British Embassy
Belgrade

UK | RS Reform assistance
to Serbia
Подршка реформама
у Србији

UKaid
from the British people

GOOD
GOVERNANCE
FUND

TOWARDS A PAPERLESS ADMINISTRATION

eIDAS implementation best practices of European Union members

Ka administraciji
bez suvišnih papira

Author: Justas Urbonas
Belgrade, 28 September 2018

Република Србија
МИНИСТАРСТВО ТРГОВИНЕ, ТУРИЗМА
И ТЕЛЕКОМУНИКАЦИЈА

Република Србија
МИНИСТАРСТВО КУЛТУРЕ
И ИНФОРМИСАЊА

Република Србија
МИНИСТАРСТВО ДРЖАВНЕ
УПРАВЕ И ЛОКАЛНЕ САМОУПРАВЕ

This document was developed within the project „Towards a Paperless Administration“ implemneted by NALED, European Policy Center and Pricewaterhouse Coopers, with the support of UK Government's Good Governance Fund.

The project key beneficiaries and participants in its realization are the Ministry of Trade, Tourism and Telecommunications, Ministry of Culture and Information, Ministry of Public Administration and Local Government, as institutions in charge of regulations governing this field.

1. eIDAS regulation implementation in EU Member States

European eIDAS Regulation, that was established on July 2014 and is fully applicable from July 2016, creates the regulatory environment for seamless and secure electronic interactions to be used by businesses, citizens and public authorities. It ensures that people and organizations can use their own national electronic identification schemes in their own and other EU countries, establishes the legal status as traditional paper based processes and orchestrates European internal market of electronic trust services.

eIDAS Regulation promises huge gains for Digital Single Market strategy by providing simplicity, security and trust in identification processes together with significantly decreased costs (both time and money) comparing with traditional paper based processes. Now Swedish company can participate in public tender in Croatia with authenticated and secure electronic document transactions, save days if not weeks for flights or document storage. Moreover, the purchasing organization has all proofs on participant identification, originality of contracts and other documentation. Other examples are: enrolling in a foreign university, submitting tax declarations, remotely opening a bank account, setting up a business in another Member State, authenticating for internet payments, etc.

As eIDAS Regulation is directly applicable in the EU, Member States have to do preparations:

- designate a competent national authority in charge of supervision of trust service providers;
- set effective sanctions/fines;
- perform accreditations for conformity assessment bodies (by National Accreditation Body, established in Regulation 765/2008);
- publish and maintain national Trusted Lists;
- recognize the formats of advanced electronic signatures and electronic seals in public sector bodies.

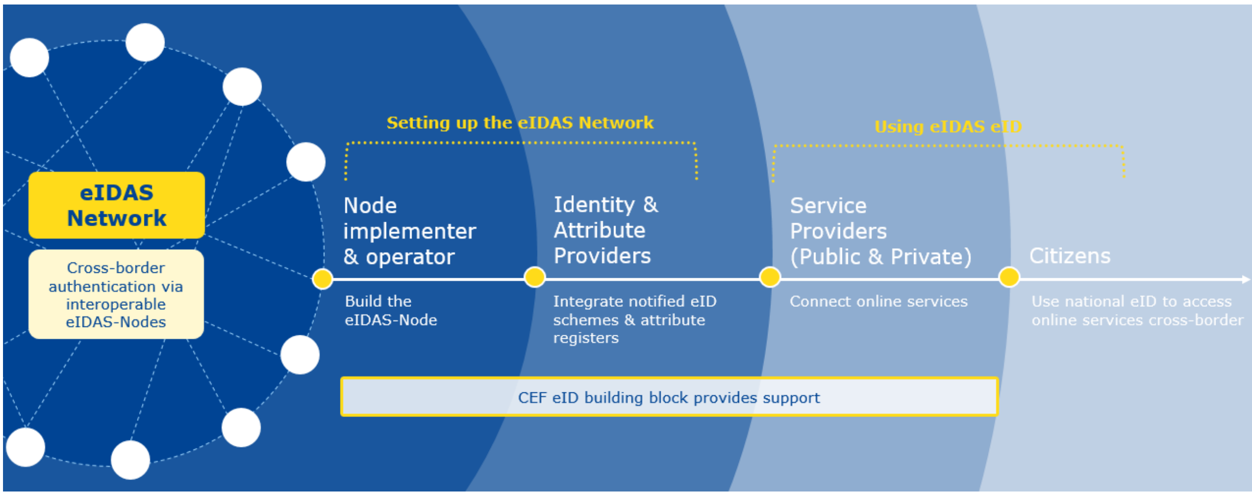
eIDAS Network
Cross-border authentication via interoperable eIDAS-Nodes
Setting up the eIDAS Network
Using eIDAS eID
Node implementer & operator
Build the eIDAS-Node
Identity & Attribute Providers
Integrate notified eID schemes & attribute registers
Service Providers (Public & Private)
Connect online services
Citizens
Use national eID to access online services cross-border
CEF eID building block provides support

Figure 1. Who is involved in eIDAS eID ecosystem? (source: European Commission website)

Trust service providers are not required or advised to provide all the trust services together. Therefore, if not needed, then it is a business decision of the trust service provider on whether to provide one, more than one or all trust services. There are no limitations to the type of organization that can be a service provider, the example set of Trusted Service provider types are provided:

Country	Types of Trusted Service providers
Estonia	Private company jointly founded by 2 large multinational banks and largest mobile operator
Lithuania	Government institutions, private company with sole timestamping purpose
UK	Telecommunications companies, mail service providers, government institutions, private companies developing cryptographic and digital identity solutions

Trusted Lists

According to eIDAS Regulation, national Trusted Lists have an important role as a provider/service is only qualified if it appears in the Trusted Lists. Consequently, the users (citizens, businesses and public administrations) only can benefit from the legal effect associated with a given qualified trust service if the service is listed in the Trusted Lists. The Trusted List Browser is available as a mobile-friendly web application.

