# Identification and Trust Techniques Compatible with eIDAS Regulation

Stefan Mocanu[1](✉), Ana Maria Chiriac[2], Cosmin Popa[2],
Radu Dobrescu[1], and Daniela Saru[1]

[1] University Politehnica of Bucharest, Splaiul Independentei 313, Bucharest, Romania
stefan.mocanu@upb.ro
[2] Ingenios.ro, George Constantinescu 2C, Bucharest, Romania

**Abstract.** This study presents the current situation (starting with January 2015) related to EU Regulation eIDAS. eIDAS represents the latest EU initiative to build a common framework for electronic identification and trust services. It was the intention of European Council to elaborate and impose a minimal legislation which should guarantee compatibility and interoperability of national identification and trust systems while still allowing the existence of local legal flavors. It is expected that eIDAS will offer safer interactions between various entities (such as private enterprises, public enterprises, citizens, administration) thus contributing to the growth of European market and the improvement of cross-border transactions. Exposure of the current state is combined with suggestions and discussions about improvements to the former eID resulting from the new regulation. A section on the implementation of interoperability framework in some member states gives a first insight into the work which will be required in the next few years for completing the implementation. This paper presents a thorough review of the main identification and trust techniques in eIDAS and the differences to previous or more local similar frameworks.

**Keywords:** eIDAS · eID · Trust · User identification · Interoperability · Electronic signature · Remote signing

## 1 Introduction

### 1.1 What Is eIDAS?

The EU eIDAS (Electronic ID and Trust Services) regulation [1] has been developed to support the existence of a single European market and secure electronic commerce. For organizations making online transactions with European citizens, the Regulation brings not only significant opportunities but also raises many new requirements.

EIDAS imposes standards for electronic identity, authentication and electronic signature. The main purpose is to encourage and support e-commerce by introducing measures to increase its security. EIDAS replaces an old European Commission directive. It is the 1999/93/EC Directive which regulates the electronic signature and has been implemented in many EU countries. As a result, all national implementations related to the electronic signature need to be re-evaluated in order to comply with

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 656–665, 2019.
https://doi.org/10.1007/978-3-030-21373-2_55

eIDAS. Unlike the Directive governing the use of electronic signatures, eIDAS has been developed in the form of a Single Regulation, which implies the existence of a single set of rules applicable to all EU countries [1, 2].

The European Council requested the Commission to create a digital single market [9, 13] by 2015, with the aim of rapid progress in the digital economy, but also because legal certainty is absolutely necessary for both citizens and businesses before they interact digitally. Figure 1 presents an overview of eIDAS framework.

