Eurosmart's feedback on an EU Digital Identity scheme (EUid)

European Commission's public consultation on an EU digital ID scheme for online transactions across Europe

Executive Summary

Eurosmart, the voice of the Digital Security Industry, is committed to enhancing security solutions that enable European citizens to enjoy a reliable and trustworthy digital experience.

eIDAS is a valuable milestone in this respect, as (1) it provides a common basis for electronic identification and electronic authentication, and (2) ensures that Trust Services appropriately fulfil their missions.

The eIDAS Regulation enables cross-border eID for over 50% of the European citizens. Efforts should be made to unleash the full potential of eIDAS solutions, in particular for identification and electronic authentication across Europe (eIDAS Chapter II). The eIDAS trusted model has been showing its benefits on business in countries where solutions have been developed, despite the persistence of diverging national rules impeding the de-facto mutual recognition of eID schemes in Europe. The trust services part (eIDAS Chapter III) is also a key achievement: worldwide players such as ADOBE or Global Sign now propose trusted solutions for the public at large.

Option 1:

Eurosmart supports **option 1** as a necessary step to consolidate the eIDAS framework. Further enhancements and extended usages of eIDs under eIDAS should be fostered. In particular, deeper harmonisation of certifications will bring more confidence and trust to stakeholders. This will also clarify the eIDAS security requirements and Levels of Assurance (LoAs). The recent adoption of the Cybersecurity Act and the coming EU CC scheme can support a smooth harmonisation.

Option 2:

The use of eIDAS solutions by private actors could be an incentive to boost the European Digital Single Market. However, the approach proposed in **option 2** may damage the current electronic identification framework as provided by chapter II of the Regulation. The system has been designed for Sovereign eIDs only. Sovereign eIDs are assets that the private sector could advantageously leverage on to develop its own

identification frameworks. Eurosmart strongly believes that eIDAS should not be revised but complemented: option 1 should be favoured.

However, as stated by the European Commission in its inception impact assessment, private actors can make a better use of eID solutions. Typically, if banks were given the capability to rely on national eID solutions to implement strong digital ID verification, this would bring trust and convenience to their KYC procedures. Better synergies between the eIDAS Regulation and AML and PSD2 directives would accelerate the deployment of national eID solutions at assurance level "High" and would stimulate their adoption by private actors.

In addition, Eurosmart recommends to the Commission not to limit the revision to option 1, but to **combine option 1 with another legislative act establishing a complementary framework for:**

- private eIDs and attribute providers;
- private services (also called relying parties) accepting them.

Furthermore, to strengthen harmonisation, Eurosmart recommends to the Commission to opt for a regulation rather than a directive. This approach is an **alternative to option 2** as currently envisioned in the impact assessment. Through this dedicated regulation, the Commission should give a mandate to the European standardisation organisations (ESOs) to define all the necessary harmonised standards, such as standards for the reuse of notified eID schemes by the private sector. In addition, this regulation should identify or request the development of a European Certification Scheme, under the Cybersecurity Act, when it comes to the evaluation of private eID schemes.

This new framework could be adopted through a new proposal for a regulation based on eIDAS. This approach should consider dedicated rules and procedures for data privacy, identity and attribute proofing; and should require harmonised standards. Such a framework will create market incentives for the use of eID schemes. It will provide the necessary means to ensure a clear legal framework and the legal certainty that relying parties need. Eurosmart proposes 9 recommendations as listed hereunder (pages 6-12).

Option3:

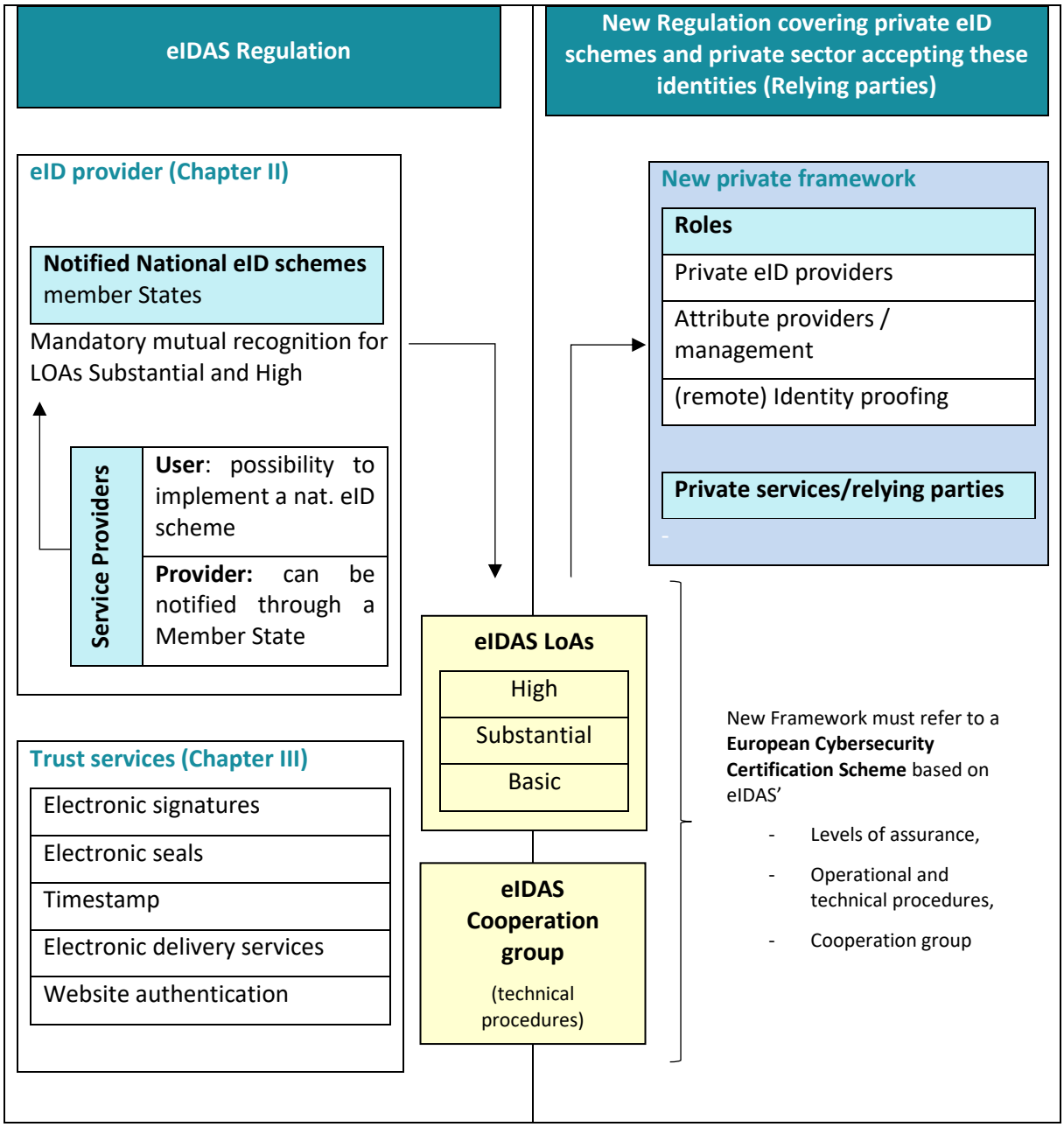
The EUid could quickly be achieved with a European label on national eIDs notified by Member States.

Overview of Eurosmart's favoured options

Option 1 remains the most urgent action that is needed to consolidate eIDAS. It will prepare the necessary blocks to create a dedicated framework for private actors who want to benefit from notified eID solutions. However, Eurosmart also recommends not to limit the revision to option 1, but **to complement it with another regulation** covering the complementary framework for (1) private eIDs and attribute providers, and (2) private services accepting them, that would leverage on eIDAS and the enhanced harmonisation brought by option 1.

Option 1: Consolidate the current eIDAS Regulation though comitology.

Eurosmart proposal for an alternative to option 2: Dedicated regulation for the private sector to make an efficient use of eID schemes.



Option 1

Option 1 (improvement of the coherence, consistency and interoperability of the eIDAS framework) remains a priority. It is Eurosmart' s preferred option. Member States and the private sector have already made investments and efforts to scale up the eIDAS framework.

1. eID scheme

It is paramount to improve and speed up the mutual recognition process of notified eID schemes. The eIDAS eID framework has demonstrated that a decentralised and technologically neutral framework remains the most robust solution to ensure interoperability and mutual recognition of eID schemes across Europe. Option 1 offers the opportunity to increase convergence of eID schemes between Member States. Amongst other, it may be achieved through the review of the following Implementing Acts:

- **2015/1502 providing a definition of LoA**, to (1) harmonise definitions, (2) reach non ambiguous technical definitions, (3) remove fragmentation resulting–amongst other – from national certification procedures, (4) introduce mandatory security certification pursuant to the Cybersecurity Act, and (5) enable identity providers to bind an eID of a natural person delivered by a Member State with an eID of a legal person and devices. We recommend that the level of assurance of the natural eID bound must be at the same or upper level of assurance of the device or legal eID issued;
- **2015/296,** to (1) strengthen harmonisation of electronic identification schemes by requiring a mandatory positive opinion of the cooperation network prior to any notification of an eID scheme, and (2) ensure that the guidance documentation prepared by the cooperation network is legally binding in all Member States;
- **2015/1501** or a new delegated act to introduce provisions for an effective deployment of eID schemes, by enforcing the following measures:
    - Mandatory notification of at least one eID scheme of LoA "Substantial" per Member States within a maximum delay;
    - Strong incitation to Member States so that they notify at least one eID scheme of LoA "High" within a maximum delay;
    - Mandatory usability within each Member State of all notified eID schemes within a maximum delay – which is currently not the case (see Annex);
    - Monitoring of usability status within each Member State by the European Commission with regular publications. Eurosmart has already conducted its own survey which can be found in the Annex.