2. Organisational structure

eIDAS regulations describes the organisational structure for control and provision of the trust services. The organisational structure is shown in a scheme bellow:

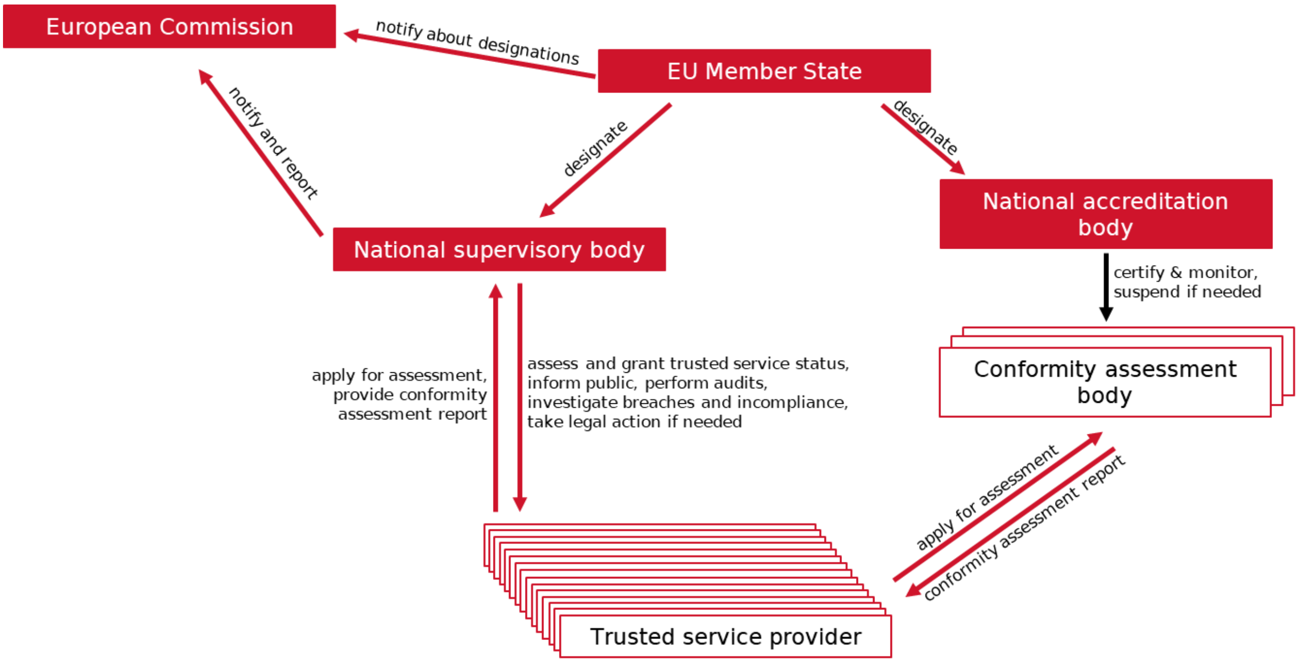
European Commission
notify about designations
EU Member State
notify and report
designate
designate
National accreditation body
National supervisory body
certify & monitor, suspend if needed
Conformity assessment body
apply for assessment, provide conformity assessment report
assess and grant trusted service status, inform public, perform audits, investigate breaches and incompliance, take legal action if needed
apply for assessment
conformity assessment report
Trusted service provider

Figure 2. Organizational structure of the trust services provision according eIDAS regulation

2.1. National accreditation body

According eIDAS regulation, a national accreditation body is responsible for issuing certifications to conformity assessment bodies and monitoring them. However, it does not require a separate accreditation body, as another EU regulation already covers accreditation body together with its duties and responsibilities; therefore, such institution already existed under EU law. Member states must formally assign responsibilities described in eIDAS to the national accreditation body. Additionally, a national accreditation body has right to suspend or withdraw accreditation certificates. It can also operate in other member states.

2.2. National supervisory body

As eIDAS regulation describes specific responsibilities that the supervisory body should be established in the law and each member state must designate a competent national authority in charge of supervision of the trust service providers and notify about the designation to the European Commission. A national supervisory body receives application for the trusted service provision from an interested trusted service provider together with its evaluation report from the conformity assessment body and decides if the approval is granted. A national supervisory body has the power of a final decision and not only accepts a report of the conformity assessment body, but can also request further information or decline the report. A national supervisory body also is responsible to include approved trusted services and trust service providers in trusted lists, including the notification of other EU countries.

2.3. Conformity assessment body

A conformity assessment body is established after passing a specific procedure and is certified as well as monitored by the national accreditation body. According to eIDAS Regulation, a conformity assessment body is performing conformity assessments against the requirements of the Regulation that includes testing, inspection and certification of the trust service providers and their services. Consequently, a conformity assessment body prepares a Conformity Assessment report detailing the findings of the audit and submits it to the national supervisory body, which ultimately decides if the trusted service provider is entitled to receive the qualified level of certification and can be referenced in the EU Trust List.

2.4. Trusted service providers

eIDAS regulation describes a trusted service provider as a natural or a legal person who provides one or more trust services, but does not specify any additional guidance regarding the structure or ownership. Consequently, trusted service providers can be and are both public and private sector organisations, which are at first evaluated by the conformity assessment body and then the second, approved by the national supervisory body to be a trusted service provider and deliver one or more trusted services in all EU member states.

2.5. Practice in UK

In UK, national accreditation body for eIDAS Regulation appointed responsibilities is UKAS (United Kingdom Accreditation Service) non-profit agency. It has certified only one conformity assessment body – BSI Assurance UK Ltd.

National supervisory body role is assigned to The Information Commissioner office, which further enforces the eIDAS Regulation and perform other related duties.

The most interesting fact is that United Kingdom has not approved any trust service providers with qualified status. However, they have multiple trust service providers with locally approved trust services.

2.6. Practice in Lithuania

Lithuania National Accreditation Bureau performs, amongst its other functions, national accreditation body functions under eIDAS regulation. However, there are no certified conformity bodies operating on Lithuania and interested trust service providers must look for conformity assessments in other member states what they successfully do – eIDAS discusses and allows such international collaboration.

National supervisory body for trust services is the Communications Regulatory Authority of the Republic of Lithuania, which is performing this duties according eIDAS regulation.

As it is stated above, Lithuania has no active conformity assessment body. Nevertheless, there are a few Trust service providers providing qualified electronic seal and qualified electronic signature services as well as qualified time stamping service, where two more service providers have their current qualified trust service status suspended/withdrawn.

2.7. Practice in Estonia

Estonia also does not have own conformity assessment body, even though Estonian Accreditation Centre can perform national accreditation body functions. Therefore, local trust service providers relies on foreign conformity assessment bodies from other EU member states. Technical Regulatory Authority is performing national supervisory body functions in Estonia.

Estonia has only one trusted services provider, which provides qualified electronic seal, qualified electronic signature and qualified time stamp services. However, this company is very actively working in many other EU member states and providing their qualified trust services.

3. Trusted services in EU member states

3.1. Types of trusted services

Under eIDAS Regulation there is a special status of Trust Services which are qualified. The status of qualified service is granted in a process that starts with an assessment by the conformity assessment body against eIDAS requirements of both provider and qualified trust service it intends to provide, which includes testing, inspection and certification of trust service providers and their services. There are two types of audits to verify compliance against the eIDAS regulation:

1. Pre-assessment: this includes the assessment of the documentation (i.e. technical, functional and organisational security measures) and their appropriateness for fulfilment of eIDAS requirements.
2. On-site audit: this includes verification of implementation of security measures, processes, network, and systems. The technical testing includes penetration testing.

The next step for trust service provider to notify the national supervisory body of its intention to become qualified and to deliver a conformity assessment report issued by a conformity assessment body, which must prove the compliance with the requirements of the eIDAS Regulation. This report does not show or prove compliance to standards, but standards can be used as a tool to demonstrate that the service provider is compliant with the requirements of the Regulations. Consequently, the supervisory body verifies if eIDAS Regulation requirements are met and grants qualified status as well as adds to the Trusted Lists. If the situation requires, a national supervisory body can also request further information or decline the report.

Both qualified and non-qualified trust service benefit from a non-discriminating clause in courts, therefore they cannot be discarded by the judge only because they are in an electronic form. In other words, both can prove the identity of the signer and are the equivalent of a wet ink signature. However, qualified trust services provide a stronger legal effect than non-qualified as it met more stringent requirements, thus is providing stronger legal certainty and technical security of electronic transactions.

Domain of trusted services	Trusted services	Type	Description of trusted services
Certificate services	Qualified certificate for electronic signature	Qualified	Certificate for electronic signatures, that is issued by a qualified trust service provider and meets eIDAS regulation requirements
	Qualified certificate for electronic seal	Qualified	Certificate for an electronic seal, that is issued by a qualified trust service provider and meets eIDAS regulation requirements
	Qualified certificate for website authentication	Qualified	Certificate for website authentication, which is issued by a qualified trust service provider and meets eIDAS regulation requirements
	Certificate for electronic signature	Non-qualified	Electronic attestation which links an electronic signature validation data to a **natural person** and confirms at least the name or the pseudonym of that person
	Certificate for electronic seal	Non-qualified	Electronic attestation that links an electronic seal validation data to a **legal person** and confirms the name of that person
	Certificate for website authentication	Non-qualified	Attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued
Validation services	Qualified validation service for qualified electronic signature	Qualified	Service provided by a qualified trust service provider who provides the validation in compliance with eIDAS regulation and allows relying parties to receive the result of the validation process in reliable, efficient, automated manner bearing advanced electronic signature or seal of the qualified validation service provider
	Qualified validation service for qualified electronic seal	Qualified	Service provided by a qualified trust service provider who provides the validation in compliance with eIDAS regulation and allows relying parties to receive the result of the validation process in reliable, efficient, automated manner bearing advanced electronic signature or seal of the qualified validation service provider
	Validation service for electronic signature	Non-qualified	Service that allows relying parties to receive the result of the validation process in reliable, efficient, automated manner
	Validation service for electronic seal	Non-qualified	Service that allows relying parties to receive the result of the validation process in reliable, efficient, automated manner
Preservation services	Qualified preservation service for qualified electronic signature	Qualified	Service provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period
	Qualified preservation service for qualified	Qualified	Service provided by a qualified trust service provider that uses procedures and technologies capable of extending the

Domain of trusted services	Trusted services	Type	Description of trusted services
	electronic seal		trustworthiness of the qualified electronic seal beyond the technological validity period
	Preservation service for electronic signature	Non-qualified	Service that uses procedures and technologies capable of extending the trustworthiness of the electronic signature beyond the technological validity period
	Preservation service for electronic seal	Non-qualified	Service that uses procedures and technologies capable of extending the trustworthiness of the electronic seal beyond the technological validity period
Time stamping services	Qualified time stamp	Qualified	Electronic time stamp which binds the date and time (linked to Coordinated Universal Time) in such a manner as to reasonably preclude the possibility of the data being changed undetectably as well as signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider
	Time stamp service	Non-qualified	Service to provide the track of actions from creation to modification time of a document
Delivery services	Qualified electronic registered delivery service	Qualified	Electronic registered delivery service which provided by a qualified trust service provider, ensure with high level of confidence the identification of the sender and addressee before sending and delivery of the data, secured by advanced signature or advanced electronic seal of a qualified trust service provider, is able to indicate any changes. All actions must be also indicated by the qualified electronic time stamp
	Electronic registered delivery service	Non-qualified	A service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations
Non-regulatory	Non-regulatory, nationally defined trust service	Non-qualified	Trust service established and defined according to requirements of national law of EU Member State

3.2. Electronic signature

A key trust service represented in the eIDAS regulation is an electronic signature, which there is defined as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign". The signature is generated by a signatory, possibly augmented with related proofs and evidences, validated by the relying party and possibly preserved for a longer term.

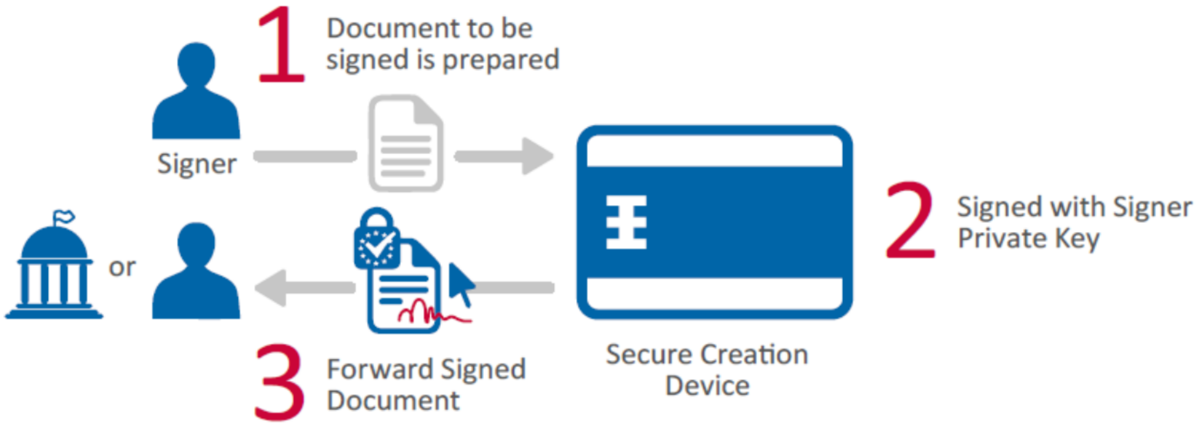
1
Document to be signed is prepared
Signer
2
Signed with Signer Private Key
or
Secure Creation Device
3
Forward Signed Document

Figure 3. Trusted Service: Qualified Electronic signature (Source: ENISA)

An electronic signature in general shall be granted the legal effect and admissibility as an evidence in legal proceedings. However, the legal assurance effect varies depending on the type of signature:

- Electronic signature;
- Advanced electronic signature (AdES) –requires some security features that ensure it is uniquely linked to the signatory, it is capable of identifying the signatory and it is linked to the data in such a manner that any subsequent change of the data is detectable;
- Qualified electronic signature (QES) – an advanced electronic signature which provides an additional level of assurance on the identity of the signatory and an enhanced protection and level of assurance on the signature creation. A special device is required for the creation of QES (a qualified signature creation device, QSCD). Qualified electronic signature benefits form the same legal assurance effect as handwritten signature.

Technical implementation might vary depending on the availability of technical innovations, but in the current state of the art, qualified electronic signatures are implemented by the means of asymmetric cryptography, where signature creation and verification process is as follows:

1. The signatory uses the private key to sign a text;
2. The verifier (also called relying party in the eIDAS Regulation) uses the signatory's public key to verify the signature.

Another characteristic of digital signatures is that if the signed text has been modified after the signature, the verification of the signature will fail (because the signature computation mixed the private key and the data to be signed the verification computation will always disclose the very same data).

The signing process is performed in the following procedure:

1. The signatory prepares the document like any kind of document (e.g. a PDF file);
2. The application prepares the data to be signed (i.e. the PDF) in a condensate (called a hash) and presents it to the signature creation device;
3. The signature creation device asks the authorisation to the signatory to sign the data, in general, though a window that pops up on the screen. The signatory authenticates to the device (e.g. (s)he enters a PIN code, or a fingerprint);
4. The signature creation device computes the signature and sends the result to the application that integrates the signature into the document.

The first recommendation for organisation intended to develop their own electronic signature is to use standards and recognised formats. Most relevant to eIDAS are:

- Signature formats - ETSI TS 103 171 v.2.1.1. (XAdES Baseline Profile), ETSI TS 103 173 v.2.2.1. (CAdES Baseline Profile), ETSI TS 103 172 v.2.2.2. (PAdES Baseline Profile) and ETSI TS 103 174 v2.2.1 (Associated Signature Container Baseline Profile);
- Open source toolkits - CEF eSignature building block
- Policies and security requirements - ETSI TS 119 172

As electronic signature is the main customer-reaching service as well as the most widely used due its identity confirmation ability, every member state has multiple entities applying to deliver this trusted service, which are from both government and private sectors. Examples of solutions presented to the market:

State Enterprise Centre of Registers (Lithuania) – qualified digital certificates issued by a government agency with a number of local partnerships with mobile service providers and banking sector. Digital certificates provided in hardware form – tokens, smartcards and code-generating devices.

Smart-ID (Estonia) – the identity service created by a joint company (owned by several multinational banks and a large mobile network operator). Smart-ID is provided as a mobile application with back-end cloud infrastructure.

3.3. Electronic seal

Another important identity proofing service that is relatively new and appeared for a first time as a qualified trust service in eIDAS regulation is the electronic seal. This service is seemingly similar to the electronic signature, but it can only be attached to or provide a proof of identity of a legal person. The creation of an electronic seal guarantees the authenticity of the document in accordance with the terms of use of the electronic seal, which are defined in the certificate or certification policy.

When an organisation interested in developing its own seal creation or validation service, the first recommendation is to use standards and recognised formats. Such standards are:

- Seal formats - ETSI TS 103 171 v.2.1.1. (XAdES Baseline Profile), ETSI TS 103 173 v.2.2.1. (CAdES Baseline Profile), ETSI TS 103 172 v.2.2.2. (PAdES Baseline Profile) and ETSI TS 103 174 v2.2.1 (Associated Signature Container Baseline Profile);
- policies and security requirements for seal creation and validation - ETSI TS 119 172.

As eIDAS gives some freedom regarding operation and controls measures of the electronic seal service, it allows creation of technical solutions, in which the seal mechanism can become a part of a device provided or authorized by "the creator of a seal". These devices create an electronic seal over electronic data processed by them. The seal can contain information on the processing schema and security conditions. Individuals or legal persons for specific dedicated tasks can then use such devices. The evidence prepared by such device can secure a business process or other trust services.

An alternative example of the usage of an electronic seal is a photo camera in which every captured image is sealed with information about the time and place, downloaded from the GPS. This stamp guarantees the authenticity of origin of images from a specific camera model and also specifies where and when the photo was taken. The entity submitting this seal is the manufacturer (or guarantor) of the camera. The camera manufacturer in this way ensures that only pictures taken with this specific camera, accompanied by data from the GPS will have this seal.

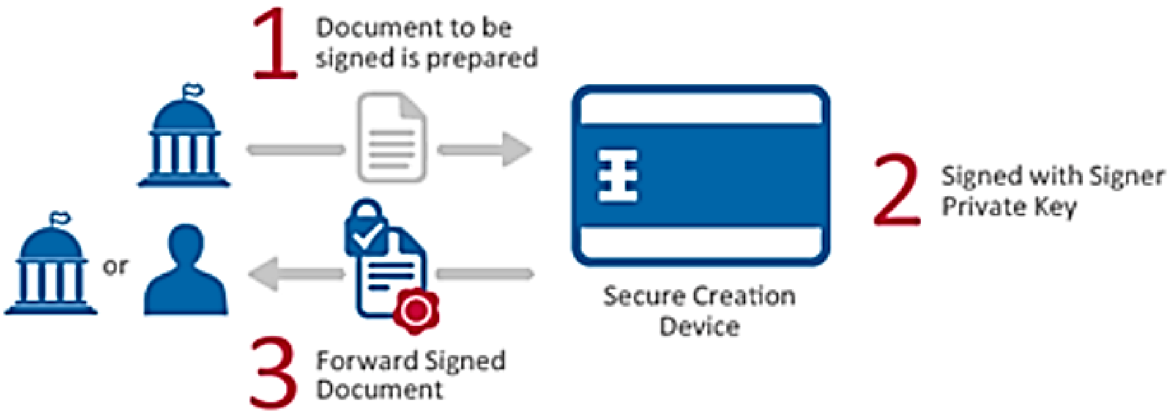
1
Document to be signed is prepared
2
Signed with Signer Private Key
Secure Creation Device
or
3
Forward Signed Document

Figure 4. Trusted Service: Qualified Electronic seal (Source: ENISA)

Electronic seals in general shall not be denied legal effect and admissibility as evidence in legal proceedings. However, legal assurance is again depending on type of signature:

- Electronic seal;
- Advanced electronic seal (AdESeal) – which requires security features that ensure it is uniquely linked to the signatory, it is capable of identifying the signatory entity and it is linked to the data in such a manner that any subsequent change of the data is detectable;
- Qualified electronic seal (QESeal) – which is an advanced electronic seal which provides additional level of assurance on the identity of the creator of the seal and an enhanced protection and level of assurance on the seal creation. A special device is required for the creation of QESeal (a qualified seal creation device). This type of seal benefits from an automatic presumption of integrity of the data and of correctness of the origin.

According to the current state of the art technologies, the electronic seal creation and verification process is as follows:

1. The creator of the seal uses the private key to seal (or in technical terms, to digitally sign) a text
2. The verifier (also called relying party in the eIDAS Regulation) uses the creator of the seal's public key to verify the digital seal

As electronic seal is can only be assigned to legal persons – the number of users as well as trusted service providers is less than those providing an electronic signature service. However almost every member state has at least one qualified electronic seal provider. An example of solution presented to market:

e-Seal – the qualified electronic seal service provider which also provides a qualified electronic signature and qualified time stamping services in their portfolio.

3.4. Time stamping

Another important trust service discussed in eIDAS regulation is a time stamp, which is more back-end service due to its nature. An electronic time stamp is a piece of data in electronic form, which binds other electronic data to a particular time establishing the evidence that this data existed at that time.

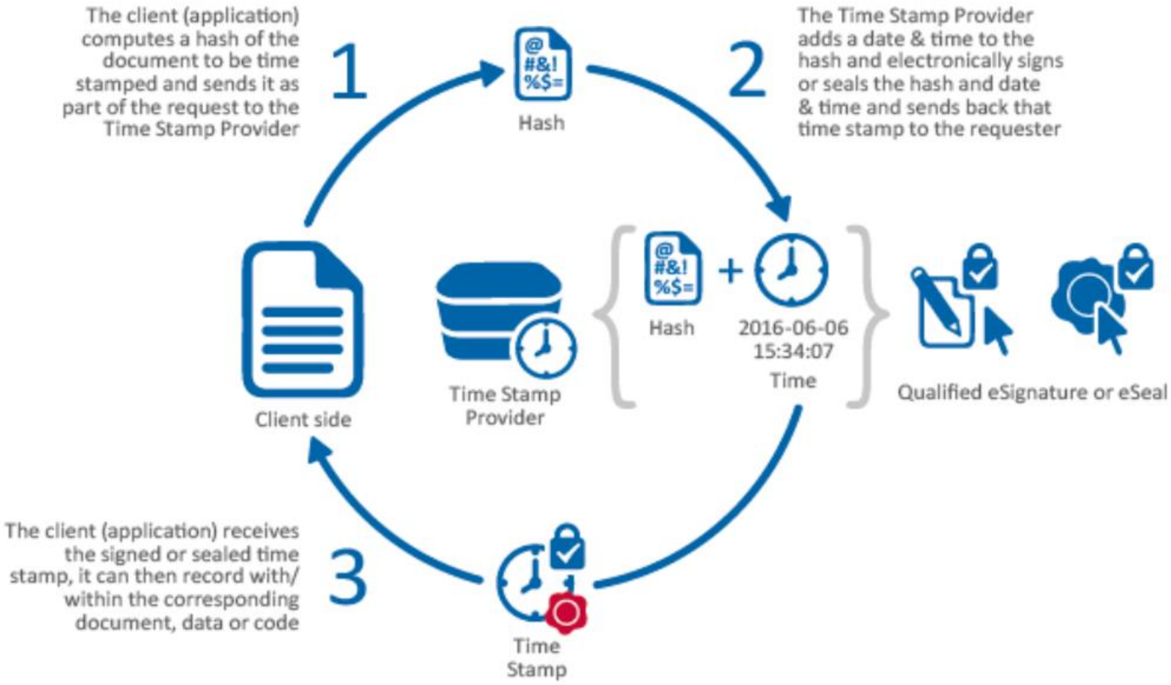
The client (application) computes a hash of the document to be time stamped and sends it as part of the request to the Time Stamp Provider
1
Hash
2
The Time Stamp Provider adds a date & time to the hash and electronically signs or seals the hash and date & time and sends back that time stamp to the requester
Client side
Time Stamp Provider
Hash
+
2016-06-06 15:34:07
Time
Qualified eSignature or eSeal
The client (application) receives the signed or sealed time stamp, it can then record with/ within the corresponding document, data or code
3
Time Stamp

Figure 5. Trusted Service: Qualified Time Stamp (Source: ENISA)

As eIDAS defines a qualified electronic time stamp is an electronic time stamp with additional assurance measures: it must be based on an accurate time source linked to Coordinated Universal Time and bind the date and time to the time stamped data in such a manner as to reasonably preclude the possibility of the data beg changed undetectably. It must also be signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider. As a result, qualified electronic time stamp enjoy, all over the EU, the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

Relevant standards regarding the creation and validation of time stamps:

- Policy and security requirements for trust service providers issuing time stamps - ETSI EN 319 421;
- Time stamping protocol and token profiles - ETSI EN 319 422.

The European Union benefit from a number of qualified time stamp providers, but as eIDAS Regulation allows – not every member state has a local trust service provider and frequently rely on the trust service provider in another member state. An example of solutions presented in market:

BaltStamp – a qualified time stamping service by provider created for that sole purpose and using advanced technics such as an atomic clock, 2048-bit private key and FIPS 140-2 compliant hardware security modules.

3.5. Electronic archiving and electronic preservation services

Electronic archiving is not a trust service under eIDAS. The objectives and targets of electronic preservation services for electronic signatures, electronic seals and certificates are directly related to the electronic archiving, though electronic archiving covers:

- Preservation services under eIDAS aims at guaranteeing the trustworthiness of a qualified electronic signature or qualified electronic seal through time and the target is the electronic signature or seal.
- Electronic archiving aims at ensuring that a document is stored in a way to guarantee its integrity, therefore the target is the document. This is left to the competence of Member States.

Electronic preservation services are directly related to ETSI standards in particular Standard: ETSI - TS 101 533-1 and Standard: ETSI - TS 101 533-2 where requirements for the Information Security Management System of Data Preservation Systems and Security requirements for Data Preservation Service Providers and recommendations on how to assess electronic data preservation services against the provisions are described. In this standard **Data Preservation System (DPS) is described as**: *set of hardware, software, policies, procedures, guidelines, practices, physical and organizational infrastructures aiming to ensure electronic data preservation for at least the period of time specified in the applicable agreements; the organizational infrastructures can be of administrative, technical, management, or legal nature.* This description emphasizes the goals and targets of electronic archiving systems.

Electronic archiving in many EU member states was established before eIDAS regulation. Because of this reason, countries used ETSI standards to describe processes and technological standards for electronic archiving. It is worth mentioning that the object of electronic archiving and preservation services is different from in trusted preservation services: electronic archiving targets electronic documents whereas preservation services targets certificates and seals. Nonetheless, these objects are closely connected as an electronic document (main data object) covers whole information including a signature or seal, timestamp and data (metadata and files).

Starting from 2000 various institutions in EU member states implemented different software solutions for document management. In the beginning they were used for document metadata storage; later scanned documents were stored together with metadata. When technology emerged software solutions were introduced which allowed to sign documents electronically. When numbers of electronic documents grew the need for long-term storage emerged. A lot of EU member states followed this need and created national systems for electronic document archiving, though in majority of cases the obligation to store electronic documents in the national system is mandatory only for government institutions and partially to businesses, but it does not involve citizens.

For practical example, we took Lithuania, which in 2011 created the Electronic archiving system. The software was created to store public sector electronic documents for the long term. This way the country wanted to solve several issues: limit amount documents stored various document management systems after they can be delivered for archiving and apply a single standard for electronic documents. This way unification of various electronic standards in electronic archiving was started.

There main requirements for storage in Lithuanian electronic archiving system are:

1) As described in ETSI - TS 101 533-1, only documents with Advanced Electronic Signatures, in any of their strains such as CAdES, XAdES, PAdES, QES, etc. can be stored in the national archiving system;
2) Each document needs to have at least two qualified time stamps (with a time difference of at least 24 hours) before placing it into national electronic archiving software. If the document does not have 2 qualified time stamps additional one can

obtained during the transition phase (first time stamp is mandatory when signing the document), though all certificates in the document should be valid;

3) When a document is placed in a national software, its original must be deleted from the other document management system. It does not mean that the copy of the document cannot be stored locally in the organisation's document management system – it can, but only information (for example in PDF) file should be maintained;
4) In Lithuania, an institution responsible for maintenance of the national archiving system is responsible for obtaining additional time stamps during the time of archiving for safe and secure preservation. In particular, a service provider/public entity responsible for archiving electronic document does not have to be a trusted service provider for preservation services, but it should use qualified preservation services provided by trusted service provider.

Additional aspects should be tackled when considering usage of solutions for document archiving:

1) **Closure evidences and time evidences –** an archiving software should ensure that the signatures (e.g. Closure Evidence) are maintained as specified in the subsequent items, so that their validity can be verified at any time during the preservation period. In order to allow the reliable verification of an AdES signature, even if its supporting certificate is revoked or expires after the signing time, a reliable time reference should always be applied to it as close as possible to the actual signing time, to provide the evidence that the AdES signatures existed before expiration or a possible revocation of the signature certificate.
2) **Standard web services for electronic document reception** – web services should use world standard technology solutions such as SOAP or JSON with clearly described WSLD or a similar scheme explaining the contents of data delivered. Web services should contain the mandatory and recommended structure for electronic document, their lists and packages.
3) **Document packaging requirements** – considering large amounts of electronic documents the reception process should be coordinated using specific packages, which cover additional information about the overall electronic document structure. These requirements should be oriented to data quality and check the information about document groups (i.e. correct numbering, correct packaging to cases, etc.) provided from the document management system or other software, which stores electronic documents. These requirements ensure that the search engine in archiving software will be able to find appropriate documents.
4) **Document acceptation procedure** – to ensure appropriated data quality, the document acceptation procedure should be implemented in the archiving system. Technical approval by software (for received data quality) and organisational approval for meeting procedures should be obtained.

As described in ETSI - TS 101 533-1 owner of electronic archiving system should cover these areas of security requirements:

1. In relation to core Processes:
   1.1. Secure log management process.
   1.2. Incoming data objects acceptance.
   1.3. Preservation core process, including Backup.
   1.4. Management of the DPS related assets processing.
   1.5. Preserved data objects exhibition/return.
   1.6. Disaster Recovery / Business Continuity Plan.
   1.7. Electronic data objects deletion.

2. In relation to EXTENDED Processes, where applicable:
   2.1. Analog data objects post-preservation deletion.
   2.2. Incoming electronic data objects scanning with Antivirus programs.
   2.3. Incoming electronic data objects format validity assessment.

Even though eIDAS became fully applicable in 2016, there are not many qualified preservation service providers in the EU. One of the reasons is that preservation service is just one part of the end software solution, which should be delivered to customers.

Europe trusted service list enlists these entities:

1. Software602 a.s. – *Czech Republic;*
2. Microsec Micro Software Engineering & Consulting Private Company Limited by Shares – *Hungary:*
3. NETLOCK Informatics and Network Privacy services Limited Company – *Hungary;*
4. Asseco Data Systems S.A. – *Poland;*
5. Trans Sped SRL – *Romania*
6. Disig a.s. – *Slovakia*
7. National Agency for Network and Electronic Services y of stored documents – *Slovakia;*
8. EDICOM CAPITAL, S.L – *Spain.*

In Lithuania there no trusted electronic preservation service provider, but electronic preservation software (owned by National department of archives) is approved by local law. This software does not cover electronic document archiving of citizens and just partially covers archiving of businesses, which does not allow to create substantial effect country wise.