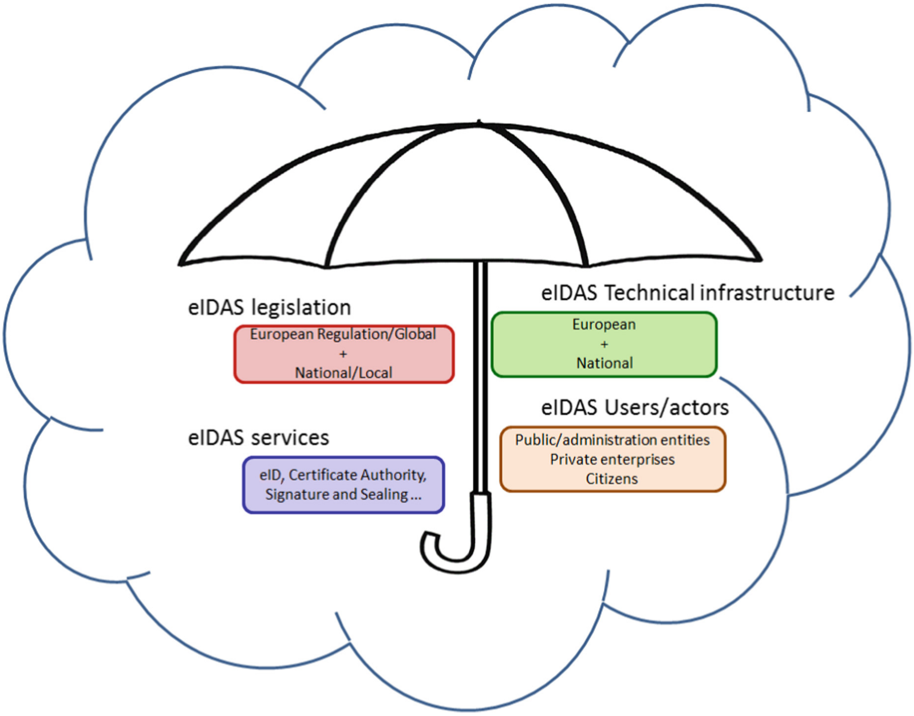

**Fig. 1.** eIDAS framework

In the previous figure, one can identify the most important components of eIDAS environment. The Regulation itself along with other European normative acts will ensure the compatibility and interoperability of all local or national subsystems. At this level, other mandatory aspects are decided. It is the case of building and maintaining a global list of trust service providers (or TSPs) or issuing technical infrastructure requirements (for example: the format of the electronic signature or the functionality of hardware devices used for generating signatures or seals). It is also the case of amending and/or adopting various standards elaborated by industry or R&D entities to cover the requirements of the Regulation. Another component of the eIDAS legislation is given by national/local legislation. The restrictions, in this case, demand that national requirements cannot be lower than global ones if the interaction with a fully compliant eIDAS entity is aimed.

The Digital Single Market features digital identification (eID) and e-Trust Services (eTS). The old directive has led to a confusing situation with regard to the multiple types of signatures of individuals and their verification methods when dealing with the issue of interaction with other parts of each Member State of the European Union.

Thus, the purpose of the regulation is that both individuals and legal entities can use their national electronic identity (eID) in any of the EU Member States to access various government services and to be able to make secure electronic transactions, taking advantage of their rights in all Member States [3].

The eIDAS regulation applies both to government entities and to private companies offering online services to EU citizens who recognize or use elements such as electronic identity, authentication, or electronic signature. For this reason, all entities in question must be able to recognize the electronic signature formats as well as the electronic identities of EU citizens, regardless of their country of origin.

These restrictions and provisions apply to services related to: tax returns (or taxes), insurance contracts, bank contracts, medical or pharmaceutical records or commercial relationships between private companies. Although on November 25th 2018, the EU leaders signed the final agreement for BREXIT [4] it is expected that UK will make efforts to be part of eIDAS environment [5] just like other non-EU countries such as Switzerland [6], Iceland or Norway [7].

## 1.2 Current State of Implementation in EU

At EU level, there are entities whose responsibility is to implement this regulation and secondary legislation has been developed to that end. Therefore, according to the Commission document, the situation at Union level is as follows:

- There are 9 member states that have defined the accreditation scheme for digital certificate providers according to the standards in force (ISO 17065/ETSI EN 319403). These states are: Spain, Belgium, Czech Republic, Austria, Slovakia, Luxembourg, Italy, Poland and Latvia.
- 15 of the member countries already have the national legislation needed to implement eIDAS. These countries are: Sweden, Estonia, Latvia, Finland, Austria, Croatia, Belgium, Malta, Poland, Slovakia, Spain, Netherlands, Czech Republic, Italy and Slovenia
- Among the member countries, 3 are in the process of developing the necessary legislation: Luxembourg, Lithuania and Germany
- Instead, Romania (along with Portugal, Greece, Bulgaria, Hungary and Ireland) is among the 6 countries where there is no detailed information on the implementation stage of eIDAS.

Although the Regulation does not require a national law to adopt the legislative decision, there are certain responsibilities that each member state of the Union has, responsibilities that need to be achieved by internal legislation. These include setting means for identifying citizens, defining sanctions and appointment of a supervisory body that will define how to check the providers and help cooperation with other Member States.

## 2 Essentials of eIDAS

There are two essential aspects of eIDAS Regulation. The first part is related to the identification services of an entity and deals with the electronic identification schemes. The second part addresses the requirements for eIDAS trust services, including e-signature, web authentication and other e-mail services.

Much of the eIDAS Regulation is focused on requirements for electronic signatures, as set out in Directive 1999/93/EC. A simplified eIDAS architecture is presented in Fig. 2.

