for the end-user, while a missing device is much more obvious) and is not scalable (mobile devices cannot be stolen remotely or with bots). The use of apps is just as user-friendly as SMS, and it can be even quicker to use because there is no need to wait to receive a text message (the user can use the code directly from an app).

5.9. Security Questions as a Form of Authentication

Through our analysis of selected Member States, we have also noted that some solutions still use security questions as a part of the authentication process.

Security questions are usually pre-prepared questions users receive when setting up an account with a service. The purpose of these questions is to confirm the user's identity periodically (as a second factor in the authentication process) or to regain access to the account if the user forgets their password by providing the correct answers to the questions (inputting the correct answer verifies the user and allows them to reset their password). The idea behind security questions is for the answers to be unique to a person and something only they would know. Typical examples are the mother's maiden name or first telephone number.

In 2015, researchers from Google and Stanford [49] analyzed Google's security questions dataset. This and a preceding experimental study performed by researchers at Microsoft [50] in 2009 showed that the most significant advantage of security questions, which was supposed to be the memorability of the provided information, is not as good as one might imagine. The two studies reported 40% to 60% failure to remember their answers to the security questions. Some other main takeaways were [50]:

- Secret questions have poor security and memorability.
- Statistical attacks and answer distribution prediction are real threats.
- Questions with an expected higher level of differences between users are not as unique as imagined because people provide false answers.
- Potentially more secure questions have a worse recall rate (i.e., less memorable) than less secure counterparts.
- Memorability decreases significantly over time (which is a problem because if security questions are used to reset passwords, they will not be used often).
- Untrue/False answers have worse memorability than truthful answers.
- Other password recovery methods (SMS and email) have a significantly higher chance of success.

Two studies [49,50] boiled down the problems with security questions into:

- Questions with common answers: Many questions have common answers shared by many users (especially in similar geographical locations).
- Questions with few possible answers: Some questions just do not have many possible answers and can be brute-forced/guessed easily.
- Publicly available answers: Information on the answers can be obtained from public (possibly leaked) records or social network profiles.

- Social engineering: Because the answers are typically not secrets by themselves and users do not perceive them as real passwords, they are more likely to be revealed inadvertently by the users to social engineering methods (e.g., phishing).
- Social guessing attack: Some answers might be easily guessable to people who know the account owner.

The studies concluded that security questions could be used to help authenticate users. Still, they should be used in combination with other methods, and for the best security practice, the technique should be replaced with other more secure alternatives.

While user-defined security questions (the users write their own security question together with the answer) might appear to be a good idea because it diversifies the range of possible answers, and in the case that security questions are stolen, it does not give the attacker possible answers (or their statistical model) to attack other services using the same security questions. However, the quality of questions and answers with the user-defined security questions lies squarely with the users and basing security around all of the users choosing good security questions and answers (e.g., not giving very obvious clues about the answer in the question) is a dangerous proposition.

For security questions to be secure, the answers to those questions should be treated the same way as passwords [51,52]. The same answer should not be given twice (even for the same security question). In the same way, a password should not be used for more than one service. Otherwise, if they are stolen, they could be used to access other services. Similar to passwords, answers to security questions should be confidential (i.e., nobody else should know the answer). To achieve confidentiality, security answers should be random values or passphrases (nonsensical passphrases constructed from multiple words are the recommended way to build secure passwords [53]; consequently, the same should apply to the security question answers). However, it is not feasible to expect users to remember such answers; therefore, a password manager is recommended to record all the security questions and answers.

Ultimately, good security questions should be treated the same way as passwords but having a backup "password" to restore the original password (i.e., using the same method twice) is nonsensical and not a good practice. While security questions are simple to deploy, traditional security answers are hackable, guessable, and vulnerable to theft in much the same way that passwords are (only even more so). Therefore, their use is not recommended as the sole user authentication or password recovery method. NIST also no longer recognizes security questions (they refer to them as pre-registered knowledge tokens) as an acceptable authenticator in their latest Special Publication 800-63-3 [54,55]. However, NIST still allows the use of security questions as knowledge-based verification—an identity verification method based on knowledge of private information associated with the claimed identity—given some restrictions on how the security questions should function (Section 5.3.2. of [54]).

