Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D3.18

Analysis of interoperability and cross-border compliance issues

Document Identification	
Due date	31 January 2022
Submission date	31 January 2022
Revision	1.0

Related WP	WP3	Dissemination Level	CO
Lead Participant	UM	Lead Author	Boštjan Kežmah (UM)
Contributing Beneficiaries	AIT, ARCH, ATOS, CNR, GUF, UM, UMU	Related Deliverables	D3.6

Abstract: The research results presented in this document represent deliverable D3.18: Analysis of interoperability and cross-border compliance issues of the eIDAS framework and are the continuation of the deliverable D3.6: Guidelines for GDPR Compliant User Experience. We start by reviewing the literature and description of the latest reports and working documents of the European Commission and ENISA, together with the proposal for the eIDAS 2. The second part analyses selected real-world eIDAS scenarios in selected Member States and identifies additional shortcomings of the current framework with the intent to suggest further additions to the proposed eIDAS 2 framework to achieve long-term cybersecurity goals in cross-border scenarios and to promote the use of identities in the commercial sector of the European Single Market. The second part investigates the current heterogeneity of privacy requirements across the Member States and its effect on the effort required to provide GDPR compliant services.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This research builds on the work already completed at the European Commission and ENISA as a basis for monitoring the current eIDAS network and proposing eIDAS 2. Additionally, we extend the deliverable D3.6: Guidelines for GDPR Compliant User Experience, where we collected and presented guidelines for the compliance with the General Data Protection Regulation (GDPR) and proposed a template tool for performing a Data Protection Impact Assessment (DPIA). This deliverable investigates GDPR heterogeneity in the EU and shows why such guides and templates must be adaptable and cannot be overly specific.

This deliverable focuses on a specific sample of selected eIDAS network cross-border use-cases with the intent to identify any deficiencies hidden under the umbrella of the already proposed global renovation of the regulation. Consequently, the study focused on specific real-world scenarios and was not based on administrative review as most existing reports.

The first part focuses on reviewing existing literature, an outline of the eIDAS network, and proposed eIDAS 2 solutions. This part of the deliverable formed a basis for the questionnaire, later distributed between the selected Member States.

The second part presents the selected use-cases and how they are supported in selected Member States. By analysing real-world implementations of the use-cases chosen, the analysis leads to the identification of detailed shortcomings of the current regulation as it is manifested in the following areas:

1. Organizational independence - looking into organizational independence issues between supervisory authorities and service providers.
2. Remote access to the banking services across borders analyses possibilities of onboarding between the selected Member States.
3. Remote video identification examines the heterogeneity of security requirements and legal grounds for remote video identification scenarios.
4. The use of electronic signatures in public administration explores the different requirements for the levels of assurance. For comparison, it uses the same cloud service - remote access to the EU Digital COVID Certificate.
5. Commercial access to the eIDAS network identifies entry barriers for the commercial sector to join the eIDAS network and the effect of anticipated market competition between the governments (Member States).
6. Biometrics as Authentication Mechanism discusses challenges of the new phenomenon – Bring Your Own Authentication Device (BYOAD).
7. Technical authentication and onboarding security requirements investigate selected cybersecurity issues with currently broadly used security mechanisms.

After laying down the use-cases and fundamental findings of the real-world scenarios, a discussion follows with the results and proposed solutions of the shortcomings identified.

The second part of the deliverable presents detailed results of the survey about the privacy heterogeneity in the EU, followed by the analysis and discussion. This part of the research is an upgrade and continuation of the study resulting in D3.6: Guidelines for GDPR Compliant User Experience.

Finally, the conclusion summarises the findings of the presented deliverable.

Document information

Contributors

Name	Partner
Antonio Skarmeta	UMU
Boštjan Kežmah	UM
Eda Marchetti	CNR
Marko Hölbl	UM
Marko Kompara	UM
Perez Baun, Juan Carlos	ATOS
Renáta Radócz	ARCHIMEDE
Tamara Bubnjar	UM

Reviewers

Name	Partner
Rahul Bobba	NEC
Alessandro Sforzin	NEC
Alzubair Hassan	UCD

History

Version	Date	Authors	Comment
0.01	2021-07-05	Boštjan Kežmah	1st Draft
0.5	2021-09-15	Marko Kompara	2nd Draft
0.7	2021-11-20	Boštjan Kežmah	3rd Draft
0.8	2021-11-27	Boštjan Kežmah	Added information from partners on the situation in their Member States
0.9	2021-12-30	Boštjan Kežmah	Review ready version
0.91	2022-01-25	Marko Kompara	Updates based on the reviews
0.92	2022-01-25	Tamara Bubnjar	Updates based on the reviews
0.93	2022-01-25	Marko Holbl	Updates based on the reviews
0.95	2022-01-26	Boštjan Kežmah	Incorporated reviewer comments and corrections.
1.0	2022-01-26	Boštjan Kežmah	Final version
1.0	2022-01-31	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

2	**2FA**	Two-Factor Authentication
A	**AdES**	Advanced Electronic Signature
B	**BYOAD**	Bring Your Own Authentication Device
C	**CA**	Certificate Authority
	CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
	CEN	European Committee for Standardization
	CNIL	Commission Nationale Informatique & Libertés (French)
	COVID	Severe Acute Respiratory Syndrome Coronavirus-2 (SARS-CoV-2)
D	**DGT**	General Directorate of Police (DGT)
	DNI	National Identity Document (Spain)
	DNIe	Documento Nacional de Identidad Electrónico (Spain)
	DPA	Data Protection Authority
	DPO	Data Protection Officer
	DTBSR	Data To Be Signed Representation
E	**EC**	European Commission
	eID	electronic IDentification
	eIDAS	electronic IDentification, Authentication and Trust Services
	EISBA	International Ethics Standards Board for Accountants
	EN	European Standard
	ENISA	European Union Agency for Cybersecurity
	EPR	Electronic Patient Record
	ETSI	European Telecommunications Standards Institute
	EU	European Union
F	**FINMA**	Swiss Financial Market Supervisory Authority
G	**GDPR**	General Data Protection Regulation

I	**ISO**	International Organization for Standardization (Organisation internationale de normalisation)
L	**LoA**	Level of assurance
M	**MD5**	Message-Digest (algorithm) 5
	MFA	Multi-Factor Authentication
	MMS	Multimedia Messaging Service
N	**NIST**	National Institute of Standards and Technology (United States of America)
O	**OTP**	One-Time Password
P	**PIN**	Personal Identification Number
	PKI	Public Key Infrastructure
	PP	Protection Profile
	PKI	Public Key Infrastructure
Q	**QES**	Qualified Electronic Signature
	QSCD	Qualified electronic Signature Creation Device
	QTSP	Qualified Trusted Service Provider
S	**SA**	Supervisory Authority
	SAD	Signature Activation Data
	SAM	Signature Activation Module
	SAP	Signature Activation Protocol
	SCAL1	Sole Control Assurance Level 1
	SCAL2	Sole Control Assurance Level 2
	SCD	Signature Creation Device
	SCDev	Signature Creation Device
	SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Spanish)
	SHA	Secure Hash Algorithm
	SIM	Subscriber Identity Module or Subscriber Identification Module
	SISBON	The central database of credit information (Slovenia)

	SMS	Short Message Service
	SPID	Sistema Pubblico di identità Digitale (Italian)
	SS7	Signalling System No.7
	SSASC	Server Signing Application Service Component
	SSCD	Secure Signature Creation Device
	SVD	Signature Validation Data
T	**TOE**	Target of evaluation
	TS	Technical Specification
	TSP	Trust Service Provider
	TW4S	Trustworthy Systems Supporting Server Signing
U	**UK**	United Kingdom
V	**VAT**	Value-added tax
	VOIP	Voice-Over-IP

1 Introduction

The task T3.7 of the work package WP3 in CyberSec4Europe is designed around European Union's recent regulations on data protection, privacy and authentication (GDPR and eIDAS). In this deliverable, we specifically look at any possible issues and differences present in their implementation across the EU Member States.

Our previous research (deliverable D3.6 - Guidelines for GDPR compliant user experience) was mainly about how to comply with the General Data Protection Regulation (GDPR), and we proposed a new template tool for performing a Data Protection Impact Assessment (DPIA). However, while working on deliverable D3.6, we have identified some challenging inconsistencies in how regulation could be applied. This could lead to interoperability issues that can be difficult to address or at least a nuisance when having to comply with such rules across multiple Member States. After identifying these harmonization issues, our research became focused on how those deficiencies might be related to the authentication and the use of cross-border identification schemes and electronic signature as defined in the eIDAS (electronic IDentification, Authentication and trust Services) framework [1]. In this deliverable, we have identified and will discuss the following weaknesses: organizational independence, remote access to the banking services, remote video identification, use of electronic signatures in public administration and remote access to the EU Digital COVID Certificate, commercial access to the eIDAS network, biometric authentication mechanisms, and finally some technical issues with mechanisms used to provide security and authentication.

In addition to the eIDAS related work, we have also continued the work from D3.6 by also investigating the areas of the GDPR that have the potential to prove as a challenge in the sense that they can be different between the EU Member States. For those areas, we have collected data from the Member States to see if there are actually any differences between the countries (all the Members States could have just implemented GDPR in the same way) and, if so, how significant or prevalent the differences are.

1.1 Deliverable Contributions

Currently, there is a big push from the EU to update the eIDAS regulation to make it more uniform across the Member States. However, except from the EU related organizations, there is very little analysis or comparisons of the eIDAS implementations. Therefore, the first part of this deliverable discusses eIDAS and identifies situations and areas (Section 3) where there are differences between the EU Member States (based on the analysis of a sample of the Member States). The problems could be different depending on the issue, but they include actual privacy/security/trust vulnerabilities, unfair markets, different authentication levels of trust, etc. The identified issues do not include situations that would be improved on by the recently proposed regulation update (i.e. eIDAS 2) and should, therefore, be considered in improving the current eIDAS regulation.

The second main contribution is similar but applies to the GDPR. As we will discuss in the section on GDPR heterogeneity (Section 4), there are some materials available on the differences in how GDPR is implemented in the individual Member States (Section 4.1). However, they are generally on a very high level, and, as we will discuss, the areas of differences that we identified could likely cause problems (or at least additional complications) in assuring compliance when doing so for more than one Member State. Although the data was collected primarily to show the differences between the EU Member States, it can also be used as a rudimentary tool to check if particular security practices are allowed in an individual country. As part of the effort on presenting these differences in a simple and understandable way, we have

also created a dynamic map that shows the situation in the EU Member States for which we were able to collect the data. You can find the map on the CyberSec4Europe website at https://cybersec4europe.eu/heterogeneity-of-data-protection-legislation-in-the-eu/.

Partial results of this deliverable were already showcased in deliverable D3.13 [2], while the rest will be included in an upcoming deliverable D3.20. The GDPR portion of this deliverable (Section 4) has also been published in a peer-reviewed paper [3]. For any related future publications or any other potential changes and additions to the research, visit our GitHub page (https://github.com/cs4ewp3/wp3/tree/main/3.7) where we plan to communicate any further developments in the research and publications.

1.2 Document structure

The first part of this document places the eIDAS regulation into the research focus and gives an overview of related work. After that, the research is split into the main aspects of harmonization issues as identified in our previous study, presented in deliverable D3.6 - Guidelines for GDPR compliant user experience.

The findings are first discussed using existing findings of the European Commission that are leading the way to the next version of the eIDAS framework (eIDAS 2 [4]). This is presented in Section 2. In Section 3, the discussion is then put into the practical perspective backed by a questionnaire disseminated between the partners of the work package task (Task 3.7).

Section 4 presents findings from the GDPR questionnaire with the data collected from the national supervisory bodies. This research extends on some of the ideas indicated in previous research (D3.6). Here it is assumed that the answers from the supervisory bodies are free from bias and present correct legal interpretation of the situation in each Member State. The results show interesting differences in implementations of some GDPR-related topics between the EU Member States.

Finally, in Section 5, we discuss the findings and provide some additional guidelines for further development of eIDAS 2 by supplementing the European Commission's conclusions that support the proposal for the renovation of the current eIDAS legislation.

2 eIDAS

The eIDAS Regulation [1] was supposed to enable the use of electronic identification means and trust services (i.e. electronic signatures, electronic seals, time stamping, registered electronic delivery and website authentication) by citizens, businesses and public administrations to access online services or manage electronic transactions.

It was supposed to provide:

- transparency and accountability: well-defined minimal obligations for Trust Service Providers (TSP) and liability;
- 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 standardisation certainty.

Even though expectations about eIDAS were high, the legal framework did not completely meet those expectations. As a result, the upgrade of the current regulation has already started.

2.1 Related Work

We could not find much research or comparison of eIDAS implementations across the EU. Some of the more general lists of comparable information between the Member States is naturally compiled by the EU itself. This includes a compilation of information regarding the implementation of the Trust Services of the eIDAS Regulation [5], eIDAS-Node implementation progress with service providers and identity providers in each country [6], the eID supported public services across the EU [7], and the Member State's strategies for eID [8].

There are case studies of individual countries and their implementations of eIDAS (e.g. [9]–[11]) but studies addressing a wider 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 [12], [13], [14], [15]. The most relevant of research here is the [16], which looks at the federated identity architectures used and analyses 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 analysed in [17]. The eID and Self-Sovereign Identity overview of the existing solutions and current projects developing and implementing the solutions are presented in [18]. 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 [19] describes authentication systems from seven countries (Germany, Belgium, Estonia, Luxembourg, Spain, Italy, and Croatia) that have completed eIDAS notification of at least one system by the beginning of 2019 and Netherlands (the author's home country). The research includes all eID systems from the selected countries, even if they have not been notified. Before the EU is notified of a system, the system is reviewed by European Commission. If the system meets 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 (ensure their services are available through that system) in one year. For each system, the author provides the basic information on the system, encryption and PKI, authentication process and any 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 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.

2.2 eIDAS Legislation

The use of new technologies for acquiring, transmitting, and collecting information brings a great deal of data and the risks facing organizations. Regulation (EU) No 910/2014, also known as the electronic Authentication and Signature Regulation, provides a legal basis in the internal market for electronic identification in the Member States. The eIDAS Regulation aims to strengthen the trust of individuals, legal persons and public authorities in the digital world and electronic transactions in the internal market to provide a common basis for legally secure electronic cooperation. The objective of the eIDAS Regulation is to facilitate at the European level the use of electronic identification resources in the individual Member States for natural and/or legal persons. Therefore, the eIDAS Regulation seeks to facilitate the use of

electronic authentication channels by means of the principle of mutual recognition and mutual acceptance of electronic identification systems for the verification of the identity of legal persons and citizens, as carried out by public authorities.

Among the innovations brought about by the eIDAS Regulation, one of the most important to highlight is the possibility of creating e-signatures remotely, where the environment for creating an e-signature on behalf of the signatory is managed by a trust service provider. When we wish to create a qualified e-signature, the e-signature service provider must ensure, through appropriate mechanisms and procedures, that the signatory has sole control over the use of its data to generate an e-signature and that the requirements for qualified e-signature are met when using the device.

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

The eIDAS was published on 17 September 2014 and entered into force on 1 July 2016. The eIDAS Regulation aims to strengthen confidence in electronic transactions in the internal market by providing a common basis for secure electronic interactions between citizens, businesses and public authorities, thereby increasing the efficiency of public and private online services, e-commerce and e-commerce in the Union. The e-signatures Directive has only established a legal framework for electronic signatures, but not for electronic identification and authentication, and related trust ancillary services. The Regulation addresses these shortcomings.

The eIDAS Regulation is divided into two parts in substance, namely:

- electronic identification, without prejudice to the electronic identity management systems and associated infrastructures of the Member States, but merely sets out the conditions under which the Member States recognise the means of electronic identification of natural and legal persons covered by the notified scheme of another State, and on the other hand
- trust services, where the Regulation governs the scope in its entirety and lays down rules for trust services, namely for electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, the retention of qualified electronic signatures and stamps and services relating to website authentication certificates.

As mentioned above, the eIDAS Regulation (only) regulates the mutual recognition of e-identification means for the purposes of cross-border authentication for an online service provided by a public sector body in a Member State. Chapter II of the Regulation [1] lays down the conditions for the mutual recognition of identification means issued under notified e-identification schemes, the level of reliability allocated to e-identification means issued under the scheme and the elements for determining the level of reliability of funding and the notification procedures, ensuring safety, accountability and forms of cooperation, and ensuring interoperability. In this context, it should be noted that a 'high level of trust in electronic identity can be said when the e-identification means under the e-identification scheme is manufactured/issued in accordance with the prescribed technical specifications, standards, and procedures, including technical controls, which prevent the risk of misuse or altering identity. A low and medium level of reliability only ensures a reduction in the risk of abuse or change of identity.

The eIDAS does not require the Member States to introduce certain e-identification means (e.g. an e-ID card) but to decide what means and with what level of reliability they will use or require to access online services. It is also up to them to decide whether to involve the private sector in the acquisition of these funds.

The eIDAS Regulation divides electronic signatures into:

- "ordinary" electronic,
- advanced electronic signatures and
- qualified electronic signatures.

In doing so, advanced digital signatures are divided into two subtypes:

- advanced electronic signature and
- advanced digital signature, supported by a qualified certificate for electronic signatures.

The eIDAS Regulation sets requirements only for advanced and qualified e-signatures and does not regulate so-called ordinary e-signatures. Under the eIDAS Regulation, the functions of advanced and qualified e-signatures are expressions of will, signatory identification and integrity. The functions of advanced and qualified electronic stamps are confirmation of origin and integrity, while a "plain" digital signature — including, for example, handwritten signature, clickwrap signatures, signatures with signature plates, a mouse signature, and similar solutions - does not have these features. As a result, companies (as e-service providers) must assess which level of e-signature corresponds to their legal or contractual obligations or business needs, which they do on the basis of a risk assessment. The assessment is thus the subject of an assessment of the risk of possible non-compliance with the regulatory or contractual obligations or the potential costs of the dispute with the e-service user of which the e-signature is part, as well as the benefits of maintaining the originality and integrity of the e-signed documents or data in the long term.

2.2.1 Purpose of the eIDAS Regulation

The eIDAS Regulation provides a common foundation for secure electronic interaction between citizens, businesses and public authorities. The Regulation aims at increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union. To this end, it includes provisions for electronic identification and trust services. The provisions on electronic identification are new as this topic was not addressed in the previous 1999/93/EC Directive superseded by the eIDAS Regulation. These provisions are detailed in Articles 6 to 16 of the regulation and refer to notions of electronic identification, electronic identification means and electronic identification schemes:

- **"Electronic identification"** relates to the process of using personal identification data in an electronic form, uniquely representing either a natural or a legal person or a natural person representing a legal person.
- **"Electronic identification means"** is the material and/or immaterial unit containing the personal identification data and which is used for authentication to an online service, and
- **"Electronic identification scheme"** is the system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing legal persons.