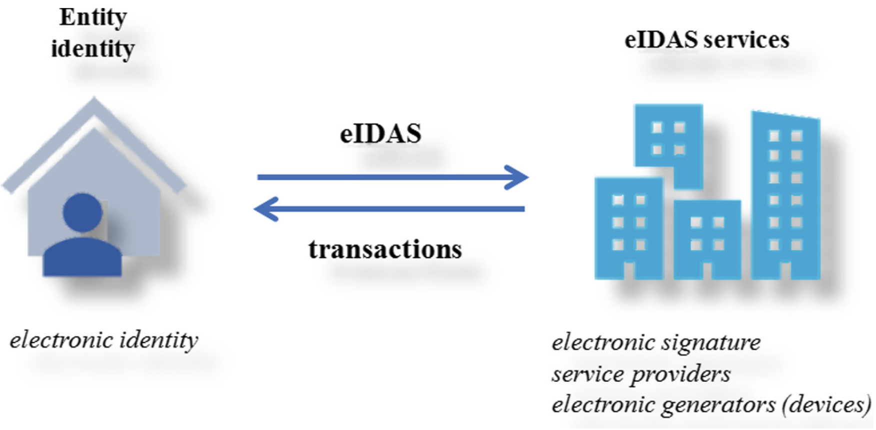

**Fig. 2.** Simplified eIDAS architecture

As depicted in the previous figure, there are 3 key elements related to the eIDAS working environment [8]. First is related to electronic signature and aims to define a structure and the format of the electronic signature as well as the means to place the signature in various document formats. The second is related to Trust Service Providers (TSPs) which are certified entities that can provide the necessary information to develop and support trust services. The third is related to various hardware devices (hardware security module - HSM) that will be used to generate secure electronic signatures. Since these devices will be manipulated by regular users, they must be reliable, easy to use and user friendly.

Figure 3 presents a possible scenario for integrating eID with trust services as presented in eIDAS.

Figure 3 describes the following situation: Ion is a Romanian citizen that is using the services of a German bank. When logging on the e-banking application, Ion's e-identity must be confirmed. After this, Ion can fill banking documents but, in order for these to become effective, they must be signed via a Qualified Trust Service Provider. Based on Ion's interactions with the National Identity Provider and the

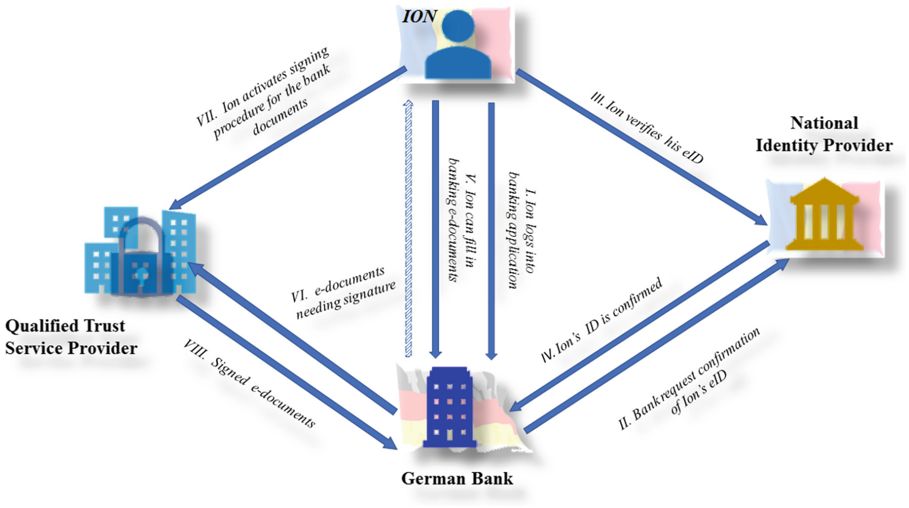
ION
National
Identity Provider
Qualified Trust
Service Provider
German Bank
I. Ion logs into banking application
II. Bank request confirmation of Ion's eID
III. Ion verifies his eID
IV. Ion's ID is confirmed
V. Ion can fill in banking e-documents
VI. e-documents needing signature
VII. Ion activates signing procedure for the bank documents
VIII. Signed e-documents

**Fig. 3.** eID and trust services in eIDAS

Qualified Trust Service Provider, he can use a third's party services (in this case, a bank) without needing additional means (such as a token) to authenticate. This scenarios has a lot of advantages since it can be easily replicated and scaled to an undefined number of relations without the need for the client to use supplemental eID and trust services. In other words, it is easy to avoid the situation in which a client works with several banks, for example, and is forced to carry with him and use all the time many tokens. This is very close to "one size fits all" philosophy.