Also, option 1 should leverage on the possibility already given to the cooperation network under implementing act 2015/296 to provide guidance to Member States with regards to key technologies for eID schemes, such as (1) biometry, (2) optical authentication of identity documents (relying on its security features), or (3) identity derivation from an identity document (such as national identity card using the chip OR using optical authentication relying on its security features) onto a mobile phone.

2. Trust services

With regards to Trust Services (eIDAS Chapter III), option 1 offers the opportunity to make the most of the EU standards already developed by CEN and ETSI through Mandate M/460[1]. Eurosmart recommends the mandatory use of EU standards by means of Implementing Acts to demonstrate conformity with the provisions of eIDAS.

Such standards would ensure a concrete link between eID services (Chapter II of the eIDAS Regulation) and Trust Services (Chapter II). They are also necessary to enhance the use of notified eID services by trusted services.

Eurosmart also recommends improving Implementing Act 2016/650 laying down requirements for security assessment of QSCD. Its provisions are clear and unambiguous when it comes to smartcard-based QSCD. However, some Member States still adopted additional requirements, hence creating fragmented national procedures for smartcard-based QSCD.

When it comes to server-based QSCD the provisions are so fuzzy and ambiguous that it has led to major fragmentation amongst Member States, but above all, major differences between solutions certified within different Member States. Eurosmart urges the European Commission to harmonise the security assessment of server-based QSCD by (1) relying on Common Criteria methodology, and (2) referencing mandatory protection profiles covering all the needed components for server signing : the component holding the signature key indeed, but also the server application managing the signature process, and the component managing the remote identification and authentication of the signatory. In that respect, some Member States have prepared some useful deliverables that could be considered (e.g. ANSSI).

Last but not least, the European Commission should consider preparing guidance to clarify numerous situations where (1) articles are unclear, or too open and thus leading to fragmentation, or (2) national divergence has been noticed. For instance, a guidance should be prepared

- for article 24(1) listing the conditions to be met to issue qualified certificates for Trust Services. The list of options is too diverse, and the way to assess them depends on national authorities, leading to fragmentation and a situation where a large spectrum of solutions offering very different levels of security are eligible for these provisions;
- for Implementing Act 2016/650 where national procedures for smartcard-based QSCD are very different between Member States and lead again to fragmentation.

However, this list is not exhaustive. Key stakeholders from sectors using the eIDAS Regulation could provide useful feedback, notably on all the sources of fragmentation they are facing and that should be eliminated.

In addition, the optimisation of eIDAS should be implemented through concrete projects supported by the Digital Europe Programme. The eIDAS coordination between the Member States should be enhanced (e.g. nodes, infrastructures) and become mandatory in specific fields (e.g. health, social and tax services, interaction of legal persons with public services). The time window for restoring Europe's digital sovereignty is narrow, and a practical implementation of "eIDAS 2.0" should be completed by 2021.

[1] Standardisation mandate to the European Standardisation Organisations in the field of information and communication technologies applied to electronic signatures. https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=442#

Option 2

Option 2 aims at enhancing the involvement of private actors within the eIDAS framework. Sovereign eIDs are assets the private sector could advantageously leverage on to develop its own identification framework.

Eurosmart warns against an implementation of option 2 that would enable Private eIDs to compete with eIDAS-notified eID schemes. Europe would run the risk of slowing down the efforts made to achieve the current eIDAS framework. This loss of valuable time would be detrimental to the deployment of eID solutions across Europe. It would discourage both Member States and EU private actors to invest in trustworthy eID solutions. This backlog would finally be a burden on the development of Europe's strategic autonomy. The current version of eIDAS provides high-end and trustworthy eID solutions only. They are mostly based on legal identity. This level of confidence cannot be ensured as such by private identity providers.

However, there is a clear market need for private actors to use privately issued eIDs. A dedicated legal framework for private eIDs can be considered but should not impede the necessary consolidation of the existing eIDAS framework.

Eurosmart considers that the right legislative act to meet these objectives is a regulation in order to ensure the needed level of harmonisation. Using a directive would be detrimental to the objective of a global digital identity usable within EU across public and private sectors as it would open the door to numerous fragmentations.

This dedicated legal framework must refer to the current eIDAS Regulation (and implementing acts) on the following points:

- **Definition of Levels of assurance** that should be reused for eIDs issued by private sectors under this new regulation. Furthermore, to demonstrate compliance with the requirements of a given LoA, their technical definition should leverage on a **certification scheme prepared under the Cybersecurity Act**, which should be referenced in the regulation;
- **The Cooperation group** should supervise the technical criteria applicable to the LoA.