The regulation introduces several provisions, which aim to build a framework allowing citizens to use their electronic identification means across borders with a shared level of trust. The provisions primarily encompass the following elements, in particular:

- **Notification:** an electronic identification scheme can be notified to the Commission in order to benefit from cross-border recognition. Member States can submit eID schemes for prenotification following a pre-defined template that describes the key principles of the scheme. The Commission Implementing Decision (EU) 2015/1984 defines the circumstances, formats and procedures of notification for eID schemes. It also provides a notification form to be used by the Member States.

The prenotified schemes are reviewed by eID experts during a peer-review process. The eIDAS Cooperation Network then issues an opinion regarding the compliance of the electronic identification scheme with eIDAS provisions (especially regarding the compliance with the requirements on the claimed Level of assurance (LoA)). The Commission Implementing Decision (EU) 2015/296 details the conditions on the cooperation between the Member States, including the peer-review of the schemes.

- **Mutual recognition:** electronic identification means that have been issued under notified electronic identification schemes shall be recognised for cross-border authentication to access public online services. This mutual recognition is only mandatory for online services that require electronic identification means with at least a Substantial LoA (meaning Substantial or High) and for eID schemes whose LoA matches the level required by the online service. For instance, a German public service requiring a High LoA electronic identification means shall accept Belgian electronic identification means issued under a scheme notified to the Commission for the High LoA. The CIR (EU) 2015/1501 provides further requirements for the interoperability framework that supports cross-border authentication.
- **Level of assurance (LoA):** the Regulation introduces three levels of assurance for electronic identification means issued under notified electronic identification schemes: Low, Substantial and High. The LoA of the electronic identification means refers to the degree of confidence that can be put in the claimed identity of a person during an electronic identification using this electronic identification means. The CIR (EU) 2015/1502 describes the minimum requirements to be met for each LoA. It mainly details the requirements expected for the initial identity proofing before issuing the electronic identification means, for the electronic identification means characteristics (design, issuance and activation, lifecycle management), for the authentication process and the general requirements for organisation and management (including requirements for identity providers issuing these electronic identification means).

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 the assurance level High. In 2018, the number of notification processes increased notably, with six Member States notifying eID schemes between September and the end of December 2018 [20]:

- Italy, with its SPID scheme, which 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 assurance level High.
- Belgium, Croatia, Luxembourg, and Spain notified eID schemes based on their electronic national identity cards for assurance level High.

In 2019, six more Member States notified their eID schemes for the first time [20]:

- Portugal and the Czech Republic with eID schemes based on the electronic national identity card for the assurance level High.
- The UK with GOV.UK Verify, with eID means issued by private players (bank, post office, etc.) appointed by the UK government, for the assurance levels Low and Substantial. (Remember: The UK is not anymore a member of the European Union).
- The Netherlands with a business-oriented scheme (for legal persons) for the levels Substantial and High depending on the identity provider (3 identity providers identified in the schemes providing various eID means). Slovakia with an eID card-based scheme for nationals and foreigners for the assurance level High.

- Latvia with a card-based scheme (eID card and dedicated card) and a mobile application for the assurance levels Substantial and High.

In 2019, two countries notified a second eID scheme [20]:

- Italy with a scheme based on electronic identity cards for the assurance level High.
- 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 the assurance level High.

2.3 The outlook - eIDAS 2

Since the entering into force of the eID part of the Regulation in September 2018, only 14 Member States have notified at least one eID scheme. As a result, only 59 % of EU residents have access to trusted and secure eID schemes across borders. Only seven schemes are entirely mobile, responding to current user expectations. As not all technical nodes to 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 [2].

As a result of current shortcomings, a new proposed Regulation (EU) [4] was published on June 3rd, 2021, aiming to amend the eIDAS Regulation by establishing the new framework for the "European Digital Identity" (aspiring to be known as the "EUid" or "eIDAS 2" or "eIDAS 2.0"). This proposal, which is not yet final, seeks to enhance the eIDAS further to cause a paradigm shift in European digital identification of citizens and companies.

Currently, the eIDAS Regulation covers the following layers of electronic identification and trust services [1]:

- lays down the conditions under which the Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
- lays down rules for trust services, in particular for electronic transactions; and
- establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

As can be clearly understood from the subject matter of eIDAS Regulation, it is primarily aimed at conditions and rules for mutual recognition of electronic identification means and focused on electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication. eIDAS Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants [1].

Aiming at governmental and other public use made eIDAS somewhat confined to the services in official matters. Consequently, there has been little uptake of trust services in the commercial sector, even though market circumstances favoured electronic transactions following covid-19 limitations of face-to-face communication.

Apart from the overall limitations of the reach of eIDAS Regulation, some technical issues arose that are limiting the use of electronic identification means in the commercial sector. As defined in eIDAS, person identification data means a set of data enabling the identification of a natural or legal person [1]. In real-

world technical implementations, this data is limited to unique identifiers in electronic certificates that have no immediate meaning. Therefore the users of electronic identification means and person identification data have limited use of data that is immediately available. Consequently, for businesses to get expanded information about the entity, they must be connected to the eIDAS network. Once connected to the eIDAS network, there are different solutions on how the owner of the data controls which properties of the personal data set will be available to the recipient of the personal data.

Some sets of data may not even be available (for example, information about education) or may not be in the appropriate form. For example, information about age may be calculated from the date of birth. However, there is no need for the data recipient to get such detailed information as information about the age would suffice in some circumstances, thus failing to reach the principle of data minimisation. Because of these limitations, the primary added value of current eIDAS legislation is in mutual recognition between the Member States and definition of electronic signature and seal, their use and connection with the handwritten signature.

European Digital Identity Wallets are personal digital wallets that allow citizens to digitally identify themselves and store and manage identity data and official documents in electronic format. These may include a driving licence, medical prescriptions or education qualifications. With the wallet, citizens will be able to prove their identity where necessary, to access services online, share digital documents, or simply to prove a specific personal attribute, such as age, without revealing their identity or other personal details. Citizens will always have full control of the data they share [4].

Considering the current limitations of eIDAS, the Commission envisioned three policy options for the further development of eIDAS [2] as follows:

- The first option presents a low level of ambition and a set of measures mainly aiming to strengthen the effectiveness and efficiency of the current eIDAS Regulation. By imposing mandatory notification of national eIDs and streamlining the existing instruments available to achieve mutual recognition, the first option is based on meeting the needs of citizens by relying on the availability of diverse national eID schemes that aim to become interoperable.
- The second option presents a medium ambition level and mainly aims to extend the possibilities for the secure exchange of data linked to identity, complementing government eIDs and supporting the current shift towards attribute-based identity services. The aim of this option would have been to meet user demand and create a new qualified trust service for the provision of electronic attestations of attributes linked to trusted sources and enforceable cross-border. This would have extended the scope of the current eIDAS Regulation and supported as many use cases as possible, relying on the need to verify identity attributes linked to a person with a high level of assurance.
- The third and preferred option presents the highest level of ambition and aims to regulate the provision of a highly secure personal digital identity wallet issued by the Member States. The preferred option was considered to address the objectives of this initiative in the most effective way. To fully address the policy objectives, the preferred option builds on most measures assessed under option one (reliance on legal identities attested to by Member States and the availability of mutually recognised eID means) and option two (electronic attestations of attributes legally recognised cross border).

Considering the high entry threshold to connect to the eIDAS network, the first option will have the least impact on the Single Market. As already discussed, businesses would still have to connect to the eIDAS network to get information about the attributes.

According to the Commission, the positive environmental impact is expected to be greatest for the third option, which is expected to improve to the maximum extent the take-up and usability of eID, bringing positive impacts on the emissions reduction related to public service delivery.

Although European Commission recognized the need to bring the eIDAS framework to the next level to make it broadly available 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 on how to address authentication security issues already identified by ENISA [20] and how to relate the use of biometrics with the GDPR and the cybersecurity liability of the device providers.

3 eIDAS Implementation Issues

The evaluation of the eIDAS Regulation revealed that the current Regulation falls short of addressing new market demands, mostly due to its inherent limitations to the public sector, the limited possibilities, and 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 falling outside the scope of eIDAS, such as those offered by social media providers and financial institutions, raise privacy and data protection concerns. They cannot effectively respond 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 [2].

To verify selected findings of the European Commission and their effect on real-world use-cases, we have selected a subset of identified issues and collected information on real-world use in selected Member States. The represented Member States are the home countries of this task's partners. We selected the sample using a non-statistical method to focus on scenarios that were either emphasized in the preparatory documents for the eIDAS 2 proposals or were identified during our previous research in the field of personal data protection (deliverable D3.6).

Based on the sample, we have prepared a guided questionnaire/interview. It can be found in Annex A: eIDAS Questionnaire of this document.

3.1 Organizational Independence

Managing a (Qualified) electronic Signature/Seal Creation Device ((Q)SCD) or creating a (qualified) signature on behalf of signers are trust services for which the eIDAS Regulation does not specify a qualified level. In other words, only (Qualified) Trusted Service Providers ((Q)TSP) that have been granted a qualified status pursuant to Article 21 of the eIDAS Regulation for one or more of the qualified trust services (QTS) specified in the eIDAS Regulation may generate or manage electronic creation data on behalf of the signer. As these TSPs are qualified, they must use trustworthy systems and products that meet the requirements of Article 24(2), in particular points e) and f) [21].

CEN EN 419 221-5 may apply when the electronic signature creation data or electronic seal creation data is held in an entirely, but not necessarily exclusively, user-managed environment. When combined, the two protection profiles apply to a qualified trust service provider managing the electronic signature creation data or electronic seal creation data on behalf of a signatory or of a creator of a seal. However, the verification of assumptions made by the Protection Profiles (PP) on the target of the evaluation's environment needs to be ensured. In the context of eIDAS, for a QTSP, this is a task carried out by the supervisory body. Consequently, a certified QSCD can only be officially recognised as such once the QTSP has been duly supervised to manage the QSCD according to requirements and assumptions on the environment provided in the PPs (and possibly as specified in complementary policy documents like ETSI TS 319 431-1). This requires that the supervisory body supervises the qualified trust service for which the QTSP is granted a

qualified status as well as the QSCD management, starting with the verification that the QSCD is certified and then verifying any requirement on the environment which needs to be duly implemented by the QTSP [21].

An ENISA report suggests that there is shared responsibility between the TSP managing the QSCD to work with appropriate TSP issuing certificates (CA) and on the CA to work with an appropriate TSP for the management of QSCD. For qualified devices management and qualified certificates issuance, the verification that such requirements are followed falls under supervision by competent supervisory bodies.

ENISA suggested back in 2018 [22] that explanations on the role of supervision (that is mandatory), and ideally a pointer to the checklist to clearly identify the elements to be checked by the audit underlying the supervision process should be provided directly in the amended version of Commission Implementing Decision (EU) 2016/650. Alternatively, this information could be provided as a link toward a "to be issued" Implementing Act referred to by Article 29. Given that a certain amount of coordination among stakeholders is required to achieve a global trust level, it would be pertinent to provide a way to advertise the elements of supervision. Besides the official compilation of Member States notification on SSCDs and QSCDs, the trusted list of the country where QTSP operates might provide an indication when the QTSP manages a QSCD duly in accordance with eIDAS.

Alternatively, the list of notified SSCDs and QSCDs compiled by the European Commission might also be used for this purpose. This would be important to inform the market and organizations that wish to implement qualified electronic seals or signatures conformant to eIDAS [21].

During our initial scoping research and literature review, we identified an additional possible issue with the role of supervision, that is, organizational independence.

We learned that in Slovenia, the supervisory body is the same organization as is providing the trust services. In essence, that means the same organization 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 of the questionnaire was to find out whether there are similar occurrences of organizational independence issues in selected Member States.

Member State	**Findings**
Italy[1]	The supervisory authority for trust services provides qualified trust services at the same time. National Register of the Resident Population, Administrative Procedure Management System, Storage
Slovenia[2]	The supervisory authority is itself providing qualified trust services. Ministry of Public Administration

[1] https://www.agid.gov.it/en/platforms/national-register-of-the-resident-population
[2] https://spot.gov.si/sl/dejavnosti-in-poklici/dovoljenja/kvalificirani-status/#e11438

Spain[3]	The supervisory authority for trust services provides non-qualified trust services at the same time. Ministry of Economic Affairs and Digital Transformation
Switzerland	The system is decentralized, and there is no apparent single, centralized supervisory authority.

Table 1: Organizational independence for partner countries

The results of the questionnaire show a pattern where supervisory authorities are providing trust services at the same time.

This is contradictory to the families of standards 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. 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 scepticism [23].

Similarly, according to the ISO 19011 [24], auditors should be independent of the activity being audited wherever practicable and should, in all cases, act in a manner that is free from bias and conflict of interest.

Since cybersecurity incurs costs, providing the function of supervision and provision of services in the same entity could affect the independence, at least in appearance. This arrangement could also affect the competition in the market as the main entity that is offering trust services and defining legislation or even access to the eIDAS network is also competing with other service providers in a closed market.

3.2 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 [25]:

- eSignature – will help citizens sign legal documents and email 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 real 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 that, for example, my son's birthday present arrives safely.

[3] https://portal.mineco.gob.es/es-es/Paginas/default.aspx

The European Commission also envisioned the basic use case for opening a cross-border bank account. An EU citizen is temporarily relocated from Spain to Luxemburg for business reasons [26]. She is opening a bank account in Luxemburg before travelling. The citizen uses her Spanish eID so that the bank in Luxemburg can verify her age and identity. There is no need for her to visit Luxemburg to open a bank account personally. The bank carries out checks on her financial record based on data of her eID (Due Diligence). The citizen does not have to provide additional information, and the bank can swiftly give a green light.

The objective of Regulation (EU) 910/2014 of the European Parliament and of the Council (the eIDAS Regulation) is to enable the cross-border recognition of government-issued electronic identification (eIDs) to access public services and to establish a Union market for trust services recognized across borders with the same legal status as the traditional equivalent paper-based processes [27].

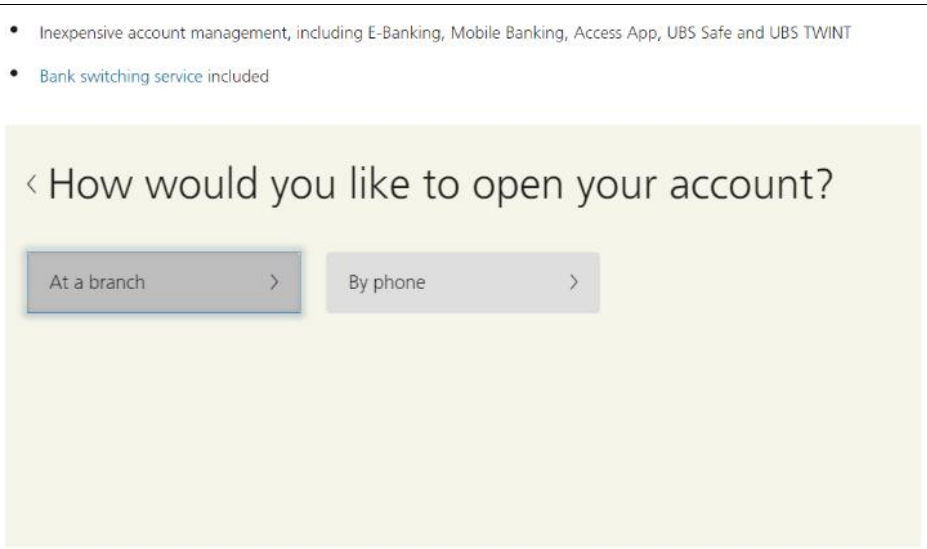
As local regulation could hinder envisioned scenarios, we looked at envisioned local scenarios in selected Member States according to our sample.

Member State	**Findings**
Italy	Currently, no matter if you're a resident, a temporary worker, a student, a tourist, or a professional travelling often for business - you have to provide the local branch of an Italian bank the same set of documents as the Italians do: • Identification, such as a valid passport, identity card, or driver's license • Italian tax code, called codice fiscale, as well as Certificato di Attribuzione del Codice Fiscale that comes with the tax code • Proof of address in Italy, and enrollment on the university program for students, of residence permit or work contract The proposals using the simple and transparent system for the payments to the Public Administration are similar to pagoPA, which is the national platform. According to your habits and preferences, it allows you to choose how to pay taxes, 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"[4]. 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 "Rules on the system for the exchange of information on the indebtedness of natural persons (a.k.a. SISBON) – article 18" with the inclusion of eIDAS trusted service providers that are now equal to Slovenian trusted service providers. Electronic identification must meet requirements for "high assurance level".

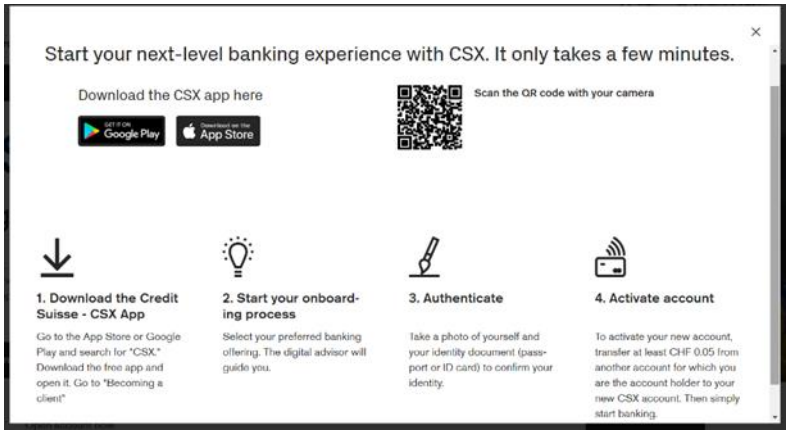
[4] http://www.pisrs.si/Pis.web/pregledPredpisa?id=DRUG4429

	Regardless of the legal basis, none of the Slovenian banks currently provide a remote onboarding service. To provide such a service, the bank would have to be included in the eIDAS network to access attributes of the identity provided. Even though the new Electronic Identification and Trust Services Act envisions the usage of 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 in 2017 the use of video-identification processes by financial entities.[5] It defines a level of assurance high, as required by the "Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo" (Law 10/2010, of April 28, on the prevention of money laundering and financing of terrorism). The process involves the exhibition of identity documents, as well as a set of technical (unique device, "streaming" immediate recording) and organizational (qualified professionals) measures. These bank accounts are not subject to specific limitations beyond what was established in Article 12 of Law 10/2010 (i.e. copies of the official documentation must be obtained within a month from the beginning of the business relationship).[6]
Switzerland	Previously, opening a bank account was only possible upon providing a personal identification document on-site and a hand-written signature. 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 recognised provider of certification services in accordance with the Swiss Electronic Signature Act (ZertES) of 19 December 2003 suffices as authentication. Restrictions on assurance levels when opening such an account were not able to be identified, as prior registration is necessary to find such information. When opening an account at the UBS Bank, for example, there are two options available shown below:

[5] https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf
[6] https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737



However, Credit Suisse Bank offers the ability to open an account remotely in full via an app.