Solutions, which are presented to the market by qualified trusted service providers:

1. SecuSign Preservation services provided by **software602 company** which is developing document management systems and providing a qualified electronic signature service.
2. EDICOMLta qualified electronic signature service is provided by **EDICOM** – one of the largest international companies in the development of platforms for data transmission between companies or e-invoicing. The service deploys a platform certified for the safekeeping of e-documents for the period of time required by companies or set by the legislation in each case. The solution ensures permanent access and retrieval of 100% of documents loaded in the platform, as well as managing proofs endorsing the integrating.

3.6. Electronic delivery services

Electronic delivery is a trust service, which targets delivery of electronic documents and ensures with high level of confidence the identification of the sender and addressee before sending and delivery of the electronic document. Electronic delivery services are an alternative to a standard delivery of paper document originals. It is also a legitimate way to identify time when a document was sent or received.

Electronic delivery services are directly related to ETSI standards in particular Standard: ETSI TS 102 640-1 V2.1.1 - Electronic Signatures and Infrastructures (ESI) - Registered Electronic Mail (REM) where requirements for architectural structure of REM is specified. The standard describe two types of REM operation: "Store and Forward" (S&F), and "Store and Notify" (S&N). Different REM types of operation can be applied in REM software, though in each of them evidence about the sending fact and the receiving fact should be generated.

As trusted electronic delivery service is usually understood as a delivery in one single software solution. As explained before, in many EU member states a lot of document management software and other software, which has electronic documents, were established, but an electronic document exchange between them is not a common feature for the majority of them. Here electronic delivery services can be applied and ensure trusted delivery not only for businesses, citizens or government entities, but also for software solutions, which could use electronic delivery service for electronic document delivery to other software solutions.

A practical example in Lithuania, which in 2014 created Electronic delivery system, shows that an electronic delivery can be a good measure for transactions for G2C, G2B and G2G electronic documents delivery. The software was created with the purpose to ensure electronic document delivery in a quick and secured manner. It allowed government entities to send and receive documents directly to their document management systems, while keeping track of send and received facts.

The main features for electronic delivery in Lithuania are:

1. Electronic documents can be exchanged by any registered legal or physical body as well as for software solutions;
2. Authentication for registered bodies is required before any transaction;
3. Electronic delivery can be used only for qualified electronic documents, which have qualified electronic signature or seal certificate;
4. Software solutions can send multiple electronic documents through e. delivery software at once.

Additional aspects should be tackled when considering usage of solutions for electronic document delivery:

1) **Common software for delivery –** trusted electronic delivery does not cover the interaction between different software solutions, but if the common agreement or regulation country wise would exist, the electronic delivery from different software solutions would also be possible. To reach this goal it is necessary to agree on a common exchange for all software providers, so that any software solution would have a connection to the electronic delivery solution.
2) **Standard web services for electronic document delivery** – web services should use world standard technology solutions such as SOAP or JSON with clearly described WSLD or similar scheme explaining the contents of data delivered. Web services should contain mandatory and recommended structure for electronic document delivery.

In Lithuania there no trusted electronic delivery service provider, but electronic delivery software (owned by Lithuanian post) is approved by local law. This software does not cover electronic document delivery in these areas B2B, B2C, C2C, which does not allow larger expansion of the electronic delivery solution.

Situation with trusted electronic delivery service is similar to preservation service providers in the EU. One of the reasons for the low number of service providers is a common agreement to use single solutions to exchange information on a national or multinational level.

Europe trusted service list enlists these entities, which provided electronic delivery services:

1. Connect Solutions – *Belgium;*
2. AR24 – *France;*
3. 1&1 De-Mail GmbH – *Germany;*
4. Deutsche Post AG – *Germany;*
5. T-Systems International GmbH – *Germany;*
6. Asseco Data Systems S.A. – *Poland;*
7. EIUS d.o.o.x – *Slovenia.*

Example electronic delivery service available to market:

Aangetekende.email is a qualified registered delivery service from Connect Solutions bvba (Belgium), which is developing solutions for document digitalization.

After registration of both sender and recipient on the platform, the exchange can be performed in simple steps:

1. The sender logs on to the platform with the eID and draws up a new message. After compiling message with attachments, the sender signs the message electronically with the eID.

2. Connect Solutions puts an electronic seal and time stamp on the message as a proof of sending.
3. The sender can download the message, including the electronic seal and time stamp from the outbox.
4. The recipient logs on to the platform with the eID and signs the message for a receipt with the eID from the inbox.
5. Connect Solutions puts an electronic seal and time stamp on the message as proof of receipt.

Both sender and recipient can download the message, including electronic signatures of the sender and recipient and electronic seals and time stamps of Connect Solutions as proof of sending/receipt in their respective outbox/inbox.

4. Recommendations how trusted services should be treated in Serbia

4.1. Establishment of organisational structure

Considering best practices in EU member states, we recommend to describe from a high-level perspective the overall organisational structure in the law. As such, we recommend to state in the law only the main responsibilities of organisations, and leaving them the possibility to elaborate detailed description of processes related to trusted services and electronic identification schemes.

4.2. Main institutions

We present here the main institutions that have to be established.

1. **National accreditation body**
   - The National accreditation body must be a single entity per member state, and must operate as a non-profit organisation. eIDAS regulation describes main responsibilities for National accreditation bodies including: accreditation , monitoring, suspending and withdrawing accreditation certificates. For Serbia we recommend to dedicate to the Accreditation Body of Serbia all accreditation responsibilities related to trusted services. As a short-term (intermediate) solution, other accreditation bodies from EU member states could perform accreditation process in Serbia.

2. **National supervisory body**
   - The eIDAS regulation and other related legal documents doesn't describe which institution should be assigned with supervisory responsibilities for trusted services. The lack of regulations countries should be taken seriously and address dedication of responsibilities with caution.
   - On one hand, in EU member states, the supervisory body for trusted service providers and organisation responsible for identification schemes implementation are usually two different institutions. In particular, the decisions for specific responsibilities in EU member states were dedicated according to the historically established domains of competences for institutions and people who worked there, hence enabling the split of responsibilities for trusted services supervision and national identification schemes in different domains (under different ministries). This kind of structure raises problems for subordination and some political decisions. On the other hand, the superposition of work in the same ministry doesn't create any problems.
   - **For Serbia we recommend to establish a supervisory body in the same domain as the institution responsible for national identification scheme is established (it might even be the same institution). We recommend to dedicate the supervisory body responsibilities as described in section 2 for institution, which already exists and has needed competences.**

3. **Conformity assessment body**
    - In the EU, there is no requirement for each member state to have a conformity assessment body, leaving the opportunity to use any existing / approved conformity assessment body within the EU. In EU member states, the conformity assessment body is established after passing specific procedure, which is certified as well as monitored by national accreditation body.
    - Since Serbia is not an EU member state, the eIDAS regulation is not applicable. Hence, there is no sound reason for Serbia to establish its own conformity body, and we recommend for Serbia **to use conformity assessment bodies approved by EU member states.** This way Serbia will not have to create any procedures for conformity assessment body for compliance confirmation, evaluation, etc.
    - It is important to note that the expertise of **the conformity assessment body can be used to check trusted service providers compliance with eIDAS regulations.** For this reason, amendments in the law should indicate conformity assessment bodies that can be used in Serbia.

4. **Trusted service providers**
    - In EU member states, the public and private entities approved by National supervisory body as trusted service providers can operate and deliver services in all EU member states. As Serbia is not an EU member state, service providers approved in Serbia as trusted service providers will be limited to the territory of Serbia. Nonetheless, Serbia is free to use trusted service providers operating in the EU.
    - As such, the Serbian legislation should be adapted to indicate that trusted services providers in the EU can also deliver services in Serbia. Besides, trusted services can create a new niche in market that can be used by local public and private entities. In particular, practice in the EU shows that trusted services can successfully be provided both by public entities and business entities; yet noting that major part of trusted services providers are businesses.
    - **We recommended for Serbia to establish a regulation, which allows the provision of trusted services by any entity should it be approved by the National supervisory body and having all procedures in place. In addition, we recommend to allow the market to use trusted services provided by EU trusted service providers[1].**

4.3. Trusted services

All trusted services in the context of eIDAS should be considered as separated services.

In the EU, there are a lot of service providers which implements trusted services (provided by other entities) in their software solutions. In particular, these providers develop document management systems, e-service portals, e-banking portals etc.

We recommend **for Serbia to focus on regulating trusted services whilst creating a dialogue with the market in order to prepare end-to-end software solutions where trusted services can be implemented (software solutions should have easy access and good user experience). In order to foster the usage of trusted services, the Government can create a demand for trusted services in the market through public initiatives (i.e. electronic delivery or archiving). These initiatives can then later be used by businesses or citizens.**

1. **Certificate services**
    - Certificate services are primary for the physical person, allowing identification of physical persons. Without this service no trusted services for physical person can be

[1] Trusted service providers browser is available https://webgate.ec.europa.eu/tl-browser/#/

available. eIDAS regulates different types of physical and virtual certificates and certificate creation devices.

- One of the toughest things in EU countries was to create real usage of certificate services, and this requires a clear and easy certificate issuance process. At this point of time, for the majority of EU countries, mobile certificates (integrated in SIM cards) are mostly used. One of the reasons is the easily accessible distribution channel – mobile operators have many sales points.
- In addition, a new type of certificate – cloud/virtual certificate – is emerging. The cloud certificate issuance procedure is directly related to the already existing certificate issued for physical person (i.e. with non-qualified certificate (e. banking), only non-qualified cloud certificate can be obtained; qualified certificate is necessary to obtain qualified cloud/virtual certificate).
- **We recommended for Serbia to leave the creation of certificate services to trusted service providers and only to regulate new solution introduction process (compliance and approval). We also recommend to include mobile operators in the certificate issuance processes, because mobile certificates can bring similar benefits as cloud/virtual ones. Healthy competition or cooperation between business and government entities can create new and more advanced solutions for certificate services. For this reason, technologies for trusted services should not be limited to one or several solutions.**

2. **Validation services**
   - Validation services are not directly connected to user experience, but yet they are very important for the identification / validity proof and software solutions development. Usually these services are connected to end software solutions and the user only receives information about the validity of signature or seal; all processes being performed on the backend of the software. It is important to mention that a minority of EU countries have validation service providers. As such, in the EU, a majority of EU member states uses validation service from service providers located in different countries.
   - **We recommend for Serbia to use EU trusted service providers for the validation services. As mentioned before, this service directly relates with providers of other trusted services and the establishment of validation service provider in Serbia might not generate enough demand, and hence not be financially beneficial.**

3. **Preservation services**
   - It is important to mention that the goal of trusted preservation services is closely related to electronic archiving, but in a narrower area. Preservation services are oriented towards the extension of trustworthiness in electronic signatures and electronic seals, whereas Electronic archiving covers areas like electronic document storage, document original and their copies, electronic document packages and process how electronic documents are received into electronic archiving systems.
   - **We recommend for Serbia to consider preservation services and electronic archiving as related but distinct topics as there might be different service providers for both electronic archiving and preservation services. In the EU, not all member states have service providers for qualified preservation services, mainly due to difficult security and process requirements for qualified preservation service providers. However, in the EU, service providers can provide services for other member states. Therefore, to use services provided by service providers in the EU, Serbia should translate these into the local legislation. On the other hand, Serbian businesses or public entities could also create and provide these services. In any case, these services should be evaluated by the conformity assessment body and later approved by the supervisory body. Certificates and seals storage preservation services for the end users should not be delivered as standalone services.**

4. **Time stamping services**
   - Timestamping service is a complementary service used to bind the date and the time to the electronic signature or electronic seal in order to preclude the possibility of changing undetectably data. It is also used in the process of electronic preservation service, providing additional time stamps to enhance security of electronic signature and electronic seal.
     We recommend for Serbia to raise awareness among businesses and to establish local service providers for timestamping services. This could also be a good business opportunity in the future when usage of electronic documents, signature and seals will develop in Serbia. Besides, the cooperation between different trusted service providers should be encouraged as well – as eIDAS allow trusted service to be separated. Any trusted service provider should provide to software providers clear services for their implementation.

5. **Delivery services**
   - Documents delivery between different government, business entities and citizens is the goal of trusted delivery services. These services allow, in a legitimised manner, the exchange of electronic documents for all physical bodies (including citizens) in all EU member states. It can also cover many technical issues related to the timing of delivery and the delivery of the original document. **For Serbia, it is recommend to use unified or integrated solutions provided by trusted service providers, which allow to deliver documents from one entity (citizen) to another. One of the main problems when delivery service are considered is the integration between different software solutions as trusted service provider can deliver closed software solutions, which will not deliver services between all bodies in the country. That is why Serbia should apply a single standard for delivery, which would ensure delivery between different software solutions. In addition, we recommend prioritisation of electronic document exchange between governmental institutions and use of solutions provided by market for this purpose. This way, new products could be developed, which would later serve the needs of citizens, businesses and government institutions.**