Moreover, Eurosmart calls on the European Commission to apply the **nine following recommendations** when preparing the new legislative act:

1. Ensure consistency on the Levels of Assurance (LoA) between private eID solutions and notified eIDs under eIDAS

1.1. The future regulation should rely on the definition of LoA brought by eIDAS

The three eIDAS levels of assurance (LoA) for eID must be the reference for the private sector. Otherwise, this would hamper a large use of digital identities within the EU, as notified eIDs under eIDAS would not be comparable to future private initiatives. This would cause private service providers to face fragmentation, trust model issues, and incur supplemental costs, which would impede a large acceptation of private attributes and/or eIDs. In short this would ruin the efforts and benefits brought by the eIDAS Regulation so far.

Reaching the goal of a large acceptation of digital identity in the EU implies leveraging on the definition of LoA brought by the eIDAS Regulation for the future eID framework.

A certification scheme, pursuant to the Cybersecurity Act, remains the privileged way to demonstrate that the requirements of a given LoA are reached. Eurosmart strongly encourages to investigate this option.

1.2. Ensure that the needs of private service providers meet the available eID scheme

National eID schemes are mostly notified at level "High" under eIDAS. On the other hand, private service providers prefer relying on eID schemes with LoA "Substantial" as it provides a good trade-off between (1) the cost incurred to technically support an eID scheme, and (2) the risks of fraud resulting from the usage of an eID. Therefore, a large ecosystem of eID scheme of LoA "Substantial" is needed to meet today's needs of private service providers, otherwise it will face a strong distortion of offer.

Nevertheless, usages (present or future) that would rely on LoA "High" should not be pushed aside, and the deployment of eID schemes of LoA "High" should also be maintained and promoted to prepare future uses that will require the strongest levels of assurance.

Therefore, future private initiatives should focus on the deployment of private eIDs of LoA "Substantial", but also of LoA "High" to meet future needs. In parallel, the European Commission should put in place mechanisms under eIDAS to encourage Member States that have notified eID schemes with LoA "High" to also notify eID schemes with LoA "Substantial".

2. Data protection: the need for a new framework

From a legal point of view, the European Commission's impact assessment suggests defining rules for platforms directly through other legislation (i.e. Digital Services Act for data governance model). Eurosmart strongly advocates for the complete definition of requirements for platforms and all other private entities which may provide or make use of eIDs **through a new framework**. Doing so would not impede the deployment and use of existing eID schemes under eIDAS, as they deal with national sovereign identities.

Furthermore, Eurosmart welcomes the proposal from the European Commission to introduce specific requirements applicable to the private sector. This will foster the deployment and use of private solutions that rely on notified eID schemes by demonstrating to users that their data are safe, but also by clarifying for private sectors how to implement the requirements enacted in GDPR. However, the European Commission should aim at correcting the current limitations of GDPR resulting from national divergences and interpretations and leading to fragmentation. In particular, these requirements should meet the following principles:

- **Technology neutral**: these requirements should not exclude or overrule any technology. The requirements should be applicable to any kind of technology, present or future. In that regards, biometry should not be overruled;
- **Open to innovation**: these requirements should leave room for innovation and experimentation to test emerging technologies;
- **Strengthen Europe's sovereignty**: prescribe data to be stored and processed only on EU territory -without any exceptions- and by European entities only. Furthermore, compliance with this requirement should be demonstrated through a mandatory audit conducted under the supervision of a European Data Protection Authority.

3. Rely on the existing federated and decentralised eIDAS nodes

The eIDAS federated and decentralised model allows the concrete implementation of mutual recognition through the eIDAS nodes. Each Member State sets up a node, i.e. an interface which communicates with other nodes to request or provide cross-border identification and authentication. A software (eIDAS-Node software) has been developed under the Connecting Europe Facility (CEF) programme and is being re-used by most of the Member States for the roll-out of their nodes. The deployment of eIDAS nodes all over Europe is a major step forward for the interconnection and interoperability of eID schemes. Despite such a progress, there is still a lot to do. A lot has been invested by Member States and the European Commission over the past years to set up these nodes which are functional today. Therefore, it is essential to leverage on the eIDAS nodes for the deployment of the future private eID solutions. Eurosmart recommends that the future framework do not constitute a second layer above the eIDAS nodes -that would be available to public and private sector- but enhance the existing eIDAS nodes.

Furthermore, Eurosmart recommends supporting the federated and decentralised model actively. Even if it deserves strong improvement, the decentralised approach is the more sustainable and secure approach. The eIDAS model avoids the "single point of failure" issue. Europe already faced two security breaches in 2019 which impacted two nodes but without putting at risk the complete eIDAS nodes infrastructure. The future framework must rely on this federative approach. An EU centralised model would be highly vulnerable to potential attacks and cybersecurity threats would be more challenging to mitigate, as shown by the 2007 Cyberattacks in Estonia on centralised infrastructures.

Eurosmart recommends that the future framework regulation fully rely on the existing eIDAS nodes framework and extends it where necessary.

4. Take advantage of the Cybersecurity Act certification framework

As stated in the impact assessment, ever-increasing number of electronic ID solutions are being developed. All answer different needs from public services, or the private sector such as banking or social networks. To ensure a trustworthy development of the Digital single market, the certification of eID schemes at the adequate security level is of utmost importance, as it is the trust anchor to access any IT infrastructure. A cybersecurity breach on an eID scheme could lead to major damages both on citizens but also on critical infrastructure themselves. Such major risks should be countered through mandatory security certification imposed on eID schemes, whether they are deployed under the eIDAS regulation, or the future framework for private actors.

Eurosmart calls on the European Commission to rely on the Cybersecurity Act when it comes to the security certification of eID schemes. An alignment between 1) the Levels Of Assurance (LoA) - defined by the eIDAS Regulation -and which should be reused by the future regulation as proposed in 1- and 2) the Cybersecurity Act, would solve the issue of fragmentation, hence simplifying certification for companies. This would also clearly demonstrate the security of eID schemes.

For the sake of consistency, the eIDAS levels of assurance should follow or refer to the three levels of the Cybersecurity Act:

eIDAS LoA	Cyber Act's Security levels
High: "[…] **the purpose of which is to prevent misuse or alteration of the identity"** (Article 8 (c)). "**Protect against attackers with high attack potential"** (§2.2.1, IA 2015/1502)	**High**: includes penetration testing.
Substantial	**Substantial**: conformity
Low	**Basic**: self-certification

5. Rely on a strongly established identity

The cornerstone for the acceptance of such private solutions is a trusted identity. It implies that the identity presented by a holder using an eID, it means that the identity meets the following criteria:

- It is genuine;
- It is bound to the holder;
- The holder has been verified as being the holder of the claimed identity.

Furthermore, the eID should be bound to the legal identity delivered by its State. This would ensure that the holder of an eID delivered under the future framework is liable for any of his actions, and may be sued if needed.

Therefore, the recognised private eID solutions should be built on a legal identity delivered by a Member State or a notified eID under the eIDAS Regulation at level "substantial" at least. In particular, when the eID is delivered by a private entity, it should be solely based on a valid identity document issued by a Member State, testifying the legal identity of the holder. In that respect, identity cards, which enjoy a high quality and harmonised enrolment procedure pursuant to regulation 2019/1157, should be used as a levier. Any eID providers should be encouraged to use national identity card as a mean for an applicant to prove his/her identity. Using other identity documents should still remain possible provided the same trust in the enrolment procedure is achieved and demonstrated. However, it may imply providing complementary proofs when providing an identity document which is not an identity card.

Eurosmart calls on the European Commission to require private eID providers to accept valid identity card pursuant to Regulation 2019/1157 as a means to be delivered as well as eID. Using other identity document may be allowed provided the same trust in the enrolment procedure is achieved and demonstrated, possibly by using complementary proofs.

6. Rely on a strong identity proofing

In order to be accepted and trusted, private eIDs should ensure a strong binding between the claimed identity and the holder. It is of the utmost importance as a transaction involving an eID is usually made online without any physical interaction.

A strong binding between the claimed identity and the holder requires a strong identity proofing prior to the issuance of the eID by the eID provider. In particular, it requires the eID provider to:

- Collect identity information pertaining to the holder;
- Verify the origin and genuiness of the identity information;
- Verify that the identity information is bound to the applicant. Biometric comparison technologies can be very useful to ensure this binding as a reference biometry provided in the identity information could be used to check that the applicant is the legitimate holder of these identity information. In that respect, biometric comparison technologies may be very useful to achieve a strong binding, and thus should not be impeded by unnecessary or excessive regulation.

Eurosmart calls on the European Commission (1) to mandate a strong identity proofing to be performed by the eID provider under the future framework, and (2) not to impede the usage of biometric comparison technologies by unnecessary or excessive regulation.

Furthermore, the future regulation should also acknowledge current and future trends where remote identity proofing – meaning without face to face interaction at the same physical location - is more and more demanded (1) by users for convenience, but also (2) by eID providers as it allows reducing costs, and better efficiency. Therefore, it should be made sure that remote identity proofing is allowed by the future framework. It is a key factor of success. Otherwise, the regulation would miss its target. Eurosmart calls on the European Commission to allow remote identity proofing – meaning without face to face interaction at the same physical location - in the future framework.

Last but not least, it may be worth considering a dedicated role for identity proofing, sorted out from the one of eID provider. This would be justified given the utmost importance and criticality of identity proofing for trust in private eID solutions under the new framework. In addition, a high level of skills and technologies is needed to perform identity proofing tasks. eID providers may not be willing to invest to properly perform this step or may not consider it as being part of their activities.

The role of identity proofing would feed eID providers with identities that have been correctly verified; so that it could issue and manage the corresponding eID. This role could also be of interest for the financial sector falling under PSD2 or AMLD, where Know Your Customer (KYC) is mandated. This sector could also benefit from the applicable liability regime. Eurosmart calls on the European Commission to introduce in the future framework a dedicated role for identity proofing, with the corresponding responsibilities and liabilities. As proposed in 7, a protective liability regime for the users of identity proofing should be applied to the entity performing identity proofing.

7. A protective liability regime for accepting entities

The ambition of this alternative to option 2 is to set up a legal and trusted ecosystem across private actors. Indeed, it entails setting up the interoperability framework required to interconnect identity providers (guaranteeing electronic identity) and service providers (using electronic identity). However, this is not sufficient. The liability regime applicable in case of fraud on the electronic identity is instrumental to encourage private sectors to accept and trust such private attributes and eIDs under the future framework.

The private sector will only be willing to accept eID solutions defined under the future framework provided it brings clear benefits, mainly a complete legal protection in case of identity fraud. In that regards, Eurosmart calls on to replicate the liability regime applicable for qualified trust service provider under eIDAS (article 13(1)) - which is fairly protective for accepting entities - and apply it to eID providers. In particular, the two following aspects, which are instrumental to create trust within private accepting entities, should be incorporated in a new regulation:

- eID provider under the future framework should be liable for any damage caused intentionally or negligently to any natural or legal persons due to failure to comply with any applicable obligations;
- The intention or negligence of the eID provider under the future framework should be presumed unless it proves that the damage occurred without intention or negligence.

8. Consider enhanced usages

Beyond regular eID, the future regulation should also consider innovative and enhanced eID services providing privacy to users. Eurosmart calls on the European Commission to include the following eID services in the future regulation:

- **Authentication without identification or identity**. This service allows demonstrating that an individual belongs to a group or a category of user, without disclosing any identity or identification information. This may be useful to access a service only requiring belonging to a group;
- **Provision of pseudonyms**. This service allows disclosing a pseudonym – not linked to the identity of the holder – but allowing the third party to link a connection with a former connection.
- **Selective disclosure of attributes.** This service allows the user to disclose a selected set of attributes to a third party. The selected set of attributes is conveyed to the third party in a manner ensuring its integrity and authenticity, after successful consent of the holder;
- **Disclosure of attestation.** This service allows the user to disclose attestation to a third party. The attestation is an electronic credential demonstrating the user meets a set of requested criteria but without disclosing the underlying attributes (e.g. the majority of the holder is asserted without disclosing the date of birth);
- **Attribute management.** This service adds a third stakeholder – attribute provider - in the regular eID ecosystem made up with (1) eID provider and (2) service provider. The attribute provider is an entity holding attributes related to the holder, which are unknown or not managed by the eID provider. As such, the attribute provider could provide to a service provider some attributes related to the holder after successful identification, authentication and verification of its consent. This concept is of particular relevance for sector such as finance or health where third party holding attributes related to the holder frequently intervenes (e.g. national authorities indicating whether someone is a politically exposed person, other financial institution that may confirm a successful KYC, insurance company that may indicate the health coverage…). In order to ensure that the future new regulation does not miss its target and is a success, it should be designed to meet the requirements of the financial and health sector which are paramount for the deployment of eIDs. Thus, the future regulation should include in its scope the concept of attribute management/provider, and clearly define its roles, responsibilities and liabilities. As proposed in 7, a protective liability regime for the entity receiving the attributes should be applied to the attribute provider.

9. Strong binding of attributes with a notified eID under eIDAS

More globally, citizens using their self-sovereign identity will collect all along their digital journey, attributes, credentials, or any certified assertions from various private attribute providers. These private attributes are related to user's day to day activities with academic, corporate, associations, etc... Private stakeholders should have the capability to present their own attributes – e.g. university degree, professional qualification or experience, corporate attestation of work, status, proof of residence, financial solvency, etc. - and to have them bound with eIDAS identification. Doing so, a private attribute can be linked with an eIDAS pivotal attribute whereby enhancing the level of confidence a Relying party can lend to such private attribute. As a simplistic example, an attestation of graduation signed and issued by a private domain and featuring user's name can be bound to the same user's name validated through the eIDAS identification process. Technically, bridging private attributes with eIDAS can be done in several ways and can easily be under the control of users thanks to data minimisation or user consent capabilities. The user could even make use of its own electronic identity document (e.g. its electronic national identity card) delivered by its national eID scheme as an additional authentication factor involved in the process of eIDAS binding. Besides, the ramp up of mobile driving license applications is paving the way to mobile identity, making soon available user personal devices to perform the bridging. Such bridging would strengthen the trust in private attributes while preserving the supremacy of sovereign digital identities.

Option 3

Option 3 proposes the implementation of a European Digital Identity scheme (EUid) for Member States' nationals that would be complementary to notified eIDs under the eIDAS Regulation, and would be usable to access both online public services and also private services.

Eurosmart considers option 3 as a promising and ambitious option. However, due to its complexity, its full implementation would probably take more than five years whereas efforts should be focused on option 1.

The EUid could quickly be achieved with a European label on national eIDs notified by Member States.

Conclusion

Eurosmart strongly supports option 1 with an additional regulation to enhance the use of eIDs by private actors. This combined approach preserves the eIDAS framework and tackles the issue of (1) deployment, (2) usage, and (3) advanced forms of private digital identity through a dedicated new regulation. Eurosmart stresses that leaving the eIDAS Regulation unchanged – even though some adjustments are needed (refer to propositions for option 1) – is instrumental to preserve the private and public ecosystem that has been created and benefits that have been brought thanks to this regulation. While indeed this ecosystem and the benefits need to be strengthened, this could only be achieved thanks to legal stability. Reshuffling the regulation to introduce new provisions related to private digital identity would vanish all the breakthroughs that have been achieved over the last six years, and lead to a major step back for digital identity. Furthermore, it would require again several years to get the first achievements resulting from this new legal framework. Last but not least, it may not be well perceived by Member States that have invested a lot on the eIDAS Regulation over the last years to set up notified eID schemes.

Annex 1: Implementation of the eIDAS nodes: State of play

Eurosmart contacted national contact points to conduct this short study on the implementation of the eIDAS nodes. The collected results point towards the need to implement option 1. Some boxes remain empty due to lack of data.

Disclaimer: The study was realised from May to August 2020, the situation might have evolved during this period of time. If you notice an obsolete or inaccurate data, please do not hesitate to report it to us (camille.dornier@eurosmart.com).

eIDAS interconnection: state of play (May-August 2020)

Country	Status of the node	Receiving eIDs from	Sending eIDs to	Additional comments
Austria	In Prod.	Estonia, Germany, Italy, Spain. In progress: Belgium, Croatia, Luxembourg, Portugal.	No notification so far.	
Belgium	In Prod.	Croatia, Estonia, Germany, Italy, Luxembourg, Lithuania, Slovakia, Spain.	No view on what the other countries have implemented.	
Bulgaria	In Prod.	None	No notification so far.	
Croatia	In Prod.	Belgium, Germany, Malta, Netherlands, Slovenia, Sweden, Luxembourg. In progress: Austria, Cyprus, the Czech Republic, Estonia, Spain, Lithuania,	Belgium, Germany, Malta, Netherlands, Slovenia, Sweden, Luxembourg and Norway.	

		Latvia, Poland, Portugal, the UK, Bulgaria, Denmark, Ireland, Italy and Slovakia.		
Cyprus	Under develop.	Testing mode with 6 other Member States.	No notification so far.	Production of the node expected for the summer. Cyprus has an eID scheme with LoA low. Cyprus is in the process of developing a national scheme with LoA high. The eID scheme would be put in place in Q1-Q2 2021. Cyprus will subsequently start the notification process.
Czech Republic	In Prod.	Germany. In the process of integrating other countries according to notified eID schemes.	None.	The Czech eIDAS node is running, but - with regard to the notified eID cards, Czech Republic was doing some adjustments of their eID system at the time of the study. The time needed to adjust this eID system was estimated to several weeks.
Denmark	In Prod.	-	-	
Estonia	In Prod.	Belgium, Croatia, Italy, Germany, Latvia, Luxembourg, Portugal, Spain.	Austria, Belgium, Croatia, Denmark, Finland, Greece, Italy, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Sweden, UK	
Finland	Under develop.	Estonia, Italy, Germany.	No notification so far.	
France	N/A	None	None.	France will pre-notify its eID schemes by the end of 2020 or early 2021. The French eIDAS node is being audited until October 2020. A testing

				phase will follow but remains to be planned.
Germany	In Prod.	No overview because of the decentralised approach.	Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, Greece, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Slovakia, Slovenia, Spain, Sweden, the UK.	The German eIDAS Connectors (receiving nodes) are operated by other parties that are not under German federal administration's direct control. The German team does not know the exact number of eIDAS Connectors in Germany, and, hence could not provide further details on received eIDs. Services that are connected to the eIDAS network, via their eIDAS Connector, are to be accessible by all notified eID means that fall under the mutual recognition obligation. However, the implementation status is not always satisfactory.
Greece	Under develop.	-	-	
Hungary	Under develop.	-	-	
Ireland	Under develop.	-	-	
Italy	In Prod.	Belgium, Croatia, Estonia, Germany, Luxembourg, Portugal, Slovakia, Spain, the UK. In progress: Czech Republic, Latvia, Netherlands.	Austria, Belgium, Croatia, Denmark, Estonia, Finland, Greece, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Slovakia, Slovenia, Spain, Sweden, UK	
Latvia	Under develop.	Germany, Italy, Estonia, Spain, Croatia, Luxembourg, Belgium, Portugal.	Croatia, Spain, Portugal, Italy, Lithuania, Estonia, Luxembourg.	