CIM Bank also gives the option to open bank accounts online and collaborates with a Swisscom trusted service provider to authenticate signatures.

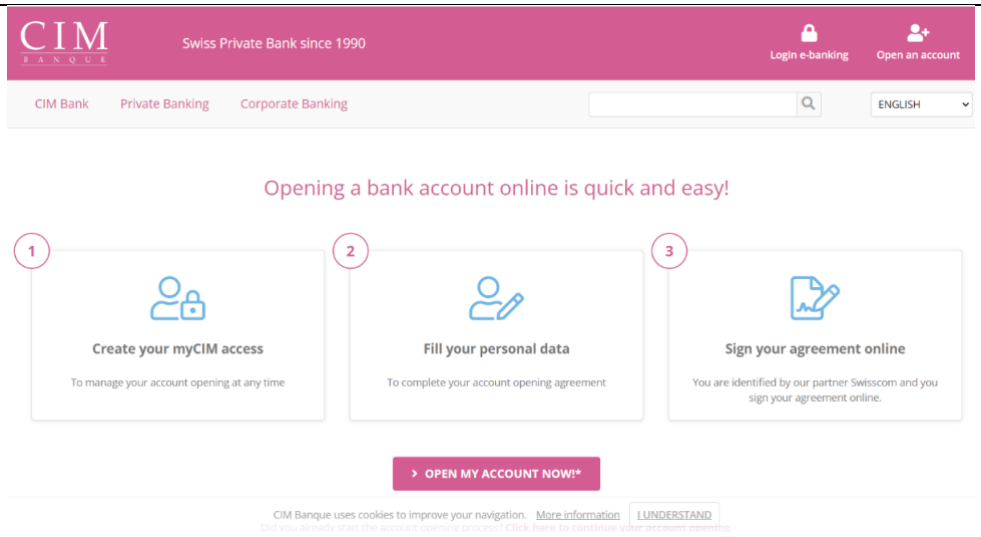
	

Table 2: Remote access to banking services for partner countries

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

3.3 Remote Video Identification

The use of video identification is allowed in some Member States, even for onboarding for the banking services (Spain).

According to some sources [28], based on the recently approved Order ETD/465/2021, of May 6th, 2021, regulating the remote video identification methods for issuing qualified electronic certificates, Spain is currently the EU country with the most electronic trust service providers. The new legislation helped increase this number because allowing video identification makes it more interesting/viable for companies to sell such services.

By means of the instruments regulated in eIDAS, it is possible to use these trust services as well as associated electronic documents as evidence in legal proceedings across the EU Member States contributing to their general usability within the Member States 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 they would do for their paper equivalent [22].

This leads to a question of how different requirements for video identification might affect 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 if eIDAS is followed strictly.

In marginal scenarios, a citizen of one Member State could even obtain a digital identity using remote video identification in another Member State and later use that identification in its own State. This could already be the case, for example, if the bank in Spain decided to provide banking services and trust services

according to eIDAS to be freely used by her customers. Consequently, the questions of regulating requirements for remote video identification are invading the regulation area of the eIDAS network.

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. Usually, the service is available 7 days a week, from 9.00 to 21.00. The Online Recognition can be performed via SPID every day 24 hours a day through PC or Smartphone.
Slovenia	In Slovenia, there is a Prevention of Money Laundering and Terrorist Financing Act[7]. This is the only Act that defines special requirements regarding remote video-electronic identification. The intent of the provisions is the prevention of money laundering and is not directly relevant for remote video identification for the issuance of identities. Currently, none of the trusted service providers in Slovenia provide remote video identification services that would result in the issuance of electronic identification (either low, substantial, or high), according to eIDAS. A local provider (Telekom Slovenije) provides remote video identification services, but only in closed environments. This means it provides identification as a service to a specific customer (e.g. an insurance company) for their purposes and under their policy (it is only accepted for purposes defined by that organization). Therefore, identification can only be used in that closed environment and does not meet eIDAS requirements. Under the Electronic Identification and Trust Services Act[8], electronic identities issued by the Republic of Slovenia can be issued only to Slovenian citizens at least six years old or to foreigners who have a domicile or temporary residence in the Republic of Slovenia. There are no other special requirements for any private trusted service providers.

[7] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7132
[8] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7550

Spain	The "Ley 6/2020[9], de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza" (Law 6/2020, of November 11, regulating certain aspects of electronic trust services) authorized other methods for identification, such as identification via videoconference or video-identification with a level of security equal to the physical personation 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)). Also, the procedure followed for the identification may appear in the certificate.[10] Futhermore, the "Orden ETD/465/2021[11], de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos" (Order ETD/465/2021, of May 6, regulating remote video identification methods for the issuance of electronic certificates), applies to qualified public and private providers of trust services established in Spain or with a permanent establishment located in Spain, as far as their services are not already supervised by the authority of different Member State. It contains specific requirements regarding security aspects, identity documents, facilities and the remote identification process.
Switzerland	Since FINMA Circular 2016/7 "Video and online identification" 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 zone. 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 video identification concerns an individual, a legal entity or more than one contracting party.

Table 3: Remote video identification for partner countries

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.

[9] https://www.boe.es/buscar/act.php?id=BOE-A-2020-14046

[11] https://www.boe.es/eli/es/o/2021/05/06/etd465/dof/spa/pdf

3.4 The Use of Electronic Signature in Public Administration

During the scoping overview phase of this research, we have learned that many businesses have little understanding of the requirements of the assurance level when doing business with their customer. eIDAS provides different levels of assurance and different kinds of electronic signatures. Every level of assurance and every kind of electronic signature brings additional costs and complexity into the information system and user experience. Businesses are therefore reluctant to use higher levels of assurance than necessary.

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

The question was whether there are any public services that do not require qualified electronic signature when filing claims (e.g. reporting taxes and similar services) and if there is any regulation that specifically defines assurance levels for different procedures, at least for the public services.

Member State	**Findings**
Italy	Authentication is always required. If an electronic signature is not available, 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 electronically filing tax-related claims anymore. Clicking a button in the web application suffices but logging into the web application still requires assurance of high level. Electronic Identification and Trust Services Act[12], Article 15, provides provisions for the definition of the required assurance level that will be 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 the "Ley 30/2015 del Procedimiento Administrativo Común de las Administraciones Públicas"[13] (Law 30/2015 on the Common Administrative Procedure of Public Administrations) 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 the Article 11 (Administrative Procedure). Only the electronic signature will be mandatory in terms of 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.

[12] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7550
[13] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565

Switzerland	Government level electronic services do not require any qualified electronic signature. However, the Electronic Patient Record (EPR) will start being introduced gradually during 2021 in every region of Switzerland. The Federal Act on the Electronic Patient Record stipulates how the EPR should be organised and made secure from a technical point of view. Each EPR provider is assessed, certified and regularly inspected. SwissID will be used during the login as means of patient verification. In this specific example, SwissID can be obtained only via in-person verification.

Table 4: The use of electronic signature in public administration for partner countries

Similar to previous questions, there is too much heterogeneity to move on to the case study that could directly compare requirements in similar scenarios.

Even though different levels of assurance and different kinds of signatures are defined in the eIDAS, there is little convergence in understanding what levels should be used in specific use-cases.

The government may even decide to take the risk of an electronic signature not being automatically recognized as equal to a hand-written signature by the law. When the government is not promoting the use of the highest assurance levels and qualified electronic signatures with its services, the technology is not available at the citizen level. Thus, these levels of security have little penetration in the commercial market.

Commercial services that require higher levels of assurance (e.g. banking, 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.

3.5 Remote Access to EU Digital COVID Certificate

Because of heterogeneity, we could not directly compare required assurance levels on a broad scale. Hence, we have introduced a more specific requirement, that is remote access to the EU Digital COVID Certificate.

The EU Digital COVID Certificate is a standard document across all Member States. From a cybersecurity perspective, one could expect that for the same kind of document with the same personal data and with the same power of proof, the authentication mechanisms would be comparable and require the same level of assurance.

Member State	**Findings**
Italy	Access is granted by using a substantial level of authentication for the digital identity. In this case, with the Public Digital Identity System, you can access online services of the Public Administration (such as the EU Digital COVID Certificate) and private adherents.
Slovenia	A substantial or high assurance level is required to access EU Digital COVID Certificate in Slovenia.

Spain	A high assurance level is required to access the EU Digital COVID Certificate in Spain. Citizens can make use of any of the means recognized in the access to public services (DNIe (National Identity Document), electronic certificate or Cl@ve), as well as additional means for those who do not have any of the means previously mentioned (e.g. creation of an account via a specific code), but that require personation of the individual at the health institution as a prior step.
Switzerland	A substantial or high assurance level is required to access the EU Digital COVID Certificate. The Certification system[14] is open source, and a public security test has been taken.

Table 5: Remote access to the EU digital COVID certificate for partner countries

In the selected sample of the Member States, the minimum assurance level to access the EU Digital COVID certificate was the same across all the Member States.

3.6 Commercial Access to eIDAS Network

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

The basic requirement is that access to the eIDAS network needs to have legal grounds. 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.

Member State	**Findings**
Italy	The private sector can also benefit from the digital identity, improving the user experience and management of customers' personal data. SPID also allows access to public services of the member states of the European Union and of companies or traders who have chosen it as an identification tool.[15,16] Companies from the other Member States can also access eIDAS services.

[14] https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/covid-zertifikat/covid-zertifikat-pruefer-aussteller-technische-informationen.html#-128733039
[15] https://www.spid.gov.it/cos-e-spid/
[16] https://www.eid.gov.it/abilita-eidas

Slovenia	Slovenia has an Electronic Identification and Trust Services Act[17]. This Act allows organizations providing electronic services to use electronic identity issued by the government. Executive regulation does not yet exist at this time; therefore, further technical and other requirements and/or pricing are still unknown.
Spain	The "Real Decreto 203/2021 por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos"[18] (Royal Decree 203/2021 approving the Regulations for the performance and operation of the public sector by electronic means) has regulated, in its third additional provision, the Electronic Identification Interoperability Node of the Kingdom of Spain, 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, 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 (a.k.a. ZertES). No pricing list is available. Under art 3(2), when a foreign provider has already obtained recognition by a foreign recognition body, the Swiss recognition body may recognise it if it is proved that: • the recognition was granted in accordance with foreign law; • the rules of the 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.

Table 6: Commercial access to eIDAS network for partner countries

The results from the selected Member States vary. Some Member States do not allow access for the public sector (Spain), access is envisioned but not implemented (Slovenia), or access is allowed even for foreign businesses (Italy).

[17] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7550
[18] https://www.boe.es/buscar/act.php?id=BOE-A-2021-5032

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 start to build.

Companies will have the option to choose an eIDAS network entry point and consequently control their costs. That will put pressure on the public providers to stay competitive or local nodes may start to lose interest.

This may also have a negative impact. If there is too much open competition between trusted service providers in different Member States, that may have a direct effect on the security of the network in the different Member States. Security incurs costs. If security requirements in some Member State are lower than in other Member State, this will give local providers a competitive advantage. Consequently, care must be put into requiring the exact basic security requirements in all Member States.

3.7 Biometrics as Authentication Mechanism - BYOAD

In the private sector, especially banking and the general public identity providers (e.g. Google, Microsoft), we see the rise of the use of biometrics.

Unfortunately, such use of biometrics is currently "a grey area". The use cases are mostly based on the biometric capabilities of current mobile devices. That means that 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 the use of such devices. Even though these devices have a direct impact on the security of the service for the end-user, the banks don't 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 her own selection of the mobile device and the final security of the service will vary depending on the device selected. 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 is affecting the security services provided according to eIDAS.

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 case 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 May 6, regulating the methods of remote identification by video for the issuance of qualified electronic certificates.
Switzerland	SwissID App allows the use of Touch ID on Apple devices.

Table 7: Biometrics as an authentication mechanism for partner countries

The results of the survey show differentiation of the authentication market. Even though the banks have high authentication security requirements and are offering mobile banking solutions that are based on biometric solutions provided in modern mobile devices, this technology has not met broad recognition in authentication mechanisms offered in eIDAS services. The only surveyed country that supports biometric authentication in eIDAS services in Switzerland (member of the European Economic Area, not the EU).

3.8 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 organisational arrangements. Standards provide a generally accepted means to meet requirements with existing technology, whilst, if necessary, the market can develop alternative solutions as new technology emerges to further feed into the standardisation life cycle. In the specific context of 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 on-going.[19]

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 mainly references ISO/IEC 27002:2013.

According to the 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 remotely controls the signing key 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 for the purpose of signing 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 Signature Activation Data (SAD) be available in the local environment. The SAD brings three elements together:

- Signer authentication
- Signing key
- Data to be signed (DTBS/R(s))

In ensuring that the signees/signing parties have sole control of their signing keys, the signature operation requires authorization. This is performed by a Signature Activation Module (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 that exists between the three SAD elements while ensuring that the signer is authenticated.

[19] Assessment of Standards related to eIDAS: Recommendations to support the technical implementation of the eIDAS Regulation, ENISA, November 2018, https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas/at_download/fullReport

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 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 in order 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 directly perform signee authentication, it must assume that part, if not all, of the authentication has taken place and then rely on the assertion provided. 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 [22], at the time of writing of Commission Implementing Decision 2016/650, there were no available standards for signing devices operated by a trust service provider in a secure environment that aim 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 signature/seals and
- trust service providers creating qualified electronic signature/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) [29] clearly defines the scope of remote signing standards (Figure 1).

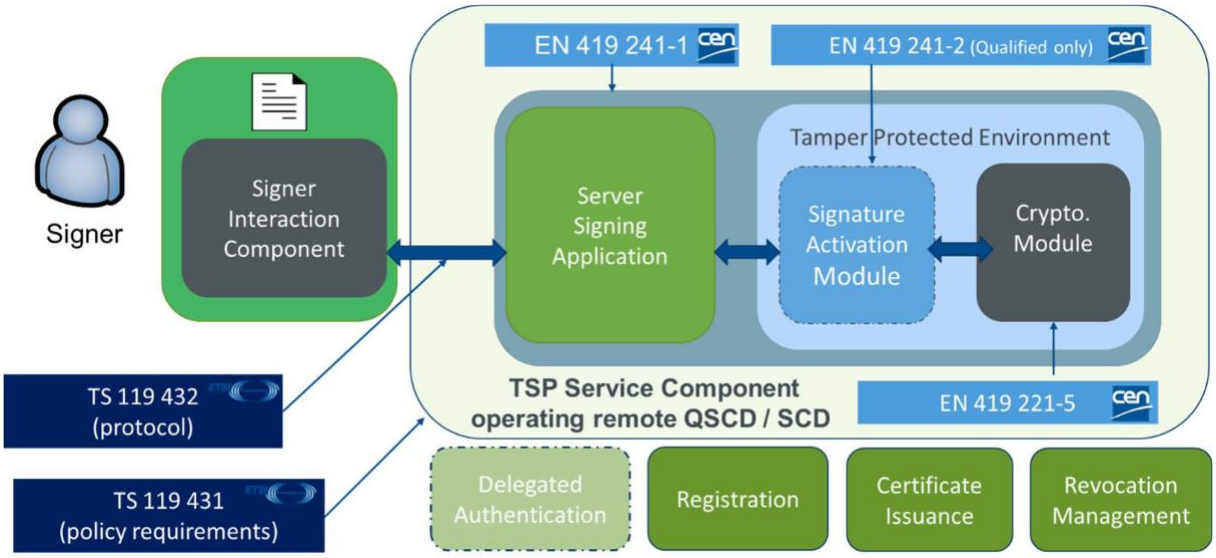


Figure 1: Scope of standards on the different remote signing components [29]

According to the ETSI TS 119 432 V1.2.1 (2020-10) [30], there are two models of SSASC activation.

With the SCAL1 model (Figure 2), 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.

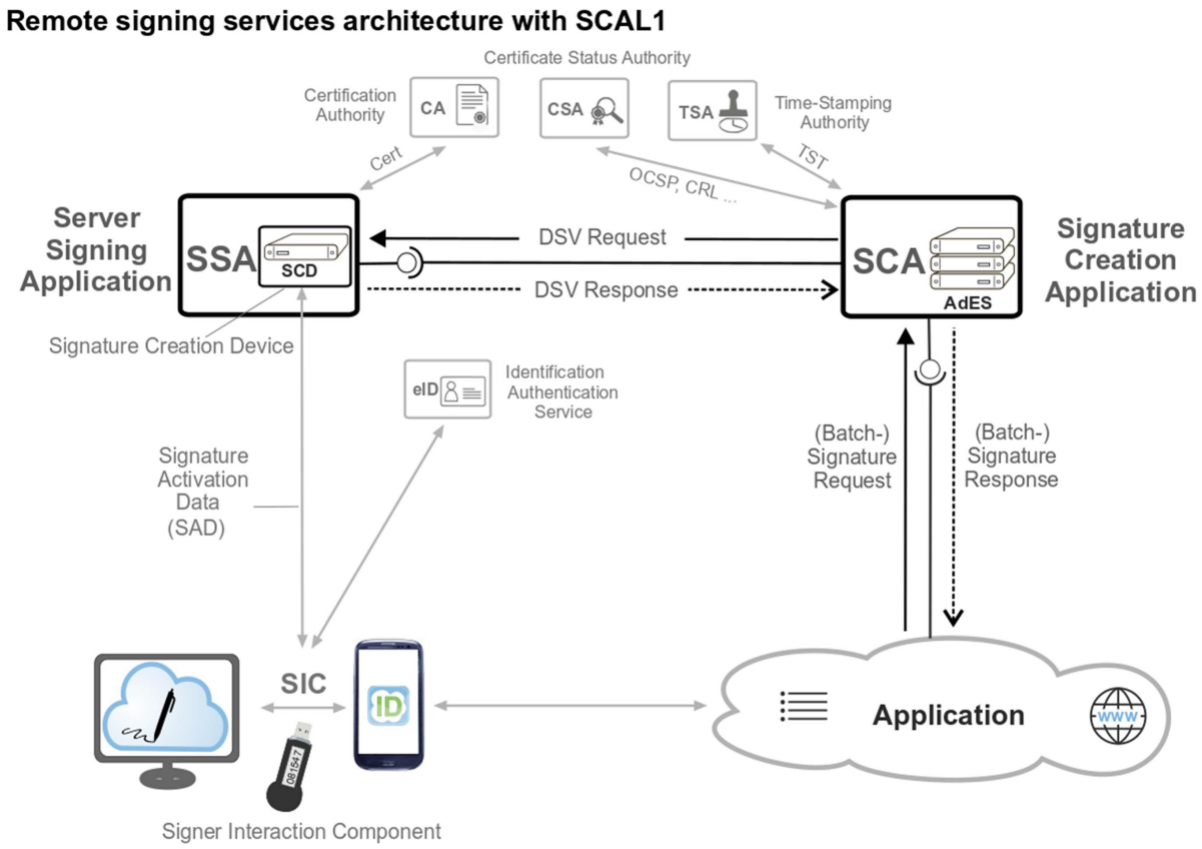


Figure 2: Remote signing services architecture with SCAL1 [30]

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 (Figure 3), the signing keys are used with a high level of confidence, under the sole control of the signer. 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.

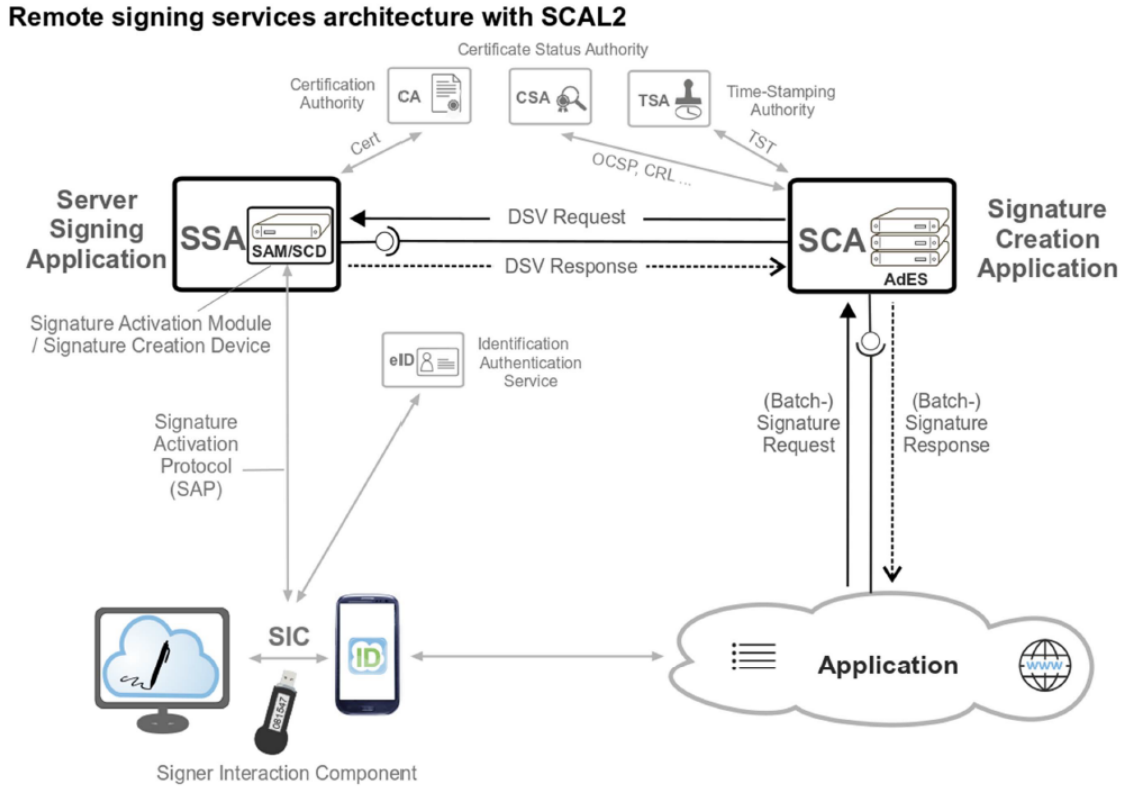


Figure 3: Remote signing services architecture with SCAL2 [30]

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

SCAL2 refers to a level of assurance "substantial" 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 signing in place of the person actually registered by the TSP having issued the certificate [22].

The downgrade of the level of assurance is the result of signing data with the qualified digital signature, even though assurance levels to use the service and assurance level provided by the service 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 separate authentication factors, such as 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 in possession of 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 level plus additional means to protect the electronic identification scheme against duplication and tampering. 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 PIN.

As ENISA already points out [22], the (Q)TSP issuing the certificate will issue a certificate with a high level of assurance to a certain 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, but EN 419 241-1 does not require the (Q)TSP to enrol 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 a user A. User A can impersonate user B to receive an authentication means from the TSP managing the key and by this way would be able to create 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 on the sole control of the signature creation data by the signatory or the control on 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. But this is not necessarily pro-actively verified 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 reliably protected 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; it rather affects the entity managing the device that may apply stricter policies when a QSCD is used for the creation of electronic signatures. In the end, the QSCD must ensure that the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use or misuse by a third party, independently of the service (creation of seals or creation of signature) available [22].

To understand how successful are regulations and related standards in providing authentication security to end-users, we performed a survey of selected services in the selected Member States in the sample.

3.8.1 Italy

In Italy, the on-boarding is harmonized between providers to such a level that the recognition methods (Figure 4) of the identity can be depicted for all available providers.

Recognition method

- in person
- via webcam
- audio-video by bank transfer
- CIE (Carta d'Identità Elettronica), CNS (Carta Nazionale dei Servizi) or digital signature

Figure 4: Recognition methods in Italy

After the registration, further authentication is left to the trusted service provider. In a publicly available identity provider registry,[20] there is a very descriptive table of OTP mechanisms used by the trusted service providers. According to the table in Figure 5, 8 of 9 trusted service providers are also offering SMS codes for OTP (One-Time Password).

[20] https://www.spid.gov.it/en/what-is-spid/how-to-choose-between-digital-identity-providers/

IDENTITY PROVIDER	SECURITY LEVELS	GEOGRAPHICAL AREA	RECOGNITION IN PERSON	REMOTE RECOGNITION	RECOGNITION CIE*, CNS	Sending the OTP code also via sms	RAO	
aruba.it ID	①②③	IT EU	✓		✓	No		Discover more
InfoCert ID	①②	IT EU	✓	via webcam	✓	YES paid service		Discover more
intesa ID	①②③	IT EU	✓	Via webcam (paid service)		YES Free service		Discover more
lepida	①②	IT EU	✓	Via webcam (paid service) Audio-video with bank transfer (payment to charity)	✓	YES Free service		Discover more
NamirialID	①②	IT EU	✓	Via webcam (paid service)	✓	YES Free service		Discover more
Poste ID nuovo spid	①②③	IT EU	✓	PosteID App with CIE and PIN (free of charge) PosteID App with electronic document without PIN or bank transfer (subject to charge)	✓	YES Free service	✓	Discover more
SIELTE id	①②③	IT EU	✓	Identifica App with CIE (free) or via Webcam (free)	✓	Yes Free service	✓	Discover more
SpidItalia REGISTER.IT	①②	IT EU	✓	Via webcam (paid service)	✓	YES Free service		Discover more
TIM id	①②	IT EU	✓	Via webcam (paid service)	✓	YES Free service		Discover more

Figure 5: Overview of Italian identity providers

3.8.2 Slovenia

For example, 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 the assurance level high and possibility to create qualified electronic signature in the cloud.

When accessing the service, the user enters a username (e-mail address) and password in the first step (Figure 6).

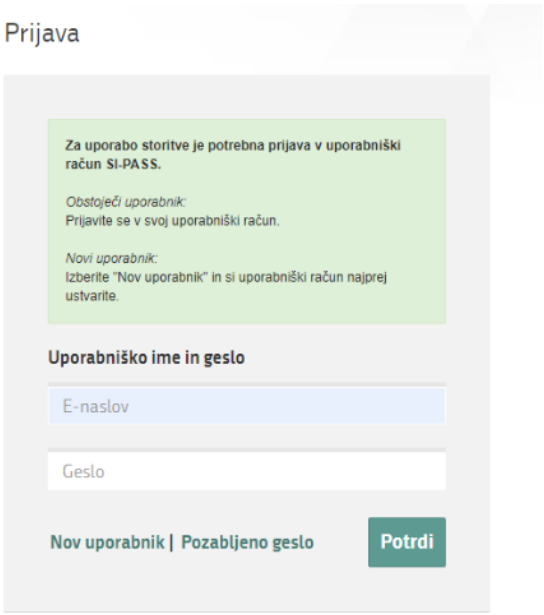


Figure 6: Authentication (password step) in Slovenian SI-PASS

In the second step, the user enters his mobile phone number (Figure 7).

Figure 7: Authentication (SMS step) in Slovenian SI-PASS

After receiving an SMS message, the user enters the one-time password from the SMS message into the web form (Figure 8).

Figure 8: Returning the OTP received by SMS in Slovenian SI-PASS

The second example is SI-TRUST user registration (the basis for SMS-PASS service). The user must enter the information, as seen in Figure 9. They include e-mail, 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 tax number is not a private number in many cases. For example, this information is automatically published for a natural person with VAT business registration.

Figure 9: Registration form in Slovenian SI-TRUST

If the user wants to register for a new identity, they 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 gets a new one-time password over snail-mail to his home address. After finishing the registration, the user gets a full identity with a high assurance level and access to the qualified certificate on a certified hardware device (QSCD) in the cloud.

3.8.3 Spain

According to the Law 6/2020 and the Order ETD/465/2021, of May 6, 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 for remote identification offered by private trust services in Spain, such as the Identity validation of an ID card:

1. Information regarding the document that needs to be validated is sent to the trust service.
2. The trust service sends a link to the person to attach or capture their documents.
3. Once the documentation is received, the trust service provider extracts the data and confirms its validity.
4. The trust service generates a certificate with all the data from the process and the results from validations, and if required, might maintain custody over the evidence.

The public sector uses the Cl@ve service.

Cl@ve is not a trust service, but a method for electronic identification and electronic signature based on electronic certificates custodied by the Public Administration. Therefore, it is provided by the Government to access public services. When registering in Cl@ve, the following options appear:

1. Register (Identification)

According to the screenshot (Figure 10), it is possible to register via physical visit at a Register Office or online:

a) Via electronic certificate or DNIe (therefore, using other electronic identification means)
b) Without any prior electronic identification means.

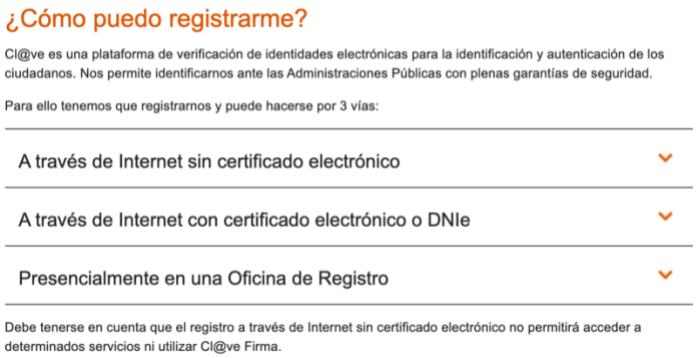


Figure 10: Registration in Spanish Cl@ve

However, while the two first options correspond to a high level of assurance, the online registration without using a prior electronic identification means will correspond to a "Basic" level of assurance. Therefore, it will not be possible to access certain services or use Cl@ve Firma (electronic signature).

a) **Register with a prior electronic identification means (electronic certificate or DNIe)**

1. Select the option "Register in Cl@ve with an electronic certificate or DNIe".
2. Introduce the DNI (National Identity Document) number and its expiration date (date of issuance in case of permanent validity). See Figure 11.

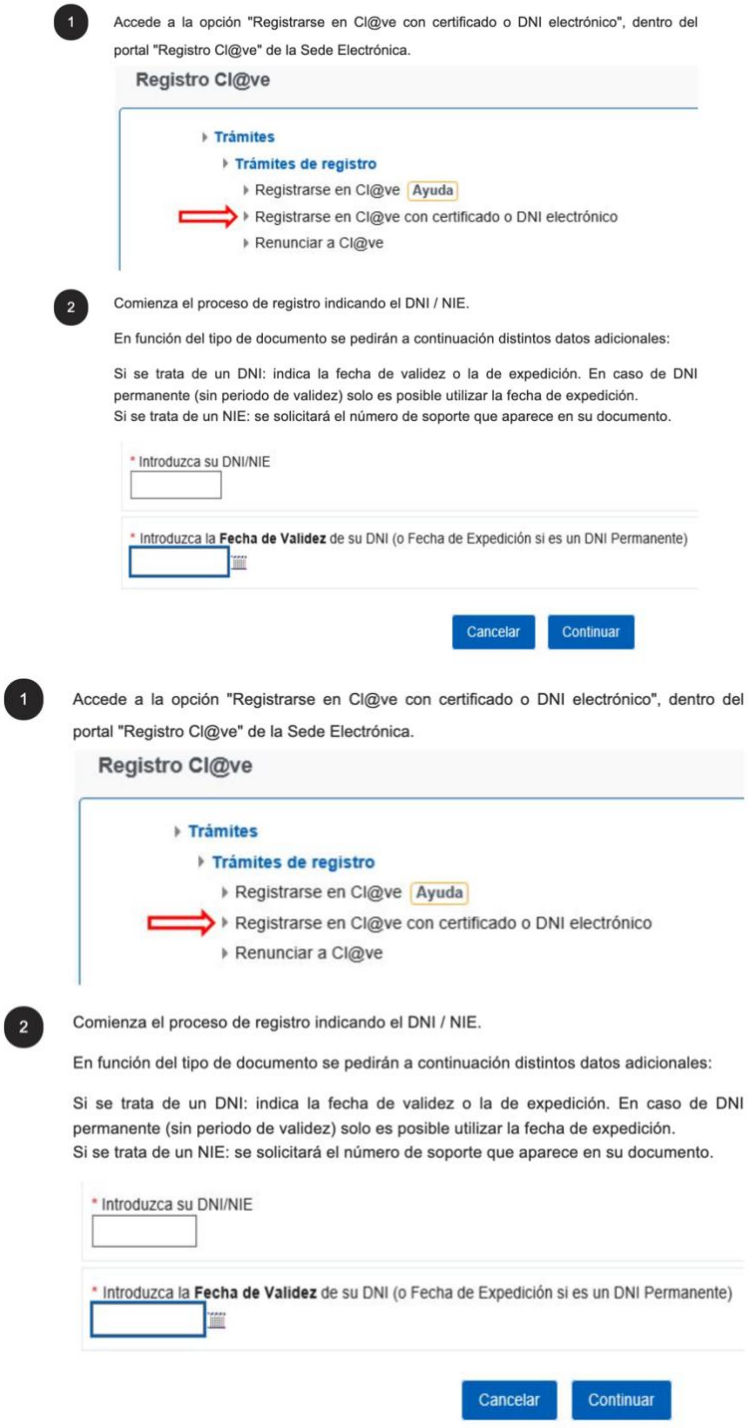


Figure 11: Register with a prior electronic identification means (part one) in Spanish Cl@ve

3. Identify with your electronic certificate or your DNIe. The data will be uploaded automatically, verify the information is correct and press “Send”.

4. Provide **your phone number to receive the PIN codes** for Cl@ve and an email address (Figure 12).

Figure 12: Register with a prior electronic identification means (part two) in Spanish Cl@ve

5. Registration is confirmed. Remember that the PIN codes are personal and non-transferable (Figure 13).

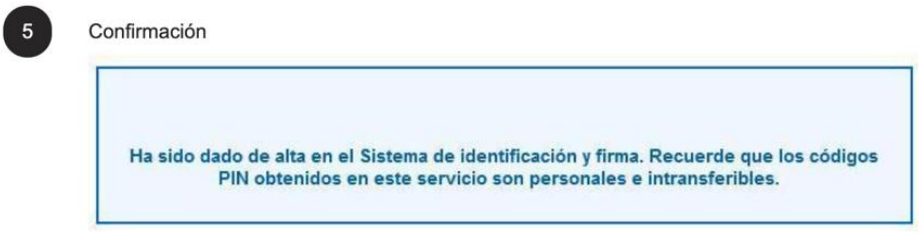


Figure 13: Register with a prior electronic identification means (finished) in Spanish Cl@ve

b) Register online without a prior electronic identification means:

1. The number of the DNI (National Identity Document) and its expiration date are required (date of issuance in case of permanent validity). See Figure 14.

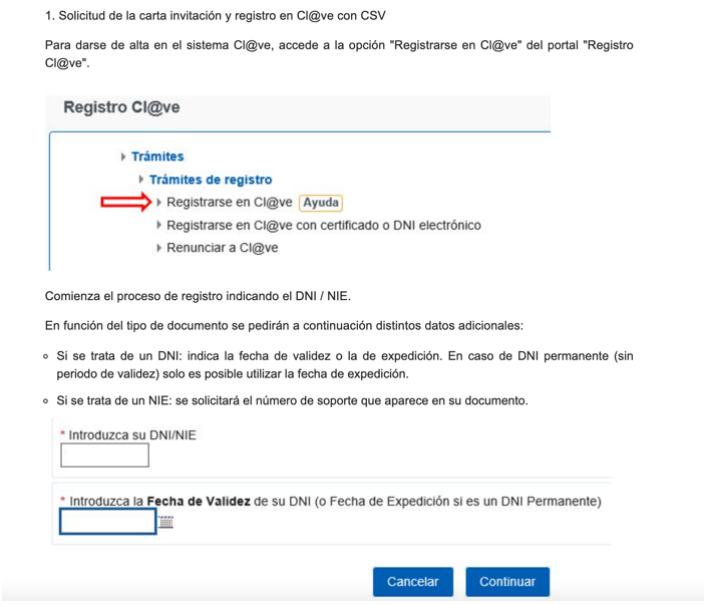


Figure 14: Register online without a prior electronic identification means (part one) in Spanish Cl@ve

2. Request a letter that will be sent to the user's tax domicile (Figure 15).

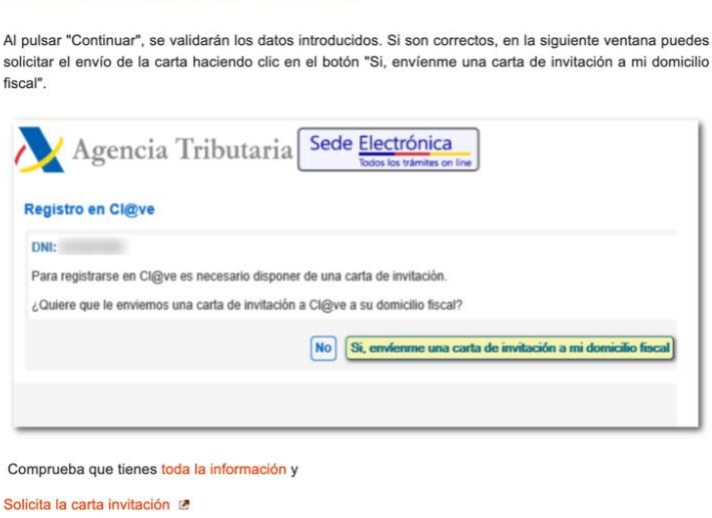


Figure 15: Register online without a prior electronic identification means (part two) in Spanish Cl@ve

3. The invitation letter will contain a Secure Verification Code.
4. Come back to "Register in Cl@ve", then select the option "I already have an invitation letter" (Figure 16).

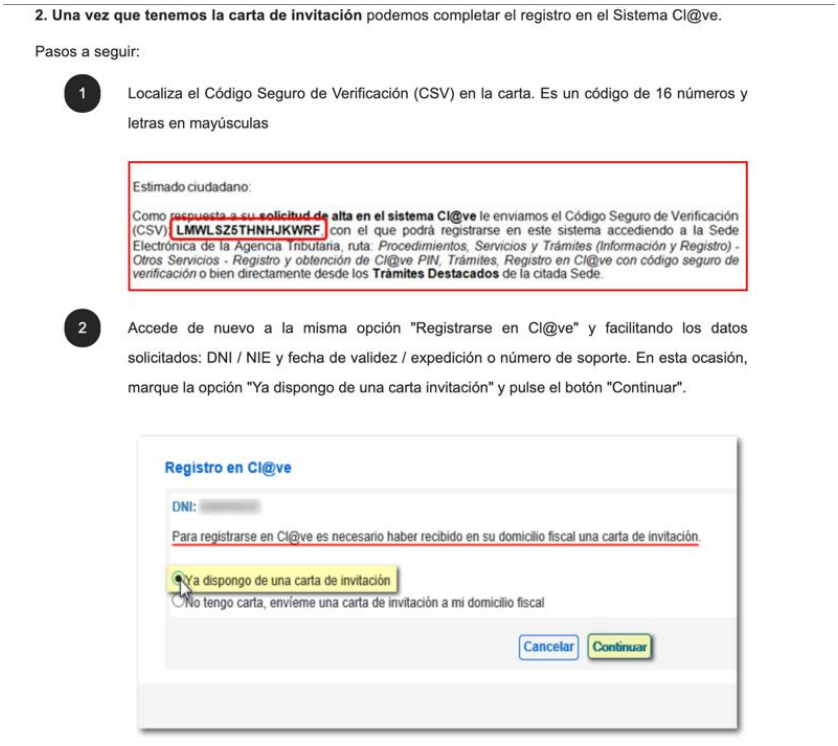


Figure 16: Register online without a prior electronic identification means (part three) in Spanish Cl@ve

5. Introduce the verification code (Figure 17).

Figure 17: Register online without a prior electronic identification means (part four) in Spanish Cl@ve

6. Provide your phone number and an email address (Figure 18).

Figure 18: Register online without a prior electronic identification means (part five) in Spanish Cl@ve

7. Registration is confirmed. Remember that the PIN codes are personal and non-transferable (Figure 19).

Figure 19: Register online without a prior electronic identification means (finished) in Spanish Cl@ve

2. Using Cl@ve (Authentication)

a) **Cl@ve PIN** (occasional use)

In the case of Cl@ve PIN, the user will be redirected to the following screen (Figure 20) where the DNI (National Identity Document) number, as well as **a PIN code that will be sent to the mobile number** previously introduced (or via de Cl@ve app), must be provided. This PIN code will just be valid for a limited period.

Figure 20: Authentication with a PIN in Spanish Cl@ve

b) Cl@ve Permanente (User and Password)

In the case of Cl@ve Permanente, the electronic identification means uses the DNI (National Identity Document) number and a password (Figure 21).

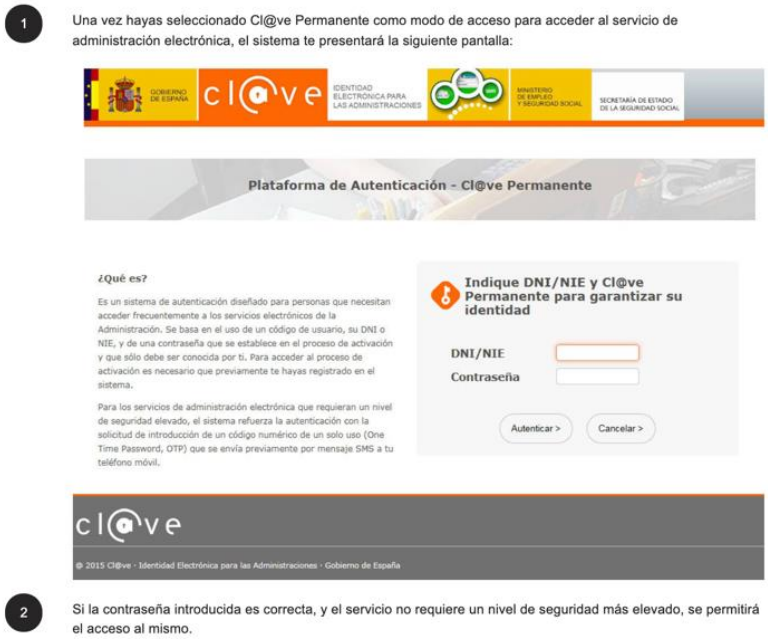


Figure 21: Authentication with username and password in Spanish Cl@ve

Nevertheless, **in the case the service to access requires a high level of security, the user will be sent an OTP to their mobile phone number** (Figure 22).

Figure 22: Additional authentication with OTP in Spanish Cl@ve

c) Cl@ve Firma (Electronic signature)

To use Cl@ve Fima (Electronic Signature), it is necessary to have registered with a high level of assurance ("Nivel Avanzado"), as well as to have activated Cl@ve Permanente. The electronic certificate for the signature will be generated automatically at the moment of the first signature or when desired by the user. These certificates are securely held by the DGT (General Directorate of Police).

The signature process will occur according to the highest level of security, therefore requiring the user and password of Cl@ve Permanente and **the OTP sent to the user's phone number**.

3.8.4 Switzerland

SwissID offers a remote registration only for certain acts. For the rest, in-person identification is mandatory. The figure below (Figure 23) gives an overview of when remote registration is sufficient and when verification in person is required.

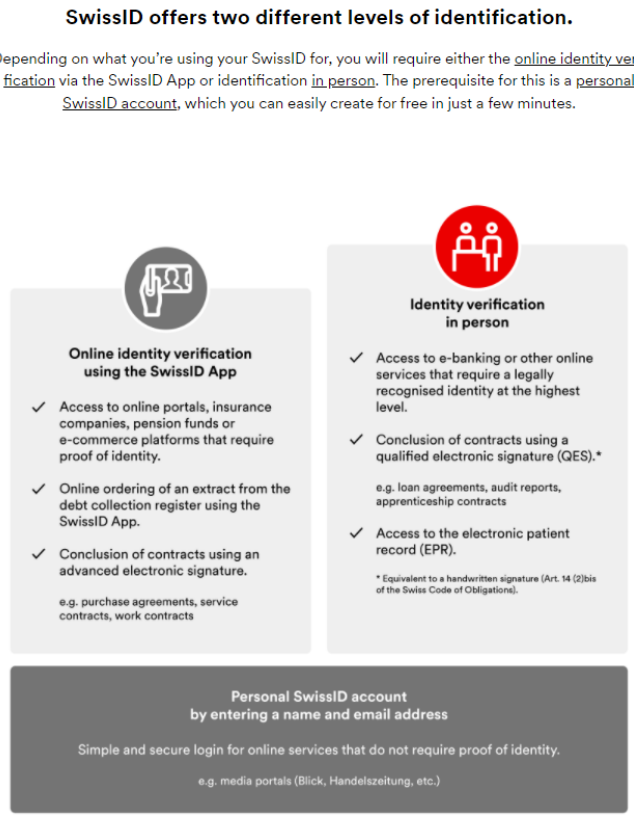


Figure 23: Usability of Online and in-person registration methods in Swiss SwissID.

First, the user needs to download the free app (Figure 24).

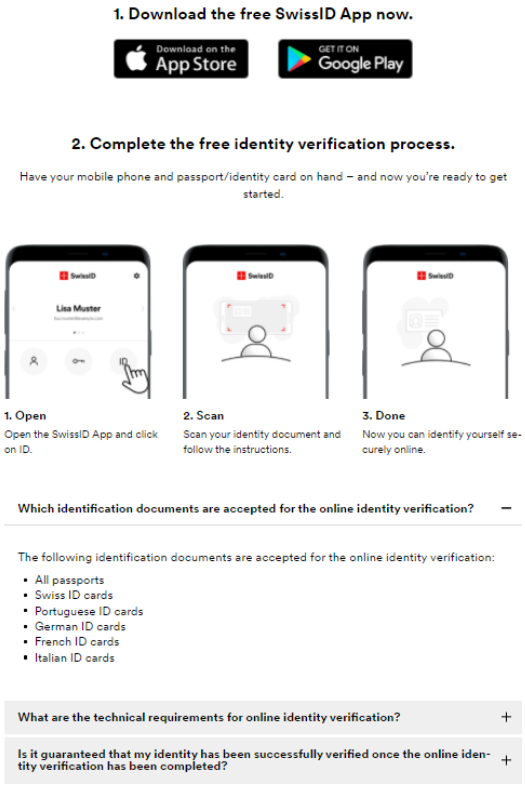


Figure 24: Download instructions for the Swiss SwissID app

Then the user creates an account by filling out a form, as shown below (Figure 25).

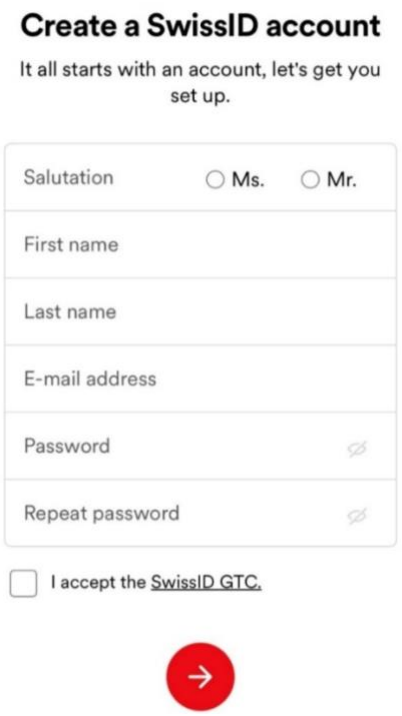


Figure 25: Registration in the Swiss SwissID.

There are specific requirements for the password, as shown below (Figure 26).

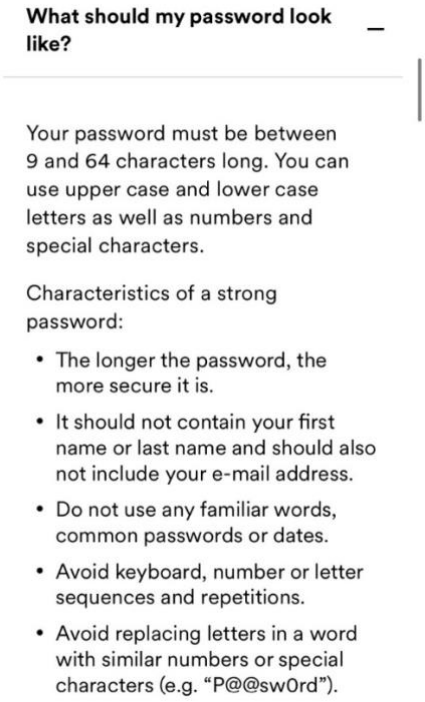


Figure 26: Password requirements in the Swiss SwissID.

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 (Figure 27).

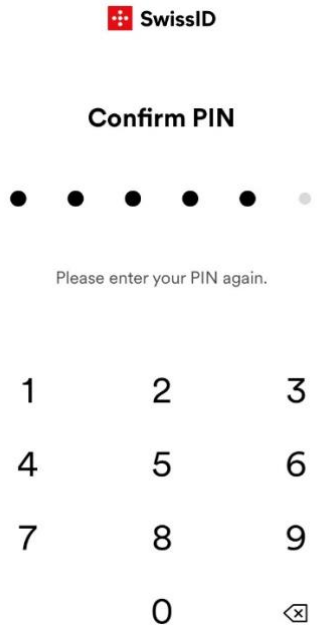


Figure 27: PIN confirmation in the Swiss SwissID.

The user can then activate the two-factor authentication (Figure 28). **This is not mandatory**.

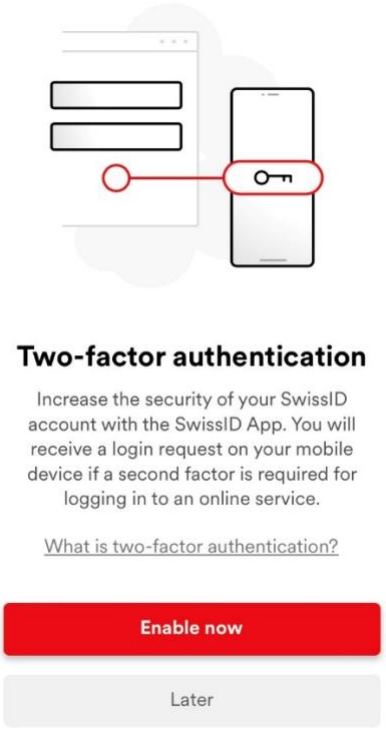


Figure 28: Two-factor authentication in the Swiss SwissID.

If a touch ID is available on the user's smartphone, **there is also the option to use Touch ID** instead of PIN (Figure 29).

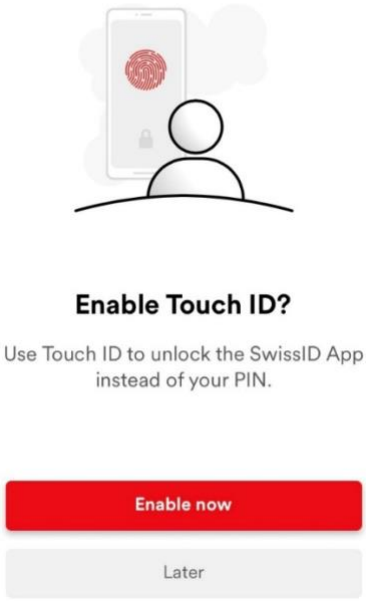


Figure 29: Option to use Touch ID instead of a PIN in the Swiss SwissID.

The user must then verify their identity by scanning an identity document and recording his face on a video (Figure 30).

Figure 30: Identity verification in the Swiss SwissID.

If the user forgets their email or password, specific procedures are in place, as shown in the screenshots (Figure 31). After 5 wrong inputs, the account is blocked.

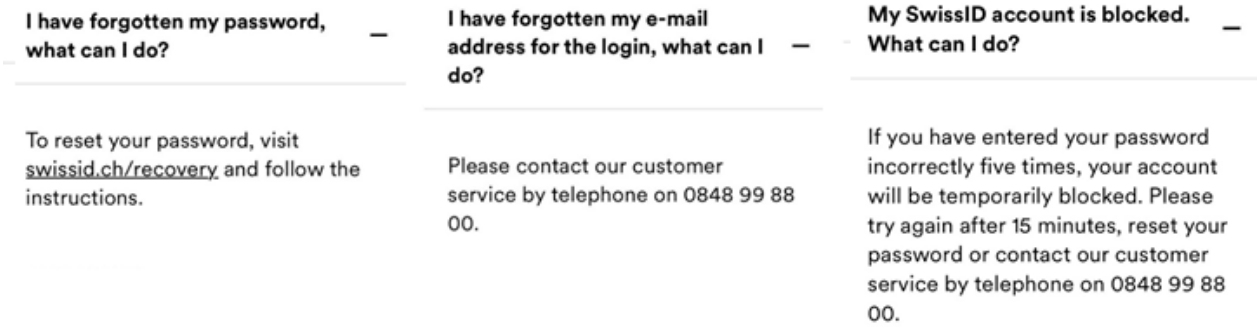


Figure 31: Credentials recovery in the Swiss SwissID.

3.8.5 SMS as the second factor in multi-factor authentication

Since all Member States use SMS as a second factor in multi-factor authentication, we summarize the state-of-the-art findings in the use of SMS as an authentication factor.

In 2016 NIST (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. 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 the purpose of authentication (essentially, a method for delivering a one-time use code for multi-factor authentication). This proposed recommendation has caused a big stir in the media, and they posted a blog post [31] documenting their reasons for the decision. They noted that SMS communication is not all mobile phone-based anymore, and a message can easily change between SMS, MMS, or data message to some other internet service (e.g. WhatsApp message). For this reason, they recommended verifying that the phone number is attached to a mobile phone before, allowing SMS as an out-of-band second authentication factor. Secondly, NIST expressed their scepticism of using SMS as a secure channel because attacks against it that could be performed on a large scale were becoming more successful and efficient.

These reasons and the fact that, considering how old this technology already is, 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 is still completely acceptable to use SMS as a second factor, its usefulness is decreasing and using it will very likely not satisfy the security standards and requirements of the future. They suggested developers in the future consider using other methods before choosing SMS as the second factor, which is, for some, almost like the default choice. Deprecating out-of-bound authentication with SMS does not mean that multi-factor authentication is any less valid and in fact, NIST have themselves emphasised that using SMS messages is still much more secure than only using a single factor for authentication. The difference between multi-factor authentication (MFA) and two-factor authentication (2FA) is that MFA requires at least two factors to be used, while 2FA requires exactly two factors. As such, two-factor authentication is multi-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 [32], published in 2017. However, the recommendations maintain that the possession of a mobile device should be authenticated by a SIM card and methods that do not prove possession of a specific device (e.g. voice-over-IP (VOIP)) should not be used. The largest reason for the recommendation's removal probably stands with the media outcry at the recommendation and lobbying by interested organisations [33].

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 [34] describing such an attack, and among other potential ways to exploit it, they mention the possibility to use it to bypass 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 the location of your phone. One attack that showed such vulnerabilities was the SS7 attack (SS7 stands for Signalling System No.7 protocol) [35]. The attack allows access to the 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 [36] and [37].

As a result of such attacks and vulnerabilities, the calls to stop using SMS-enabled two-factor authentication have become louder. Authentication services like the SI-PASS (and others, as discussed in previous sections) 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 do exist and steering away from using SMS-based two-factor authentication would also improve the trust users have in the system.

Given all the shortcomings of using SMS as the second factor, there are good reasons why it is hard to replace. They primarily revolve around its simplicity to use and deploy, but there is also the fact that users have grown familiar with it because it is one of the oldest second factors deployed on mass. 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 serious 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 basically just as user friendly as the use of SMS, and it can be even quicker to use because there is no need to wait to receive a text message (the user can directly use the code from an app).

3.8.6 Security questions as a form of authentication

Through our analysis in 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 get asked when setting up an account with a service. The purpose of these questions is to periodically confirm the user's identity (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. Common examples are the mother's maiden name or first telephone number.

In 2015 researchers from Google and Stanford [38] have analysed Google's security questions data set. This and a preceding experimental study performed by researchers at Microsoft [39] in 2009 have both shown that the biggest 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 and up to 60% failure to remember their answers to the security questions, respectively. Some other main take-aways were [38]:

- Secret questions have poor security and memorability.
- Statistical attacks and answer distribution prediction are a real threat.
- 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. are less memorable) than less secure counterparts.
- Memorability significantly decreases over time (which is a problem because if security questions are used for the purpose of resetting a password, 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.

The two studies [38], [39] 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 therefore be easily brute-forced/guessed.
- 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 inadvertently revealed by the users to social engineering methods (e.g. phishing).
- Social guessing attack: some of the answers might be easily guessable to people who know the account owner.

The conclusions of the studies were that security questions can be used to help authenticate users, but 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 lie 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 in the same way as passwords [40], [41]. 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, in case they are stolen, they could be used to gain access to other services. Like 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 [42], and consequently, the same applies 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. It can also be used to generate the random values that can be used as the answers.

Ultimately, good security questions should be treated in 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 a sole method for either user authentication or password recovery. NIST also no longer recognises security questions (they refer to them as pre-registered knowledge tokens) as an acceptable authenticator in their latest Special Publication 800-63-3 [43], [44]. 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 [43]).

Slovenian SI-PASS allows users to write their own security question, 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, favourite colour), this is not a piece of information known exclusively to the user. In Slovenia, an individual's tax number is known at least 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 in the latter.

3.8.7 Notability of changes in digital signatures

While analysing the authentication security, we came across the eIDAS requirement that does not directly relate to authentication. Because of its importance for the understanding and recognition of qualified electronic signatures, we have decided to include the finding in this report.

Article 26 of eIDAS sets the requirements for advanced electronic signature. Under (d), it states an advanced electronic signature must be linked to the data signed therewith in such a way 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 is, for multiple reasons, firstly 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 has not been changed or rather that any change to it is detected (which is exactly 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). Considering a hash function gets as an input a message of any length but outputs a value of fixed length, it is obvious that multiple messages will produce the same hash value (there is no going around this problem). The probability of two different messages producing 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 is dependent on the size of its output, where the upper bound is limited by the principle of the so-called birthday problem. The number of tries (e.g. how many messages we would need to hash and compare) is estimated with the $\sqrt{2^{n+1} * (-\ln(1-p))}$ formula, where n is the output size of the hash function and p is the probability we would want to achieve [45]. For example, the SHA-256, which is a commonly used hashing algorithm in digital signatures, would have a n of 256. To have a 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 $1{,}36 \times 10^{77}$ tries. For comparison, the probability of winning a lottery is one in $1{,}4 \times 10^{7}$. 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 the reason previously popular hash functions (e.g. MD5 and SHA-1) are no longer recommended for use. They fell out of favour immediately after an example of a collision was demonstrated (i.e. it became feasible to actually generate messages with the same hash value [46]). 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 completely guarantee 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 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 currently stands, digital signatures arguably do not meet them.

3.9 Findings and Discussion

The European Commission is already accepting the fact that remote electronic signature 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 overall regulatory and supervisory framework for trust service providers [4].

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

First, issues with the heterogeneous requirements comparing different supervisory authorities lead to material differences as already established in the working documents. We concluded that this might also be the result of organizational independence. According to our sample, we identified the pattern where supervisory authorities are providing trust services at the same time. This is contrary to other supervision and certification schemes, e.g. the organizational independence of auditors according to the International standard of Auditing 200 and ISO 19011. Segregation of duties has been historically introduced for a good reason. In practice, segregation of levels of defence, for example, is in widespread use. Similarly, the increasing number of information systems and best practices suggest organizational separation of the chief information officer and chief information security officer. The main advantage is avoiding professional bias when weighing security costs and the impact on available resources versus security improvements. We introduce budget bias into the equation by allowing organizational dependence of the supervisory body and trusted service provider. Further, such an arrangement may introduce unfair competition on the market as the government is both a supervisory authority and service provider. Consequently, we suggest that eIDAS 2 follows the best practices of other certification and supervisory schemes regarding the organizational independence of the supervisory body.

Second, looking at the banking example proposed in eIDAS 2 presentations, we identified additional obstacles to cross-border on-boarding 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. We concluded that eIDAS 2 could not solve cross-border banking on-boarding by itself if it does not impose requirements that some services (e.g. onboarding in banking) have to be explicitly allowed in all Member States under the provisions in eIDAS 2.

Third, we found additional shortcomings of regulation regarding video identification. The limitations are not only bound to the fact whether some Member State does or does not allow remote video identification. Looking from a broader perspective eIDAS network should be equally recognized 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. Accordingly, we should look at the market as an open, competitive single market, even though it is a market between the governments.

Member States with lower security standards may become more attractive for the businesses that can open their offices in other Member State just to acquire remote video identification services according to the criteria in that Member State as not all Member States are closing in in the sense that remote video identification would not be allowed for the citizens of other Member States. Businesses adapt and will search for the cheapest services. The governments will have to understand that they are competing in the market. This is another strong argument favouring the further regulation of security standards, not only for remote video identification but also for other foreseen services, e.g. authentication. Not everything has to be included in the eIDAS regulation itself. Some parts of technical requirements should stay in the technical standards, but these should increase their update iteration of adapting to new market and technology trends.

Fourth, there is little convergence in understanding what levels of assurance should be used in specific use-cases. This opens many questions for the 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. Because there was no incentive from the government to promote and use services requiring higher assurance levels, the methods, technology, and electronic IDs are not available to the citizens when conducting business on the market. This leads to companies promoting eIDAS and questioning whether this is a business opportunity at all.

Fifth, there are very different practices of allowing commercial access to the eIDAS network between 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. That 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 start to build. We emphasize again that without the detailed regulation of minimum security standards, this may lead to the deterioration of cybersecurity requirements.

Sixth, even though we haven't found an example of biometrics being used in the EU Member States, we found that 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. Since providers don't have contracts with the providers of such devices and there is no certification scheme, this area needs further research. We are proposing the term "Bring Your Own Authentication Device – BYOAD" for such scenarios. All eIDAS, banking and other sectors could benefit from a clear understanding of whether such use of biometrics is allowed (currently, this could be a grey area according to the GDPR, as data controllers are not in essence processing biometrics data, but it is used in the use-case). 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.

Seventh, the authentication mechanisms in the eIDAS network across the Member States are using technical solutions with questionable security attributes, like 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 they also have further reached (e.g. banking). Considering the stakes at play, it is better not to trade ease of use for actual security. This is especially true because alternatives do exist and steering away from using SMS-based two-factor authentication would also improve the trust users have in the system. Therefore, current standards may not be detailed or current enough to support the latest findings in cybersecurity. This finding is another indication that a call to increase the speed of security standards development is justified.

Finally, when analysing security requirements of electronic signatures, it became evident that eIDAS uses very strict wording regarding capabilities of the qualified electronic signature, that "any subsequent change in the data is detectable". According to current state-of-the-art technologies used to create electronic signatures, this is not entirely true. To avoid any differences in how courts in different Member States may explain and understand this term, we suggest that it be amended in a way that will refer to how existing technology works.

4 GDPR Heterogeneity in the EU

The interoperability and cross-border compliance deliverable addresses issues related to eIDAS implementation and legislation differences in EU member states, ultimately hampering the idea of a Single European Market. To a lesser degree, this is also true for the differences between Member states from the General Data Protection Regulation (GDPR [47]) perspective. Therefore, precise knowledge of the regulations applicable in a given case is becoming increasingly important.

This section is on the topic of GDPR differences between the Member States. GDPR allows for the Member States to define or change some parts of the regulation in the way they wish. The prime example of this is the consent age[21] set at 16 (persons aged 16 years and older do not require parental consent) in the GDPR. However, the regulation allows individual countries to change this and go as low as 13 years old. Member States can also have additional legislation that builds on top of the GDPR.

To get a better picture of the current situation in the EU, we will gather information from Supervisory Authorities (SA; a.k.a. Data Protection Authority - DPA). Each Member State's own SA should be the best equipped to give information on their national legislation and policies on data protection. The results of this work will provide users with an easy tool to compare the rules on some data protection topics in an individual Member States. This research has already been published in a peer-reviewed journal [3].

4.1 Related Work

Cataloguing and/or comparing legislation between countries can be very difficult, especially when done on any larger scale. The subject itself is very complex and, at times, convoluted. When this is done internationally, the complexity of local languages (often national legislations are not translated or easily accessible) makes it almost impossible for a small group to achieve. Therefore, these types of research are often done by large organisations that either have contacts in many countries or are reputable enough to get help in any country they need. The alternative approach we used is to survey people for each of the required locations to get them to give you the wanted information, which is not difficult to obtain for them. This section presents the state-of-the-art in the available sources for GDPR related comparison between EU Member States.

For the specific field of data protection, there has not been much study of relevant legislation on a large scale (i.e. including a large number of countries) or comparison between them. However, we have found three [48]–[50] such collections that include many countries. Two of the three collections title themselves worldwide, while the third contains information on thirty countries (the first two contain many more) worldwide. These are very general in their information and more or less just point or name the main legislation that covers data privacy. As such, while GDPR is mentioned in the EU Member States, it is not

[21] GDPR, Article 8, paragraph 1.

the focus of the studies. These, therefore, only contain a list of relevant legislation and not much information on what the legislation itself dictates, they are not targeting GDPR issues (and by extent, are not centred on the EU), and do not give the users much in the way of comparing policies across multiple countries.

S. Park et al. [51] surveys the state of data protection legislation in the selected countries in relation to the implementation of Digital Forensic Readiness. The authors looked at, among others, the EU as a unit and at Germany as a specific representative. For the EU, the focus was GDPR with additional legislation present in Germany and its effects. The French Supervisory Authority CNIL has prepared a solution for a very specific condition set by the GDPR (Article 45), under which the transfer of personal data to third countries is allowed if the European Commission has confirmed a suitable level of data protection provided by the receiving country's national laws. The CNIL's map [52] on data protection around the world illustrates which countries have adequate data protection laws and for which other means of sufficiently protecting the data must be guaranteed before transferring the data.

The possibility of adapting and modifying the GDPR by each of the Member States with national law derogations was purposefully a part of the GDPR to allow for greater flexibility. The most probable areas for derogations were discussed by W. Long and F. Blythe in [53], A. Clearwater and B. Philbrook in [54], and J. Vangadesan and N. Pook in [55]. A comparison of privacy and data protection legislation and policies in the EU (looking at eight Member States at the time) was also performed by B. Custers et al. [56]. The study also considered the importance/situation of data protection in a country by looking at the general public's awareness, media coverage, its importance in political debates etc. However, the research was done shortly before the GDPR came into force. While the study did consider the upcoming regulation, it could not predict the changes in national legislation.

Finally, there are three studies that are the closest to the work of this paper. All three are centred on identifying derogations from the GDPR and how it is supplemented in the EU. The first [57] covers 16 current Member States. The second study [58] included 13 Member States, while the third survey [59] collected information for 21 Member States. All three were made before the UK's exit from the EU. As a result, all three also include the data for the UK. All three collections provide relevant information from national legislations and policies for a variety of topics. There are only two general topics that are present in all three and are also included in our study. They are processing sensitive data and the designation of a data protection officer. Other topics that have some overlap with our study include information on SAs, data protection for employees, consent for children, and processing of deceased's data. All three studies present the results in a textual form. While this allows for more information, it is less than ideal for comparison (there is still a lot of work on the user to extract the necessary information and compare), especially as the level of detail is often different between countries. Our study, presented in this deliverable, collected more targeted information. This, together with the presentation method we have used (a dynamic map), allows for easier comparison between the Member States.

4.2 Survey Outline

In the previous section on related work, we have mentioned some studies that have collected derogations permitted by the GDPR in the EU Member States. When designing our own aspects to compare in the EU, we have decided to go a different route and focus on topics that could potentially also affect how data protection is implemented differently between the Member States regardless of GDPR. One such example is the collection of biometric data on electronic signatures. Firstly, let us distinguish electronic signatures, which are typically obtained by signing your name on a type of touchscreen, from digital signatures, which are a cryptographic authentication mechanism [60]. When signing your name on an electronic device,

sensors can measure the pressure of the pen, the speed, the tilt, etc., of the signing process. All these data are considered biometric data because it is produced from the technical processing of a natural person's physical, physiological, or behavioural characteristics. Similar characteristics of signatures can be obtained from close examination of actual physical signatures, which is why just mimicking the look of a signature does not make a convincing forgery (at least to an expert). This is the same reason all the biometric data is collected during an electronic signature. However, some countries do not allow the processing of biometric data for this purpose. Meaning electronic signatures are nothing more than images of signatures. Such differences between the Member States have the potential to cause problems related to the legitimacy of signatures, where a signature could be valid in one country but invalid in another (either because it does not contain biometric data, or because it does and is consequently a case of illegal processing of biometric data).

Some of the important aspects of data protection that often involve personal information are not discussed much in the GDPR and could become troublesome to implement under its requirements. Here we are primarily thinking of the processing of personal data in audit trails and the problems surrounding the processing of personal data in backups. Therefore, we were interested if individual Member States have made legislations to more clearly define the requirements and how they can be achieved. Note that the results are only limited to legislation and do not include any guidelines or rulings that Supervisory Authorities might have made on how personal data should be handled in audit trails and backups.

The inclusion of anonymisation as a form of avoiding having to comply with the GDPR and pseudonymisation as a method of complying with the GDPR is very interesting, especially with the open questions of when does personal data become truly anonymous and how can we tell it is. Therefore, we were interested in whether any of the Member States have any additional legislation on the two topics where they might explain the requirements in more detail. Finally, as already discussed in the related literature, we have also included some of the topics that were also included in the previous studies.

Collecting the data for the Member States on our own was not an option, as sourcing the information from foreign legislation and policies would be far too time-consuming if at all possible because they might not have an English translation. That is why we chose to use a survey. The first time, we have distributed the survey among CyberSec4Europe project partners (this work was made as part of the project) [61]. With more than 40 partners, the project covers the majority of the Member States. The survey was given to Data Protection Officers (DPO). By collecting multiple responses for the same country, we were able to check for the consistency of the replies. Unfortunately, the results were very inconsistent, and we received varied feedback for the same Member State. This was an obvious problem and an indication that even asking DPOs, who should know national data protection laws and policies fairly well, provides inaccurate data. With an understanding that the survey contained some very specific questions that the DPOs would not need to know the answer to from their day-to-day work, we decided to scrap the collected data and made a more ambitious plan to contact all the Supervisory Authorities and collect the data from them.

4.3 Collected Data

To collect the best possible quality of data, we chose to collect the data directly from national Supervisory Authorities. A SA is an independent public authority that supervises the application of European data protection law, including GDPR. Each EU Member State must have a SA, which has investigative and corrective powers, provides expert advice on data protection issues, and handles any raised complaints. However, collecting responses from SAs is more difficult because there is only one per Member State, and they might not be inclined to participate in unsolicited research. Even though they are the best entity to answer the prepared data protection questions, we expected to not get a response from every SA. To have the best possible feedback, we have repeatedly asked for their participation and have collected the data between April 2020 and June 2021.

The information-gathering was centred around processing different forms of (special) data (e.g. biometrics) and any additional legislation or policies upgrading the GDPR requirements. The full questionnaire is attached as Annex B: GDPR Questionnaire. The survey collected data for the following topics:

1. Any other legislation on the use of biometry (other than the GDPR).
2. Any other specific legislation on privacy, specifically with relation to
    a. Video surveillance,
    b. Photography,
    c. Anonymisation,
    d. Pseudonymization, and/or
    e. Audit trails.
3. Any additional legislation that extends specific sections of the GDPR, specifically with relation to
    a. Verification of parental consent,
    b. Processing data of the deceased,
    c. Processing of genetic data,
    d. Use of biometric data for the purpose of identification,
    e. Processing of health data,
    f. Processing of data on the sex life of individuals,
    g. Processing of data on sexual orientation,
    h. Erasure of personal data,
    i. Data Protection Officer designation/appointment, and/or
    j. Supervisory Authority consultations.
4. Any additional legislation on backing up of data.
5. Whether or not the use of biometrics is allowed for the electronic acquisition of handwritten signatures.
6. Whether or not the use of biometrics is allowed in a work environment (e.g. opening of server rooms with a fingerprint).
7. Minimum age of persons that do not require consent from a holder of parental responsibility.

4.4 Result Analysis and Discussion

In the survey, we have managed to receive feedback from 19 (Austria, Belgium, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, Greece, Germany, Hungary, Latvia, Luxembourg, Malta, Poland, Romania, Slovakia, Slovenia, and Spain) out of the 27 Member States. The responses were collected between April 2020 and June 2021 in many repeated solicitations of Supervisory Authorities to participate in the survey.

We compared the collected data with the complementary data from [58] and [59] previously mentioned in the related work section. The most similar data collected and, therefore, the most appropriate for comparison were the data regarding the age of consent for children and the additional regulations surrounding the data of the deceased. The consent age, which we could compare with both other studies, was identical in all three studies except for the information on the Czech Republic. The result from [59] indicates the consent age is 13, while our inquiry and that of the [58] received information that it is 15. We were able to confirm from a separate source that the consent age in the Czech Republic is, in fact, 15 years of age. The information on the additional legislation surrounding the processing of deceased person data was only collected in [58], and we could therefore only compare our results to theirs. The cross-section of the collected results in the two studies did not show any mismatch. The two points of comparison give us high confidence in the trustworthiness of the data collected in our study.

Following is a table (Table 8) that represents the collected data from the Supervisory Authorities. In the table columns are the 19 Member States that we have collected the data for. Rows represent the topics (i.e. questions in the survey) we have collected data for. Rows or rather topics are marked with the same numbers and letters as previously listed in the survey outline section. For example, any specific legislation on video surveillance is marked with *2a* because in the previous section, "Any other specific legislation on privacy, specifically with relation to" is numbered with a *2* and "Video surveillance" is under point *a*.

The answers "yes" (the Member State has additional or more specific legislation on the topic) and "no" (the Member State does not have additional or more specific legislation and the original GDPR applies) that are represented by the cross-section between the Member States and topics in Table 8, are colour coded green and red, respectively.

Topics marked from 1 to 4 contain the information on whether a Member State has additional/specific legislation on that topic. How many of the topics are covered with other or additional legislation (number of green squares for each of the Member States) is summed in a row marked as "SUM". Topics marked with numbers 5 and 6 are specific questions regarding the use of biometrics, and we do not include them in the analysis of specific or additional legislation in the Member States. They are also different because the green colour of a cell in these two rows means that a Member State allows the use of (not that it has additional legislation on like in previous rows) biometrics for the electronic acquisition of handwritten signatures (row marked with No. 6) or biometrics in a work environment (row marked with No. 7). The very last parameter (row marked with No. 7) is the consent age - the age after which individuals no longer need parental consent. We also produce the total number of green cells across all Member States included in the survey for each topic. This information is in the far most right column (marked "SUM"). It gives information on how commonly a certain topic is covered in additional legislation (topics marked 1-4) or how frequently the use of biometrics is allowed for collecting signatures or in a work environment (topics marked with No. 5 and 6) across the Member States.

	Austria	Belgium	Croatia	Cyprus	Czechia	Denmark	Estonia	Finland	Germany	Greece	Hungary	Latvia	Luxembourg	Malta	Poland	Romania	Slovakia	Slovenia	Spain	SUM
1																				11 (58%)
2a																				15 (79%)
2b																				1 (5%)
2c																				2 (11%)
2d																				3 (16%)
2e																				4 (21%)
3a																				4 (21%)
3b																				4 (21%)
3c																				12 (63%)
3d																				9 (47%)
3e																				11 (58%)
3f																				2 (11%)
3g																				2 (11%)
3h																				5 (26%)
3i																				4 (21%)
3j																				5 (26%)
4																				1 (5%)
SUM	3	5	6	4	1	4	3	13	8	2	10	8	0	0	1	6	6	3	12	

5																			10 (53%)
6																			15 (79%)
7	14	13	16	14	15	13	13	13	16	15	16	13	16	13	16	16	16	16	14	

Table 8: GDPR heterogeneity in the EU.

The results show that in the majority of the cases, Member States do not have many additional/specific legislations. We have found that only 95 cases have additional/specific legislation (topics marked from 1 to 4) of the maximum possible of 323 – which is 29,4%. This can be seen from the predominately red colour of Table 8.

The topics most often additionally covered with legislation other than the GDPR are in the area of biometry use (row marked with No. 1; in 11 of the 19 countries), video surveillance (2a; 15) processing genetic data (3c; 12), using the biometric data for the purpose of identification (3d; 9), and processing of health data (3e; 11). On the other end of the spectrum is the legislation on photography (2b) and data backups (4) which have further legislation only in one Member State each. They are closely followed by additional legislation on anonymisation (2c) and extensions on GDPR rules regarding the processing of data on the sex life (3f) and sexual orientation (3g), each with legislation in only two countries.

Luxemburg and Malta are the only countries that do not have any additional legislation on the topics covered in our survey; all other included Member States have at least one topic where they have other/additional legislation to the GDPR. Other countries with little additional legislation on the topics covered in this survey (topics marked from 1 to 4 in Table 8, up to a maximum of 17) include Czechia (1), Poland (1), and Greece (2).

Based on the feedback from the SAs, the most additional legislation relevant to the discussed topics are in Finland (13 green fields in topics from 1 to 4, from possible 17), Spain (12), Hungary (10), Germany (8), and Latvia (8). The use of biometrics for the electronic acquisition of handwritten signatures (row marked with No. 5) is allowed in 10 of the 19 surveyed countries – so a very even split. In contrast, only four Member States do not allow biometrics in a work environment (row marked with No. 5; Greece, Malta, Slovakia, and Slovenia). This could indicate that the Member States are interested in limiting the use of biometric data but do not wish to limit businesses.

The results of the survey have also been integrated into a dynamic map, enabling the users to quickly navigate through the different topics of information and compare the EU Member States at a glance. The map has been published at https://cybersec4europe.eu/heterogeneity-of-data-protection-legislation-in-the-eu/. The published map is depicted in Figure 32. The figure also shows what specific additional legislation is present in Spain, but naturally, users can hover over any of the countries covered in the survey to get its information.

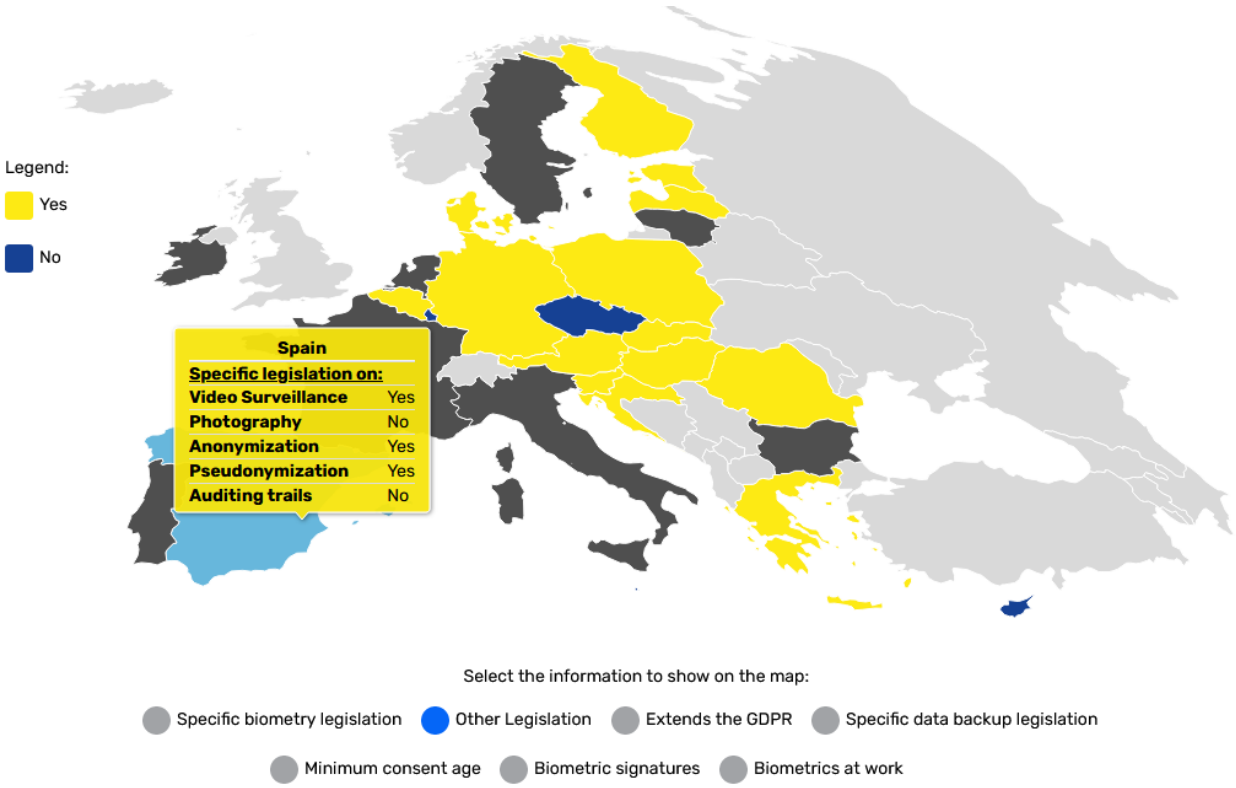


Figure 32: Map of data protection in EU, showing the additional legislation in Spain.

5 Conclusion

This research extends the work already completed at the European Commission and ENISA as a basis for improving the current eIDAS framework. Therefore, we also considered the proposed solutions to develop eIDAS 2. The most important value in eIDAS 2 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 many eIDAS deficiencies already discussed in the existing literature.

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

The first hidden deficiency was identified in a pattern where supervisory authorities are providing trust services at the same time. This is not compliant with current auditing and certification standards and brings forward at least a question of perceived independence. As governments are operating important eIDAS nodes simultaneously, this may lead to simplifying security requirements as far as legislation, and underlying standards allow. Cybersecurity incurs costs, and lowering the bar is a convenient and quick solution. Further, it may affect market competition.

When studying the real-world feasibility of envisioned use-cases in the banking scenarios according to the proposed target of eIDAS 2, we discovered that eIDAS legislation itself might not guarantee universal cross-border use of identities. The main reasons are additional limitations and requirements for the local banking sector that may differ across the Member States. Currently, according to our sample, even if the banks embraced the eIDAS network, opening a bank account in another Member State would not yet be possible.

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. Some Member States have already put limitations on the use of identities acquired using video identification for this reason.

Even though we found that required assurance levels for remotely accessing EU Digital COVID Certificate were the same across the sample of the Member States, there are no clear rules on when to use what level of assurance. As the level of assurance incurs costs, some governments are lowering the bar for some of the governmental services. That affects the dissemination of the technology, making it unavailable to businesses when they need them. There are additional reasons for promoting the highest assurance levels at the government level.

We found that inter-government competition is already building while analysing commercial access to the eIDAS network. With some governments providing access to foreign commercial entities, competition between local regulations will emerge. Even though this may be good for the competition, it also has downsides with the pressure on the costs and later on the level of cybersecurity. For that reason, minimum security standards should be planned carefully and as straightforward as possible to minimize different interpretations.

Connecting eIDAS to GDPR in the field of biometrics, we found that the phenomenon that we called "Bring Your Own Authentication Device – BYOAD" is rising. It is becoming a grey area that has little control over. The 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 prevalent use in the eIDAS network. Because of the simplicity

of these solutions for the end-user, this is just a question of time. This justifies the decision to implement the rules for using BYOAD technologies in a single place for all industrial sectors.

While we took the in-depth analysis of remote on-boarding and authentication practices in the eIDAS network, we found that many prevalent solutions are not following the latest security guidelines. Examples are the use of SMS for OTP passwords and the use of security questions. In practice, therefore, solution providers are trading security for simplicity. This is an additional reason for requiring security characteristics in more detail and following the latest state-of-the-art security methods.

Extensive GDPR privacy obligations for controllers and processors require substantive implementation effort. Even with the carefully planned and executed compliance efforts, cross-border compliance challenges within the EU will persist because GDPR gives the EU Member States certain autonomy regarding data protection governance. Therefore, Member States can enact legislation with additional limitations or requirements than the GDPR. Not all Member States, for example, allow biometrics to be used to obtain handwritten signatures. The use of biometrics for access control is also prohibited or restricted in some Member States. As a result, services or products designed for one Member State are only partially compatible with legislation in the other Member States. Similarly, disparities in the minimum age for consent will necessitate service providers adapting their software and other solutions to account for differences between the Member States. Though putting their software and other solutions in place may appear simple, understanding, collecting, and adhering to various regulations in all Member States is not.

This research suggests that despite embedded freedom, the Member States do not have many additional/specific laws building on top of the GDPR. We discovered that additional or more specific laws are in place for only 29.4% of the cases discussed in this research. A relatively low proportion justifies discussion whether this freedom is inevitable, especially with consequences for the optimal use of resources and the Single European market in mind.

This research did have some limitations. Because of the complexities involved (e.g. language barriers and learning about large amounts of legislation), the effort required would be too large without substantive external help. We reduced this workload by relying on Supervisory Authorities, meaning we must take whoever filled out the survey's word on it. Updating the information would require a repeated process of querying the Supervisory Authorities for the information. The other more obvious limitations are the missing EU Member States not included in the study (because we were dependent on participation from Supervisory Authorities) and the limited number of topics we had in the survey. The last two limitations are also the basis for future work.

As such, in future work, we would like to extend the list of topics to discuss and compare between countries as well as 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 of the Member States and potentially analysing them with the help of appropriate persons with adequate legal backgrounds from the respective countries.

5.1 eIDAS Recommendations Summary

Following our findings and conclusions, we are summarizing our eIDAS related recommendations presented in this deliverable:

- 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 explicitly allowed in all Member States under the provisions of eIDAS 2 to avoid local limitations and even prohibition of the use of eIDAS services.
- Security baseline should be established for the remote identification services to avoid degradation of remote identification because of the market competition and to avoid exclusion of specific services or even Member States from the network based on inadequate security standards.
- We should achieve higher market penetration of the highest level of assurance to empower citizens to use any service at any time without additional effort. Promoting or even requiring the use of a substantial level of assurance 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 the 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.
- We should build a strategy for using “Bring Your Own Authentication Device” solutions as this approach is getting 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 justified. Current standards are falling behind the latest cybersecurity developments and even in referencing the latest sibling security standards.
- The definition of the capabilities of the qualified electronic signature should be changed to reflect actual state-of-the-art technologies used to create electronic signatures to avoid different interpretations.

References

[1] "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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed Jan. 10, 2022).

[2] J. Resende, "D3.13 - Updated version of enablers and components," 2021.

[3] M. Hölbl, B. Kežmah, and M. Kompara, "Data Protection Heterogeneity in the European Union," *Applied Sciences 2021, Vol. 11, Page 10912*, vol. 11, no. 22, p. 10912, Nov. 2021, doi: 10.3390/APP112210912.

[4] "Proposal for 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." European Commission, 2021. Accessed: Jan. 10, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN&qid=1622704576563

[5] European Commission, "Compilation of information provided by Member States with regard to the implementation of the Trust Services chapter of the eIDAS Regulation," 2021. Accessed: Dec. 06, 2021. [Online]. Available: https://ec.europa.eu/futurium/en/content/information-member-states-regard-implementation-trust-services-chapter-eidas-regulation.html

[6] "eID Documentation - Country overview." https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview (accessed Dec. 06, 2021).

[7] "eID for You." https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+for+You#eIDforYou-eid (accessed Dec. 06, 2021).

[8] M. Pedroli, G. O'Neill, A. Fravolini, and L. Marcon, "Overview of Member States' eID strategies." Accessed: Dec. 06, 2021. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/National+Strategies

[9] S. Lips, N. Bharosa, and D. Draheim, "eIDAS Implementation Challenges: The Case of Estonia and the Netherlands," *Communications in Computer and Information Science*, vol. 1349, pp. 75–89, Nov. 2020, doi: 10.1007/978-3-030-67238-6_6.

[10] J. Rocha, "Spanish and Portuguese eIDAS node evolution for electronic identification of European citizens," *EATIS '20: Proceedings of the 10th Euro-American Conference on Telematics and Information Systems*, vol. Part F166737, 2020, doi: 10.1145/3401895.3402094.

[11] V. Tsap, S. Lips, and D. Draheim, "eID Public Acceptance in Estonia: towards Understanding the Citizen," *The 21st Annual International Conference on Digital Government Research*, 2020, doi: 10.1145/3396956.

[12] H. Kubicek, "Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries," *Identity in the Information Society*, vol. 3, no. 1, pp. 5–26, Apr. 2010, doi: 10.1007/S12394-010-0052-0.

[13] D. Berbecaru, A. Atzeni, M. de Benedictis, and P. Smiraglia, "Towards Stronger Data Security in an eID Management Infrastructure," *Proceedings - 2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2017*, pp. 391–395, Apr. 2017, doi: 10.1109/PDP.2017.90.

[14] K. Shrishak, Z. Erkin, and R. Schaar, "Enhancing user privacy in federated eID schemes," *2016 8th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2016*, Dec. 2016, doi: 10.1109/NTMS.2016.7792448.

[15] T. Lenz and B. Zwattendorfer, "Towards cross-border authorization in European eID federations," in *2016 IEEE Trustcom/BigDataSE/ISPA*, 2016, pp. 426–434. doi: 10.1109/TRUSTCOM.2016.0093.

[16] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas, "Federated identity architecture of the European eID System," *IEEE Access*, vol. 6, pp. 75302–75326, 2018, doi: 10.1109/ACCESS.2018.2882870.

[17] F. Morgner, P. Bastian, and M. Fischlin, "Securing Transactions with the eIDAS Protocols," *WISTP 2016: Information Security Theory and Practice*, vol. 9895 LNCS, pp. 3–18, 2016, doi: 10.1007/978-3-319-45931-8_1.

[18] D. Pöhn, M. Grabatin, and W. Hommel, "eID and Self-Sovereign Identity Usage: An Overview," *Electronics 2021, Vol. 10, Page 2811*, vol. 10, no. 22, p. 2811, Nov. 2021, doi: 10.3390/ELECTRONICS10222811.

[19] F. Roelofs, "Analysis and comparison of identification and authentication systems under the eIDAS regulation," 2019. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjMh4ST8sf0AhVEQvEDHbY7BWgQFnoECAYQAQ&url=https%3A%2F%2Fwww.ru.nl%2Fpublish%2Fpages%2F769526%2Fz02_masterthesis_floris_roelofs_final.pdf&usg=AOvVaw2KDdshL9Op9Rcj38Jcbhwl

[20] M. Guillaume, S. Bounjoua, and C. Clemot, *eIDAS compliant eID Solutions*. ENISA, 2020. Accessed: Jan. 04, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions

[21] "Recommendations for technical implementation of the eIDAS Regulation — ENISA," Dec. 2019. Accessed: Jan. 10, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/towards-a-harmonised-conformity-assessment-scheme-for-qtsp-qts

[22] "Assessment of Standards related to eIDAS," Dec. 2018. Accessed: Jan. 10, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

[23] "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. [Online]. Available: https://www.ifac.org/system/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf

[24] "ISO 19011:2018, Guidelines for auditing management systems."

[25] "Electronic identification (eID) and Trust Eervices for citizens: eIDAS Solutions." [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54410

[26] "Electronic ID and Trust Services in action: Open a bank account." [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54412

[27] "Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework." European Commission , Jun. 14, 2021. Accessed: Jan. 10, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H0946

[28] C. Morgado, "New eiDAS 2 proposal: The new paradigm of European Digital Identification," *Cuatrecasas*, Jul. 23, 2021. https://www.cuatrecasas.com/en/spain/article/new-eidas-2-proposal-the-new-paradigm-of-european-digital-identification (accessed Jan. 10, 2022).

[29] "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." ETSI, May 2021. Accessed: Jan. 10, 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.02.01_60/ts_11943101v010201p.pdf

[30] "ETSI TS 119 432 V1.2.1 (2020-10), Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation." ETSI, 2020.

[31] "Questions…and buzz surrounding draft NIST Special Publication 800-63-3," *NIST*. https://www.nist.gov/blogs/cybersecurity-insights/questionsand-buzz-surrounding-draft-nist-special-publication-800-63-3 (accessed Dec. 16, 2021).

[32] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital Identity Guidelines," Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63-3.

[33] W. Dudley, "Rollback! The United States NIST NO LONGER recommends 'Deprecating SMS for 2FA,'" *SAP Blogs*, Jul. 06, 2017. https://blogs.sap.com/2017/07/06/rollback-the-united-states-nist-no-longer-recommends-deprecating-sms-for-2fa/ (accessed Dec. 16, 2021).

[34] "Beware of the Sim Swapping Fraud!," *ENISA*, Dec. 06, 2021. https://www.enisa.europa.eu/news/enisa-news/beware-of-the-sim-swapping-fraud (accessed Dec. 16, 2021).

[35] "SS7 network security analysis report," Feb. 2020. Accessed: Dec. 16, 2021. [Online]. Available: https://positive-tech.com/expert-lab/research/ss7-network-security-analysis-2020/

[36] J. Cox, "Hackers Are Breaking Directly Into AT&T, T-Mobile, and Sprint to Take Over Customer Phone Numbers," *VICE*, Jan. 10, 2020. https://www.vice.com/en/article/5dmbjx/how-hackers-are-breaking-into-att-tmobile-sprint-to-sim-swap-yeh?utm_source=vicetwitterus (accessed Dec. 16, 2021).

[37] J. Cox, "A Hacker Got All My Texts for $16," *VICE*, Mar. 15, 2021. https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber (accessed Dec. 16, 2021).

[38] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google," 2015. Accessed: Dec. 17, 2021. [Online]. Available: https://research.google/pubs/pub43783/

[39] S. Schechter, A. J. B. Brush, and S. Egelman, "It's no secret Measuring the security and reliability of authentication via 'secret' questions," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 375–390, 2009, doi: 10.1109/SP.2009.11.

[40] M. Gontovnikas, "Are Your Security Questions As Safe As You Think?," *auth0 Blog*, Oct. 30, 2017. https://auth0.com/blog/are-your-security-questions-as-safe-as-you-think/ (accessed Dec. 17, 2021).

[41] M. J. Haber, "Security Questions Pose a High Risk: Learn Tips & Tricks to Mitigate the Threat," *BeyondTrust*, Jun. 05, 2020. https://www.beyondtrust.com/blog/entry/reused-security-questions-can-pose-a-high-risk-learn-tips-tricks-to-mitigate-the-threat (accessed Dec. 17, 2021).

[42] P. Grassi *et al.*, "NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management," Jun. 2017. doi: 10.6028/NIST.SP.800-63B.

[43] P. A. Grassi *et al.*, "NIST Special Publication 800-63A - Digital identity guidelines: Enrollment and identity proofing Requirements," Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63A.

[44] "NIST SP 800-63 Digital Identity Guidelines-FAQ," Jul. 05, 2020. https://pages.nist.gov/800-63-FAQ/ (accessed Dec. 17, 2021).

[45] J. Preshing, "Hash Collision Probabilities," May 04, 2011. https://preshing.com/20110504/hash-collision-probabilities/ (accessed Jan. 04, 2022).

[46] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The first collision for full SHA-1," 2017, Accessed: Jan. 04, 2022. [Online]. Available: https://shattered.io

[47] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *European Union*, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed Oct. 11, 2021).

[48] "Data Protection and Privacy Legislation Worldwide," *United Nations Conference on Trade and Development*, 2020. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed Aug. 30, 2021).

[49] " Data Protection Laws of the World," *DLA Piper*. https://www.dlapiperdataprotection.com/ (accessed Aug. 30, 2021).

[50] "A Practical Guide to Data Privacy Laws by Country," *i-Sight Software*, Mar. 05, 2021. https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/ (accessed Aug. 30, 2021).

[51] S. Park *et al.*, "A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement," *Digital Investigation*, vol. 24, pp. S93–S100, Mar. 2018, doi: 10.1016/J.DIIN.2018.01.012.

[52] "Data protection around the world," *CNIL (Commission Nationale de l'Informatique et des Libertés)*, Nov. 23, 2020. https://www.cnil.fr/en/data-protection-around-the-world (accessed Oct. 11, 2021).

[53] W. Long and F. Blythe, "Member States' detogations undermine the GDPR," *Privacy Laws & Business*, May 2016. https://www.sidley.com/~/media/publications/gdpr-derogations.pdf (accessed Aug. 19, 2021).

[54] A. Clearwater and B. Philbrook, "GDPR Derogations and How to Prepare for Member State Variation," *CPO Magazine*, Sep. 29, 2017. https://www.cpomagazine.com/data-protection/gdpr-derogations-prepare-member-state-variation/ (accessed Sep. 01, 2021).

[55] J. Vengadesan and N. Pook, "United with differences: key GDPR derogations across Europe," *Penningtons Manches Cooper*, Mar. 26, 2019. https://www.penningtonslaw.com/news-publications/latest-news/2019/united-with-differences-key-gdpr-derogations-across-europe (accessed Aug. 19, 2021).

[56] B. Custers, F. Dechesne, A. M. Sears, T. Tani, and S. van der Hof, "A comparison of data protection legislation and policies across the EU," *Computer Law & Security Review*, vol. 34, no. 2, pp. 234–243, Apr. 2018, doi: 10.1016/J.CLSR.2017.09.001.

[57] "Data protection comparison," *activeMind.legal*. https://www.activemind.legal/law/ (accessed Aug. 19, 2021).

[58] "GDPR Tracker," *Bird & Bird*. https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker (accessed Aug. 30, 2021).

[59] "GDPR Derogations Tracker," *Latham & Watkins*, Apr. 2018. https://gdpr.lw.com/Home/Derogations (accessed Aug. 19, 2021).

[60] P. Mutabazi, "What is the Difference Between Digital Signatures and Electronic Signatures?," *LinkedIn*, May 23, 2021. https://www.linkedin.com/pulse/what-difference-between-digital-signatures-electronic-mutabazi (accessed Oct. 11, 2021).

[61] "CyberSec4Europe - European Cybersecurity Competence Network." https://cybersec4europe.eu/ (accessed Oct. 11, 2021).

Annex A: eIDAS Questionnaire

5.2 Introductory information

To successfully fill out this Questionnaire, you need some experience with the practical use of electronic identification and electronic signature services in your Member State and at least basic knowledge of eIDAS (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG). For some specific questions, you may need to refer to the publicly available policy of the selected trust service provider.

For your convenience, we are providing citation from eIDAS regarding the assurance levels (Article 8, Paragraph 2):

a) assurance level **low** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;

b) assurance level **substantial** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;

c) assurance level **high** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

Please note that it is not intended that you define assurance levels. This is to be determined either by the trust service provider or user of the trust services.

5.3 Questionnaire

1. Name of the Member State:

Please identify the Member State for further processing of the Questionnaire.

2. Is the supervisory body in the Member State providing trust services at the same time? Please state the name and address of the supervisory body.

This is a question of organizational independence. Having the same organization providing supervisory activities and providing trust services effectively means that the supervisory body is supervising itself. The supervisory body should be free from conflicts of interest and undue influence in all matters regarding to supervision.

3. 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 services providers when opening such an account? Are there any further restrictions on banking services with this account (e.g. renting a loan)?

This question intends to identify any additional limitations on the use of trust services in selected Member State. eIDAS was meant to be universal. If any local restrictions exist, they directly influence the European single market and introduce cross-border issues. Please also identify any rules that may have been withdrawn recently. Please list any other limitations you may be aware of besides the banking sector.

4. Can you get qualified certificate remotely, e.g. by using remote video identification? Are there any Member State level rules defining requirements for video identification?

We are trying to identify actual use cases for eIDAS Article 24, paragraph 1/d, where other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence are allowed. We are especially interested in complete remote identification to identify any differences in requirements in the different Member States. Because identities are mutually recognised between Member States, such differences should not exist because they represent the by-pass of local regulation in another Member State where such an identity could be used. If there is such a provider in your Member State, please determine if citizens of other Member States can obtain eIDAS identity with that provider (because that would present direct bypass of local rules), e.g. a trust services provider in Germany issues identity in Germany for Slovenian citizen remotely (using video identification) under German rules, although such video identification would not meet requirements of the local regulations in Slovenia).

5. Are you familiar with any government level electronic services that don't require qualified electronic signature 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?

The intent of the question is the identification of requirements for assurance levels. Assurance levels are only listed in eIDAS, but there are no clear guidelines on what level of assurance is needed depending on the provided service. We are trying to find the services in different Member States that require different assurance levels for the same service.

6. Can you access EU Digital COVID Certificate using electronic means? If yes, what assurance level do you need to access the certificate?

We are identifying different levels of assurance for access to the same data in the various Member States. For an explanation on Assurance levels, please look at Article 8 of eIDAS. For every electronic identification that you own, the assurance level for that electronic identification is clearly stated in the publicly available policy. The service you are using also usually clearly states the assurance level of identification that you can use to access the service.

7. 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?

Despite the intent of eIDAS to be accessible to private businesses, local regulation in the Member States may vary. We are identifying if and under what requirements and costs the businesses may access eIDAS identities in your Member State.

8. Are you aware of any trust services based on biometric authentication?

This question is intended to identify any use-cases of biometric authentication. Many banks are now using some sort of BYOAD (bring your own authentication device) like mobile phones without certification scheme, SLA agreement or any other assurance of the quality of service. This is partially because the use of biometrics is very limited according to the GDPR (and even further prohibited in some Member States). Please state if you can access identity using biometric authentication (like using a fingerprint on your mobile phone).

9. Please describe online (remote) process of trusted service registration and use (authentication for the use of identity).

We are identifying actual use-cases of remote registration with the trusted service providers. Please select and describe at least one (preferably all) possibilities of obtaining identity from the trusted service provider remotely. We are interested in detailed procedure of what you have to provide to get a new identity and how do you use that identity (authentication scheme). You don't have to assess if the use-case is compliant with the current best practice. Please just describe the process in detail and if possible, provide screenshots and translate all input fields. Please pay attention to details like using SMS as additional password, entering security questions in case of forgotten password and similar.

Annex B: GDPR Questionnaire

Specific personal data processing restrictions in the EU Member States (for Supervisory Authorities)

Research on differences in specific EU personal data processing restrictions.

Dear survey participant,

Thank you for your willingness to participate in the survey. The results of the survey will provide a basis for research on the harmonisation of privacy-related issues throughout the EU with an emphasis on biometrics. If you are interested in the outcome, you will have the possibility to request access to research results at the end of the survey.

Basic knowledge of privacy-related regulation in your member state and basic technical knowledge is required to finish this survey with the emphasis on acquiring handwritten signatures in an electronic manner (for example, using biometric electronic signature pads at the point of sale). If you don't possess this kind of knowledge, please forward this survey to a colleague who does.

The survey should take, on average, around five minutes.

Funding

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929.

There are 18 questions in this survey.

Please select your Member State

Choose one of the following answers

Please choose **only one** of the following:

- Austria
- Belgium

- Bulgaria
- Croatia
- Cyprus
- Czechia
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden

Do you have a special privacy regulation (other than GDPR) regarding biometrics in your Member State?

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

Make a comment on your choice here:

If the regulation is only based on GDPR, please answer NO. Answer YES only if there is a local regulation that applies, either based on GDPR or previous Directive 95/46/EC and is still in force.

Are you aware of any special privacy regulation regarding the following in your Member State:

Please choose **all** that apply:

- Video surveillance
- Biometrics

- Photography (of natural persons regarding personal data protection)
- Anonymisation
- Pseudonymisation
- Audit trails regarding personal data processing (e.g. additional requirements of logging data processing activities like entering, changing or deleting personal data)
- Other:

If the regulation is only based on GDPR, please don't select an option. Select an option only if there is a separate, specific local regulation that applies, either based on GDPR or previous Directive 95/46/EC and is still in force.

Are you aware of any special privacy regulation regarding the following in your Member State:

Please choose **all** that apply:

- Additional requirements for verifying that consent is given or authorised by the holder of parental responsibility for the child (under Paragraph 2, Article 8 of the GDPR).
- Rules regarding the processing of personal data of deceased persons (under the Recital (24) of the GDPR).
- Rules regarding the processing of genetic personal data (under Paragraph 1, Article 9 of the GDPR).
- Rules regarding the processing of biometric personal data for the purpose of uniquely identifying a natural person (under Paragraph 1, Article 9 of the GDPR).
- Rules regarding the processing of data concerning personal health (under Paragraph 1, Article 9 of the GDPR).
- Rules regarding the processing of data concerning natural person's sex life (under Paragraph 1, Article 9 of the GDPR).
- Rules regarding the processing of data concerning natural person's sexual orientation (under Paragraph 1, Article 9 of the GDPR).
- Rules regarding the erasure of personal data (under Paragraph 1, Article 17 of the GDPR).
- Rules about the designation of the data protection officer (DPO) regarding mandatory designation and/or its tasks (under Article 37 of the GDPR).
- Rules regarding consultation with the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing (under Paragraph 4, Article 36 of the GDPR).
- Other:

If the regulation is only based on GDPR, please don't select an option. Select an option only if there is a separate, specific local regulation that applies, either based on GDPR or previous Directive 95/46/EC and is still in force.

To the best of your knowledge, is there any formal regulation regarding erasure of personal data from backup data (e.g. from backup tapes)?

Please choose **only one** of the following:

- Yes

- No

Make a comment on your choice here:

The question is about any detailed instructions/regulation on how to handle erasure of personal data from backup copies when the data subject exercises "the right to be forgotten" (under the Article 17 of the GDPR).

You have indicated, that in your country, there is formal regulation regarding erasure of personal data from backup copies (e.g. from backup tapes). Please, provide the title of the regulation or a link to the electronic version of the regulation (preferably in English).

Please write your answer here (only if previously indicated):

The question is about any detailed instructions/regulation on how to handle erasure of personal data from backup copies when the data subject exercises "the right to be forgotten" (under the Article 17 of the GDPR).

What is the minimum age of a child for which the processing of personal data is lawful without prior consent given by the holder of parental responsibility over for the child (under the Article 8 of the GDPR).

Please choose **only one** of the following:

- 13
- 14
- 15
- 16
- 17
- 18

The question is about whether the age of a child at which the processing of the personal data is lawful without consent given by the holder of parental responsibility for the child has been lowered in your Member State (under the GDPR, the age is 16 years but can be lowered down to 13 years of age). If there were no changes in you Member State, please select 16.

You have indicated that the minimum age of a child for which the processing of personal data is lawful without prior consent given by the holder of parental responsibility for the child is not 16. Please, provide the title of the regulation or a link to the electronic version of the regulation (preferably in English) where this is defined.

Please write your answer here (only age different from 16):

The question is about whether the age of a child at which the processing of the personal data is lawful without consent given by the holder of parental responsibility for the child has been lowered in your Member State (under the GDPR, the age is 16 years but can be lowered down to 13 years of age).

To the best of your knowledge, is the use of biometrics for electronic acquisition of handwritten signature allowed in your member state (e.g. by using electronic pads at the point of sale)?

Please choose **only one** of the following:

- Yes
- No

Make a comment on your choice here:

The question is about any regulatory requirements that prohibit the use of biometrics when acquiring handwritten signature using electronic means, for example, a customer signing a contract in electronic form at the point of sale by using an electronic pad that acquires pressure, speed of signing etc. besides the picture of the handwritten signature. Even if the data controller/organisation needs some special permit to use biometrics, please answer with a "Yes" as it is generally possible to use biometrics.

To the best of your knowledge, is in your Member State the use of biometrics generally allowed in a work environment (e.g. for opening a server room with a fingerprint)?

Please choose **only one** of the following:

- Yes
- No

Make a comment on your choice here:

"Generally allowed" means that it is not strictly prohibited. Even if the data controller/organisation needs some special permit to use biometrics, please answer with a "Yes" as it is generally possible to use biometrics.

You have indicated there is formal regulation regarding the use of biometrics other than the GDPR. Please provide the title of the regulation regarding the use of biometrics (in original language).

Please write your answer here (only if previously indicated):

Title of the regulation in the original language.

You have indicated there is formal regulation regarding the use of biometrics other than the GDPR. Please provide the title of the regulation regarding the use of biometrics (in English).

Please write your answer here (only if previously indicated):

Title of the regulation in English language.

You have indicated there is formal regulation regarding the use of biometrics other than the GDPR. Please provide a link to the electronic version of the regulation (in original language).

Please write your answer here (only if previously indicated):

URI to the full text of the regulation in original language.

You have indicated there is formal regulation regarding the use of biometrics other than the GDPR. Please provide a link to the electronic version of the regulation (in English, if translation exists).

Please write your answer here (only if previously indicated):

URI to the full text of the regulation in English language.

You have indicated there is formal regulation regarding the use of biometrics other than the GDPR. Since when is this restriction in force (year)?

Please enter a date (only if previously indicated):

Please provide the year when this restriction entered into the force.

You have indicated there is formal regulation regarding the use of biometrics other than the GDPR. Please briefly describe the essential limitations of using biometrics or other specifics of your local regulation.

Please write your answer here:

Short description of essential limitations set forth by the regulation regarding the use of biometrics for customers and/or employees. Please only describe specific limitations by special regulation in your member state – do not repeat or describe GDPR requirements and limitations.

Thank you very much for your time and effort to complete this survey. The results will be used for further harmonisation of the Single European Market in the field of privacy regulation.
If you have provided contact information and requested access to research results, we will deliver the report to your contact address once the research is complete.

Thank you for completing this survey.