## 2.1 User Identification and Trust in eIDAS

### Electronic Identification (e-Identification or eID)

With the increase of online services now available even in remote regions, methods of uniquely identifying users had to be developed. It is the case of eID which must ensure secure access to online services and electronic transactions made by each individual. eID maps the virtual presence of a person to his or her physical identity so this will be allowed to use various online services. Until now, existing eIDs across Europe could not be used in other countries but the one they were issued in. Lack of an unitary legislation framework obstructed or, at least, did not facilitate cross border transactions, banking or healthcare transactions or other similar processes between entities located in different countries [9]. eIDAS Regulation comes to fix this problem by giving the eIDs the legal validity for cross-border transactions [11, 12] and allowing them to have the same legal status as traditional paper-based processes.

Previous aims and scopes of eIDs are not only preserved but also extended in eIDAS. The user must benefit from a fast, easy and secure access to electronic services regardless of their supplier (that can be local or national administrative entities [18], public or private enterprises, individuals etc.) under a strict protection of his personal data. The extensions refer to accessing transnational services that may include: European wide identity (which will improve frequent border crossing based transactions), European travel or health insurance (which will reduce time wasting and formalities in case of critical events), banking (as presented in Fig. 3), business and many other situations in which various short or long term exchanges and transactions. Let's take, for example, the case of students that are involved in programs like ERASMUS. Today, in many European countries, for these students temporary local ID cards are issued. Once eIDAS will be fully operational, these formalities will no longer be necessary, saving a lot of time and resources. In this respect, a survey [2] was initiated by the European Commission in May 2017.

Although the electronic identification of the citizen musts be done by their national authority, eIDAS Regulation imposes that electronic IDs of all EU citizens must be recognized in all EU countries, regardless their place of issue. In this respect, eIDAS regulation does not aim to level national standards on identity management so it allows different eID methods as long as they are interoperable. These provisions will apply to government services and any other services that rely on identities issued by national authorities. For these reasons, there is more pressure on the public entities and less to the private entities since the latter will only need to use information not generate it.

There are three levels of safety of eIDAS identification schemes: low, substantial and high. All EU entities must accept the level of safety considered by the issuing authority. This will generate the possibility of giving individual access to services that require a certain level of safety.

Prior to eIDAS, several similar initiatives were carried, some of their ideas being imported into eIDAS. One of the projects, STORK (Secure idenTity acrOss boRders linked [10, 11], failed to be implemented due to the lack of legislative support. With the lesson learnt, eIDAS came not only with the technical aspects necessary for the implementation of cross-border identification but also the necessary legal framework. There are reports [14] which reveal the fact that some national eID systems are already classified as "high" on the safety scaled of eIDAS.

### Web Authentication

With web authentication, eID users can be recognized anywhere when they need certain services. The Regulation stipulates the use of verification and validation certificates for website authentication, as means to guarantee a trust service [1, 16].

Online services dedicated to integrating digital security providers, managers and consumers at high levels of security must, in turn, meet certain standards of identity certification. In this regard, we investigated several studies conducted by the European Network and Information Security Agency (ENISA) on Qualified Web Authorization Certificates [16, 17]. These specifications are an integral part of the eIDAS Regulation and provide standards on which Digital Identity Providers can qualify for TLS (SSL) identity as well as the security conditions that a website has to meet to qualify as provider of secure online services.

### Electronic Signature (eSignature)

User identification, electronic or physical, is, most of the times, not enough for guaranteeing that a transaction or agreement is valid and will be carried out without problems. For this reason, the handwritten signature is applied on paper documents and an electronic equivalent is needed for electronic documents.