The Slovenian SI-PASS allows users to write their own security questions, but it gives "What is your tax number?" as a security question example. While tax number does not appear to be a terrible option because it cannot be guessed (like, for example, favorite color), this is not a piece of information known exclusively to the user. In Slovenia, an individual's tax number is known to some people at the financial administration (together with some other government administrations for adjusting taxation, e.g., child support) and your employer. If you are self-employed, then the tax number is public information. Therefore, having your tax number as a security answer is bad in the first case and a terrible option. Ultimately, security questions are not a strong authentication method and should not be used for trusted services.

5.10. Notability of Changes by Hash Algorithms in Digital Signatures

While analyzing the authentication security, we came across the eIDAS requirement that does not relate directly to authentication. Because of its importance for understanding

and recognizing qualified electronic signatures as identical to hand signatures, we have decided to include the finding in this report.

Article 26 of eIDAS sets the requirements for an advanced electronic signature. Under (d), it states that an advanced electronic signature must be linked to the data signed in addition to that so that any subsequent change in the data is detectable. Simply put, if any change is made to the data for which a signature was made, the change should be detectable from that signature. The wording in eIDAS is absolute ("any subsequent change in the data is detectable"), while cryptographic elements that achieve this in currently used state-of-the-art digital signatures only ensure this with overwhelming probability and not with absolute certainty.

Modern digital signatures that are currently in use are made using asymmetric encryption. However, before encryption is performed over the data, the data are, for multiple reasons, first hashed. A cryptographic hash function is a one-way process that takes an input of variable length and produces an output of fixed length. The hash function outputs are measured in bits (e.g., 256 bits, in which case the output will be a random string of 256 zeros and ones). The result is called a hash. It provides integrity and could be explained as a form of a unique data fingerprint. In this context, data integrity ensures data have not been changed, or any change to them is detected (which is precisely what the eIDAS requires of the advanced electronic signatures). However, hash functions do not actually ensure that every possible change is detectable. They only make it highly unlikely to find two messages that produce the same hash (changes between these two messages would not be detectable by this hashing algorithm because the hash value would be the same). Since a hash function obtains a message of any length as input but outputs a fixed length value, multiple messages will produce the same hash value. The probability of two different messages resulting in the same hash value is governed by the function's resistance to collisions (two different messages producing the same hash value is called a collision). The collision resistance of a perfect (truly random) cryptographic hash function depends on its output size, where the principle of the so-called birthday problem limits the upper bound. The number of attempts (e.g., how many messages we would need to hash and compare) is estimated with the $\sqrt{2^{n+1} \times (-\ln(1-p))}$ formula, where n is the output size of the hash function and p is the probability we would want to achieve [56]. For example, the SHA-256, which is a commonly used hashing algorithm in digital signatures, would have an n of 256. To obtain 50% of finding a collision ($p = 0.5$), we would have to try hashing approximately 4×10^{38} messages. The alternative SHA-512 would take approximately 1.36×10^{77} tries. For comparison, the probability of winning a lottery is one in 1.4×10^{7}. The probability of finding a collision of two messages with such size outputs is therefore extremely low, but it is not zero. Collision attacks are why previously popular hash functions (e.g., MD5 and SHA-1) are no longer recommended. They fell out of favor immediately after an example of a collision was demonstrated (i.e., it became feasible to actually generate messages with the same hash value [57]). This is exactly because this vulnerability could be exploited in digital signatures (collision vulnerability is not as critical for other primary hash use cases, such as password hashing).

In summary, hash functions are used in digital signatures to provide integrity, which ensures changes to the signed data are noticeable. However, hash functions only provide this with an extremely high probability and do not guarantee completely that two different sets of data will be discerned as different. This means that both produce the same signature and can also be exchanged with the same signature. Ultimately, the absolute wording in eIDAS could cause national courts to no longer consider digital signatures as meeting advanced electronic signature requirements because they do not ensure that every change is detectable. Therefore, it would be better if eIDAS would, in Article 26 (d), require the detectability of any changes with a high enough probability, or it could provide more information on when the condition is met because, as it stands currently, digital signatures arguably do not meet them.