		In the process of integrating other countries according to the notified eID schemes.		
Lithuania	In Prod.	Germany, Greece, Italy, Latvia, Luxembourg, Portugal, Spain, Sweden. Test with over 18 countries.	None.	eID notified on 21 August 2020. Discussions started with Baltic countries for these countries to accept the Lithuanian eID as soon as possible. Not all Lithuanian service providers accept data of foreign people. This problem is currently being fixed.
Luxembourg	In Prod.	Belgium, Croatia, Estonia, Germany, Italy, Spain.	Austria, Belgium, Croatia, Denmark, Estonia, Italy, Latvia, Malta, the Netherlands, Slovakia, Slovenia, Spain, Sweden, the UK.	
Malta	In Prod.	Belgium, Croatia, Estonia, Germany, Italy, Luxembourg, Portugal, Spain, the UK.	No notification so far.	A date for notification remains to be determined.
Netherlands	In Prod.	Belgium, Croatia, Estonia, Germany, Italy, Luxembourg, Spain.	None so far.	DigiD was notified on 21 August 2020. Using DigiD in other Member States should be possible from August 2021.
Poland	In Prod.	-	-	
Portugal	In Prod.	Belgium, Estonia, Italy, Latvia, Lithuania, Luxembourg, Slovakia, Slovenia, Spain.	Belgium, Estonia, Italy, Latvia, Lithuania, Luxembourg, Slovakia, Slovenia, Spain.	
Romania	Under develop.	None	None	
Slovakia	In Prod.	Belgium, Croatia, Estonia, Germany, Italy, Luxembourg, Portugal, Spain, t In progress: Czech Republic, Denmark, the Netherlands, Poland, the UK.	Belgium, Czech Republic, Italy, Spain.	

Slovenia	In Prod.	-	-
Spain	In Prod.	Belgium, Croatia, Estonia, Germany, Italy, Latvia, Luxembourg, Portugal, Slovakia.	Austria, Belgium, Croatia, Denmark, Estonia, Greece, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Slovakia, Sweden, United Kingdom.
Sweden	In Prod.	Belgium, Croatia, Estonia, Germany, Italy, Luxembourg, Spain.	No notification so far.
United Kingdom	In Prod.	-	-

Obstacles to smooth implementation of eIDAS: a national perspective

A few issues were identified by the national contact points as obstacles to a smooth implementation of eIDAS. Such obstacles are both legislative, e.g. missing elements in the legislation, and technical.

Identity matching

Identity matching was mentioned a few times as a challenge faced by national administrations. It seems to be the biggest problem when it comes to the implementation of eIDAS. Some Member States do not have persistent identifiers – or such persistent identifiers are provided as an optional attribute, which makes it difficult to match the identity data stored in a particular public sector body with the information on the identified/authenticated person received through the process of electronic identification. This renders recognition of foreign identities harder.

Implementing Regulation 2015/1501 establishes that the minimum data set for a natural or legal person shall contain a unique identifier (beside name, surname and birthdate for a natural person, and beside the legal name for a legal person). According to the current technical specifications, the unique identifier is composed as follows:

1. The first part is the Nationality Code of the identifier
    - This is one of the ISO 3166-1 alpha-2 codes, followed by a slash ("/")
2. The second part is the Nationality Code of the destination country or international organization
    - This is one of the ISO 3166-1 alpha-2 codes, followed by a slash ("/")
3. The third part a combination of readable characters
    - **This uniquely identifies the identity asserted in the country of origin but does not necessarily reveal any discernible correspondence with the subject's actual identifier (for example, username, fiscal number etc)**

Example: ES/AT/02635542Y (Spanish eIDNumber for an Austrian SP)

Some national contact points underline that the current legislation is not enough to provide a reliable matching between the physical and digital identity of a person. Clearer technical specifications and more stable identifiers were mentioned as possible solutions to this problem.

National contact points also raised the issue of the lack of relevant attributes for several services. The list of mandatory attributes laid down by Implementing Regulation 2015/1501 is limited, e.g. it does not include the fiscal residence, which hampers the use of eIDAS for some purposes (e.g. Know-Your Customer).

Technical problems

First, different types of implementations (middleware vs proxy) of eIDAS nodes render interoperability and governance more difficult.

Secondly, the trust establishment model was cited as a problematic issue. The configuration of the trust information, metadata and certificates, between the eIDAS nodes must be done manually. This can result in technical problems when interconnecting the eIDAS nodes. At least one national contact point advocated for an automated trust establishment mechanism, such as trust lists for qualified certificates.

Finally, another point raised was the need to upgrade the version of the eIDAS node at much faster pace than expected. New versions of the eIDAS node are frequently released, and there is no information on the release of a future finalised version which could be used for a longer period of time.

Difficult cross-border communication

Cross-border communication was another issue mentioned as an obstacle to smooth implementation. Contact with other Member States to make an eID accepted is not always seamless.

In addition, there is no list of public sector services that can be used through eIDAS authentication for each Member State.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **Huawei**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 3635 | mail contact@eurosmart.com