The use of electronic signatures has grown steadily in electronic transactions, both in the governmental/local administration and private environments. As presented in [8] the usage of electronic signature had an increase rate of 2.5 from 2012 and 2014 (interval for which certain data is available) and is estimated to have an increase rate of 4 (between 2012 and 2015) and of about 6 (between 2012 and 2016). By the moment this study was elaborated, no certain data for 2015, 2016 and 2017 were published. Other statistics reveal that, in present, over 43.3% of private companies use electronic signature,

The electronic signature must fulfill two functions:

- Authenticate signer
- Offer the guarantee that a document was not been modified in any ways after the signature was inserted.

The signature itself (container and content) can be presented in various forms: email signature, scan or picture of a written signature, signature generated by a dedicated device or application. For a higher level of trust, eIDAS brings two new types of electronic signature: Advanced Electronic Signature (AES) and Qualified Electronic Signature (QES).

The advanced electronic signature must meet the demands of a regular electronic signature by uniquely identifying the signer and guarantying that the signed document was not altered after the signing but also it must guarantee that the signer himself was in control of the signing process. Simply put, the AES must exceed a simple electronic signature by containing elements capable to eliminate identity theft.

The qualified electronic signature is a particular case of advanced electronic signature. The QES must be supported by a qualified creation device and, in addition, by a qualified "public key" certificate issued by a TSP. It has been mentioned before that TSP and the generator devices list is managed at global level so they must undergo a sever assessment process before being invested as "qualified". The qualified electronic signature is the only type of electronic signature that will have the same legal value with the written signature so it will not be subject of a potential legal dispute. The other types of electronic signatures may have the same functionality but they are not as strong so a possible legal dispute related to a signed document must be settled in a court of law.

### Remote Signature

eIDAS allows the use of remote signing services. In the case of a local signature, the user will create it by using a security hardware device. Remote signing is an alternative to local signature creation by providing a remote signature creation mechanism. For this to be possible, the signing keys are no longer on a portable device but are provided remotely via a service that simulates a physical HSM. Thus, the user is no longer dependent on a physical device that can be lost, stolen, or deteriorated. Currently, this approach appears to be largely preferred by the general public.

The general idea is to replace the physical HSMs with an online service provided by a TSP where the user's signing keys are held. A similar idea was presented in [15].

The signature functionality and recognition by third parties is totally the same but the signing process can be done by using a smartphone or computer with a minimal web-browser. This novelty approach introduced by eIDAS is highly supporting the online transactions which exhibit continuous growth. Another important help is coming from the high degree of penetration and use of smartphones which eliminate any constraints when it comes to mobile access of web services.

A remote signing procedure is presented in Fig. 4. As one can see, the procedure is simple and requires very few resources from the user. The TSP receives requests from the users via a safe channel (for example, HTTPS), is generating electronic signatures and sends them back to the users. The generation process is based on the users' signing keys stored on the HSMs hosted by the TSP. Upon request, each user is activating his own signing key based on some secure credentials. Since the entire signature generation process is at the TSP level, it is mandatory that a high level of security is implemented on site. Users' devices (smartphones or computers) must have multiple layers of security when are being used for remote signing purposes. For example, the access for regular non-critical applications (phone, Waze, weather etc.) can be granted based on a simple PIN but the access for credentials should require stronger security (longer passwords, biometric features etc.).

