eIDAS Open Public Consultation

Fields marked with * are mandatory.

1

Introduction

Digital identity enables transactions in the digital world. In a hyper connected world, the ability to establish individual identities of natural persons, legal entities, machines and devices uniquely, accurately, quickly and securely is going to be critical and has a considerable potential for wealth creation.

The COVID-19 crisis clearly demonstrates the need to provide all European citizens and businesses quickly with a universally accepted, trusted digital identity and with trust services such as eSignatures to allow for seamless business continuity in the Single Market and to access to crucial and sensitive public online services such as in eHealth, eGovernment or eJustice. Universally accepted trusted identification and authentication enables effective protection of personal data in the online world. At the same time, it promotes business cases based on a discretionary disclosure of data and creates the conditions for a responsible and accountable management of data and artificial intelligence in society. Using these opportunities contributes to the recovery of the European economy and to the European digital autonomy. The revision of the eIDAS Regulation is therefore part of the Commission's response to the crisis.

With the adoption of the eIDAS Regulation in 2014, the EU broke new ground globally by introducing a first cross-border framework for trusted digital identities and the so-called trust services such as electronic signatures that can be used to sign documents in the online world, much like one signs a document with a pen in the offline world. The eIDAS Regulation is meant to ensure secure and seamless electronic interaction between citizens, businesses and public authorities. This should increase trust in the internal market and make online services more effective. The European Commission is currently evaluating this r e g u l a t o r y   f r a m e w o r k .

The eIDAS Regulation ensures:

- that individuals and businesses can use their own national electronic identification schemes (eIDs) to authenticate when accessing public online services in other EU Member States. This is achieved by establishing an interoperability framework and by enforcing mutual legal recognition of notified schemes;
- the development of a European internal market for electronic Trust Services (electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication) recognised across borders with the same legal status as traditional paper based processes.

The Commission will assess to what extent the eIDAS framework remains fit for purpose, i.e., to deliver the

intended outcomes, results and impacts and whether it is appropriate to modify the scope of the Regulation or its specific provisions, taking into account the experience gained in the application, as well as technological, market and legal developments.

In its Communication on Shaping Europe's Digital Future, published on 19th February 2020, the Commission took the position that universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them. The Commission will consider revising the eIDAS Regulation to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

The aim of this public consultation is to collect feedback on drivers and barriers to the development and uptake of eID and trust services in Europe and on the impacts of the options for delivering an EU digital identity. It targets broad public (e.g. citizens and end-users, including older persons and persons with disabilities) as well as companies directly impacted by the eIDAS Regulation (e.g. trust service providers, identity providers), competent authorities in the Member States, international organisations and concerned stakeholders on the eIDAS framework.

2 About you

* Language of my contribution

○ Bulgarian

○ Croatian

○ Czech

○ Danish

○ Dutch

◉ English

○ Estonian

○ Finnish

○ French

○ Gaelic

○ German

○ Greek

○ Hungarian

○ Italian

○ Latvian

○ Lithuanian

○ Maltese

○ Polish

○ Portuguese

- ○ Romanian
- ○ Slovak
- ○ Slovenian
- ○ Spanish
- ○ Swedish

* I am giving my contribution as
- ○ Academic/research institution
- ● Business association
- ○ Company/business organisation
- ○ Consumer organisation
- ○ EU citizen
- ○ Environmental organisation
- ○ Non-EU citizen
- ○ Non-governmental organisation (NGO)
- ○ Public authority
- ○ Trade union
- ○ Other

* First name

Camille

* Surname

Dornier

* Email (this won't be published)

camille.dornier@eurosmart.com

* Organisation name

255 character(s) maximum

Eurosmart

* Organisation size
- ● Micro (1 to 9 employees)

○ Small (10 to 49 employees)

○ Medium (50 to 249 employees)

○ Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the [transparency register](). It's a voluntary database for organisations seeking to influence EU decision-making.

```
21856815315-64
```

*Country of origin

Please add your country of origin, or that of your organisation.

○ Afghanistan	○ Djibouti	○ Libya	○ Saint Martin
○ Åland Islands	○ Dominica	○ Liechtenstein	○ Saint Pierre and Miquelon
○ Albania	○ Dominican Republic	○ Lithuania	○ Saint Vincent and the Grenadines
○ Algeria	○ Ecuador	○ Luxembourg	○ Samoa
○ American Samoa	○ Egypt	○ Macau	○ San Marino
○ Andorra	○ El Salvador	○ Madagascar	○ São Tomé and Príncipe
○ Angola	○ Equatorial Guinea	○ Malawi	○ Saudi Arabia
○ Anguilla	○ Eritrea	○ Malaysia	○ Senegal
○ Antarctica	○ Estonia	○ Maldives	○ Serbia
○ Antigua and Barbuda	○ Eswatini	○ Mali	○ Seychelles
○ Argentina	○ Ethiopia	○ Malta	○ Sierra Leone
○ Armenia	○ Falkland Islands	○ Marshall Islands	○ Singapore
○ Aruba	○ Faroe Islands	○ Martinique	○ Sint Maarten
○ Australia	○ Fiji	○ Mauritania	○ Slovakia
○ Austria	○ Finland	○ Mauritius	○ Slovenia
○ Azerbaijan	○ France	○ Mayotte	○ Solomon Islands

○ Bahamas	○ French Guiana	○ Mexico	○ Somalia
○ Bahrain	○ French Polynesia	○ Micronesia	○ South Africa
○ Bangladesh	○ French Southern and Antarctic Lands	○ Moldova	○ South Georgia and the South Sandwich Islands
○ Barbados	○ Gabon	○ Monaco	○ South Korea
○ Belarus	○ Georgia	○ Mongolia	○ South Sudan
● Belgium	○ Germany	○ Montenegro	○ Spain
○ Belize	○ Ghana	○ Montserrat	○ Sri Lanka
○ Benin	○ Gibraltar	○ Morocco	○ Sudan
○ Bermuda	○ Greece	○ Mozambique	○ Suriname
○ Bhutan	○ Greenland	○ Myanmar /Burma	○ Svalbard and Jan Mayen
○ Bolivia	○ Grenada	○ Namibia	○ Sweden
○ Bonaire Saint Eustatius and Saba	○ Guadeloupe	○ Nauru	○ Switzerland
○ Bosnia and Herzegovina	○ Guam	○ Nepal	○ Syria
○ Botswana	○ Guatemala	○ Netherlands	○ Taiwan
○ Bouvet Island	○ Guernsey	○ New Caledonia	○ Tajikistan
○ Brazil	○ Guinea	○ New Zealand	○ Tanzania
○ British Indian Ocean Territory	○ Guinea-Bissau	○ Nicaragua	○ Thailand
○ British Virgin Islands	○ Guyana	○ Niger	○ The Gambia
○ Brunei	○ Haiti	○ Nigeria	○ Timor-Leste
○ Bulgaria	○ Heard Island and McDonald Islands	○ Niue	○ Togo
○ Burkina Faso	○ Honduras	○ Norfolk Island	○ Tokelau
○ Burundi	○ Hong Kong	○ Northern Mariana Islands	○ Tonga

- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus

- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia

- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy

- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen

○ Czechia	○ Lebanon	○ Saint Helena Ascension and Tristan da Cunha	○ Zambia
○ Democratic Republic of the Congo	○ Lesotho	○ Saint Kitts and Nevis	○ Zimbabwe
○ Denmark	○ Liberia	○ Saint Lucia	

* Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

○ **Anonymous**

Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.

◉ **Public**

Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

☑ I agree with the [personal data protection provisions](#)

3 General questions about electronic identification (eID)

Individuals and businesses can use under eIDAS their own national electronic identification schemes (eIDs) (e.g. government issued eID cards/Apps) to authenticate when accessing public online services in other EU Member States. This is achieved by establishing interoperability of different national eIDs and enforcing mutual legal recognition of notified schemes.

In the context of this consultation, an eID is a means of electronic identification (it ascertains "who you are") and authentication (it proves that "you are who you say you are") issued by an organisation to be used in a wide range of online services provided by different organisations. A national identity card that can be used in eGovernment services provided by several agencies, or a social network login account that you can use in several online shops would qualify as eIDs, but the credentials given to you by your bank to access exclusively their online banking services would not.

* Do you have an electronic identification means (eID) which can be used to access online services?

◉ Yes

○ No

◉ Don't know

What type(s) of eID do you use?

☑ eIDs provided by my government or other public authority

☐ Personal user accounts provided by social networks or online platforms

☐ eIDs provided by other private sector organisations (e.g. trust service providers, banks, mobile operators)

☐ Other

* How often do you use your eID to access or use online services?

◯ Everyday

◉ Once or twice a week

◯ Once a month

◯ Less than once a month

◯ Never

◯ I don't know / no opinion

For what services do you use or would you like to use your eID?

	I already use my eID	I would like to use my eID
Public services (e.g. fill in your tax form, request certificates, ...)	◉	◯
Utility services (energy, water supply), telecom services	◯	◉
Medical (eHealth) services	◉	◯
Open a bank account	◯	◉
Shop online	◯	◉
Access online platforms (e.g. social networks, my online streaming account)	◯	◉
Other	◯	◉

* Have you found the availability of the eID means or the electronic trust services (e.g. electronic signature) particularly useful during the lockdown measures introduced due to the COVID-19 crisis?

◉ Yes

◯ No

If yes, what solutions have you used and for what services?

	eIDs provided by my government or other public authority	eIDs provided by other private sector organisations	Personal user accounts provided by social networks or online platforms	Electronic signature	Other electronic trust services (e.g. eSeals, Time Stamps)
Online public services (eGovernment)	☐	☐	☐	☐	☐
eHealth services	☐	☐	☐	☐	☐
Financial services	☐	☐	☐	☐	☐
COVID-19 specific online services (e.g. reporting symptoms, test results, requesting benefits/allowance)	☐	☐	☐	☐	☐
Concluding contracts remotely	☐	☐	☐	☐	☐
Online shopping	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐

If Other, please specify:

The eIDAS Regulation ensures that individuals and businesses can use their own national electronic identification schemes (eIDs) to authenticate when accessing public online services in other EU Member States. This is achieved by establishing interoperability and enforcing mutual legal recognition of the so-called notified schemes. The list of notified national eID schemes is published here.

*Are you aware that you can use one of the notified national eID schemes to access online public services in other EU Member States?

- ◉ Yes
- ○ No

*If you have one of these notified eIDs - have you ever used it to access online services in another EU Member State than your country of residence?

- ○ Yes
- ◉ No
- ○ Don't know

*How important for you is the ability to use your eID to access public services in other EU Member States?

- ◉ Very important
- ○ Somewhat important
- ○ Not really important
- ○ Don't know

*How important for you is to have a secure single digital ID that could serve for all online services (both public and private) that provides you with the control over the use of your personal data?

- ◉ Very important
- ○ Somewhat important
- ○ Not really important
- ○ Don't know

*How important for you is the ability to use your eID on your mobile phone?

○ Very important

○ Somewhat important

○ Not really important

○ Don't know

4 General questions about electronic trust services

The eIDAS Regulation aimed to create a European internal market for electronic trust services - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based processes.

* Have you ever used electronic trust services (e.g. eSignature, eSeal or Timestamp)?

● Yes

○ No

○ Don't know

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The availability and offer of electronic trust services in the EU is **sufficient**.	○	●	○	○	○	○
* The eIDAS Regulation needs to be strengthened as a response to the COVID-19 crisis	○	●	○	○	○	○
* Providing the same legal effect to electronic trust services (e.g. qualified e-signature is equivalent to handwritten one) helped increase their **take-up**.	●	○	○	○	○	○
* I feel more comfortable and confident to use electronic trust services now compared to five years ago.	●	○	○	○	○	○

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* Public administrations should should roll out more public services, making better use ofelectronic trust services in their contact with citizens and businesses.	◉	◯	◯	◯	◯	◯

*Do you think that additional trust services should be regulated at EU level?

- ◯ Yes
- ◉ No
- ◯ Don't know

5 Specific questions on electronic identity (eID)

To answer these more specific questions would require a certain knowledge of the eIDAS Regulation.

*Would you like to answer more specific questions about rules on eID under the eIDAS Regulation and the future digital identity?

- ◉ Yes
- ◯ No

*Are you replying as:

- ◯ End-user of eID (e.g. citizen, company)
- ◯ Provider of online services (public sector)
- ◯ Provider of online services (private sector)
- ◯ Provider of Identity and Authentication solutions and / or technologies and IT solutions in this area (e.g. software, hardware, services)
- ◯ Think tank, research, academic institution or individual expert
- ◉ Trade/business/professional association or other interest representation organisation
- ◯ Public policy maker
- ◯ Non-governmental organisation
- ◯ Other

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The **number of online public services** to be accessed in a cross-border context by using one of the published national eID schemes has considerably increased due to eIDAS.	○	●	○	○	○	○
* The eIDAS Regulation provides an **adequate legal framework** for cross-border electronic identification in Europe.	○	●	○	○	○	○
* The eIDAS legal framework for cross-border electronic identification in Europe.should be strengthened as a response to the COVID-19 crisis.	○	●	○	○	○	○
* The scope of the eIDAS Regulation should be extended to provide a **level playing field** for the private economic actors operating in the field of electronic identification.	○	○	○	●	○	○
* The **interoperability framework** established by the eIDAS is optimal and supports sufficiently the mutual recognition of the eID schemes.	○	○	●	○	○	○

Do you agree that the use of electronic identification to access online public services across borders contributes to:

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* Enhancing user friendliness	●	○	○	○	○	○
* Saving time	●	○	○	○	○	○
* Saving money	●	○	○	○	○	○
* The simplification of the administrative procedure	●	○	○	○	○	○
* An increase of service quality	●	○	○	○	○	○
* An increase of service security	●	○	○	○	○	○
* The protection of personal data	●	○	○	○	○	○

* The better access to services in another EU country	◉	○	○	○	○	○
* An increase of the certainty on the authenticity of the users' identity	◉	○	○	○	○	○
* Enhancing clarity on the liability of the provider of the electronic identity	◉	○	○	○	○	○
* The access to services to a larger group of users thanks to the uptake of eID	◉	○	○	○	○	○

* In your opinion, are there currently any factors limiting the cross-border use of electronic identification?

- ◉ Yes
- ○ No
- ○ Don't know

* What are the factors limiting the cross-border use of electronic identification?

- ☐ Lack of awareness
- ☐ No need for it / Not relevant
- ☑ Limited number of [notified]() eID schemes
- ☐ Lack of availability of relevant public services
- ☐ Lack of trust
- ☐ Preference for paper-based solutions or face-to-face interactions
- ☐ Too expensive
- ☐ Too complicated / not user-friendly / accessibility barriers for persons with disabilities
- ☐ Privacy concerns
- ☑ Legal obstacles (example: face-to-face interaction required by national legislation)
- ☑ Limited scope of eID schemes notified under the eIDAS Regulation (governmentally issued/recognised eIDs only)
- ☐ Suboptimal interoperability framework
- ☐ Other

* To what extent do you agree that the eIDAS Regulation has achieved its objectives with regard to electronic identification?

The objectives were: to enhance trust in electronic transactions in the internal market by providing a common foundation for secure and seamless electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public online services in the EU.

The Regulation ensures that individuals and businesses can use their own national electronic identification schemes (eIDs) to authenticate when accessing public online services in other EU Member States, by establishing interoperability and enforcing mutual legal recognition of notified schemes.

○ Strongly agree

○ Agree

◉ Neither agree nor disagree

○ Disagree

○ Strongly disagree

○ I don't know / no opinion

Please elaborate on how the eIDAS Regulation has/not achieved its objectives with regard to electronic identification.

Do not hesitate to further elaborate on your previous answers.

eIDAS has already achieved a lot by allowing mutual recognition to be implemented in over half of the Member States. A majority of notified eID schemes were notified at level "High", which shows that Member States opted for highly trustworthy eIDs. Such eIDs are mostly based on legal identity. This is a major step forward to increase trust in the digital world.

In addition, the decentralised approach (eIDAS nodes) has proven to be effective. The "single point of failure" was avoided, as shown by two security breaches in 2019 which impacted two nodes but without putting at risk the complete eIDAS nodes infrastructure.

However, the full potential of eIDAS has not been reached. Further enhancements and extended usages of eIDs under eIDAS should be fostered. These improvements require technical optimisations (implementing acts, standards, guidance) rather than a revision of the eIDAS Regulation.

1)   Consolidating the eIDAS framework

The main factor limiting the cross-border use of electronic identification is the fact that not all Member States have notified an eID scheme to date. Only 50% of EU citizens are currently covered by a notified eID. Member States should be strongly encouraged to notify at least one eID scheme of LoA "Substantial" or "High" within a maximum delay. Therefore, the entire EU population would be covered by the mutual recognition principle.

A second limiting factor is the imperfect usability of notified eIDs falling under the mutual recognition obligation. The application of this obligation is not always satisfactory. It is sometimes due to technical difficulties encountered by Member States to set up and maintain their eIDAS nodes.

A third limiting factor relates to diverging rules among Member States. This is the case for Levels of Assurance (LoA) Criteria (Implementing Regulation 2015/1502), which are too vague and leave too much space for interpretation. The lack of clarity of these criteria (1) impedes the interoperability of eID schemes and above all (2) prevents Member States from sharing a common understanding of their meaning. A legally binding document is needed to bring convergence.

In addition, harmonisation of certifications would 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.

Last but not least, more guidance from the cooperation network is needed. Guidance should be given on the conformity of a proposed eID scheme (not yet notified) with eIDAS, especially with the criteria laid down in Article 7. This could help to speed up the overall notification process (pre-notification, peer review, notification). More guidance is also needed on biometry, optical authentication of identity documents and identity derivation from an identity document.

2)   Establishing a new framework for private eID schemes

There is a clear market need for private actors to use privately issued eIDs. However, the eIDAS Regulation should be left untouched as reopening the legal act might threaten years of efforts and accomplishment. Instead, a dedicated legislative regulation should be adopted for:
•   private eIDs and attribute providers;
•   private services (also called relying parties) accepting them.

Private eID solutions should build on legal identities delivered by Member States or notified eIDs under eIDAS at level "Substantial" or "High". More particularly, private eID providers should be encouraged to rely on identity cards which benefit from a wide use, high quality and harmonised enrolment across the EU. 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.

Likewise, this new dedicated act should reuse the definition of LoA given by eIDAS and should leverage on certification schemes prepared under the Cybersecurity Act -to demonstrate that the requirements of a given LoA are met.

Furthermore, the European Commission should mandate a strong identity proofing to be performed by the eID provider under the future framework. In addition, the usage of biometric comparison technologies for identity proofing should not be hampered by unnecessary or excessive regulation.

There is also a need for specific requirements on data protection for the private sector. These requirements should strengthen Europe's sovereignty. Data should be stored and processed only on EU territory and only by European entities.

Finally, the use of private eID solutions requires an adequate liability framework, which provides guarantees to entities accepting such eIDs. Accepting entities should not be held liable in case of fraud and subsequent damage. It should be established that eID providers are those liable in case of fraud.

* In your opinion, should the eIDAS Regulation or its implementation be improved?
- ◉ Yes
- ○ No
- ○ Don't know

Which of the following corrective actions should be taken?

- ☑ Adopting guidelines to improve legal coherence and consistency
- ☑ Further harmonisation through requirements established in secondary legislation (implementing acts), standardisation and the introduction of certification to the advantage of particularly convenient and secure solutions
- ☐ A shift from voluntary to mandatory notification of national eID schemes
- ☐ An obligation for Member States to make authentication available to the private sector
- ☐ Introduction of new private sector digital identity trust services for identification, authentication and provision of attributes
- ☐ Introduction of an obligation for the public sector to recognise attributes, credentials and attestations issued in electronic form by trust service providers and public authorities registered as authoritative sources
- ☑ Introduction of an obligation for the private sector to recognise trusted digital identities: eIDs notified under eIDAS and trust services for identification, authentication and provision of attributes
- ☑ Provision of identification for non-human entities (e.g AI agents, IoT devices)

*In your opinion, should there be a single and universally accepted European digital identity scheme, complementary to the national publicly issued electronic identities, allowing for a simple, trusted and secure possibility for citizens to identify themselves online?
- ◯ Yes
- ◯ No
- ◉ Don't know

*Which possible dis-advantages of such single and uniform European digital identity scheme are you concerned of?
- ☑ Complexity of set-up and Governance
- ☐ Lack of flexibility to adapt to technological developments and changing user needs
- ☑ Overlap with existing solutions
- ☑ Discouragement of innovation and investments into alternative eID solutions
- ☐ State surveillance concerns
- ☑ Set up and operational costs
- ☑ Other

Please specify and/or set-out other possible dis-advantages:

> Setting up such a European digital identity scheme would take a long time, probably more than five years. The focus should be on improving the implementation of eIDAS.

Please share any additional statements, documents, position papers concerning eID under the eIDAS framework and the future of digital identity.

c48899ca-067a-439e-8fe7-5add01498a45/2020_09_03_Eurosmart-feedback-EUid.pdf
4b06e979-44b4-4ab2-9bae-dd30100f298b/Eurosmart_study_eIDAS_nodes_interconnection_final.pdf

6 Specific questions on trust services

To answer these more specific questions would require a certain knowledge of the eIDAS Regulation.

* Would you like to answer more specific questions about trust services and the eIDAS Regulation?
- ◉ Yes
- ○ No

* Are you replying as:
- ○ User of electronic trust services (e.g. citizen, company, public or private service provider)
- ○ Provider of electronic trust services
- ○ Supplier of technologies and IT solutions for electronic trust services (e.g. software, hardware, services)
- ○ Think tank, research, academic institution or individual expert
- ◉ Trade/business/professional association or other interest representation organisation
- ○ Public policy maker
- ○ Supervisory body
- ○ Conformity assessment body
- ○ Non-governmental organisation
- ○ Other

* Which of the following trust services are relevant to you?
The selected trust services will trigger separate questions for each trust service regulate under eIDAS.

☑ Electronic signature

☑ Electronic seal

☑ Electronic timestamp

☑ Electronic registered delivery service

☑ Website authentication

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The eIDAS Regulation increased the **availability** of electronic trust services in the EU.	◉	○	○	○	○	○
* The level and scope of **governance and supervision** of electronic trust services established under the eIDAS Regulation are **adequate** to ensure harmonisation at EU level.	○	○	◉	○	○	○
* The eIDAS Regulation has put in place conditions conducive to trust services based on **decentralised solutions** (including through distributed ledger technologies).	○	◉	○	○	○	○
* The **legal effect** provided to trust services by the eIDAS Regulation (e.g. qualified e-signature is equivalent to handwritten one) helped increase their **admissibility** in legal proceedings.	◉	○	○	○	○	○
* The cross-border **legal effect** provided to trust services by the eIDAS Regulation helped increase their **take-up**.	◉	○	○	○	○	○
* The **assessment** procedure for becoming a **qualified** trust service provider is **adequate**.	○	○	○	◉	○	○

* The eIDAS Regulation is a more **effective tool** to regulate trust services than actions taken at national level.	◉	○	○	○	○	○
* The provisions of the eIDAS Regulation on trust services have **enhanced trust** in electronic transactions.	◉	○	○	○	○	○
* **Repealing the eIDAS** Regulation would have negative consequences for trust services in Europe.	◉	○	○	○	○	○

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The eIDAS Regulation has increased the **availability** of **electronic signature** in the EU.	◉	○	○	○	○	○
* The **availability** of **electronic signature** in the EU should be extended as a result of the COVID-19 crisis	○	◉	○	○	○	○
* The **use** of **electronic signature** has increased in Europe for the last 3 years.	○	◉	○	○	○	○
* The eIDAS regulatory framework creates a **level playing field** for **electronic signature** in Europe.	◉	○	○	○	○	○
* The eIDAS Regulation does not hinder **technological developments** in the **electronic signature** market.	○	◉	○	○	○	○
* Citizens, businesses and public administrations in Europe can **effectively benefit from the advantages** of **electronic signature**.	◉	○	○	○	○	○
* The eIDAS Regulation has ensured **interoperability** of **electronic signature**.	○	◉	○	○	○	○

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The eIDAS Regulation has increased the **availability** of **electronic seal** in the EU.	○	○	○	○	○	●
* The **availability** of **electronic seal** in the EU should be extended as a result of the COVID-19 crisis	○	○	○	○	○	●
* The **use** of **electronic seal** has increased in Europe for the last 3 years.	○	○	○	○	○	●
* The eIDAS regulatory framework creates a **level playing field** for **electronic seal** in Europe.	○	○	○	○	○	●
* The eIDAS Regulation does not hinder **technological developments** in the **electronic seal** market.	○	○	○	○	○	●
* Citizens, businesses and public administrations in Europe can **effectively benefit from the advantages** of **electronic seal**.	○	○	○	○	○	●
* The eIDAS Regulation has ensured **interoperability** of **electronic seal**.	○	○	○	○	○	●

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The eIDAS Regulation has increased the **availability** of **electronic timestamp** in the EU.	○	○	○	○	○	●

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The **availability** of **electronic timestamp** in the EU should be extended as a result of the COVID-19 crisis	○	○	○	○	○	●
* The **use** of **electronic timestamp** has increased in Europe for the last 3 years.	○	○	○	○	○	●
* The eIDAS regulatory framework creates a **level playing field** for **electronic timestamp** in Europe.	○	○	○	○	○	●
* The eIDAS Regulation does not hinder **technological developments** in the **electronic timestamp** market.	○	○	○	○	○	●
* Citizens, businesses and public administrations in Europe can **effectively benefit from the advantages** of **electronic timestamp**.	○	○	○	○	○	●
* The eIDAS Regulation has ensured **interoperability** of **electronic timestamp**.	○	○	○	○	○	●

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The eIDAS Regulation has increased the **availability** of **electronic registered delivery service** in the EU.	○	○	○	○	○	●
* The **availability** of **electronic registered delivery service** in the EU should be extended as a result of the COVID-19 crisis	○	○	○	○	○	●
* The **use** of **electronic registered delivery service** has increased in Europe for the last 3 years.	○	○	○	○	○	●

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The eIDAS regulatory framework creates a **level playing field** for **electronic registered delivery service** in Europe.	○	○	○	○	○	◉
* The eIDAS Regulation does not hinder **technological developments** in the **electronic registered delivery service** market.	○	○	○	○	○	◉
* Citizens, businesses and public administrations in Europe can **effectively benefit from the advantages** of **electronic registered delivery service**.	○	○	○	○	○	◉
* The eIDAS Regulation has ensured **interoperability** of **electronic registered delivery service**.	○	○	○	○	○	◉

To what extent do you agree or disagree with the following statements?

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* The eIDAS Regulation has increased the **availability** of **website authentication** in the EU.	○	○	○	○	○	◉
* The **availability** of **website authentication** in the EU should be extended as a result of the COVID-19 crisis	○	○	○	○	○	◉
* The **use** of **website authentication** has increased in Europe for the last 3 years.	○	○	○	○	○	◉
* The eIDAS regulatory framework creates a **level playing field** for **website authentication** in Europe.	○	○	○	○	○	◉
* The eIDAS Regulation does not hinder **technological developments** in the **website authentication** market.	○	○	○	○	○	◉

* Citizens, businesses and public administrations in Europe can **effectively benefit from the advantages** of **website authentication**.	○	○	○	○	○	●
* The eIDAS Regulation has ensured **interoperability** of **website authentication**.	○	○	○	○	○	●

* Please specify which additional trust services should be regulated at EU level:

- ☐ Electronic identification and authentication
- ☐ Provision of trusted attributes (uniquely linked to a verified identity – e.g. proof-of-age, credentials – professional qualifications, entitlements – Know-Your-Customer)
- ☐ eArchiving
- ☐ Delegated management of signature keys
- ☐ Operation of distributed ledgers storing electronic evidences
- ☐ Operation of identity hubs storing personal data of behalf of the users
- ☐ Other
- ☑ No need for additional trust services, the current scope is sufficient

Do you agree that the use of trust services established by the eIDAS Regulation contributes to:

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	I don't know / no opinion
* Enhancing user friendliness	●	○	○	○	○	○
* Saving time	●	○	○	○	○	○
* Saving money	●	○	○	○	○	○
* The simplification of the administrative procedure	●	○	○	○	○	○
* An increase of service quality	●	○	○	○	○	○
* An increase of service security	●	○	○	○	○	○
* The protection of personal data	●	○	○	○	○	○

* Ensuring legal certainty	⦿	○	○	○	○	○

* Do you think the legal effect provided to electronic documents by the eIDAS Regulation has effectively increased their take-up and admissibility in legal proceedings?

Art. 46 of the eIDAS regulation states that "An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form."

- ⦿ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree
- ○ I don't know / no opinion

* In your opinion, are there any factors limiting the use of electronic trust services?

- ⦿ Yes
- ○ No
- ○ Don't know

* What are the factors limiting the use of electronic trust services?

- ☑ Lack of awareness
- ☐ No need for it / Not relevant
- ☑ Lack of availability for relevant services
- ☑ Lack of trust or fraud concerns
- ☐ Preference for paper-based solutions or face-to-face interactions
- ☐ Too expensive
- ☐ Too complicated / not user-friendly / accessibility barriers for persons with disabilites
- ☐ Privacy concerns
- ☐ Not enough legal certainty
- ☐ Other

* To what extent do you agree that the eIDAS Regulation has achieved its objectives with regard to electronic trust services?

The objectives were: to seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure and seamless electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the EU.

The Regulation ensures the development of a European internal market for electronic Trust Services (electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication) recognised across borders with the same legal status as traditional paper based processes.

- ◉ Strongly agree
- ○ Agree
- ○ Neither agree nor disagree
- ○ Disagree
- ○ Strongly disagree
- ○ I don't know / no opinion

Please elaborate how the eIDAS Regulation has/not achieved its objectives with regard to electronic trust services.

Do not hesitate to elaborate on your previous answers.

> The trust services part of the eIDAS Regulation is a key achievement: worldwide players such as ADOBE or Global Sign now propose trusted solutions for the public at large.
>
> However, harmonisation of the market has not been fully achieved. Some implementing acts lack of clarity, hence leading to diverging interpretations and market fragmentation. More precisely, there is a lack of harmonisation regarding the conditions to be met to issue qualified certificates for Trust Services (Article 24 (1) of eIDAS). There is also a need for a common accreditation process for Conformity Assessment Bodies.
>
> In addition, the following particular points deserve improvement:
>
> Qualified Signature Creation Device:
> When it comes to server-based QSCD, the provisions of Implementing Act 2016/650 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.
>
> Qualified Web Authentication Certificate (QWAC):
> There is a clear reluctance of W3C and world-class internet browsers to integrate EU certificates.

How could the eIDAS Regulation or its implementation be improved with regard to trust services?

> Eurosmart recommends the following measures:
>
> 1) Make use of standards
>
> 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 foster the use of notified eID services by trusted services.
>
> 2) Prepare guidance on conditions of issuance of qualified certificates
>
> 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.

3) QSCD: complement Implementing Act 2016/650

Eurosmart also recommends improving Implementing Act 2016/650 laying down requirements for security assessment of QSCD. 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).

In addition, guidance on national procedures for smartcard based QSCD should be issued as such procedures considerably diverge from one Member State to another.

4) Harmonise the accreditation process for CABs

Eurosmart recommends harmonising the accreditation process for CABs, based on ETSI EN 319 403.

5) Promote the use of EU QWAC

The use of EU QWAC should be fostered, which requires to overcome the reluctance of W3C and internet browsers. This is more than a technical matter but also an issue of digital sovereignty. EU QWAC should be the prerequisite for the EU online trust. It should also be the basis for PSD2 web certificates.

Please share any additional statement, document, position paper regarding trust services and eIDAS.

The maximum file size is 1 MB
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Contact

CNECT-H4@ec.europa.eu