6. Discussion

The European Commission is already accepting that remote electronic signatures and seal creation devices need additional guidance. The new qualified trust service for the management of remote electronic signature and seal creation devices would bring considerable security, uniformity, legal certainty, and consumer choice benefits, both linked to the certification of the qualified signature creation devices and in relation to the requirements to be fulfilled by the qualified trust service providers managing such devices. The new additions would reinforce the trust service providers' overall regulatory and supervisory framework [1].

Our investigation of the situations in the selected countries implementing eIDAS concluded that all the issues in the working documents leading to eIDAS 2 have additional shortcomings that need further attention.

This research extends the work already completed at the European Commission and ENISA to improve the current eIDAS framework. Therefore, we also considered the proposed solutions to develop eIDAS 2.0. The most important value in eIDAS 2.0 would come from decoupling identity attributes from the network itself, thus lowering the barrier for businesses to use them. Joining the eIDAS network has a steep implementation curve and presents an important market barrier with an uncertain outcome because of the many eIDAS deficiencies already discussed in the existing literature.

To provide a good overview of our findings, we summarize the main ones here.

First, issues with the heterogeneous requirements comparing different supervisory authorities lead to differences. According to our investigation, we identified a pattern where supervisory authorities also provide trust services (at the same time), which is in contrast to other supervision and certification schemes, e.g., the organizational independence of auditors according to the International Standard of Auditing 200 and ISO 19011 schemes regarding the organizational independence of the supervisory body.

Second, looking at the banking example proposed in the eIDAS 2 presentations, we identified additional obstacles to cross-border onboarding in the banking sector. The banking sector has specific requirements in every Member State in the sample. Consequently, there is no universal process nor a universal set of documents to be provided to the bank to open a banking account. In some cases, there are additional limitations according to local banking regulations.

Third, we found additional shortcomings in regulation regarding video identification. The limitations are not only bound to whether some Member State does or does not allow remote video identification. Looking from a broader perspective, the eIDAS network should be recognized equally in all Member States. Different security requirements for remote video identification may lead to some schemes not being recognized in some Member States. Further, higher security requirements increase costs, making trusted service providers in the Member States with higher standards uncompetitive. Fourth, there is little convergence in understanding what levels of assurance should be used in specific use cases. This opens many questions for businesses as they try to understand what level of assurance they need. With some governments lowering their assurance level requirements for comparable services in the other Member States, simplification and lowering of the costs become a market issue.

Fifth, very different practices allow commercial access to the eIDAS network between the selected Member States. Some Member States do not allow access for the private sector, access is envisioned but not implemented, or access is allowed, even for foreign businesses.

Sixth, even though we have not found an example of biometrics being used in the EU Member States, Switzerland is already using biometrics in mobile devices to protect access to identity. Considering the widespread use of such solutions in the banking sector, there is little doubt that this technology will also find its way into the eIDAS network.

Seventh, the authentication mechanisms in the eIDAS network across the Member States use technical solutions with questionable security attributes, such as SMS OTP codes. Some Member States are even turning to security questions that are deemed obsolete. These

solutions are not only used in cloud signature solutions but have also reached further (e.g., banking).

Finally, when analyzing the security requirements of electronic signatures, it became evident that eIDAS uses very strict wording regarding the capabilities of the qualified electronic signature, that "any subsequent change in the data is detectable". According to the current state-of-the-art technologies used to create electronic signatures, this is not entirely true.

Following our findings, we summarize our eIDAS-related recommendations as follows:

- eIDAS 2 should follow the best practices of other certification and supervisory schemes regarding the organizational independence of the supervisory body.
- Essential services for the single market (e.g., banking) should be allowed explicitly in all Member States under the provisions of eIDAS 2 to avoid local limitations and even the prohibition of the use of eIDAS services.
- A security baseline should be established for the remote identification services to avoid degradation of remote identification because of the market competition and to avoid excluding specific services or the Member States from the network based on inadequate security standards.
- Higher market penetration of the highest assurance level needs to be achieved to empower citizens to use any service anytime without additional effort. Promoting or even requiring the use of a substantial assurance level in the public sector wherever possible would support this effort.
- Access to the eIDAS network should be allowed explicitly to the private sector in all Member States. Any limitation to access the eIDAS network through another Member State should at least be discouraged to promote competition between the Member States.
- A strategy for the "Bring Your Own Authentication Device" solution needs to be built, as this approach is gaining traction. At the same time, it represents a "grey area," at least when combined with biometrics. We propose further research in current state-of-the-art use cases with the intent to identify best practices and definitions of the feasible legal framework for such use of biometric devices.
- An increase in the speed of security standards development is vital as current standards are falling behind the latest cybersecurity developments.

The definition of the capabilities of the qualified electronic signature should be changed to reflect existing state-of-the-art technologies used to create electronic signatures to avoid different interpretations.

7. Conclusions

This paper focused on selected use cases with the intent to identify any deficiencies hidden under the umbrella of global renovation of the legislation. Consequently, it focused on specific real-world scenarios and was not based on an administrative review as most existing reports are.

Based on our investigation, we identified several issues. The first hidden deficiency is the situation where supervisory authorities also provide trust services simultaneously. This is not compliant with the Auditing and Certification Standards. When studying the real-world feasibility of envisioned use cases in the banking scenarios, we discovered that the eIDAS legislation might not guarantee universal cross-border use of identities. Limitations and cross-border differences in remote video identification might bring even more heterogeneity to the level where the differences may lead to different levels of trust in the obtained title and difficulties in cross-border recognition. As an assurance level incurs costs, some governments are lowering the bar for some governmental services. However, there are additional reasons for promoting the highest assurance levels at the government level. We found that inter-government competition exists, and some governments provide access to foreign commercial entities. Even though this may be good for the competition, it also has downsides with the pressure on the costs and, later, the level of cybersecurity.

For that reason, minimum security standards should be planned carefully and as straightforwardly as possible to minimize different interpretations. Further, we found that the phenomenon that we named "Bring Your Own Authentication Device—BYOAD" is rising. Devices owned by the consumers are not certified, and cloud service providers do not have contracts with the providers of the biometric security solutions as they once had before mobile phones started taking the function of "offline" authentication devices. For now, this is more widespread in the banking sector, and we have not yet identified its prevalent use in the eIDAS network. While we analyzed remote onboarding and authentication practices in the eIDAS network, we found that many prevalent solutions do not follow the latest security guidelines. Examples are the use of SMS for OTP passwords and the use of security questions. Often, solution providers trade security for simplicity. Although developing and deploying software and solutions may appear simple, understanding, collecting, and adhering to the various Regulations in all Member States is not.

In future work, we would like to extend the list of topics to discuss and compare between countries and include all the EU Member States missing in this study. Furthermore, we would like to delve into more detail for each topic by including lists of relevant national laws for each Member State and potentially analyzing them with the help of appropriate persons with adequate legal backgrounds from the respective countries.

Author Contributions: Conceptualization, M.H. and B.K.; methodology, M.K.; validation, M.H. and B.K.; formal analysis, M.H., B.K., and M.K.; supervision, M.H.; writing—original draft preparation, M.H. and M.K.; writing—review and editing, M.H., M.H., and B.K.; funding acquisition, M.H. All authors have read and agreed to the published version of the manuscript.

Funding: The authors acknowledge the financial support from the European Union's Horizon 2020 Research and Innovation Program under the CyberSec4Europe project (Grant Agreement No. 830929) and the Slovenian Research Agency (Research Core funding No. P2-0057).

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thank our collaborators from Atos Spain S.A. (Spain), Archimede Solutions SARL (Switzerland), the Italian National Research Council (Italy), and University of Murcia (Spain) for helping us collect the data on implementations of eIDAS in their respective countries.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. EU. Regulation (Eu) 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. 2014. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed on 1 December 2022).
2. Guillaume, M.; Bounjoua, S.; Clemot, C. eIDAS compliant eID Solutions. ENISA. 2020. Available online: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions (accessed on 1 December 2022).
3. Kirova, M.; Eichholtzer, M. Overview of Pre-Notified and Notified Eid Schemes under Eidas. Eid User Community. 2019. Available online: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (accessed on 1 December 2022).
4. Resende, J. D3.13 - Updated Version of Enablers and Components, Cybersec4europe. 2021. Available online: https://cybersec4europe.eu/wp-content/uploads/2022/02/D3.13-Updated-version-of-enablers-and-components-v3.0-submitted.pdf (accessed on 1 December 2022).
5. EU. Proposal gor a Regulation of the European Parliament and of the Council Amending Regulation (Eu) No 910/2014 As Regards Establishing a Framework for a European Digital Identity. 2021. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281 (accessed on 1 December 2022).
6. EU. Compilation of Information Provided by Member States with Regard to The Implementation of the Trust Services Chapter of the Eidas Regulation. 2017. Available online: https://ec.europa.eu/futurium/en/content/information-member-states-regard-implementation-trust-services-chapter-eidas-regulation.html (accessed on 1 December 2022).
7. EU. Eid Documentation—Country Overview. 2020. Available online: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview (accessed on 1 December 2022).

8. EU. eID Documentation—eID for You. 2020. Available online: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+for+You#eIDforYou-eid (accessed on 1 December 2022).
9. Pedroli, M.; O'Neill, G.; Fravolini, A.; Marcon, L. Overview of Member States' Eid Strategies. 2021. Available online: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/National+Strategies (accessed on 1 December 2022).
10. Lips, S.; Bharosa, N.; Draheim, D. eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. *Commun. Comput. Inform. Sci.* **2020**, *1349*, 75–89. [CrossRef]
11. Rocha, J. Spanish and Portuguese eIDAS node evolution for electronic identification of European citizens. In Proceedings of the EATIS '20: Proceedings of the 10th Euro-American Conference on Telematics and Information Systems, Aveiro, Portugal, 25–27 November 2020; pp. 1–5. [CrossRef]
12. Tsap, V.; Lips, S.; Draheim, D. eID Public Acceptance in Estonia: Towards Understanding the Citizen. In Proceedings of the 21st Annual International Conference on Digital Government Research, Seoul, Korea, 15–19 June 2020. [CrossRef]
13. Kubicek, H. Introduction: Conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries. *Ident. Inform. Soc.* **2010**, *3*, 5–26. [CrossRef]
14. Berbecaru, D.; Atzeni, A.; De Benedictis, M.; Smiraglia, P. Towards Stronger Data Security in An Eid Management Infrastructure. In Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), St. Petersburg, Russia, 6–8 March 2017; pp. 391–395. [CrossRef]
15. Shrishak, K.; Erkin, Z.; Schaar, R. Enhancing User Privacy in Federated eID Schemes. In Proceedings of the 8th IFIPInternational Conference on New Technologies, Mobility and Security (Ntms), Larnaca, Cyprus, 21–23 November 2016. [CrossRef]
16. Lenz, T.; Zwattendorfer, B. Towards cross-border authorisation in European eID federations. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016. [CrossRef]
17. Carretero, J.; Izquierdo-Moreno, G.; Vasile-Cabezas, M.; Garcia-Blas, J. Federated Identity Architecture of the European eID System. *IEEE Access* **2018**, *6*, 75302–75326. [CrossRef]
18. Morgner, F.; Bastian, P.; Fischlin, M. Securing Transactions with the eIDAS Protocols, Information Security Theory and Practice. *Lecture Notes Comput. Sci.* **2016**, *9895*, 3–18. [CrossRef]
19. Phn, D.; Grabatin, M.; Hommel, W. eID and Self-Sovereign Identity Usage: An Overview. *Electronics* **2021**, *10*, 2811. [CrossRef]
20. Roelofs, F. Analysis and Comparison of Identification and Authentication Systems Under the Eidas Regulation, Msc Radbound University. 2019. Available online: https://www.ru.nl/publish/pages/769526/z02_masterthesis_floris_roelofs_final.pdf (accessed on 1 December 2022).
21. IFAC. International Standard on Auditing 200: Overall objectives of the independent auditor and the conduct o fan audit in accordance with international standards on auditing, IFAC. 2009. Available online: https://www.ifac.org/system/files/meetings/files/3393.pdf (accessed on 1 December 2022).
22. *ISO. 19011:2018*; Guidelines for Auditing Management Systems. Available online: https://www.iso.org/standard/70017.html/.
23. EU. Electronic Identification (Eid) and Trust Eervices for Citizens: Eidas Solutions. Available online: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54410 (accessed on 1 December 2022).
24. EU. Electronic Id and Trust Services in Action: Open A Bank Account. Available online: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54412 (accessed on 1 December 2022).
25. Slovenia. Rules on the System for the Exchange of Information on the Indebtedness of Natural Persons (Sisbon). No. 65/17, 6/18, 68/18 and 97/21.18. Available online: http://www.pisrs.si/Pis.web/pregledPredpisa?id=DRUG4429 (accessed on 18 June 2021).
26. Spain. Autorización De Procedimientos De Vídeo-Identificación. Madrid: Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. 2017. Available online: https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf (accessed on 1 December 2022).
27. Spain, Ley 10/2010, De 28 De Abril, De Prevención Del Blanqueo De Capitales Y De La Financiación Del Terrorismo. BOE No. 236. Available online: https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737 (accessed on 1 December 2022).
28. Turner, D.M. Understanding ZertES - the Swiss Federal Law on Electronic Signatures. Cryptomathic. 2016. Available online: https://www.cryptomathic.com/news-events/blog/understanding-zertes-the-swiss-federal-law-on-electronic-signatures (accessed on 1 December 2022).
29. Spain. Orden Etd/465/2021, De 6 De Mayo, Por La Que Se Regulan Los Métodos De Identificación Remota Por Vídeo Para La Expedición De Certificados Electrónicos Cualificados. BOE No. 115. Madrid: MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. 2021. Available online: https://www.boe.es/eli/es/o/2021/05/06/etd465/dof/spa/pdf (accessed on 1 December 2022).
30. ENISA. Assessment of Standards related to eIDAS," ENISA. 2018. Available online: https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas (accessed on 1 December 2022).
31. Spain. Prevention of Money Laundering and Terrorist Financing Act. No. 68/16, 81/19, 91/20 and 2/21. Available online: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7132 (accessed on 7 January 2021).
32. Spain. Electronic Identification and Trust Services Act. No. 121/21 and 189/21. Available online: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7550 (accessed on 3 December 2021).
33. Spain. Ley 6/2020, De 11 De Noviembre, Reguladora De Determinados Aspectos De Los Servicios Electrónicos De Confianza. BOE No. 298. Available online: https://www.boe.es/buscar/act.php?id=BOE-A-2020-14046 (accessed on 1 December 2022).

34. Switzerland. Due Diligence Requirements for Client Onboarding Via Digital Channels, Finma Circular 2016/7: Video And Online Identification. 2016. Available online: https://www.finma.ch/~{}/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2016-07-20210506.pdf?sc_lang=en (accessed on 1 December 2022).
35. Spain. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. *BOE No. 236*. Available online: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565 (accessed on 1 December 2022).
36. Italy. Cos'è SPID. Rome: Agenzia per l'Italia digitale. Available online: https://www.spid.gov.it/cos-e-spid/ (accessed on 1 December 2022).
37. Italy. How to Enable Eidas Login for Public Service Providers Participating In The Public Digital Identity System (Spid). Rome: Agenzia Per l'italia Digitale. Available online: https://www.eid.gov.it/abilita-eidas (accessed on 1 December 2022).
38. Spain. Real Decreto 203/2021, De 30 De Marzo, Por El Que Se Aprueba El Reglamento De Actuación Y Funcionamiento Del Sector Público Por Medios Electrónicos BOE No. 77. Available online: https://www.boe.es/buscar/act.php?id=BOE-A-2021-5032 (accessed on 1 December 2022).
39. ETSI Technical Specification, ETSI TS 119 431-1 - V1.2.1, Electronic Signatures and Infrastructures (Esi); Policy and Security Requirements for Trust Service Providers; Part 1: Tsp Service Components Operating a Remote Qscd Scdev. 2021. Available online: https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.02.01_60/ts_11943101v010201p.pdf (accessed on 1 December 2022).
40. ETSI Technical Specification, ETSI TS 119 432 V1.2.1 (2020-10), Electronic Signatures and Infrastructures (Esi); Protocols for Remote Digital Signature Creation. 2020. Available online: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf (accessed on 1 December 2022).
41. Italy. How To Choose Between Digital Identity Providers. Agenzia Per l'italia Digitale. Available online: https://www.spid.gov.it/en/what-is-spid/how-to-choose-between-digital-identity-providers/ (accessed on 1 December 2022).
42. NIST; Grassi, P.A.; Garcia, M.E.; Fenton, J.L. Digital Identity Guidelines. 2017. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf (accessed on 1 December 2022).
43. NIST. Questions . . . and buzz surrounding draft NIST Special Publication 800-63-3. Available online: https://www.nist.gov/blogs/cybersecurity-insights/questionsand-buzz-surrounding-draft-nist-special-publication-800-63-3 (accessed on 1 December 2022).
44. Dudley, W. Rollback! The United States NIST NO LONGER recommends "Deprecating SMS for 2FA". 2017. Available online: https://blogs.sap.com/2017/07/06/rollback-the-united-states-nist-no-longer-recommends-deprecating-sms-for-2fa/ (accessed on 1 December 2022).
45. ENISA. Beware of the Sim Swapping Fraud! 2021. Available online: https://www.enisa.europa.eu/news/enisa-news/beware-of-the-sim-swapping-fraud (accessed on 1 December 2022).
46. Positive Technologies, Ss7 Network Security Analysis Report. 2020. Available online: https://www.ptsecurity.com/upload/iblock/3fc/3fce640add5eb5ba9476d416eb0c7f4d.pdf (accessed on 1 December 2022).
47. Cox, J. Hackers Are Breaking Directly Into AT&T, T-Mobile, and Sprint to Take Over Customer Phone Numbers, VICE. 2020. Available online: https://www.vice.com/en/article/5dmbjx/how-hackers-are-breaking-into-att-tmobile-sprint-to-sim-swap-yeh (accessed on 1 December 2022).
48. Cox, J. A Hacker Got All My Texts for $16, VICE. 2021. Available online: https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber (accessed on 1 December 2022).
49. Bonneau, J.; Bursztein, E.; Caron, I.; Jackson, R.; Williamson, M. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In Proceedings of the WWW'15 - Proceedings of the 22nd international conference on World Wide Web, Rio de Janeiro, Brazil, 13–17 May 2015; pp. 141–150101145273627727416 91.
50. Schechter, S.; Brush, A.J.B.; Egelman, S. It's no secret Measuring the security and reliability of authentication via 'secret' questions. In Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, Oakland, CA, USA, 17–20 May 2009; pp. 375–390. [CrossRef]
51. Gontovnikas, M. Are Your Security Questions as Safe as You Think?, auth0 Blog. 2017. Available online: https://auth0.com/blog/are-your-security-questions-as-safe-as-you-think/ (accessed on 1 December 2022).
52. Haber, H. Security Questions Pose a High Risk: Learn Tips & Tricks to Mitigate the Threat, BeyondTrust Blog. 2022. Available online: https://www.beyondtrust.com/blog/entry/reused-security-questions-can-pose-a-high-risk-learn-tips-tricks-to-mitigate-the-threat (accessed on 1 December 2022).
53. Grassi, P. NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology (NIST). 2017. Available online: https://csrc.nist.gov/publications/detail/sp/800-63b/final (accessed on 1 December 2022).
54. Grassi, P.A. NIST Special Publication 800-63A - Digital identity guidelines: Enrollment and Identity Proofing Requirements, National Institute of Standards and Technology (Nist). 2017. Available online: https://pages.nist.gov/800-63-3/sp800-63a.html (accessed on 1 December 2022).
55. NIST. NIST SP 800-63 Digital Identity Guidelines-FAQ. 2022. Available online: https://pages.nist.gov/800-63-FAQ/ (accessed on 1 December 2022).

56. Preshing, J. Hash Collision Probabilities, Preshing on Programming. 2011. Available online: https://preshing.com/20110504/hash-collision-probabilities/ (accessed on 1 December 2022).
57. Stevens, M.; Bursztein, E.; Karpman, P.; Albertini, A.; Markov, Y. The First Collision for Full SHA-1. *Lect. Notes Comput. Sci.* **2011**, *10401*, 570–596. [CrossRef]