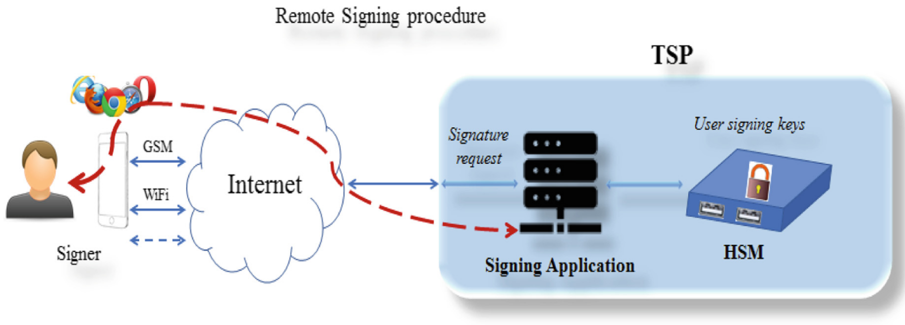

**Fig. 4.** eIDAS remote signing procedure

Depending on the security of the signature request and signing key activation, eIDAS refers to 2 levels of remote signing. In fact, this is related to the entity where signing key activation is done at the TSP. In case of Level 1 remote signing, the key activation is made inside the signing application (see Fig. 4). This makes the signing application the only entity where user's activation request is received, processed and executed. Level 1 remote signing does not impose special restrictions to HSMs which can be any certified module. This approach may raise some questions or suspicions related to the fact that TSP's signing application obtains the user's activation key. Higher level of security is granted by Level 2 remote signing. In this case, the signature activation is done by the HSMs (see Fig. 4), whilst the signing application only receives and passes the user's activation data without executing it. This way, the risk of compromising the user's data is reduced to minimum.

## 3 Conclusions

In this paper, an investigation over the electronic identification and trust techniques from eIDAS is presented. The eIDAS Regulation seeks to create a unique and safe EU market for government agencies, public and private enterprises and online service providers.

Prior to eIDAS adoption, the heterogeneity of national or local electronic identity and trust systems prevented any efforts of making them compatible and interoperable. The solution for these problems came under the form of a mandatory legislative act issued by EU for harmonizing electronic identification and trust services.

The functionality and philosophy behind eIDAS are presented together with the stages of implementation in various countries of EU. The main electronic identification techniques and differences to the former ones are analyzed and presented in detail. Trust aspects related to the user, as individual, are also presented under various forms of electronic signature.

Although eIDAS aims to unite the European legislation in its field, it must be pointed that eIDAS will not enforce a common, unique identification system but will ensure the compatibility and interoperability of national systems. This should be totally transparent to the end user which should only benefit from the advantages derived from the implementation of the new regulation.

**Acknowledgement.** The work has been funded through the research project COOPID mySMIS-115656.

## References

1. European Parliament: 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, Official Journal of the European Union, OJ L 257, pp. 73–114, 28 August 2014
2. European Comission. https://ec.europa.eu/digital-single-market/en/news/feasibility-study-cross-border-use-eid-and-authentication-services-eidas-compliant-support-0
3. European Commission. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
4. European Council: Special meeting of the European Council (Art. 50), 25 November 2018. https://www.consilium.europa.eu/en/meetings/european-council/2018/11/25/
5. ComputerWeekly: EU sees eIDAS regulation come into full force, September 2018
6. KPMG Switzerland: Swiss companies must comply with eIDAS for digital access to EU markets. https://blog.kpmg.ch/swiss-companies-must-comply-eidas-digital-access-eu-markets/
7. Norwegian Communication Authority. https://eng.nkom.no/technical/trust-services/eidas/eidas-regulation
8. Thales: The Impact of the European eIDAS Regulation. www.thales-esecurity.com
9. European Comission. https://ec.europa.eu/digital-single-market/en/e-identification
10. Leitold, H., Zwattendorfer, B.: STORK: architecture, implementation and pilots. In: ISSE 2010 Securing Electronic Business Processes, pp 131–142 (2010)

11. Sideridis, Alexander B., Protopappas, L., Tsiafoulis, S., Pimenidis, E.: Smart cross-border e-Gov systems and applications. In: Katsikas, Sokratis K., Sideridis, Alexander B. (eds.) e-Democracy 2015. CCIS, vol. 570, pp. 151–165. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-27164-4_11
12. Secure ID News. https://www.secureidnews.com/news-item/eidas-digital-id-finds-use-in-cross-border-european-banking/
13. European Comission. https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas
14. Federal Office for Information Security: eIDAS Notification of the German eID. https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html
15. Zwattendorfer, B., Tauber, A.: Secure cloud authentication using eIDS. In: Proceedings of IEEE CCIS2012 (2012)
16. ENISA: Qualified Website Authentication Certificates, December 2015. https://www.enisa.europa.eu/
17. ENISA: Security guidelines on the appropriate use of qualified website authentication certificates, December 2016. https://www.enisa.europa.eu/
18. Pimenidis, E., Georgiadis, C.K.: Can e-Government applications contribute to performance improvement in public administration? Int. J. Oper. Res. Inf. Syst. **5**(1), 48–57 (2014)
19. European Commission. https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas