EU4Digital

EU4Digital: supporting digital economy and society in the Eastern Partnership

Legal and Technical Maturity Assessment of Trust and eID services in Eastern Partner Countries

March 2020

Table of contents

1 Executive Summary

The development of common frameworks and standards related to trust services and electronic identification are part of the six achievement areas of the EU Digital Single Market. A Digital Single Market (DSM) is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and engage in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.

In order to promote trust between citizens and organisations across the EU, the Regulation (EU) No 910 (hereafter the eIDAS Regulation), on electronic identification and trust services for electronic transactions in the internal market was drafted in 2014. The regulation stipulates the regulatory framework for electronic identification of natural and legal persons and for a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

Through the adoption of eIDAS it is possible to use these trust services as well as associated electronic documents as evidence in legal proceedings across the EU Member States contributing to their general usability within Member States and across borders. While the legal validity of trust services is warranted, Courts (or other adjudication bodies) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

Additionally, the eIDAS Regulation identifies trust in the online environment to leverage economic and social development. Standards for trust services need to be available to ensure solutions that are interoperable and provide coherent levels of trust. Whilst the eIDAS Regulation provides a common set of requirements, it does not necessarily identify how these requirements may be met following existing technology and organisational arrangements in place. Standards provide a generally accepted means to meet requirements with existing technology, whilst if necessary, the market can develop alternative solutions as new technology emerges to further feed into the standardisation life cycle.

1.1 Context

As part of the EU4Digital project the Trust and Security stream coordinates activities related to the promotion and increased usage of trust services between the EU member countries and the Eastern Partnership (EaP) member countries.

The main objective of the Trust and Security stream is to create the regional roadmap and national action plans towards mutual recognition of electronic identification means in the EaP region, based on eIDAS and in full compliance with the EU acquis for the EaP countries.

For mutual recognition of electronic identification means it is necessary to understand the current situation in different countries. According to eIDAS the electronic signature creating devices must correspond to certain criteria, but the means currently in use are different. During this activity the current situation in different EaP countries will be analysed both from organisational, juridical and technological perspective.

On 1 July 2016 the Regulation (EU) No 910/2014 entered in effect across all EU member states. Trust services providers across EU are required to comply with the eIDAS Regulation if they want to have their trust services recognised as means of identification and as evidence in legal proceedings across the EU Member States.

The eIDAS Regulation on electronic identification and trust services for electronic transactions in the internal market provides a regulatory environment for electronic identification of natural and legal persons and for a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication and it repeals Directive 1999/93/EC3. Under the eIDAS Regulation it is possible to use the trust services as well as electronic documents as evidence in legal proceedings in all EU Member States contributing to their cross-border use.

At their core, the signatures, seals, time stamps, registered delivery services and certificates for website authentication ensure that the integrity and non-repudiation of an electronic/digital information is maintained during the life cycle of that electronic/digital information.

In the eIDAS Regulation the following trust services are defined:

- electronic signature / qualified electronic signature;
- electronic seal / qualified electronic seal;

- electronic timestamp / qualified electronic timestamp;
- qualified website authentication certificate;
- electronic registered delivery service / qualified electronic registered delivery service;
- validation service / qualified validation service;
- preservation service / qualified preservation service.

The main objective of the present maturity assessment of trust and identification services (eID) is to identify the compatibility of the regulatory framework related to trust and eID of each of the EaP member countries with the ones currently used by the EU member states. The second objective of the maturity assessment is to assess the maturity of the trust and eID services from a regulatory, process and technical perspective in order to identify the measures that need to be adopted to enable cross-border mutual recognition of trust and electronic eID services between the EU and the EaP member countries.

1.2 Legal Assessment Results

EaP countries are currently offering most of the trust and eID services using compatible technologies with those deployed by the EU member states. The main differences between how the trust and eID services are delivered by each of the six EaP countries is determined by the regulatory frameworks which are implemented in their respective countries.

For each EaP country we reviewed the main regulatory frameworks and laws related to:

- trust services and digital signatures;
- electronic identification;
- data privacy and protection.

Based on the analysis of the legal frameworks, the answers gathered during interviews and the answers provided through questionnaires we compiled the following overview related to the delivery of trust and eID services in the EaP countries from a regulatory perspective.

Table A. Types of trust services delivered by Eastern Partnership countries

Country	Electronic Signatures	Electronic Seals	Website Authentication Certificates	eID	Mobile ID	Timestamp Services	Validation Services	Preservation Services	Remote signing Services
Armenia	YES	NO	NO	YES	YES	YES	YES	NO	NO
Azerbaijan	YES	YES	YES	YES	YES	YES	YES	YES	YES
Belarus	YES	YES	NO	NO	YES	YES	YES	NO	YES
Georgia	YES	YES	NO	YES	YES	YES	YES	NO	YES
Moldova	YES	NO	NO	YES	YES	YES	YES	NO	NO
Ukraine	YES	YES	NO	YES	YES	YES	YES	YES	YES

All EaP countries are offering electronic signatures and qualified electronic signatures:

Table B. Qualified electronic certificates availability in Eastern Partnership countries

Country	Electronic certificates	Qualified electronic certificates
Armenia	NO	YES
Azerbaijan	NO	YES
Belarus	NO	YES
Georgia	YES	YES

Country	Electronic certificates	Qualified electronic certificates
Moldova	NO	YES
Ukraine	YES	YES

Except for Moldova all other EaP countries perform audits of their TSPs based on a government approved audit scheme. More than half of the countries use also a secondary audit scheme based on an independent or industry accepted standards.

Table C. Implemented trust services audit schemes

Country	Government audit scheme	Independent or industry led audit scheme	Internal audit or self-assessment
Armenia	YES	YES	YES
Azerbaijan	YES	YES	YES
Belarus	YES	NO	YES
Georgia	YES	YES	NO
Moldova	YES	NO	YES
Ukraine	YES	YES	YES

Most EaP countries adopted their legal and regulatory frameworks related to trust and eID services based on national needs and requirements. Moldova and Ukraine followed the recommendations of the eIDAS Regulation while Azerbaijan adopted the CA Browser Forum recommendations (Webtrust).

Table D. Qualified electronic certificates availability in Eastern Partnership countries

Country	Based on EU eIDAS Regulation recommendations	Based on CA/Browser Forum recommendations	Based only on national needs and requirements
Armenia	NO	NO	YES
Azerbaijan	NO	YES	YES
Belarus	NO	NO	YES
Georgia	NO	NO	YES
Moldova	YES	NO	YES
Ukraine	YES	NO	NO

Even though all EaP countries have defined regulatory frameworks related to personal data protection and privacy, only two countries, Belarus and Moldova, adopted a subset of recommendations and best practices from the GDPR Regulation. All other EaP countries have defined data protection and privacy frameworks based on using their national needs and requirements.

Table E. Adoption of international guidelines and best practices for data protection and privacy

Country	Based on EU GDPR-Directive requirements	Based only on national needs and requirements
Armenia	NO	YES
Azerbaijan	NO	YES
Belarus	YES	YES
Georgia	NO	YES
Moldova	YES	YES
Ukraine	NO	YES

1.3 Technical Assessment Results

EaP countries are currently offering most of the trust and eID services using compatible technologies with those deployed by the EU member states. During the assessment we focused on identifying how many of the services described in the eIDAS Regulation are currently offered by the EaP countries. We identified the following services as being widely offered by the EaP countries:

- electronic signatures;
- electronic seals;
- timestamp services;
- revocation and validation services;
- eID and Mobile ID;
- preservation services.

The types of electronic signatures currently issued by each of the six EaP countries is presented below. All six EaP countries are issuing qualified electronic signatures and except for Armenia and Moldova the remaining EaP countries can also issue qualified remote signatures.

Table F. Types of electronic signatures delivered

Country	Unqualified electronic signature	Qualified electronic signature	Qualified remote signature
Armenia	NO	YES	NO
Azerbaijan	YES	YES	YES
Belarus	NO	YES	YES
Georgia	YES	YES	YES
Moldova	NO	YES	NO
Ukraine	YES	YES	YES

Except for Belarus, all other EaP countries can issue advanced electronic signatures using at least one of the following “AdES” extensions.

Table G. Advanced signature profiles used by Eastern Partnership countries

Country	CAdES	XAdES	PAdES	PKCS#7	DSS
Armenia	YES	YES	YES	YES	NO
Azerbaijan	YES	YES	YES	YES	NO
Belarus	NO	NO	NO	YES	NO
Georgia	YES	YES	YES	NO	NO
Moldova	YES	YES	YES	YES	YES
Ukraine	YES	YES	YES	YES	NO

While assessing the usage of electronic seals in the EaP countries, one key comment must be given: in all EaP countries the electronic signature of an individual who is entitled and has the power to sign documents on behalf of an organisation/entity enjoys the same benefits of an individual using an electronic seal to perform the same actions on behalf of an organisation. It was observed that in Eastern Partnership countries electronic signatures are used for the purposes for which electronic seals were created, and thus we recommend for Eastern Partnership countries to strengthen the use of electronic seals by organizations as opposed to electronic signatures for specific business use cases.

From the technical perspective there are small differences between electronic certificates and electronic seals, mainly in the certificate fields and profile, differences which can be overcome with ease in order to issue electronic seals.

Table H. Types of electronic seals delivered

Country	Unqualified electronic seals	Qualified electronic seals
Armenia	NO	YES
Azerbaijan	YES	YES
Belarus	NO	YES
Georgia	YES	YES
Moldova	NO	NO
Ukraine	YES	YES

Except for Belarus all EaP countries use one of the internationally accepted protocols for timestamps.

Table I. Types of electronic timestamps delivered

Country	RFC 3161 Time Stamp Protocol	DSS XML Time Stamping Profile
Armenia	YES	NO
Azerbaijan	YES	NO
Belarus	NO	NO
Georgia	YES	NO
Moldova	YES	NO
Ukraine	YES	YES

All EaP countries are currently providing both the CRL and the OCSP protocol for certificate revocation status and validity status.

Table J. Types of certificate validation mechanisms delivered

Country	Certificate Revocation List (CRL)	Online Certificate Status Protocol (OCSP)
Armenia	YES	YES
Azerbaijan	YES	YES
Belarus	YES	YES
Georgia	YES	YES
Moldova	YES	YES
Ukraine	YES	YES

All EaP countries are currently offering at least a form of electronic identification, either through eIDs or through mobile IDs.

Table K. Means of electronic identification in Eastern Partnership countries

Country	Electronic Identification	Mobile ID
Armenia	YES	YES
Azerbaijan	YES	YES

Country	Electronic Identification	Mobile ID
Belarus	NO	YES
Georgia	YES	YES
Moldova	YES	YES
Ukraine	YES	YES

Certificate preservation services ensure that signed objects don't lose their evidential value in case cryptographic algorithms become weak, and they maintain the integrity and authenticity of signed data for long periods of time, beyond the validity of the electronic certificate. In the EU there are only a few TSP service providers who are able to provide certificate preservation services. Azerbaijan and Ukraine are the only countries in the EaP who offer certificate preservation services.

Table L. Certificate preservation services in Eastern Partnership countries

Country	Certificate preservation services	Qualified certificate preservation services
Armenia	NO	NO
Azerbaijan	YES	YES
Belarus	NO	NO
Georgia	NO	NO
Moldova	NO	NO
Ukraine	YES	YES

1.4 Preliminary Legal and Technical Recommendations to Achieve Cross-Border Mutual Recognition of Digital Trust Services

One of the main objectives in the EaP region is to achieve cross-border mutual recognition of digital trust services with the EU members states. It is the basic requirement in a digital society to be able to recognise, and to give legal value to the will of an individual or entity expressed through an electronic mechanism, as long as that electronic mechanism is reliable, secure, ensures non-repudiation and it can be validated by all parties who recognise that electronic mechanism.

Therefore, several actions need to be performed in order to achieve this objective. In the EU cross-border mutual recognition of digital trust services was achieved by adopting the eIDAS Regulation - a regulation which provided common regulatory and technical requirements to all trust services providers in all EU member states. One of the results that came after the adoption of the eIDAS Regulation was that the trust service providers adopted compatible technical mechanisms and common workflows related to the issuance and management of digital trust services for the EU citizens.

Technical and regulatory compatibility of mechanisms used in providing digital trust services between participating countries is important for achieving cross-border mutual recognition of electronic based identification services for the civil population and companies. This distinction is important because digital trust services based on cryptography are used for various purposes including:

- encryption of electronic data;
- encryption of communications;
- electronic signatures for code-signing of software products;
- various military applications including the protection of classified information.

The EU4Digital's Trust and Security stream activities and objectives are restrained to the electronic trust services designed to ensure the identification of citizens and companies through secure electronic mechanisms that have legal value, and which enable the citizens and companies to electronically sign legal documents, contract etc.

1.5 Preliminary Legal Recommendations to Achieve Cross-Border Mutual Recognition of Digital Trust Services

From the legal maturity perspective there were two aspects which were analysed: the regulatory framework around the digital trust services and the data protection and privacy framework. Most of the countries from the EaP region have the legal maturity rating of at least 3, meaning that all digital trust services are clearly defined.

The main recommendation is to improve the maturity rating to 4. This rating can be achieved by implementing clear metrics for all processes impacting digital trust services including:

- adoption of international accepted standards for information security management (e.g. ISO 27001);
- performing regular audits of the digital trust services infrastructure and processes using international accepted standards (e.g. ISO 27001, eIDAS audit);
- regulatory clarification between the purpose of electronic signatures and electronic seals;
- regulatory clarification on the specific requirements for the mechanisms used to achieve the qualified status of digital trust services (e.g. usage of FIPS or EAL compliant technical mechanisms).

The recommendations related to the data protection and privacy regulatory aspects are the following:

- Adequate measures should be defined to ensure the protection of personal identifiable information and their accepted use, especially in the context of widespread cross-border transfer of personal identifiable information between the EU member states and the EaP countries.
- Specific measures should be defined to protect the personal identifiable information contained in the digital trust services, specially qualified digital signatures, from misuse in activities like behaviour profiling without prior user consent.

After the adoption of the GDPR Regulation, the EU member states need to ensure that adequate security controls are in place in non-EU countries to process the personal identifiable information (cross-border transfer of personal information).

1.6 Preliminary Technical Recommendations to Achieve Cross-Border Mutual Recognition of Digital Trust Services

There were three aspects from the technical maturity perspective which were analysed: the types of trust services offered, the technical compatibility of the encryption schemes and algorithms and the maturity of the processes supporting the trust services.

There are no recommendations to be given on the first two analysed aspects since the issued trust services and the encryption schemes are compatible with those currently used by the EU member states.

The technical maturity rating ranges between 2 and 4 among the six EaP region countries. The main recommendation is to improve the technical maturity rating to at least 3, meaning a defined state.

Most of the measures that should be adopted revolve around technical security controls with the aim to improve the resilience against cyber-attacks of the infrastructures who support the delivery of digital trust services. The logical and cybersecurity control should balance the physical and perimeter controls which are in place in all EaP countries, controls which are more than adequate to ensure the security of the physical locations form where the digital trust services are delivered.

2 Methodology

The legal and technical maturity assessment is based on the following activities:

- research of current trust services offered by the each of the EaP member countries;
- interviews and meetings with the relevant stakeholders form each of the EaP member countries;
- a questionnaire designed to identify statistics about the market penetration of trust services and eID in each of the EaP member countries;
- a questionnaire designed to identify the types of trust services which are currently offered by each of the EaP countries;
- a detailed legal questionnaire designed to identify and measure the organisational processes and common workflows used to provide the trust services;
- a detailed technical questionnaire designed to identify and measure the organisational processes and common workflows used to provide the trust services.

2.1 Interviews and meetings

Invitations to participate in the study was sent to the expert group and other EaP representatives, responsible for the trust and eID services in their country. The stakeholders from the EaP region involved in the project included mainly the representatives of the national cyber security authorities, national regulatory authorities/institutions, responsible for initiating and developing trust services and eID policies and regulations or ministries responsible for communication and information technologies, trust and eID services or cybersecurity. The following public organisation or national authorities were engaged:

- **Armenia** – representatives from public organisations, e.g. EKENG CJSC – Office of Implementation of Electronic Governance Infrastructure, coordinator of e-government projects in the Republic of Armenia, founded by the Government of the Republic of Armenia and Ministry of High-tech Industries of the Republic of Armenia;
- **Azerbaijan** – representatives from public authorities, e.g. Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, governmental agency within the Cabinet of Azerbaijan in charge of regulation of the communications sector and development of information technologies in the country;
- **Belarus** – representatives from public authorities under the President of the Republic of Belarus;
- **Georgia** – representatives from public authorities, e.g. LEPL Public Service Development Agency is a legal entity of public law (LEPL) operating under the management of Ministry of Justice of Georgia;
- **Moldova** – representatives from public authorities, e.g. Ministry of Economy and Infrastructure, SIS - Intelligence Service and STISC - Telecommunication Intelligence Service;
- **Ukraine** – representatives from public authorities, e.g. State Service of Special Communication and Information Protection of Ukraine and the Ministry of Digital Transformation.

2.2 Market penetration questionnaire

The market penetration questionnaire has two sections. The first section was designed to capture the general information the EaP member countries related to trust and eID services:

- country name;
- types of provided trust and eID services;
- number of trust service providers (digital signatures and eID) in the country;
- number of trust service providers as public entities;
- number of trust service providers as private entities;
- estimated volume of customers;
- jurisdictions in which the organisations operate;

- jurisdictions where employees are located;
- name of conformity assessment bodies (CAB) for trust services in the country;
- name of supervisory bodies (Regulatory Authorities) for trust services in the country.

The second section of the market penetration questionnaire was designed to gather statistical data about:

- percent of households having access to broadband internet;
- percent of people per year using e-services;
- percent of people per year using eGovernment and eBusiness services;
- percent of people using eSignatures;
- percent of businesses using eSeals;
- percent of people that have been issued an eID card (electronic identification card);
- percent of people using certificates for website authentication;
- percent of increased volume of trusted electronic documents exchanged between enterprises for cross-border trade.

2.3 Trust and eID services questionnaire

The trust and eID services questionnaire is the main questionnaire used to identify the compatibility between what types of trust services and eID services are provided and the technologies used to deliver them. Technical compatibility between the technologies used to deliver trust and eID services is important in order to enable cross-border mutual recognition of those services. The questionnaire is composed of 28 close-ended questions and it is divided into 9 sections.

2.4 Detailed legal and technical assessment questionnaires

The detailed legal and technical assessment questionnaire was designed using the internationally accepted frameworks, standards and best practices related to the delivery of trust and eID services presented in Table 1. They are based on the ETSI standards, AICPA/CICA Webtrust and the GDPR Regulation.

Table 1: Frameworks, standards and best practices used to design the legal maturity assessment

Standard	Area	Description
AICPA/CICA WebTrust Principles and Criteria for Certification Authorities	TSP Functions: Certification Authorities (CA) and Registration Authorities (RA)	Guidelines and principles for the general requirements and characteristics to operate a Trust Service Provider (TSP) with both functions RA and CA. The guidelines are applicable for general CA functions, RA functions, certificate issuance, preservation, key archival and validation services.
GDPR Regulation	Data Privacy and Protection	Data privacy and protection requirements for cross-border mutual recognition of eID and trust services between EU and EaP.
TR 119 400	Trust Service Providers Supporting Digital Signatures	Guidance on the use of standards for trust service providers supporting digital signatures
EN 319 403	Trust Service Providers Supporting Digital Signatures	Requirements for conformity assessment bodies assessing Trust Service Providers

Standard	Area	Description
EN 319 401	Trust Service Providers Supporting Digital Signatures	General Policy Requirements for Trust Service Providers
EN 319 411	Trust Service Providers Supporting Digital Signatures	Policy and security requirements for Trust Service Providers issuing certificates
EN 319 421	Trust Service Providers Supporting Digital Signatures	Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamping Signatures
TS 119 441	Trust Service Providers Supporting Digital Signatures	Policy requirements for TSP providing signature validation services
TS 119 431	Trust Service Providers Supporting Digital Signatures	Policy and security requirements for trust service providers; TSP service components
TS 119 431	Trust Service Providers Supporting Digital Signatures	Policy and security requirements for trust service providers; TSP service components
EN 319 412	Trust Service Providers Supporting Digital Signatures	Certificate Profiles
EN 319 422	Trust Service Providers Supporting Digital Signatures	Time-stamping protocol and electronic time-stamp profiles
TS 119 432	Trust Service Providers Supporting Digital Signatures	Protocols for remote digital signature creation
TS 119 442	Trust Service Providers Supporting Digital Signatures	Protocol profiles for trust service providers providing AdES digital signature validate
TR 119 100	Signature Creation and Validation	Guidance on the use of standards for signatures creation and validation
TS 119 101	Signature Creation and Validation	Policy and security requirements for applications for signature creation and signature
EN 319 102	Signature Creation and Validation	Procedures for Creation and Validation of AdES Digital Signatures
TS 119 102	Signature Creation and Validation	Procedures for Creation and Validation of AdES Digital Signatures
EN 319 122	Signature Creation and Validation	CAdES digital signatures
EN 319 132	Signature Creation and Validation	XAdES digital signatures
EN 319 142	Signature Creation and Validation	AdES digital signatures

Standard	Area	Description
EN 319 142	Signature Creation and Validation	PAdES digital signatures
EN 319 162	Signature Creation and Validation	Associated Signature Containers (ASiC)
TS 119 172	Signature Creation and Validation	Signature policies
TR 119 300	Cryptographic Suites	Business guidance on cryptographic suites
TS 119 312	Cryptographic Suites	Cryptographic Suites
SR 019510:	Preservation	Framework for standardisation of long-term data preservation services
TS 119 511	Preservation	Policy & security requirements for trust service providers providing long-term preservation
TS 119 512	Preservation	Protocols for trust service providers providing long-term preservation of digital signatures
EN 319 521	eDelivery	Policy and Security Requirements for Electronic Registered Delivery Service Providers
EN 319 531	eDelivery	Policy and Security Requirements for Electronic Registered Electronic Mail Service Providers
EN 319 522	eDelivery	Electronic Registered Delivery Services
EN 319 532	eDelivery	Registered Electronic Mail (REM) Services

Source: Developed by EU4Digital Facility

The assessments are composed of eight maturity areas totalling a number of 383 questions for the legal assessment and 521 questions for the technical assessment as presented below in Tables 2 and 3:

Table 2: Legal maturity areas

Legal Maturity Area	Number of questions
Trust Services Practice Disclosure	16
Trust Services Practice Management	11
Trust Services Environmental Controls	160
Trust Services Key Lifecycle Management	65
Trust Services Subscriber Key Lifecycle Management	14
Trust Services Certificate Lifecycle Management	36
Trust Services Cross Certificate Lifecycle Management	3
Data privacy and protection	78

Source: Developed by EU4Digital Facility

Table 3: Technical maturity areas

Technical Maturity Area	Number of questions
Trust Services Environmental Controls	221
Trust Services Key Lifecycle Management	115
Trust Services Subscriber Key Lifecycle Management	74
Trust Services Certificate Lifecycle Management	99
Trust Services Cross Certificate Lifecycle Management	12

Source: Developed by EU4Digital Facility

Table 4: Maturity areas description

Legal Maturity Area	Description
Trust Services Practice Disclosure	The means that Information regarding the TSP's business practices is made available to all subscribers and all potential relying parties
Trust Services Practice Management	The TSP maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.
Trust Services Environmental Controls	The measures and controls in place to establish and maintain a trustworthy TSP environment, that is essential to the reliability of the TSP's business processes
Trust Services Key Lifecycle Management	The effective controls maintained by TSP to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their life cycles.
Trust Services Subscriber Key Lifecycle Management	The effective controls maintained by TSP to provide reasonable assurance that the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles.
Trust Services Certificate Lifecycle Management	The effective controls maintained by TSP to provide reasonable assurance that Subscriber information was properly authenticated
Trust Services Cross Certificate Lifecycle Management	The effective controls maintained by TSP to provide reasonable assurance that subordinate CA's and cross certificate requests are accurate, authenticated and approved.
Data privacy and protection	The measures and controls in place to assure the privacy and protection of personal data.

Source: Developed by EU4Digital Facility

The questions are designed to be close-ended. Each question describes a process or best practice related to the issuance, management and destruction of trust and eID services. For each question there are six possible answers based on how the process or best practice is delivered by the trust service provider (TSP).

All TSPs operate under a regulatory framework (national or international) in each of the EaP member countries. The results of both the legal and technical maturity assessment were designed to identify if there are specific requirements mentioned in the regulatory frameworks of each EaP member country related to the technical

requirements which must be met by all TSPs, and how mature these requirements are compared to the ones described in Table 1. The maturity scale is presented in Table 5. It is composed of five maturity levels.

Table 5: Maturity levels description

Maturity Level	Description
N/A	Not applicable to the organisation / entity.
(1) Ad-Hoc	The process, function or feature exist but is not documented. The process workflow is not defined and formally assumed by the entity. Clear roles and responsivities were not defined.
(2) Managed	Parts of the process, functions and features are documented and managed. General roles and responsibilities exist but clear roles and responsivities were not defined.
(3) Defined	The process, functions and features are documented. Clear roles and responsivities are defined.
(4) Defined and Measured	The process, functions and features are documented. Clear roles and responsivities are defined. Metrics and measures are defined to measure process and functions performance.
(5) Optimised	The process, functions and features are documented. Clear roles and responsivities are defined. Metrics and measures are defined to measure process and functions performance. The processes, functions and features are controlled, audited and are being optimised based on the audit results.

Source: Developed by EU4Digital Facility

3 General presentation of trust and electronic identification services

Trust and electronic identification services at its core represent an application of public key cryptography. These algorithms are used to create electronic certificates which store specific information designed to be used as a means to ensure:

- the confidentiality of electronic information or data;
- the integrity of electronic information or data;
- the non-repudiation of a person's actions on electronic information or data.

The public key cryptography algorithms are implemented in solutions generally called Public Key Infrastructures (PKI). A PKI solution has the following components:

- A registration authority (RA) which has the processes in place to register new users into the PKI; and it also performs the identity validation of each user.
- A certification authority (CA) which has the technical processes in place to issue electronic certificates from the PKI.
- A mechanism to revoke and check the validity of issued electronic certificates via Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP).

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. PKI facilitates the secure electronic transfer of information for a range of network activities including, but not limited to, e-commerce, internet banking and confidential email. PKI enables parties to identify one another by providing authentication with digital certificates and allows reliable business communications by providing confidentiality through the use of encryption, and authentication data integrity and a reasonable basis for nonrepudiation through the use of digital signatures.

PKI uses public/private-key pairs—two mathematically related keys. Typically, one of these keys is made public, by posting it on the Internet for example, while the other remains private. Public-key cryptography works in such a way that a message encrypted with the public key can only be decrypted with the private key, and, conversely, a message signed with a private key can be verified with the public key. This technology can be used in different ways to provide the four ingredients required for trust, namely: confidentiality, authentication, integrity, and nonrepudiation.

Using PKI, a subscriber (meaning an end entity (or individual) whose public key is cryptographically bound to his or her identity in a digital certificate) has an asymmetric cryptographic key pair (meaning a public key and a private key). The subscriber's private key must be kept secret, whereas the public key may be made widely available, usually presented in the form of a digital certificate to ensure that relying parties know with confidence the identity to which the public key belongs. Using public key cryptography, the subscriber could send a message signed with his or her private key. The signature can be validated by the message recipient using the subscriber's public key. The subscriber could also encrypt a message using the recipient's public key. The message can be decrypted only with the recipient's private key.

A subscriber first obtains a public/private key pair (generated by the subscriber or for the subscriber as a service). The subscriber then goes through a registration process by submitting their public key to a Certification Authority or a Registration Authority (RA), which acts as an agent for the CA. The CA or RA verifies the identity of the subscriber in accordance with the CA's established business practices (that may be contained in a Certification Practice Statement), and then issues a digital certificate. The certificate includes the subscriber's public key and identity information, and is digitally signed by the CA, which binds the subscriber's identity to that public key. The CA also manages the subscriber's digital certificate through the certificate life cycle (meaning, from registration through revocation or expiration). In some circumstances, it remains important to manage digital certificates even after expiry or revocation so that digital signatures on stored documents held past the revocation or expiry period can be validated at a later date.

3.1 Electronic signature and non-repudiation

Electronic signature or digital signature is a mathematical technique that can be used to provide authentication, integrity, and nonrepudiation for various digital items including a message, document, or software code.

Establishing a reasonable basis for nonrepudiation requires that the private key used to create a digital signature (meaning, the signing private key) be generated and stored securely under the sole control of the user. In the event a user forgets his or her password or loses, breaks, or destroys his/her signing private key, it is acceptable to generate a new signing key pair for use from that point forward with minimal impact to the subscriber. Previously signed documents can still be verified with the user's old signature verification public key. Documents subsequently signed with the user's new signing private key must be verified with the user's new signature verification public key.

Extra care is required to secure the Certification Authority's signing private key, which is used for signing user certificates. The trustworthiness of all certificates issued by a CA depends upon the CA's protecting its private signing key. CAs securely back up their private signing key(s) for business continuity purposes to allow the CA to continue to operate in case the CA's private signing key is accidentally destroyed (but not compromised) as a result of hardware failure, for example.

Except for CA business continuity purposes, there are generally no technical or business reasons to back up a signing private key. The leading practice is for a CA's private signing key to be protected in a properly secured Hardware Security Module (HSM) deployed and maintained in compliance with leading security practices.

On the other hand, it is often desirable that a key pair used for encryption and decryption is securely backed up to ensure that encrypted data can be recovered if a user forgets his or her password or otherwise loses access to his or her decryption key. This is analogous to requiring that the combination to a safe is backed up in case the user forgets it or becomes incapacitated. As a result, a PKI typically requires two key pairs for each user: one key pair for encryption and decryption and a second key pair for signing and signature verification.

3.2 Registration Authority

A Registration Authority (RA) is an entity that is responsible for the identification and authentication of subscribers but does not sign or issue certificates. In some cases, the CA performs the subscriber registration function internally. In other cases, the CA might delegate the RA function to external registration authorities (sometimes referred to as Local Registration Authorities or LRAs) that may or may not be part of the same legal entity as the CA. In still other cases, a customer of a CA may arrange with that CA to perform the RA function itself or use its agent.

The initial registration process for a subscriber is as follows, though the steps may vary from CA to CA and also depend upon the Certificate Policy under which the certificate is to be issued. The subscriber first generates his or her own public/private key pair, which is submitted to the CA as part of the Certificate Signing Request (CSR). The CSR contains the subscriber's public key and is signed with its private key allowing the CA to verify that the subscriber is indeed in possession of the private key. In some implementations, a CA may generate the subscriber's key pair and securely deliver it to the subscriber, but this is normally done only for encryption key pairs, not signature key pairs. Then the subscriber produces proof of identity in accordance with the applicable Certificate Policy requirements and demonstrates that he or she holds the private key corresponding to the public key without disclosing the private key (typically by digitally signing a piece of data with the private key, with the subscriber's digital signature then verified by the CA).

Once the association between a person and a public key is verified, the CA issues a certificate. The CA digitally signs each certificate that it issued with its private key to provide the means for establishing authenticity and integrity of the certificate.

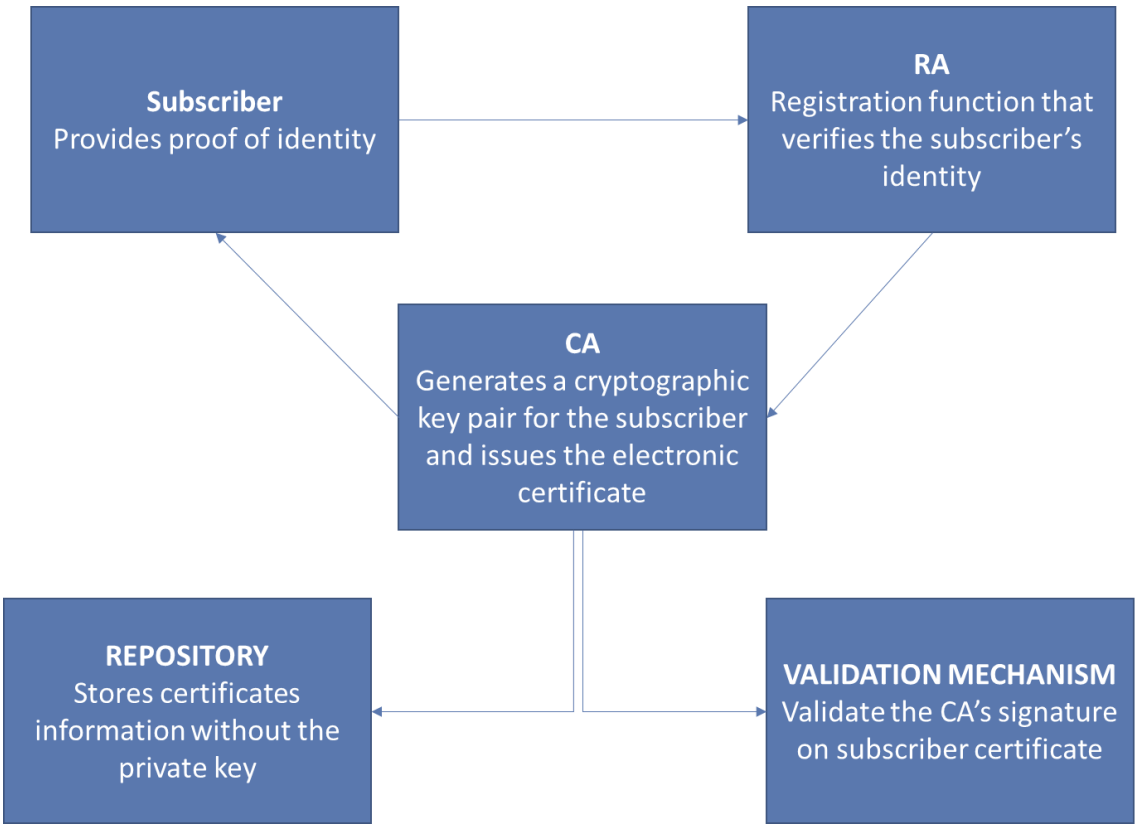
The CA then notifies the subscriber of certificate issuance and gives the subscriber an opportunity to review the contents of the certificate before it is made public. Assuming the subscriber approves the accuracy of the certificate, the subscriber will publish the certificate and/or have the CA publish it and make it available to other users. A repository is an electronic certificate database that is available online. The repository may be maintained by the CA or a third party contracted for that purpose, or by the subscriber, or by any other party. Subscribers may obtain certificates of other subscribers and certificate status information from the repository. For example, if a subscriber's certificate was revoked, the repository would indicate that the subscriber's certificate has been revoked and should not be relied upon. The ability to update the repository is typically retained by the CA. Subscribers and other relying parties would have read-only access to the repository. Because the certificates stored in the repository are digitally signed by the CA, they cannot be maliciously changed without detection, even if someone were to hack into the repository.

3.3 Certification authority

In order for these technologies to enable parties to securely communicate, the trust relationship between the user and the organisation which issues and manages the electronic signatures needs to be absolute.

A digital certificate, which is an electronic document containing information about an individual and his or her public key, is used to enforce this. This document is digitally signed by a trusted organisation referred to as a Certification Authority (CA). The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate. The digital signature placed on the public key certificate by the CA provides the cryptographic binding between the entity's public key, the entity's name, and other information in the certificate, such as a validity period. For a relying party to determine whether the certificate was issued by a legitimate CA, the relying party must verify the issuing CA's signature on the certificate.

The purpose of a CA is to manage the certificate life cycle, which includes generation and issuance, distribution, renewal and rekey, revocation, and suspension of certificates. In some cases, the CA delegates the initial registration of subscribers to Registration Authorities (RAs) that act as agents for the CA. In others, the CA also acts as the RA and may perform registration functions directly. The CA is also responsible for providing certificate status information through the issuance of Certificate Revocation Lists (CRLs) and/or the maintenance of an online status checking mechanism such as the Online Certificate Status Protocol (OSCP). Typically, the CA posts the certificates and CRLs that it has issued to a repository (such as an online directory) which is accessible to relying parties.



4 Overview of trust and electronic identification regulatory frameworks in the EaP member countries

EaP countries are currently offering most of the trust and eID services using compatible technologies with those deployed by the EU member states. The main differences between how the trust and eID services are delivered in each of the six EaP countries is determined by the regulatory frameworks which are implemented in their respective countries.

For each EaP country we reviewed the main regulatory frameworks and laws related to:

- trust services and digital signatures;
- electronic identification;
- data privacy and protection.

Table 6: Regulatory frameworks related to trust, eID and data protection in the EaP countries

Country	Legal frameworks related to trust services and eID	Legal frameworks related to data privacy and protection
Armenia	Law of the Republic of Armenia of 15 January 2005 No. ZR-40 "About the electronic document and the electronic digital signature" (as amended on 29 March 2018)	Law of the Republic of Armenia of 13 June 2015 No. ZR-49 "About personal data protection" (as amended on 23 July 2019)
Azerbaijan	Resolution of the Cabinet of Ministers of the Azerbaijan Republic of 28 January 2006 No. 27 "About approval of some regulatory legal acts connected by the digital signature and the electronic document in the Azerbaijan Republic" (as amended on 4 September 2019) Law of the Azerbaijan Republic of 9 March 2004 No. 602-IIG "About the digital signature and the electronic document" (as amended on 11 November 2016)	Law of the Azerbaijan Republic of 3 April 1998 No. 460-IG "About information, informatisation and information protection" (as amended on 19 November 2019) Resolution of the Cabinet of Ministers of the Azerbaijan Republic of 2 March 2011 No. 35 "About approval of Rules of transfer to the third parties on paid basis of the personal and collected in enterprise information systems data used" Resolution of the Cabinet of Ministers of the Azerbaijan Republic of 12 December 2010 No. 237 "About approval of "The personal data information systems which are not subject to state registration" Resolution of the Cabinet of Ministers of the Azerbaijan Republic of 17 August 2010 No. 149 "About approval of Rules of state registration of personal data information systems and cancellations of state registration" (as amended on 13 June 2014)
Belarus	Order of Operational analytical centre in case of the President of the Republic of Belarus of 8 February 2019 No. 45 "About additional measures for implementation of the Law of the Republic of Belarus of December 28, 2009 No. 113-Z "About the electronic document and the electronic digital signature" Order of Operational analytical centre in case of the President of the Republic of Belarus of 10 December 2015 No. 118 "About approval of the Regulations on	Law on Information, Informatisation and Information Protection of 10 November 2008 No. 455-Z Law on Population Register of 21 July 2008 No. 418-Z

Country	Legal frameworks related to trust services and eID	Legal frameworks related to data privacy and protection
	the State management system public keys of verification of the electronic digital signature of the Republic of Belarus" (as amended on 8 February 2019) Order of Operational analytical centre in case of the President of the Republic of Belarus of 29 November 2013 No. 89 "About approval of the Instruction about procedure for carrying out accreditation of service providers in the State management system public keys of verification of the electronic digital signature of the Republic of Belarus and control of observance of conditions of accreditation" (as amended on 8 February 2019) Law of the Republic of Belarus of 28 December 2009 No. 113-Z "About the electronic document and the electronic digital signature" (as amended on 8 November 2018)	
Georgia	Law of Georgia On Electronic Signatures and Electronic Documents	Law of Georgia On Personal Data Protection
Moldova	Order of the Government of the Republic of Moldova of 28 March 2006 No. 320 "About approval of the Regulations on procedure for application of the digital signature in electronic documents of bodies of the public power" (as amended on 20 July 2011) Order of Service of information and safety of the Republic of Moldova of 16 April 2009 No. 29 "About approval of Regulations about permission of disputable situations in the field of application of the digital signature" (as amended on 15 July 2016) Law of the Republic of Moldova of 29 May 2014 No. 91 "About the digital signature and the electronic document" (as amended on 30 November 2018) Order of the Government of the Republic of Moldova of 2 June 2014 No. 405 "About the integrated government electronic service of the digital signature (MSign)" (as amended on 8 May 2018) Order of the State office of the Republic of Moldova of 18 November 2015 No. 645 "About approval of Rules about procedure for administration of the integrated government electronic service of the signature (Msign)" Order of Service of information and safety of the Republic of Moldova of 15 July 2016 No. 70 "About	Law of the Republic of Moldova of 8 July 2011 No. 133 "About personal data protection" (as amended on 23 November 2018) Order of the Government of the Republic of Moldova of 14 December 2010 No. 1123 "About approval of Safety requirements of personal data in case of their processing in personal data information systems" Law of the Republic of Moldova of 10 October 2013 No. 229 "About approval of National strategy in personal data protection for 2013-2018 and the Action plan on its implementation" Order of the Government of the Republic of Moldova of 15 May 2012 No. 296 "About approval of the Regulations on the register of accounting of controllers of personal data"

Country	Legal frameworks related to trust services and eID	Legal frameworks related to data privacy and protection
	approval of some regulations in the sphere of the organisation of activities of suppliers of certified services in scope of the digital signature” Order of Service of information and safety of the Republic of Moldova of 15 July 2016 No. 69 “About approval of Technical regulations in the field of the strengthened qualified digital signature” (as amended on 2 May 2018) Order of the Government of the Republic of Moldova of 21 December 2016 No. 680 “About approval of the Standard agreement and Standard agreement about integration of services in application and check of authenticity of the digital signature with the integrated government electronic service of the digital signature (Msign)” Order of Service of information and safety of the Republic of Moldova of 17 March 2017 No. 25 “About approval of Regulations of the procedure of issue of the conclusions on devices of creation and/or verification of the digital signature and products for the digital signature” (as amended on 8 October 2018)	
Ukraine	Resolution of the Cabinet of Ministers of Ukraine of 23 January 2019 No. 60 “About approval of the Procedure for mutual recognition of the Ukrainian and foreign certificates of public keys, digital signatures, and also uses of information and telecommunication system of the Central Zaveritelny body for ensuring recognition in Ukraine of electronic confidential services, foreign certificates of the public keys used by provision of legally significant electronic services in the course of interaction between subjects of the different states” (as amended on 11 December 2019) Resolution of the Cabinet of Ministers of Ukraine of 16 November 2016 No. 821 “Some questions of licensing of economic activity on provision of services in the field of cryptographic information security (except services of the digital signature) and technical information security according to the list which is determined by the Cabinet of Ministers of Ukraine” Order of the Ministry of Justice of Ukraine of 1 November 2012 No. 1600/5 “About approval of the Operating procedure with electronic documents through system of electronic interaction of executive bodies with use of the digital signature” Order of Administration of Public service of special communication and information protection of	Order of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine of 8 January 2014 No. 1/02-14 “About document approval in the sphere of personal data protection” Order of the Ministry of Justice of Ukraine of 22 June 2012 No. 947/5 “About approval of the Procedure by Public service of Ukraine concerning personal data protection of the state control of compliance with law about personal data protection” (ceased to be valid since 24 January 2014) Law of Ukraine of 1 June 2010 No. 2297-VI “About personal data protection” (as amended on 3 December 2019)

Country	Legal frameworks related to trust services and eID	Legal frameworks related to data privacy and protection
	Ukraine of 24 July 2007 No. 143 “About approval of the Regulations on procedure of the state control of observance of requirements of the legislation in the field of the electronic digital signature” (as amended on 10 June 2016)	

Source: Developed by EU4Digital Facility

Based on the analysis of the legal frameworks, the answers gathered during interviews and the answers provided through questionnaires we compiled the following overview related to the delivery of trust and eID services in the EaP countries from a regulatory perspective. All EaP countries are offering electronic signatures and qualified electronic signatures as presented in Table 7 and Table 8.

Table 7: Types of trust and eID services delivered by the EaP countries

Country	Electronic Signatures	Electronic Seals	Website Authentication Certificates	eID	Mobile ID	Timestamp Services	Validation Services	Preservation Services	Remote signing Services
Armenia	YES	NO	NO	YES	YES	YES	YES	NO	NO
Azerbaijan	YES	YES	YES	YES	YES	YES	YES	YES	YES
Belarus	YES	YES	NO	NO	YES	YES	YES	NO	YES
Georgia	YES	YES	NO	YES	YES	YES	YES	NO	YES
Moldova	YES	NO	NO	YES	YES	YES	YES	NO	NO
Ukraine	YES	YES	NO	YES	YES	YES	YES	YES	YES

Source: Developed by EU4Digital Facility

Website authentication certificates and certificate preservation services are the least offered services in the EaP countries. The market for website authentication certificates is currently dominated by international commercial companies and certificate preservation services are difficult to implement and operate.

Table 8: Trust versus qualified trust services in the EaP countries

Country	Electronic certificates	Qualified electronic certificates
Armenia	NO	YES
Azerbaijan	NO	YES
Belarus	NO	YES
Georgia	YES	YES
Moldova	NO	YES
Ukraine	YES	YES

Source: Developed by EU4Digital Facility

Most EaP region countries follow the recommendations of ISO 27001, the international standard covering information security management systems, and the ETSI technical standards related to electronic signatures as presented in Table 9.

Table 9: Adoption of international standards for TSP services delivery and management

Country	ISO/IEC 27001 Information Security Management	ISO/IEC 22301 Business Continuity Management	ISO/IEC 38500 IT Governance	ETSI STANDARDS	AICPA WEBTRUST
Armenia	YES	YES	YES	YES	N/A
Azerbaijan	YES	Compatible	Compatible	YES	YES
Belarus	Compatible	Compatible	Compatible	NO	N/A
Georgia	YES	Compatible	Compatible	YES	N/A
Moldova	YES	Compatible	Compatible	YES	N/A
Ukraine	YES	Compatible	Compatible	YES	N/A

Source: Developed by EU4Digital Facility

All EaP countries offer trust and eID services to all categories of citizens and most of them offer specific trust and eID services to specific communities, like the army, emergency services or other special interest entities, as presented in Table 10.

Table 10: Trust and eID services in the EaP countries by subscriber types

Country	Citizens	Public Administrations	Private Sector	Specific community
Armenia	YES	YES	YES	YES
Azerbaijan	YES	YES	YES	YES
Belarus	YES	YES	YES	NO
Georgia	YES	YES	YES	NO
Moldova	YES	YES	YES	YES
Ukraine	YES	YES	YES	YES

Source: Developed by EU4Digital Facility

Except for Moldova all other EaP countries perform audits of their TSPs based on a government approved audit scheme. More than half of the countries use also a secondary audit scheme based on an independent or industry accepted standards, as presented in Table 11.

Table 11: Trust and eID services audit schemes in EaP countries

Country	Government audit scheme	Independent or industry led audit scheme	Internal audit or self-assessment
Armenia	YES	YES	YES
Azerbaijan	YES	YES	YES
Belarus	YES	NO	YES
Georgia	YES	YES	NO
Moldova	YES	NO	YES
Ukraine	YES	YES	YES

Source: Developed by EU4Digital Facility

As mandated by the regulatory frameworks, the internationally accepted standards (ETSI), and the industry best practices, all EaP countries request and enforce that each TSP maintains and updates the records for the following types of documents presented in Table 12.

Table 12: Documents and records which are mandatory for every TSP in the EaP countries

Country	Certification Practice Statement	Information Security Policy	Job descriptions for Trusted Roles	Inventory of Assets	Business Risk Assessmen t	Business Continuity Plan	Incident Response Plan	CA Termination Plan
Armenia	YES	YES	YES	YES	YES	YES	YES	YES
Azerbaijan	YES	YES	YES	YES	YES	YES	YES	YES
Belarus	YES	YES	YES	YES	YES	YES	YES	YES
Georgia	YES	YES	YES	YES	YES	YES	YES	YES
Moldova	YES	YES	YES	YES	YES	YES	YES	YES
Ukraine	YES	YES	YES	YES	YES	YES	YES	YES

Source: Developed by EU4Digital Facility

All EaP countries follow at least one of the internationally accepted standards for the issuance trust and eID services. The “RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” is the most used standard for the delivery of trust and eID services in the EaP countries, as presented in Table 13.

Table 13: Adopted technical standards related to trust and eID services in the EaP countries

Country	ETSI TS 101 456	ETSI TS 101 042	RFC 3647 X.509	CWA 14167	AICPA WEBTRUST	EN 319 411-1	EN 319 411-2
Armenia	YES	YES	YES	YES	N/A	YES	YES
Azerbaijan	YES	YES	YES	YES	YES	YES	YES
Belarus	N/A	N/A	YES	N/A	N/A	N/A	N/A
Georgia	N/A	N/A	N/A	N/A	N/A	YES	YES
Moldova	N/A	N/A	YES	N/A	N/A	YES	YES
Ukraine	YES	YES	YES	YES	N/A	YES	YES

Source: Developed by EU4Digital Facility

Most EaP countries adopted their legal and regulatory frameworks related to trust and eID services based on national needs and requirements. Moldova and Ukraine followed the recommendations of the eIDAS Regulation while Azerbaijan adopted the CA Browser Forum recommendations (Webtrust), as presented in Table 14.

Table 14: Internationally accepted best practices adopted in the EaP countries

Country	Based on EU eIDAS Regulation recommendations	Based on CA/Browser Forum recommendations	Based only on national needs and requirements
Armenia	NO	NO	YES
Azerbaijan	NO	YES	YES
Belarus	NO	NO	YES
Georgia	NO	NO	YES
Moldova	YES	NO	YES
Ukraine	YES	NO	NO

Source: Developed by EU4Digital Facility

Even though all EaP countries have defined regulatory frameworks related to personal data protection and privacy, only two countries, Belarus and Moldova, declare having adopted a subset of recommendations and best practices from the GDPR Regulation. All other EaP countries have defined data protection and privacy frameworks based on using their national needs and requirements, as presented in Table 15.

Table 15: Recommendations and best practices related to personal data privacy protection adopted in the EaP countries

Country	Based on EU GDPR Regulation	Based only on national requirements
Armenia	NO	YES
Azerbaijan	NO	YES
Belarus	YES	YES
Georgia	NO	YES
Moldova	YES	YES
Ukraine	NO	YES

Source: Developed by EU4Digital Facility

5 Overview of personal data protection and privacy regulatory frameworks in the EaP member countries

5.1 Armenia

The Law on Personal Data (Armenian Law), which became effective in 2015, regulates the processing of all personal information of natural persons by both the public and private sectors. The Armenian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security and breach notification obligations. In addition, the period of time within which organisations must respond to correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there is no DPO obligation.

Table 16: Regulated data privacy and data protection areas in Armenia

Data protection areas	Specific requirements
Data Protection Authority	The Law provides for the establishment of the Authorised State Body for the Protection of Personal Data Processing (Armenian DPA); however, it is not yet established.
Access and Correction	The Armenian Law does not specify a time period for responding to access requests. Corrections should be carried out (or refused) within five days after receiving the written request.
Cross-Border Transfers	Personal Data may be transferred cross border either with the consent of the individual or where the transfer is necessary to carry out processing previously consented to by the individual. In addition, DPA authorisation is required to transfer to those countries that are not on the DPA's approved list of countries that provide adequate protection. A transfer permit is required in such cases. The DPA must also approve the organisation's contractual clauses governing the transfer.
Data Security Breach Notification	The controller must make a public announcement without delay and notify the police and the DPA when a data security breach occurs.
Data Security	Encryption measures are required to protect information systems containing personal information from loss, unauthorised access, illegal use and destruction, and illegal copying and disclosure. The law also provides for the government to set security standards in information systems, physical records of biometric data and personal data storage technologies other than electronic information systems.
Legal Basis for Collection and Use	Personal information may be processed only with the consent of the individual or where such processing is provided for or required by law or where the data are publicly available.
Registration	The DPA has the right to require controllers to notify the DPA about the collection or processing of personal information; otherwise such notification is voluntary.

Source: Developed by EU4Digital Facility

5.2 Azerbaijan

The Law on Personal Data (Azerbaijani Law), which became effective in 2010, regulates the processing of all personal information of natural persons by both the public and private sectors. The Azerbaijani Law differentiates personal information according to public and confidential categories. Public data are: (i) data that are depersonalised or anonymised, (ii) data that are declared public by the individual or (iii) data that are included in an information system created for general use with the consent of the individual. A natural person's name, last name, and patronymic will always be considered as public data.

The Azerbaijani Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. In addition, the period of time within which organisations must respond to access and correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there is no data breach notification or DPO obligations.

Table 17: Regulated data privacy and data protection areas in Azerbaijan

Data protection areas	Specific requirements
Data Protection Authority	The State Register at the Ministry of Communications and Information Technologies (DPA) is responsible for registering information systems and ensuring compliance with the Azerbaijani Law.
Access and Correction	Organisations must respond to access and correction requests within seven days.
Cross-Border Transfers	Cross-border transfers are prohibited where: (i) such transfer creates a threat to the national security of the Azerbaijan Republic, or (ii) the laws of the countries to which the personal information is transferred do not provide the same level of protection as that provided by Azerbaijani laws. However, personal information can be transferred across the border to a country regardless of the level of legal protection of personal information where the individual expressly agrees to the transfer. In addition, although not expressly stated in the Law, cross border transfers are permitted where the transfer is necessary to protect the life or health of the individual. DPA authorisation is not required; however, information on such transfer and the categories of the personal information transferred must be provided to the DPA at the time of the registration of the information system. The DPA has stated informally that the cross-border transfer provisions apply to the transfer of databases (i.e. personal information of a significant number of individuals); transfers of personal information limited to one or several individuals across the border would likely trigger the rules for transfers to third parties, not the cross-border transfer rules.
Data Security	Controllers and processors must implement organisational and technical measures to guarantee the security of personal information during its collection, use and disclosure (including cross-border transfer). They must determine the risks for the security of the personal information and based on such risks must continually improve the information system in order to neutralise possible risks. There are regulations that prescribe a long list of technical organisational safety requirements. Organisations must encrypt all transmitted records. The length of the encryption key used during the transfer may not be less than 256 bit. As is evident from the registration card for information systems approved by the Regulations on the Registration and Deregistration of Information Systems, organisations must have control and audit mechanisms for the collection and processing of personal information; however, the frequency of such audits and their substance have not been specified.
Legal Basis for Collection and Use	To collect and use personal information, organisations must have a legal basis such as consent, legal requirement, or vital interests.
Registration	Information systems containing personal information must be registered with the State Register unless an exemption applies. The State Registry is maintained by the Data Computing Centre at the Ministry of Communication and Information Technologies.

Source: Developed by EU4Digital Facility

5.3 Belarus

The Law on Information, Informatisation and Protection of Information (Belarusian Law), which became effective in 2008, regulates the processing of all personal information of natural persons by both public and private sectors. Under the Belarusian Law, consent is the only permissible basis on which to process (and transfer cross-border) personal information. In addition, the law imposes special security obligations; however, there are no registration, breach notification, or DPO obligations.

Table 18: Regulated data privacy and data protection areas in Belarus

Data protection areas	Specific requirements
Data Protection Authority	There is no DPA in Belarus akin to the DPAs found in other jurisdictions. The state authority that performs any data protection-related functions is the Operative Analytics Centre of the President of the Republic of Belarus (OAC). However, to date, OAC's competence is more technical in nature and does not include any data protection-related competence. For example, the OAC is empowered to certify information technology (IT) systems, hardware and software data protection solutions, and regulate general IT and Internet relations.
Access and Correction	The Belarusian Law does not specify a time period for responding to access requests and is silent on correction rights.
Cross-Border Transfers	There are no specific limitations on cross-border transfers. By general rule, each transfer, including cross-border transfers, requires the consent of the individual.
Data Protection Officer	A special individual or department for security measures must be appointed.
Data Security	Controllers must take effective measures to ensure security of personal information from the moment of receipt until its destruction. Under the Belarusian Law and implementing regulations, this obligation includes various organisational and technical security measures. In particular, controllers must maintain a data protection system certified by the certification centres accredited by the DPA. Organisations must file annual reports on their security measures to the OAC by 30 December. In addition, there are cryptographic regulations that define legal and organisational basics of technical and cryptographic measures of information security. Controllers must comply with these regulations which among other things require that personal information be encrypted in transit.
Legal Basis for Collection and Use	Consent is required to process Personal Data. The Belarusian Law does not provide for any other legal bases such as contractual necessity, vital interests or legal requirements.

Source: Developed by EU4Digital Facility

5.4 Georgia

The Law on the Protection of Personal Data (Georgian Law), which came into effect in 2012 and was amended in 2014, regulates the processing of all personal information of natural persons by the public and private sectors. The Georgian Law requires database registration and restricts cross-border transfers to countries that do not provide adequate protection. However, there are no data breach notification, DPO, or special security obligations.

Table 19: Regulated data privacy and data protection areas in Georgia

Data protection areas	Specific requirements
Data Protection Authority	The Personal Data Protection Inspector (DPA), an independent authority, is responsible for enforcing the Georgian Law.

Access and Correction	Organisations must respond to access requests within 10 days and correction requests within 15 days.
Cross-Border Transfers	Transfers of personal information outside Georgia are permitted to countries that provide adequate protection. The DPA issued a list of approved countries that include: the EEA countries, Australia, Albania, Andorra, Argentina, New Zealand, Bosnia and Herzegovina, Israel, Canada, Croatia, Macedonia, Moldova, Monaco, Montenegro, Serbia, Ukraine and Uruguay. Where transfers are to jurisdictions that are not recognised as providing adequate protection, DPA-approved contracts are required.
Legal Basis for Collection and Use	To collect and use personal information, organisations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.
Registration	Controllers must register with the DPA prior to creation of filing systems and inclusion of new categories of data in those filing systems.

Source: Developed by EU4Digital Facility

5.5 Moldova

The Law on Personal Data Protection (Moldovan Law), which took effect in April 2012, regulates the processing of all personal information of natural persons by the public and private sectors. The Moldovan Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes data breach notification and special security obligations. However, there is no DPO obligation.

Table 20: Regulated data privacy and data protection areas in Moldova

Data protection areas	Specific requirements
Data Protection Authority	The National Centre for Personal Data Protection (DPA), an independent agency, is responsible for enforcing the Moldovan Law.
Access and Correction	Access and correction requests must be responded to without delay (no time period is specified).
Cross-Border Transfers	Personal Data may not be transferred to countries outside Moldova unless that country ensures an adequate level of protection. If the proposed transfer is to a country that is not considered adequate, one of the transfer exceptions must apply, such as consent, contractual necessity, or vital interests. DPA authorisation is also required in such cases.
Data Protection Officer	There is no obligation to have a DPO role in place.
Data Security Breach Notification	All controllers must submit to the DPA an annual report on any security incidents involving information systems during that year.
Data Security	The Moldovan Law and implementing regulations prescribe detailed security requirements which include the need to maintain and re-evaluate annually the organisation's data security policy and implement specific physical and electronic security measures, including encryption. Regular data security audits must be carried out. These audits must include an assessment of the organisation, its security measures and use of communication partners and suppliers. The results of the security audit must be documented.
Legal Basis for Collection and Use	To collect and use personal information, organisations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests and legal requirements.
Registration	Controllers and processors must register their processing for all purposes unless one of the limited exemptions applies.

Source: Developed by EU4Digital Facility

5.6 Ukraine

The Law on the Protection of Personal Data (Ukrainian Law), which came into effect in 2011, regulates the processing of all personal data of natural persons by public and private sectors. The Ukrainian Law was recently amended in September 2015. The Ukrainian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO and special security obligations. In addition, the period of time within which organisations must respond to correction requests is exceedingly short. However, there is no breach notification obligation.

Table 21: Regulated data privacy and data protection areas in Ukraine

Data protection areas	Specific requirements
Data Protection Authority	The Ukrainian Parliament Commissioner for Human Rights (DPA) is responsible for enforcement of the Law.
Access and Correction	Organisations must respond to access and correction requests within 10 days.
Cross-Border Transfers	Personal Data may be transferred to third countries that provide sufficient protection for personal information and include the EEA countries, signatories to the Council of Europe Convention and states on the DPA approved list (which is not yet adopted). Personal information can also be transferred to countries that do not provide adequate protection if a legal basis applies such as consent, contractual necessity, or vital interests. DPA authorisation is not required; however, information regarding cross-border transfers of the personal information must be included in the original registration/negotiation filed with the DPA.
Data Protection Officer	Organisations must appoint a department or a person responsible for the protection of personal information during the processing of that information.
Data Security Breach Notification	There is no obligation on any entities to give notice in the event of data security breach; however, the controller must document/log violations in course of Processing and develop an action plan in case of an unauthorised access to personal information.
Data Security	The Ukrainian Law and implementing regulations require organisations to, among other things, establish an internal security policy and implement specific security measures including employee training, data disposal measures and documentation requirements involving access and control procedures.
Legal Basis for Collection and Use	To collect and use personal information, organisations must have legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.
Registration	Controllers must file a notification with DPA about processing of certain categories of sensitive personal information such as health, biometrical and genetic data, geolocation, trade union or political or religious memberships, race ethnic or national origin, criminal records.

Source: Developed by EU4Digital Facility

6 Legal maturity assessment results related to trust and eID services in the EaP countries

6.1 Trust Services Practice Disclosure

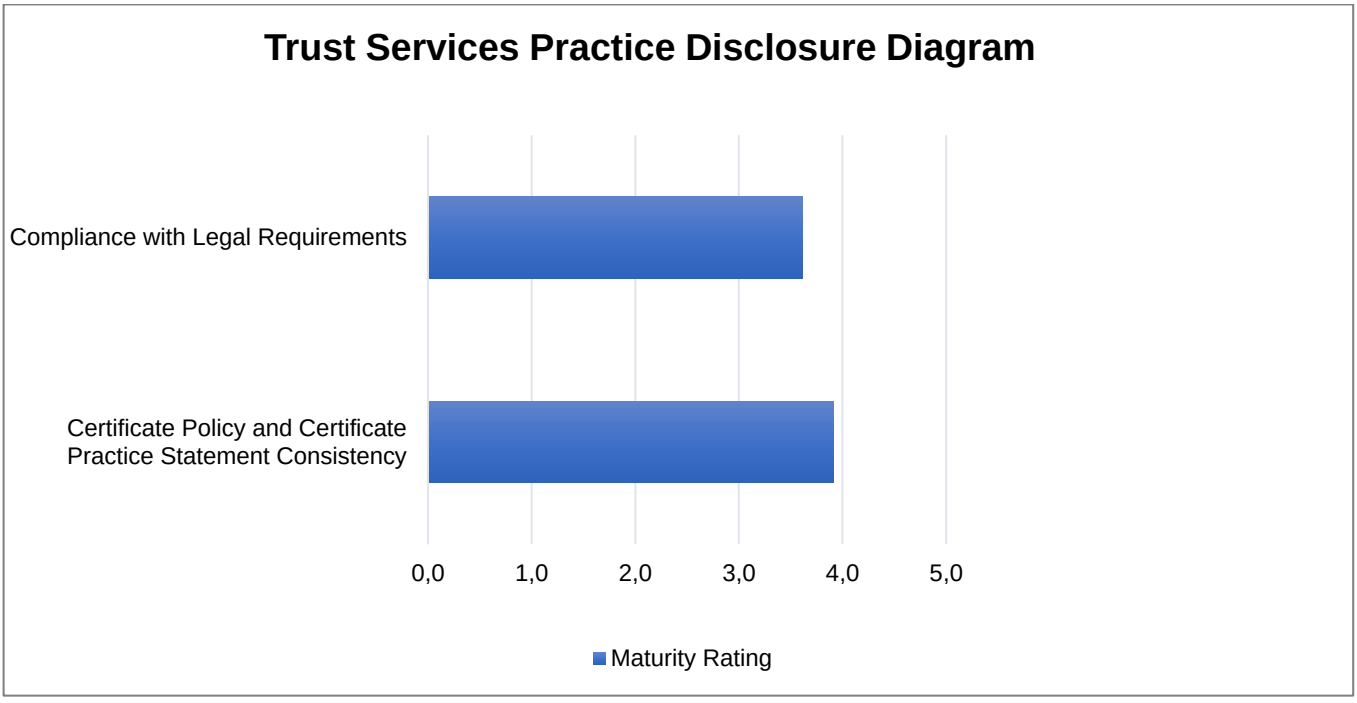
This maturity area covers the means that Information regarding the TSP's business practices is made available to all subscribers and all potential relying parties.

Table 22: Trust services practice disclosure maturity rating

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and	Answered as Optimized	Total question no.	Maturity Rating
Certificate Policy and Certificate Practice Statement Consistency	0	0	0	10	6	8	24	**3.9**
Compliance with Legal Requirements	2	1	2	33	14	20	72	**3.6**

Source: Developed by EU4Digital Facility

Figure 1: Trust services practice disclosure maturity rating



Source: Developed by EU4Digital Facility

6.2 Trust Services Practice Management

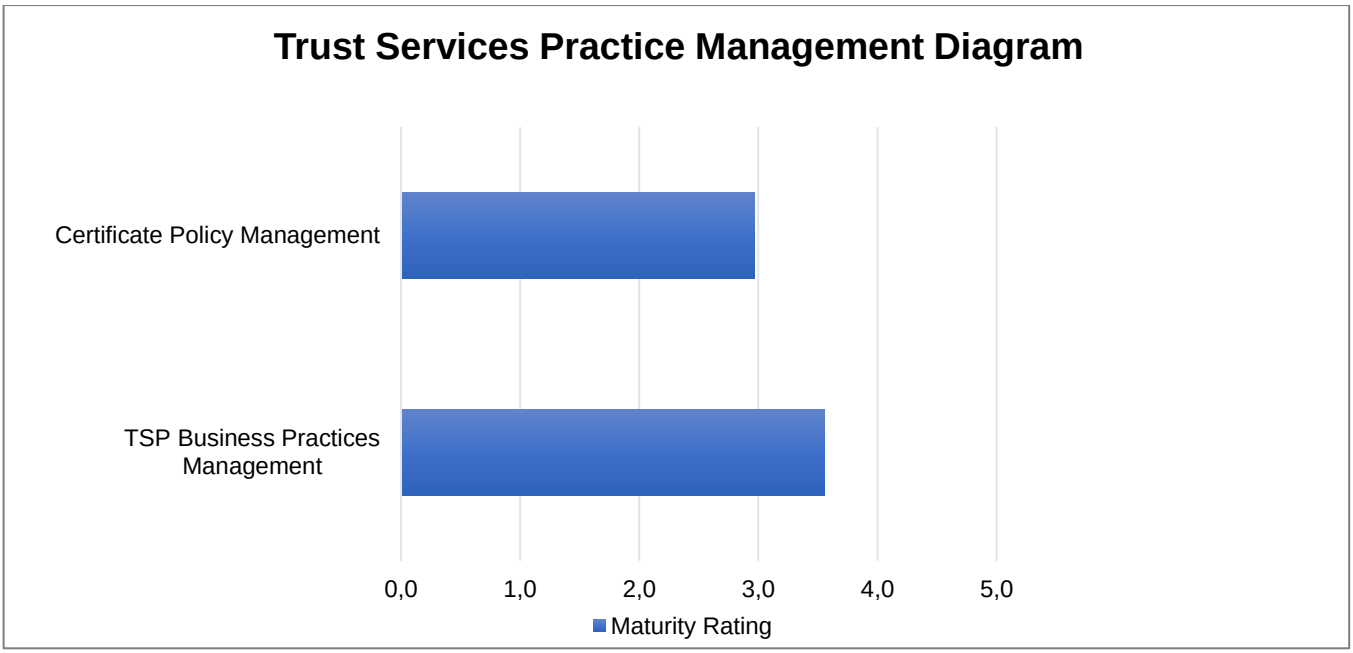
This maturity area measures how the TSP maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.

Table 23: Trust services practice management maturity rating

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
TSP Business Practices Management	2	2	1	11	9	11	36	**3.6**
Certificate Policy Management	5	2	1	10	5	7	30	**3.0**

Source: Developed by EU4Digital Facility

Figure 2: Trust services practice management maturity rating



Source: Developed by EU4Digital Facility

6.3 Trust Services Environmental Controls

This maturity area measures the controls in place to establish and maintain a trustworthy TSP environment, that is essential to the reliability of the TSP's business processes.

Table 24: Trust services environmental controls maturity rating

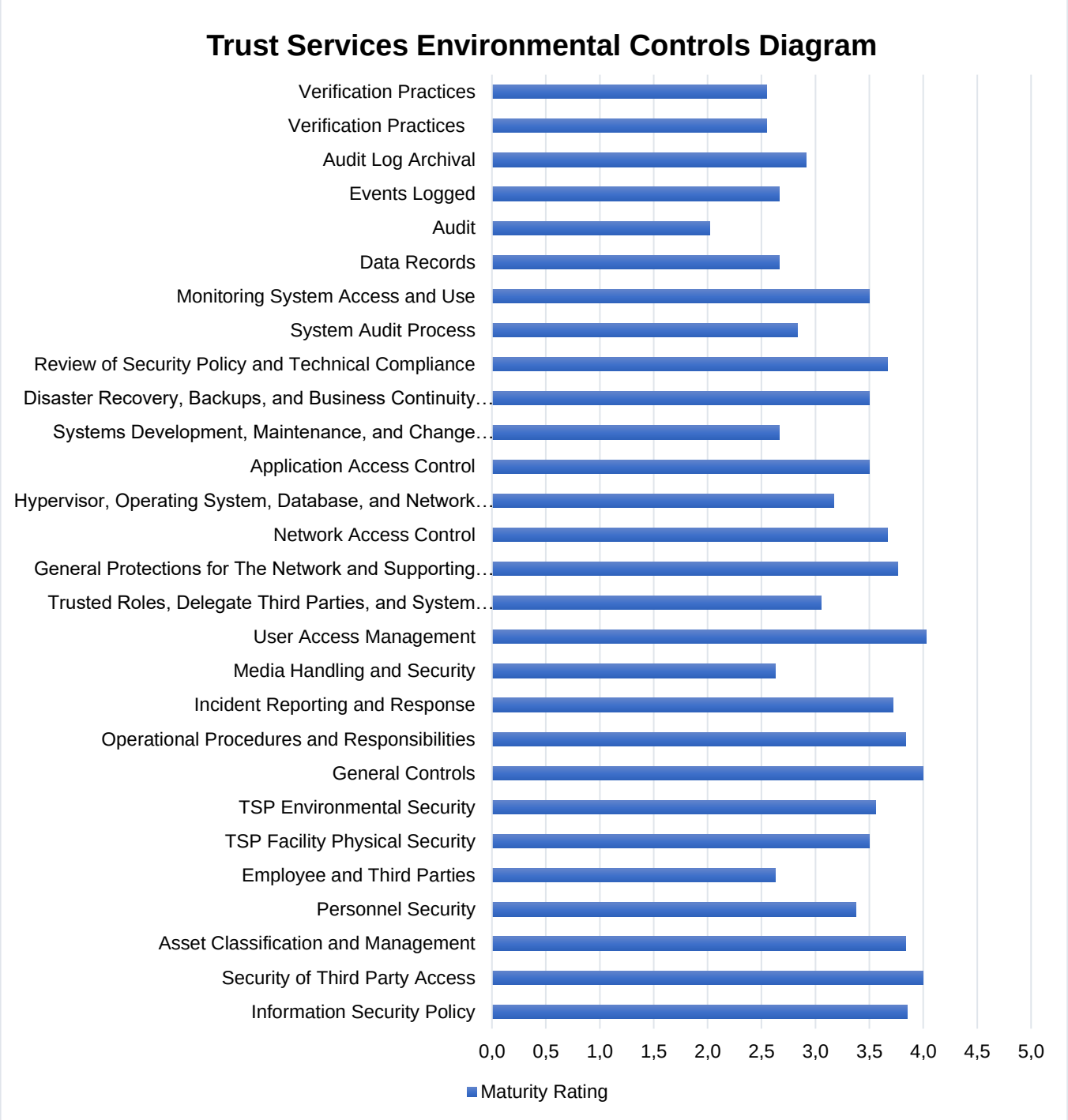
Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Information Security Policy	2	0	0	13	19	14	48	**3.9**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Security of Third-Party Access	0	0	0	2	2	2	6	**4.0**
Asset Classification and Management	0	0	1	1	2	2	6	**3.8**
Personnel Security	2	7	7	18	12	20	66	**3.4**
Employee and Third Parties	3	13	5	15	2	10	48	**2.6**
TSP Facility Physical Security	0	1	0	2	1	2	6	**3.5**
TSP Environmental Security	7	3	3	65	39	39	156	**3.6**
General Controls	0	0	0	2	2	2	6	**4.0**
Operational Procedures and Responsibilities	0	0	0	5	4	3	12	**3.8**
Incident Reporting and Response	0	0	0	8	7	3	18	**3.7**
Media Handling and Security	5	1	3	6	2	6	24	**2.6**
User Access Management	0	0	0	11	13	12	36	**4.0**
Trusted Roles, Delegate Third Parties, and System Accounts	12	9	15	48	20	28	132	**3.1**
General Protections for The Network and Supporting Systems	0	3	5	22	18	24	72	**3.8**
Network Access Control	0	0	2	4	2	4	12	**3.7**
Hypervisor, Operating System, Database, and Network Device Access Control	0	0	2	2	1	1	6	**3.2**
Application Access Control	0	0	2	1	1	2	6	**3.5**
Systems Development, Maintenance, and Change Management	3	1	3	7	0	4	18	**2.7**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Disaster Recovery, Backups, and Business Continuity Management	2	5	2	25	17	20	72	**3.5**
Review of Security Policy and Technical Compliance	0	1	0	4	4	3	12	**3.7**
System Audit Process	0	1	2	1	1	1	6	**2.8**
Monitoring System Access and Use	0	0	0	4	1	1	6	**3.5**
Data Records	2	1	1	5	1	2	12	**2.7**
Audit	22	5	0	4	5	12	48	**2.0**
Events Logged	6	7	2	27	3	8	54	**2.7**
Audit Log Archival	1	0	3	5	1	2	12	**2.9**
Verification Practices	17	8	0	8	9	17	60	**2.6**
Verification Practices	17	8	0	8	9	17	60	**2.6**

Source: Developed by EU4Digital Facility

Figure 3: Trust services environmental controls maturity rating



Source: Developed by EU4Digital Facility

6.4 Trust Services Key Lifecycle Management

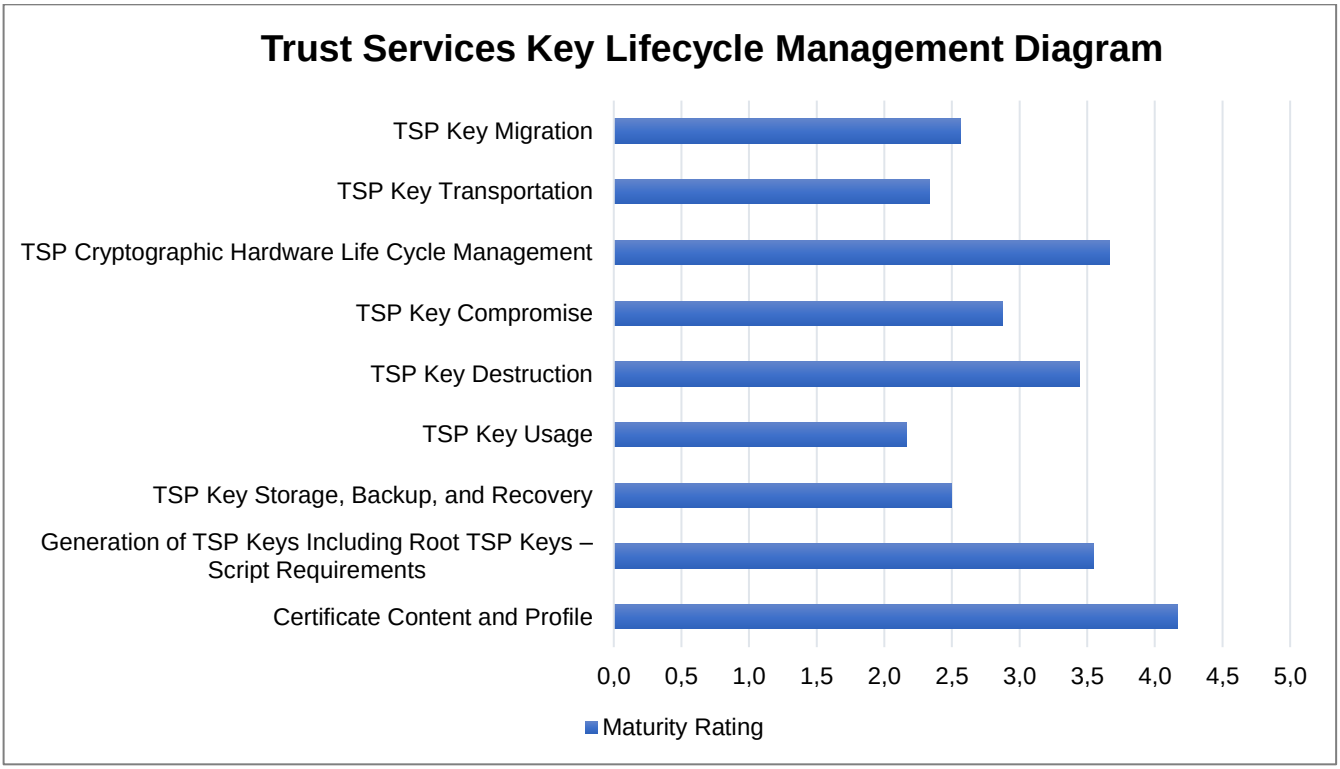
This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their life cycles.

Table 25: Trust services key lifecycle management maturity rating

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Certificate Content and Profile	1	0	0	6	18	12	36	**4.2**
Generation of TSP Keys Including Root TSP Keys – Script Requirements	7	0	0	43	17	33	102	**3.5**
TSP Key Storage, Backup, and Recovery	2	0	0	1	3	0	6	**2.5**
TSP Key Usage	2	1	0	1	1	1	6	**2.2**
TSP Key Destruction	5	3	1	26	11	20	66	**3.4**
TSP Key Compromise	3	9	4	28	1	10	54	**2.9**
TSP Cryptographic Hardware Life Cycle Management	2	0	1	10	7	10	30	**3.7**
TSP Key Transportation	5	0	0	3	1	3	12	**2.3**
TSP Key Migration	27	0	5	20	0	26	78	**2.6**

Source: Developed by EU4Digital Facility

Figure 4: Trust services key lifecycle management maturity rating



Source: Developed by EU4Digital Facility

6.5 Trust Services Subscriber Key Lifecycle Management

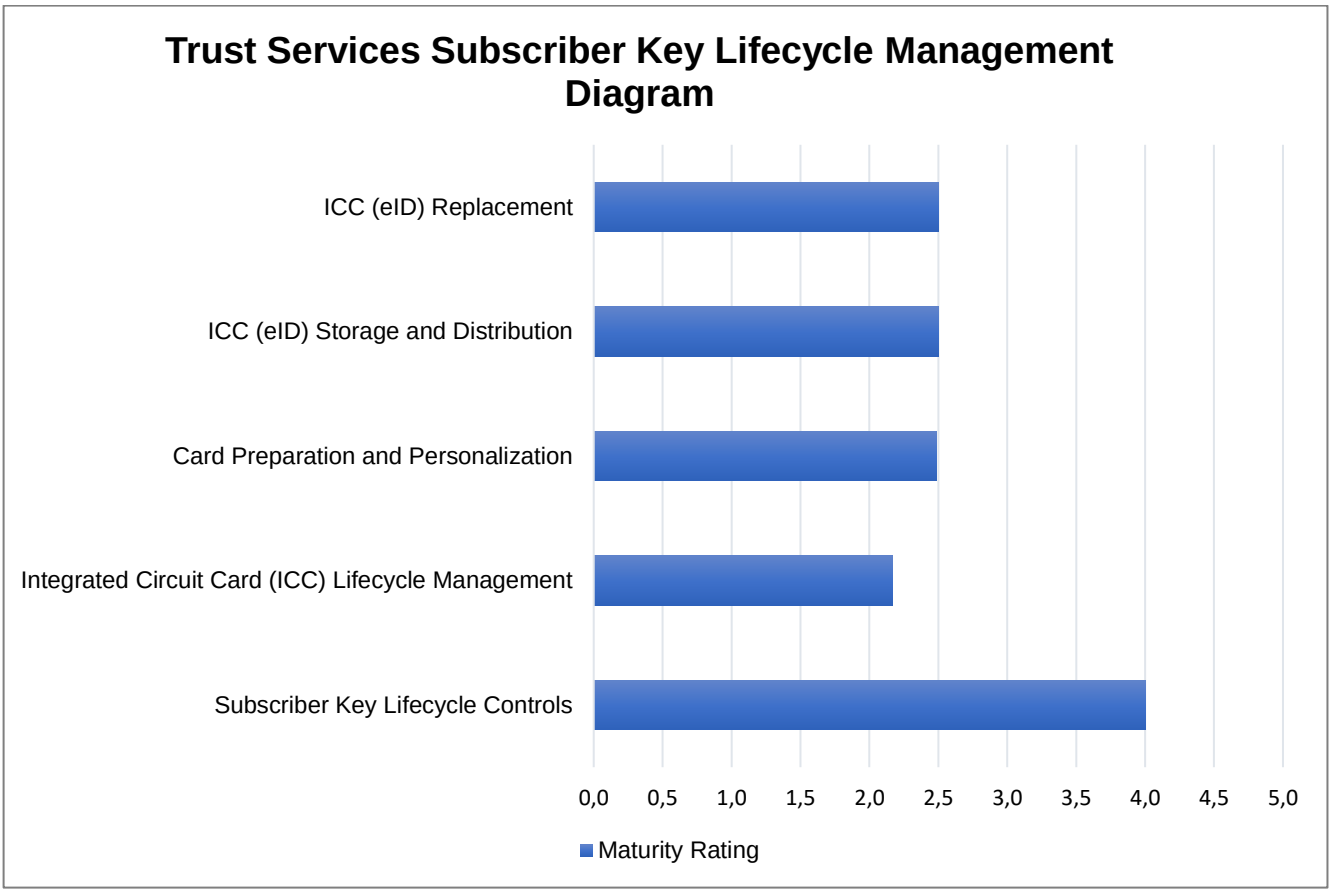
This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles.

Table 26: Trust services subscriber key lifecycle management maturity rating

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Subscriber Key Lifecycle Controls	0	0	0	2	2	2	6	**4.0**
Integrated Circuit Card (ICC) Lifecycle Management	2	0	1	1	2	0	6	**2.2**
Card Preparation and Personalisation	23	0	0	9	18	10	60	**2.5**
ICC (eID) Storage and Distribution	2	0	0	2	1	1	6	**2.5**
ICC (eID) Replacement	2	0	0	2	1	1	6	**2.5**

Source: Developed by EU4Digital Facility

Figure 5: Trust services subscriber key lifecycle management maturity rating



Source: Developed by EU4Digital Facility

6.6 Trust Services Certificate Lifecycle Management

This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that Subscriber information was properly authenticated.

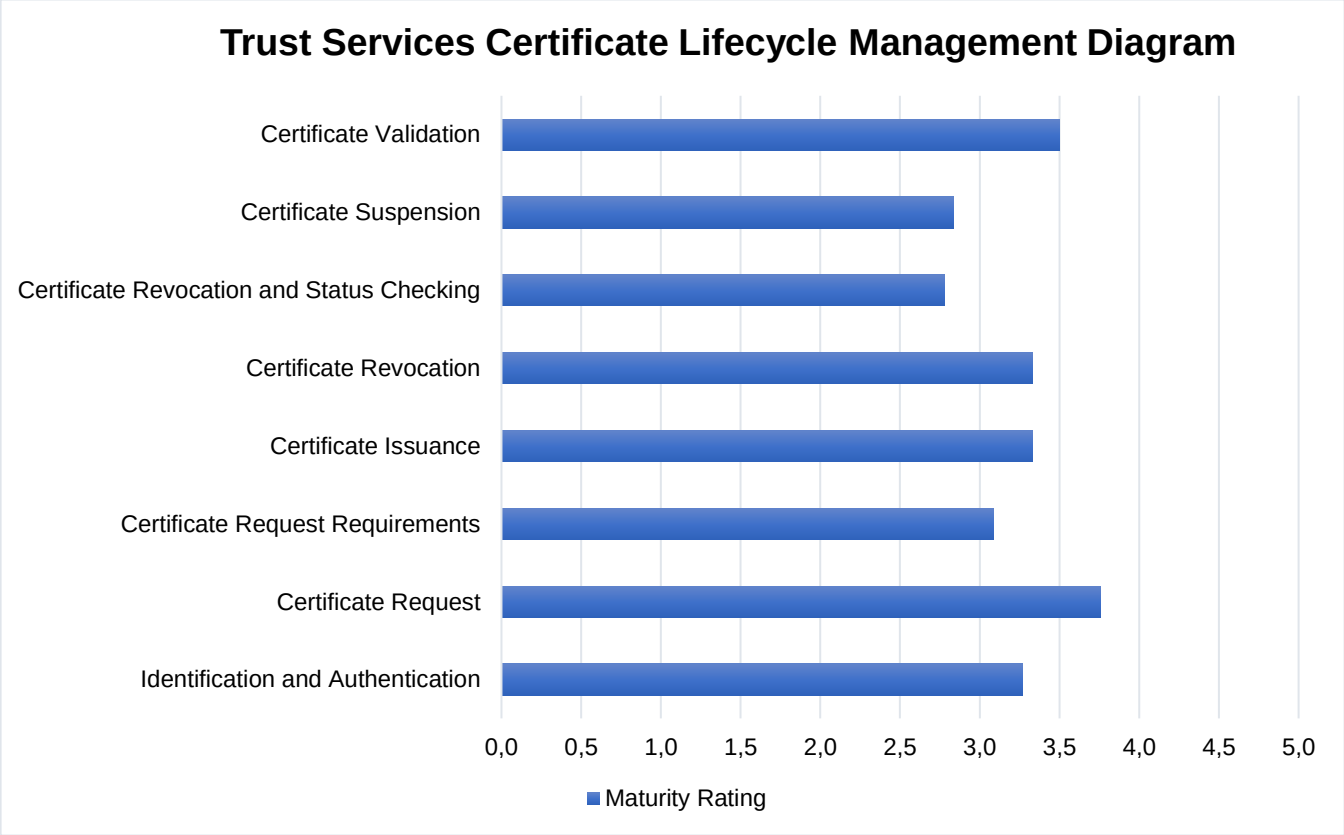
Table 27: Trust services certificate lifecycle management maturity rating

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Identification and Authentication	5	6	0	13	8	16	48	**3.3**
Certificate Request	2	0	0	23	11	18	54	**3.8**
Certificate Request Requirements	3	5	0	29	4	8	48	**3.1**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Certificate Issuance	3	0	0	3	9	3	18	**3.3**
Certificate Revocation	1	0	0	1	3	1	6	**3.3**
Certificate Revocation and Status Checking	5	1	1	5	3	4	18	**2.8**
Certificate Suspension	2	2	1	2	1	4	12	**2.8**
Certificate Validation	0	2	0	4	2	4	12	**3.5**

Source: Developed by EU4Digital Facility

Figure 6: Trust services certificate lifecycle management maturity rating



Source: Developed by EU4Digital Facility

6.7 Trust Services Cross Certificate Lifecycle Management

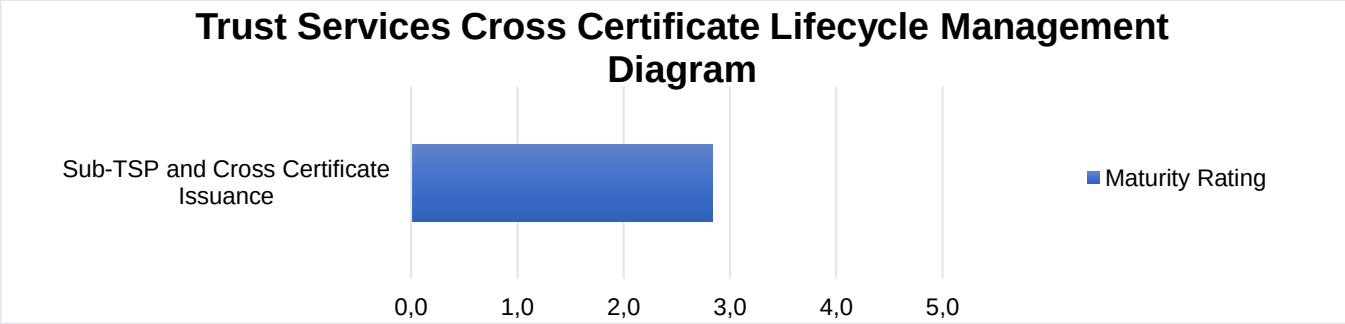
This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that subordinate CA's and cross certificate requests are accurate, authenticated and approved.

Table 28: Trust services cross certificate lifecycle management maturity rating

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Sub-TSP and Cross Certificate Issuance	6	0	0	0	9	3	18	**2.8**

Source: Developed by EU4Digital Facility

Figure 7: Trust services cross certificate lifecycle management maturity rating



Source: Developed by EU4Digital Facility

6.8 Data privacy and protection

This maturity area measures the controls in place to assure the privacy and protection of personal data.

Table 29: Data privacy and protection maturity rating

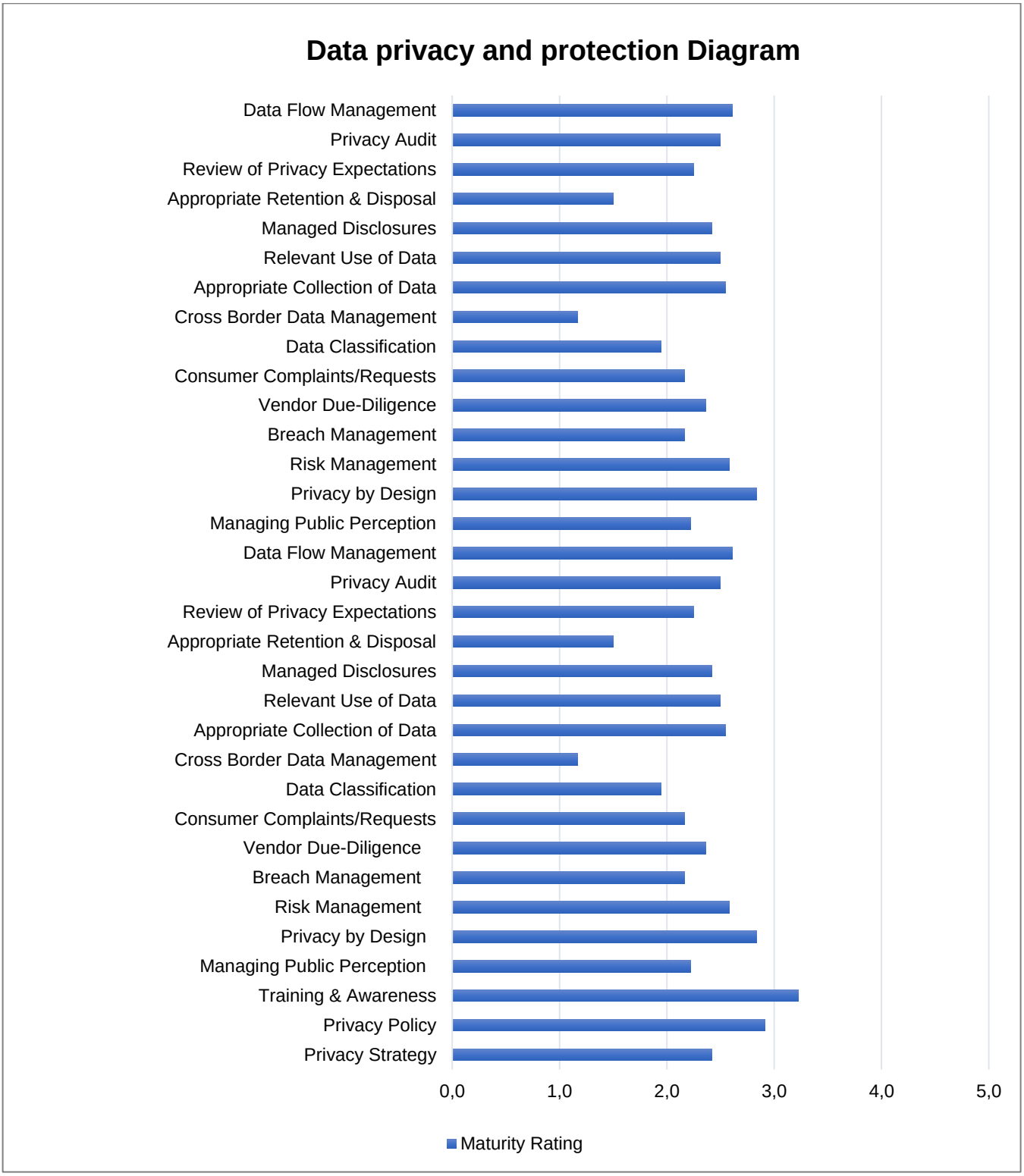
Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Privacy Strategy	3	3	0	2	0	4	12	**2.4**
Privacy Policy	4	3	2	5	2	8	24	**2.9**
Training & Awareness	3	1	0	3	2	8	18	**3.2**
Managing Public Perception	4	3	2	5	2	2	18	**2.2**
Privacy by Design	1	1	1	0	1	2	6	**2.8**
Risk Management	2	1	2	4	1	2	12	**2.6**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Breach Management	13	7	5	13	2	8	48	**2.2**
Vendor Due-Diligence	10	0	8	8	5	5	36	**2.4**
Consumer Complaints/Requests	14	4	8	12	2	8	48	**2.2**
Data Classification	5	3	3	4	1	2	18	**1.9**
Cross Border Data Management	20	0	5	0	0	5	30	**1.2**
Appropriate Collection of Data	8	2	9	14	0	9	42	**2.5**
Relevant Use of Data	11	1	11	14	0	11	48	**2.5**
Managed Disclosures	4	0	2	2	1	3	12	**2.4**
Appropriate Retention & Disposal	14	4	6	3	0	4	30	**1.5**
Review of Privacy Expectations	4	1	3	0	0	4	12	**2.3**
Privacy Audit	3	3	6	0	0	6	18	**2.5**
Data Flow Management	7	5	6	6	1	11	36	**2.6**
Managing Public Perception	4	3	2	5	2	2	18	**2.2**
Privacy by Design	1	1	1	0	1	2	6	**2.8**
Risk Management	2	1	2	4	1	2	12	**2.6**
Breach Management	13	7	5	13	2	8	48	**2.2**
Vendor Due-Diligence	10	0	8	8	5	5	36	**2.4**
Consumer Complaints/Requests	14	4	8	12	2	8	48	**2.2**
Data Classification	5	3	3	4	1	2	18	**1.9**
Cross Border Data Management	20	0	5	0	0	5	30	**1.2**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	Total question no.	Maturity Rating
Appropriate Collection of Data	8	2	9	14	0	9	42	**2.5**
Relevant Use of Data	11	1	11	14	0	11	48	**2.5**
Managed Disclosures	4	0	2	2	1	3	12	**2.4**
Appropriate Retention & Disposal	14	4	6	3	0	4	30	**1.5**
Review of Privacy Expectations	4	1	3	0	0	4	12	**2.3**
Privacy Audit	3	3	6	0	0	6	18	**2.5**
Data Flow Management	7	5	6	6	1	11	36	**2.6**

Source: Developed by EU4Digital Facility

Figure 8: Data privacy and protection maturity rating



Source: Developed by EU4Digital Facility

7 Overview of trust and electronic identification services in the EaP member countries

EaP countries are currently offering most of the trust and eID services using compatible technologies with those deployed by the EU member states. During the assessment we focused on identifying how many of the services described in the eIDAS Regulation are currently offered by the EaP countries. We identified the following services as being widely offered by the EaP countries:

- electronic signatures;
- electronic seals;
- timestamp services;
- revocation and validation services;
- eID and Mobile ID;
- preservation services.

In the next section we compare the offerings of each of the identified types of trust and eID services between the EaP countries.

7.1 Electronic signatures

An electronic signature means 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 electronic information or data.

An advanced electronic signature means an electronic signature which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- it is linked to the data signed in such a way that any subsequent change in the data is detectable.

A qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device and which is based on a qualified certificate for electronic signatures.

A remote signature provider enables users to digitally sign legally binding documents or transactions without the need for locally installed software or hardware. The digital signing keys are held in the ‘cloud’, enabling a user with the freedom and security to sign from a smartphone, tablet, or any other connected device. This typically means all user keys are stored in an encrypted database secured by a Hardware Security Module (HSM).

In the Table 30 we present the types of electronic signatures currently issued by each of the six EaP countries. All six EaP countries are issuing qualified electronic signatures and with the exception of Armenia and Moldova the remaining EaP countries can also issue qualified remote signatures.

Table 30: Types of electronic signatures issued by the EaP countries

Country	Unqualified electronic signature	Qualified electronic signature	Qualified remote signature
Armenia	NO	YES	NO
Azerbaijan	YES	YES	YES
Belarus	NO	YES	YES
Georgia	YES	YES	YES
Moldova	NO	YES	NO
Ukraine	YES	YES	YES

Source: Developed by EU4Digital Facility

Except for Belarus, all other EaP countries can issue advanced electronic signatures using at least one of the following “AdES” extensions, as presented in Table 31.

Table 31: AdES extensions and other digital signature formats used by the EaP countries

Country	CAdES	XAdES	PAdES	PKCS#7	DSS
Armenia	YES	YES	YES	YES	NO
Azerbaijan	YES	YES	YES	YES	NO
Belarus	NO	NO	NO	YES	NO
Georgia	YES	YES	YES	NO	NO
Moldova	YES	YES	YES	YES	YES
Ukraine	YES	YES	YES	YES	NO

Source: Developed by EU4Digital Facility

Except for Belarus, all other EaP countries are using compatible public key cryptographic algorithms like RSA or elliptical curve cryptography (ECC) for the TSP CA root certificates as presented in the Table 32.

Table 32: Public key cryptographic algorithms used to issue CA root certificates

Country	RSA-1024	RSA-2048	RSA-4096	ECC-256
Armenia	NO	NO	YES	NO
Azerbaijan	NO	NO	YES	YES
Belarus	NO	NO	NO	NO
Georgia	NO	NO	YES	NO
Moldova	NO	NO	YES	NO
Ukraine	NO	NO	YES	YES

Source: Developed by EU4Digital Facility

Except for Belarus, all other EaP countries are using compatible public key cryptographic algorithms like RSA or elliptical curve cryptography (ECC) to issue subscribers certificates as presented in the Table 33.

Table 33: Public key cryptographic algorithms used to issue subscribers certificates

Country	RSA-1024	RSA-2048	RSA-4096	ECC-256
Armenia	NO	YES	NO	NO
Azerbaijan	YES	YES	NO	YES
Belarus	NO	NO	NO	NO
Georgia	NO	YES	NO	NO
Moldova	NO	YES	NO	NO
Ukraine	NO	YES	YES	YES

Source: Developed by EU4Digital Facility

All EaP countries are using compatible hash functions in order to issue TSP CA root certificates as presented in the Table 34. Hashing functions are used to ensure the integrity of the electronic certificates themselves and to provide assurance to all parties that they were not compromised.

Table 34: Hash functions used in TSP CA issued root certificates

Country	SHA-1	SHA-256	SHA-384	SHA-512	HMAC - Hash Function	RIPEMD-160
Armenia	NO	YES	NO	NO	NO	NO
Azerbaijan	YES	NO	NO	YES	NO	NO
Belarus	NO	NO	NO	NO	YES	NO
Georgia	NO	YES	NO	NO	NO	NO
Moldova	YES	YES	NO	NO	NO	NO
Ukraine	NO	YES	YES	YES	NO	NO

Source: Developed by EU4Digital Facility

All EaP countries are using compatible hash functions in order to issue subscribers certificates as presented in Table 35. Hashing functions are used to ensure the integrity of the electronic certificates themselves and to provide assurance to all parties that they were not compromised.

Table 35: Hash functions used in subscriber issued certificates

Country	SHA-1	SHA-256	SHA-384	SHA-512	HMAC - Hash Function	RIPEMD-160
Armenia	NO	YES	NO	NO	NO	NO
Azerbaijan	YES	YES	NO	NO	NO	NO
Belarus	NO	NO	NO	NO	YES	NO
Georgia	NO	YES	NO	NO	NO	NO
Moldova	YES	YES	NO	NO	NO	NO
Ukraine	NO	YES	YES	YES	NO	NO

Source: Developed by EU4Digital Facility

In order to issue qualified electronic signatures, the TSP must provide an electronic mechanism which acts as a signature creation device. In most implementations HSMs are used as creation devices. HSM devices should follow and comply with internationally accepted standards. Currently with the exception of Belarus and Ukraine all countries used certified HSM devices which comply with FIPS 140-2 standard as presented in Table 36 for the creation of TSP CA root certificates and for the creation of the subscriber certificates.

Table 36: HSM CA Root creation devices compliance with international standards

Country	FIPS certified	CC (EAL) certified	No certification
Armenia	YES	NO	NO
Azerbaijan	YES	YES	NO
Belarus	NO	NO	YES
Georgia	YES	YES	NO
Moldova	YES	YES	NO
Ukraine	NO	NO	YES

Source: Developed by EU4Digital Facility

In order to issue qualified electronic signatures, the TSP must provide an electronic mechanism which acts as a signature creation device. In most implementations HSMs are used as creation devices. HSM devices should follow

and comply with internationally accepted standards. Currently with the exception of Belarus and Ukraine all countries used certified HSM devices who comply with FIPS 140-2 standard as presented in Table 22.

Table 37: HSM subscriber creation devices compliance with international standards

Country	FIPS certified	CC (EAL) certified	No certification
Armenia	YES	YES	NO
Azerbaijan	YES	YES	NO
Belarus	NO	NO	YES
Georgia	YES	YES	NO
Moldova	YES	YES	NO
Ukraine	NO	NO	YES

Source: Developed by EU4Digital Facility

7.2 Electronic seals

Electronic Seals were introduced as a solution for legal entities, allowing them to protect authenticity and integrity of electronic documents and data. An Electronic Seal is based on the same technology as an Electronic Signature and can be Advanced and Qualified. A Qualified Electronic Seal is verified with Qualified Certificate.

A seal can be considered as an electronic signature for a business or organisation. In other words, the main difference between a seal and a signature is that a signature is meant for individuals (natural persons), whereas a seal is used by a legal entity (business or organisation) and can be used by more than one person or system within the legal entity. Examples would be invoices, which are automatically generated by an accounting system or signed messages sent by a sensor in the Internet of Things.

While assessing the usage of electronic seals in the EaP countries one key comment must be given: in all EaP countries the electronic signature of an individual who is entitled and has the power to sign documents in the name of an organisation/entity enjoys the same benefits of an individual using an electronic seal to perform the same actions on behalf of an organisation. Basically, electronic signatures are used for the purposes for which electronic seals were created as presented in Table 38.

From a technical perspective there are slight differences between electronic certificates and electronic seals, mainly in the certificate fields and profile, differences which can be overcome easily in order to issue electronic seals.

Table 38: Types of electronic seals issued by the EaP countries

Country	Unqualified electronic seals	Qualified electronic seals
Armenia	NO	YES
Azerbaijan	YES	YES
Belarus	NO	YES
Georgia	YES	YES
Moldova	NO	NO
Ukraine	YES	YES

Source: Developed by EU4Digital Facility

All other findings presented in ‘Electronic signatures’ section (Tables 30-37) apply to electronic seals as well.

7.3 Electronic timestamp services

A time stamp can refer to a time code or to a digitally signed timestamp whose signer vouches for the existence of the signed document or content at the time given as part of the digital signature. Time stamps are used, for example, on contracts or medical records. A qualified electronic time stamp must meet the following requirements:

- It binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably.
- It is based on an accurate time source linked to Coordinated Universal Time.
- It is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

Except for Belarus all EaP countries use one of the internationally accepted protocols for timestamps as presented in Table 39.

Table 39: Timestamp protocols used by the EaP countries

Country	RFC 3161 Time Stamp Protocol	DSS XML Time Stamping Profile
Armenia	YES	NO
Azerbaijan	YES	NO
Belarus	NO	NO
Georgia	YES	NO
Moldova	YES	NO
Ukraine	YES	YES

Source: Developed by EU4Digital Facility

The accuracy of the timestamps is provided by the time source linked to Coordinated Universal Time. The time sources can be self-generated, national and international. National and international time sources can be used if they provide better accuracy than the self-generated time source.

Except for Belarus all EaP countries disclosed what types of time sources they are using for time stamps, as presented in Table 40.

Table 40: Time sources used by the EaP countries for timestamps

Country	Self-generated	National source	International source
Armenia	NO	NO	YES
Azerbaijan	NO	NO	YES
Belarus	NO	NO	NO
Georgia	NO	NO	YES
Moldova	NO	NO	YES
Ukraine	NO	YES	NO

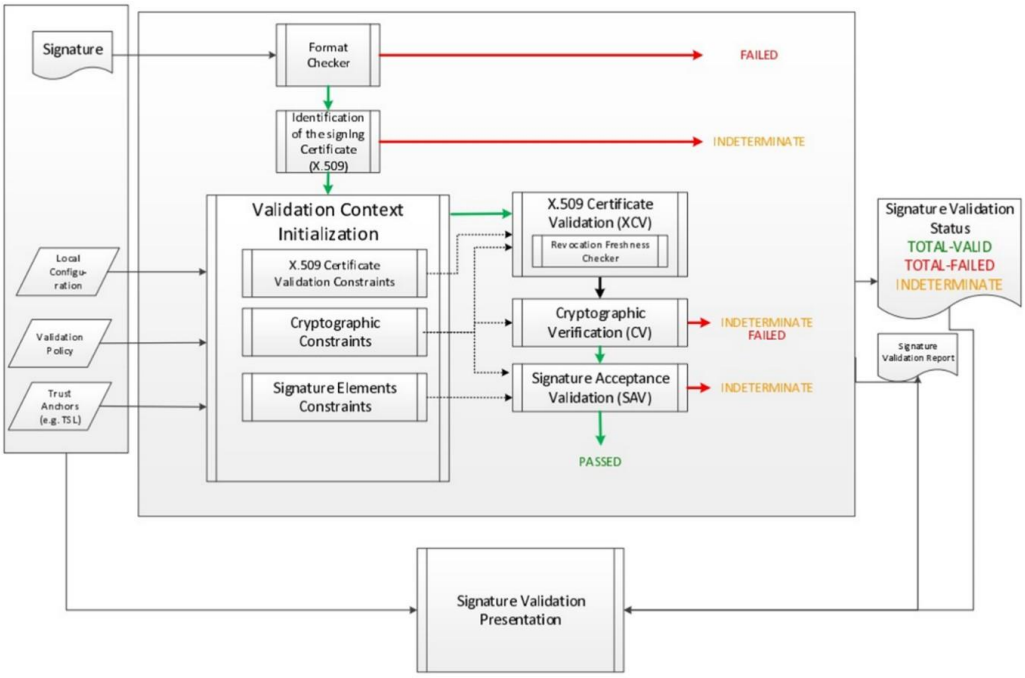
Source: Developed by EU4Digital Facility

7.4 Certificate revocation and validation services

The validation process of an electronic signature must provide one of the following three statuses: **TOTAL-FAILED**, **TOTAL-PASSED** or **INDETERMINATE**. A **TOTAL-PASSED** response indicates that the signature has passed verification and it complies with the signature validation policy. A **TOTAL-FAILED** response indicates that either the signature format is incorrect or that the digital signature value fails the verification. An **INDETERMINATE** validation response indicates that the format and digital signature verifications have not failed but there is an insufficient information to determine if the electronic signature is valid. For each of the validation checks, the validation process

must provide information justifying the reasons for the resulting status indication as a result of the check against the applicable constraints. In addition, the ETSI standard defines a consistent and accurate way for justifying statuses under a set of sub-indications[1].

Figure 9: Electronic signature validation process as described in the ETSI guidelines



Source: European Telecommunications Standards Institute (2020)

All mathematical procedures to ensure if proper encryption schemes were used and if the integrity of the electronic signature were not compromised can be performed locally. The last step of the validation process requires an online interaction with the TSP in order to check the status of the certificate.

The TSP should have in place technical mechanisms to revoke expired certificates (e.g. electronic signatures, electronic seals). TSPs should provide a mechanism to all relying parties through which the status of the electronic certificates can be queried via an online service. The most common method for certificate revocation involves the publication of a Certificate Revocation List (CRL) that contains all expired or revoked certificates. Additionally, the TSP should provide the Online Certificate Status Protocol (OCSP) as a mechanism to validate in real-time the status of an electronic certificate.

All EaP countries are currently providing both the CRL and the OCSP protocol for certificate revocation status and validity status as presented in Table 41.

Table 41: Revocation and validation services used in the EaP countries

Country	Certificate Revocation List (CRL)	Online Certificate Status Protocol (OCSP)
Armenia	YES	YES
Azerbaijan	YES	YES
Belarus	YES	YES
Georgia	YES	YES
Moldova	YES	YES

1 https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html#_the_signature_validation

Country	Certificate Revocation List (CRL)	Online Certificate Status Protocol (OCSP)
Ukraine	YES	YES

Source: Developed by EU4Digital Facility

7.5 Electronic identification (eID) and MobileID

Electronic identification is the process of using person identification data in electronic form with the purpose of uniquely representing either a natural or legal person, or a natural person representing a legal person. In practice this is usually implemented by issuing electronic identification cards. These electronic cards contain electronic chips which can store the electronic data required to identify a natural person and an electronic signature which, depending on specific characteristics described in the past sections, can be used as an unqualified or qualified electronic signature.

Another type of electronic identification comes in the form of a mobile ID. In this setup the mobile operator in a country acts as an external registration authority for the TSP. A special SIM card is used to generate the certificate key pairs, but the TSP through its certification authority is the entity which performs the issuance of the certificates and their enrolment into the TSP certificate repository.

All EaP countries are currently offering at least a form of electronic identification, either through eIDs or through mobile IDs as presented in Table 42.

Table 42: eID and Mobile ID services used in the EaP countries

Country	Electronic Identification	Mobile ID
Armenia	YES	YES
Azerbaijan	YES	YES
Belarus	NO	YES
Georgia	YES	YES
Moldova	YES	YES
Ukraine	YES	YES

Source: Developed by EU4Digital Facility

7.6 Website authentication certificates

Website authentication certificates are used to authenticate the legitimacy of an internet website or domain while also protecting the communication between the end-user and the website by using strong encryption algorithms. In order to properly function, the root certificate of the TSP must be installed on all the devices that will interact with a website that are using the TSP issued certificates. In practice there is an industry consortium represented by Microsoft, Apple and Mozilla as the leading manufacturers of electronic devices, which decide whose root certificates they will preload on all their products. These three companies manage a trusted root repository, and all TSPs that want to have their CA's listed on that repository must pass a yearly audit.

Currently with the exception of Azerbaijan, who passed a first phase audit in order to be included in the trusted root repository, none of the other five EaP countries have a TSP listed as a trusted root CA as presented in Table 43. Website authentication certificates are purchased by individuals or companies from commercial providers.

Table 43: eID and Mobile ID services used in the EaP countries

Country	Transport Layer Security (TLS) certificates
Armenia	NO
Azerbaijan	YES
Belarus	NO
Georgia	NO
Moldova	NO
Ukraine	NO

Source: Developed by EU4Digital Facility

7.7 Preservation services

Certificate preservation services ensure that signed objects don't lose their evidential value, if cryptographic algorithms become weak, and they maintain the integrity and authenticity of signed data for long periods of time, beyond the validity of the electronic certificate. In EU there are only a few TSP service providers who are able to provide certificate preservation services.

Azerbaijan and Ukraine are the only countries in the EaP who offer certificate preservation services.

Table 44: eID and Mobile ID services used in the EaP countries

Country	Certificate preservation services	Qualified certificate preservation services
Armenia	NO	NO
Azerbaijan	YES	YES
Belarus	NO	NO
Georgia	NO	NO
Moldova	NO	NO
Ukraine	YES	YES

Source: Developed by EU4Digital Facility

8 Technical maturity assessment results related to trust and eID services in the EaP countries

8.1 Trust Services Environmental Controls

This maturity area measures the controls in place to establish and maintain a trustworthy TSP environment, that is essential to the reliability of the TSP's business processes. Specifically, it measures if:

- The TSP maintains controls to provide reasonable assurance that security is planned, managed and supported within the organisation; security risks are identified and managed; the security of TSP facilities, systems and information assets accessed by third parties is maintained; the security of subscriber and relying party information is maintained when the responsibility for TSP sub-functions has been outsourced to another organisation or entity.
- The TSP maintains controls to provide reasonable assurance that TSP assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices.
- The TSP maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.
- The TSP maintains controls to provide reasonable assurance that:
    - physical access to TSP facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;
    - CA facilities and equipment are protected from environmental hazards; loss, damage or compromise of assets and interruption to business activities are prevented; compromise of information and information processing facilities is prevented.
- The TSP maintains controls to provide reasonable assurance that:
    - the secure operation of TSP information processing facilities is ensured;
    - the risk of TSP systems failure is minimised;
    - the integrity of TSP systems and information is protected against viruses and malicious software;
    - damage from security incidents and malfunctions is minimised through the use of incident reporting and response procedures; and media are securely handled to protect them from damage, theft and unauthorised access.
- The TSP maintains controls to provide reasonable assurance that TSP system access is limited to authorised individuals. Such controls provide reasonable assurance that:
    - hypervisor, operating system, database, and network device access is limited to authorised individuals with predetermined task privileges;
    - access to network segments housing TSP systems is limited to authorised individuals, applications and services and TSP application use is limited to authorised individuals.
- The TSP maintains controls to provide reasonable assurance that TSP systems development, maintenance activities, patching, and changes to TSP systems including hypervisors (where applicable), operating systems, databases, applications, network devices, and hardware are documented, tested, authorised, and properly implemented to maintain TSP system integrity.
- The TSP maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster or other type of business interruption. Such controls include, at a minimum:
    - the development and testing of a TSP business continuity plan that includes a disaster recovery process for critical components of the TSP system;
    - the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;

- creating backups of systems, data, and configuration information at regular intervals in accordance with the CA's disclosed business practices, and storage of these backups at an alternate location; and the availability of an alternate site, equipment and connectivity to enable recovery.

- The TSP maintains controls to provide reasonable assurance that potential disruptions to subscribers and relying parties are minimised as a result of the cessation or degradation of the CA's services.
- The TSP maintains controls to provide reasonable assurance that:
  - it conforms with the relevant legal, regulatory and contractual requirements;
  - compliance with the CA's security policies and procedures is ensured;
  - the effectiveness of the system audit process is maximised and interference to and from the system audit process is minimised; and unauthorised TSP system usage is detected.
- The TSP maintains controls to provide reasonable assurance that:
  - significant TSP environmental, key management, and certificate management events are accurately and appropriately logged; the confidentiality and integrity of current and archived audit logs are maintained;
  - audit logs are completely and confidentially archived in accordance with disclosed business practices; and audit logs are reviewed periodically by authorised personnel.

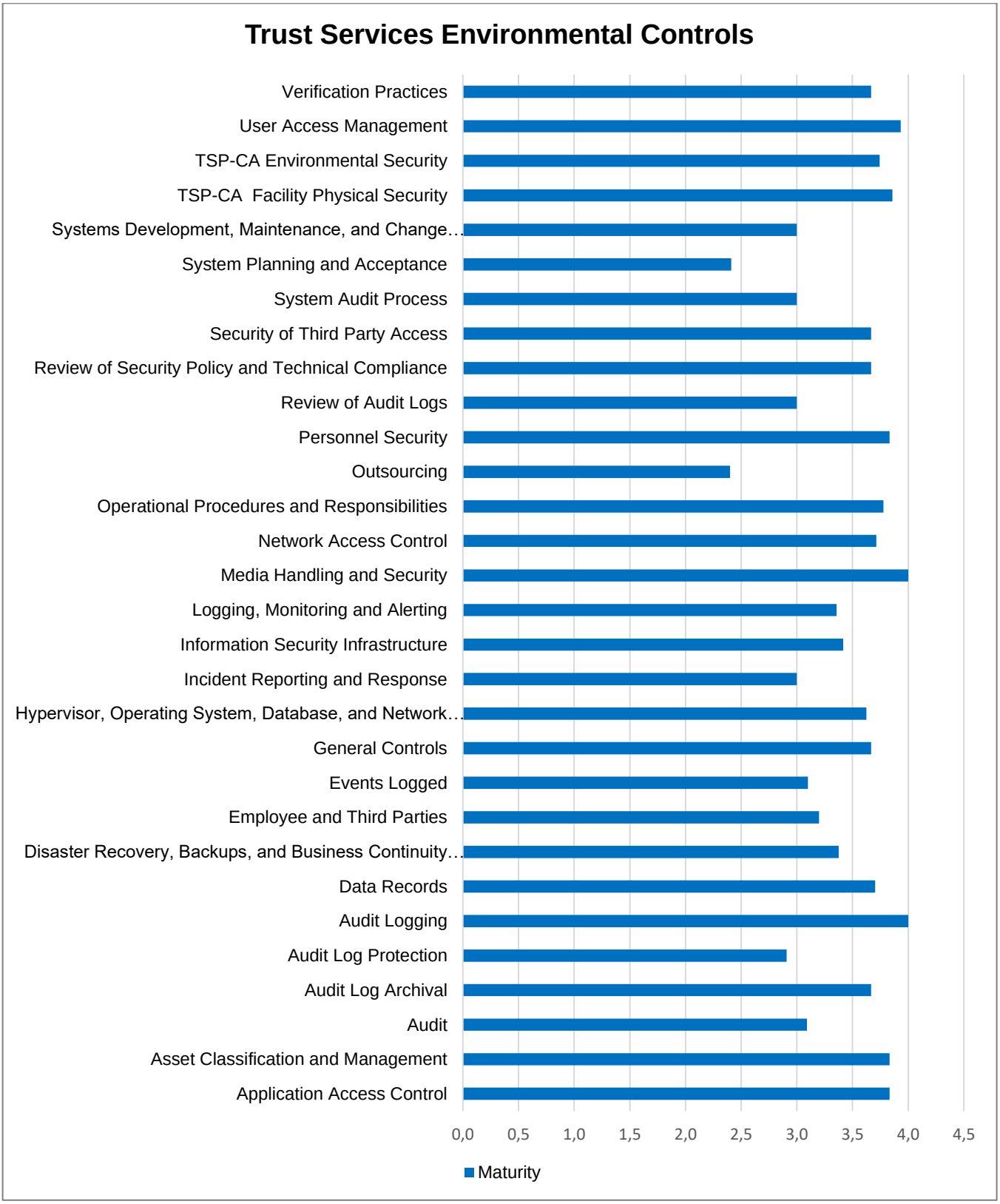
Table 45: Trust services environmental controls maturity rating by maturity area

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	No. of total questions	Maturity
Application Access Control	0	0	0	5	4	3	12	**3.8**
Asset Classification and Management	0	0	1	7	4	6	18	**3.8**
Audit	2	0	0	5	1	3	11	**3.1**
Audit Log Archival	0	0	0	3	2	1	6	**3.7**
Audit Log Protection	2	0	2	5	2	1	11	**2.9**
Audit Logging	0	0	0	12	12	12	36	**4.0**
Data Records	2	1	1	42	34	27	108	**3.7**
Disaster Recovery, Backups, and Business Continuity Management	3	0	5	18	12	10	48	**3.4**
Employee and Third Parties	4	0	0	2	4	2	10	**3.2**
Events Logged	52	6	20	103	61	68	303	**3.1**
General Controls	0	0	0	4	3	4	12	**3.7**
Hypervisor, Operating System, Database, and Network Device Access Control	2	0	0	19	13	13	48	**3.6**
Incident Reporting and Response	1	0	0	6	2	2	12	**3.0**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	No. of total questions	Maturity
Information Security Infrastructure	0	2	0	13	4	5	24	**3.4**
Logging, Monitoring and Alerting	1	1	5	16	13	6	42	**3.4**
Media Handling and Security	0	0	0	3	6	3	12	**4.0**
Network Access Control	0	0	0	15	14	11	42	**3.7**
Operational Procedures and Responsibilities	0	1	1	5	5	6	18	**3.8**
Outsourcing	6	0	0	2	2	2	10	**2.4**
Personnel Security	3	0	2	20	23	24	72	**3.8**
Review of Audit Logs	2	0	1	4	3	2	12	**3.0**
Review of Security Policy and Technical Compliance	0	0	0	3	2	1	6	**3.7**
Security of Third-Party Access	0	0	0	6	4	2	12	**3.7**
System Audit Process	0	1	1	2	1	1	6	**3.0**
System Planning and Acceptance	11	14	12	25	14	12	95	**2.4**
Systems Development, Maintenance, and Change Management	5	2	0	14	6	8	36	**3.0**
TSP-CA Facility Physical Security	4	1	1	55	45	50	155	**3.9**
TSP-CA Environmental Security	0	0	4	29	28	26	90	**3.7**
User Access Management	0	0	1	8	13	8	30	**3.9**
Verification Practices	0	0	0	6	4	2	12	**3.7**

Source: Developed by EU4Digital Facility

Figure 10: Trust services environmental controls maturity rating by maturity area



Source: Developed by EU4Digital Facility

8.2 Trust Services Key Lifecycle Management

This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their life cycles. Specifically, it measures if:

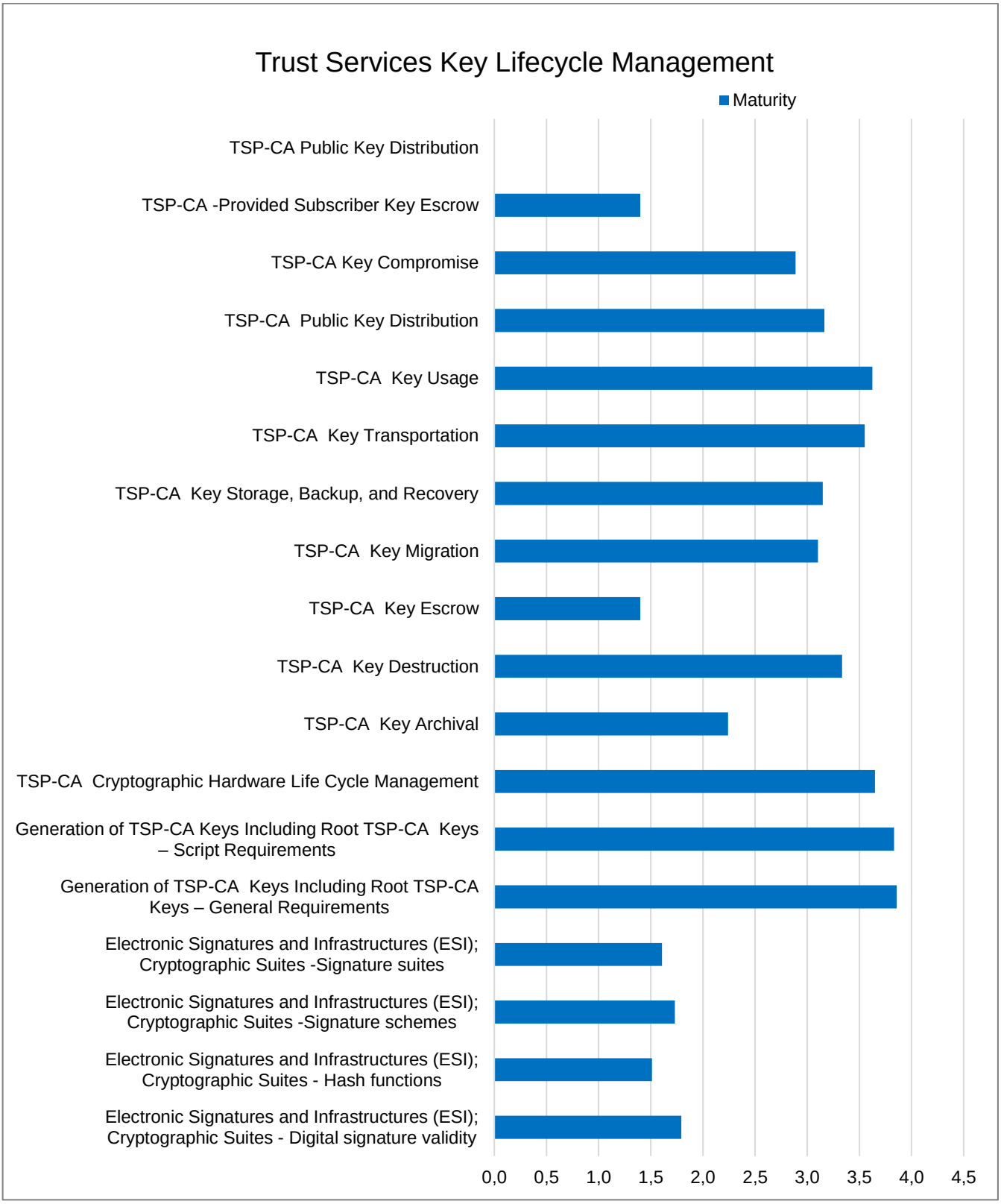
- The TSP maintains controls to provide reasonable assurance that TSP key pairs are generated in accordance with the TSP's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts.
- The TSP maintains controls to provide reasonable assurance that TSP private keys remain confidential and maintain their integrity. The TSP's private keys are backed up, stored and recovered by authorised personnel in trusted roles, using multiple person control in a physically secured environment.
- The TSP maintains controls to provide reasonable assurance that the integrity and authenticity of the TSP public keys and any associated parameters are maintained during initial and subsequent distribution.
- The TSP maintains controls to provide reasonable assurance that TSP keys are used only for their intended functions in their predetermined locations.
- The TSP maintains controls to provide reasonable assurance that archived TSP keys remain confidential, secured, and are never put back into production.
- The TSP maintains controls to provide reasonable assurance that:
    - copies of TSP keys that no longer serve valid business purposes are destroyed in accordance with the TSP's disclosed business practices; and copies of TSP keys are completely destroyed at the end of the key pair life cycle in accordance with the TSP's disclosed business practices.
- The TSP maintains controls to provide reasonable assurance that continuity of operations is maintained in the event of the compromise of the TSP's private keys and any certificates, signed with the compromised keys, are revoked and reissued.
- The TSP maintains controls to provide reasonable assurance that:
    - devices used for private key storage and recovery, and the interfaces to these devices are tested before usage for integrity;
    - access to TSP cryptographic hardware is limited to authorised personnel in trusted roles, using multiple person control; and the TSP cryptographic hardware is functioning correctly.
- The TSP maintains controls to provide reasonable assurance that escrowed TSP private signing keys remain confidential.
- The TSP maintains controls to provide reasonable assurance that:
    - CA private keys that are physically transported from one facility to another remain confidential and maintain their integrity;
    - CA hardware containing TSP private keys, and associated activation materials, are prepared for transport in a physically secure environment by authorised personnel in trusted roles, using multiple person controls, and are transported within sealed tamper evident packaging;
    - CA keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and TSP key transportation events are logged.
- The TSP maintains controls to provide reasonable assurance that:
    - CA keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration, are completed in a physically secure environment by those in Trusted Roles under multi-person control;
    - hardware and software tools used during the TSP key migration process are tested by the TSP prior to the migration event; and the TSP key migration events follow a documented script and are logged.

Table 46: Trust services key lifecycle management controls by maturity area

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and	Answered as Optimized	No. of total questions	Maturity
Electronic Signatures and Infrastructures (ESI); Cryptographic Suites – Digital signature validity	49	0	0	18	13	15	101	**1.8**
Electronic Signatures and Infrastructures (ESI); Cryptographic Suites – Hash functions	25	0	0	7	4	5	41	**1.5**
Electronic Signatures and Infrastructures (ESI); Cryptographic Suites – Signature schemes	14	0	0	6	3	3	26	**1.7**
Electronic Signatures and Infrastructures (ESI); Cryptographic Suites – Signature suites	32	0	0	11	3	9	56	**1.6**
Generation of TSP-CA Keys Including Root TSP-CA Keys – General Requirements	1	0	1	13	14	13	42	**3.9**
Generation of TSP-CA Keys Including Root TSP-CA Keys – Script Requirements	0	0	0	3	1	2	6	**3.8**
TSP-CA Cryptographic Hardware Life Cycle Management	2	0	2	24	17	15	60	**3.7**
TSP-CA Key Archival	15	0	4	1	5	5	25	**2.2**
TSP-CA Key Destruction	7	0	0	14	7	14	42	**3.3**
TSP-CA Key Escrow	8	0	0	2	2	0	10	**1.4**
TSP-CA Key Migration	6	0	1	11	5	7	29	**3.1**
TSP-CA Key Storage, Backup, and Recovery	6	0	2	6	7	7	27	**3.1**
TSP-CA Key Transportation	6	0	1	22	17	14	58	**3.6**
TSP-CA Key Usage	1	0	1	9	7	6	24	**3.6**
TSP-CA Public Key Distribution	14	0	4	25	16	13	67	**3.2**
TSP-CA Key Compromise	3	1	0	8	3	3	18	**2.9**
TSP-CA - Provided Subscriber Key Escrow	4	0	0	1	1	0	5	**1.4**
TSP-CA Public Key Distribution	0	0	0	0	0	0	0	**0.0**

Source: Developed by EU4Digital Facility

Figure 11: Trust services key lifecycle management controls by maturity area



Source: Developed by EU4Digital Facility

8.3 Trust Services Subscriber Key Lifecycle Management

This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles. It specifically measures if:

- The TSP maintains controls to provide reasonable assurance that subscriber keys generated by the TSP/RA/card bureau are generated within a secure cryptographic device based on a risk assessment and the business requirements of the TSP are in accordance with the CA's disclosed business practices; and subscriber keys generated by the TSP/RA/card bureau are securely distributed to the subscriber by the TSP/RA/card bureau) in accordance with the CA's disclosed business practices.
- The TSP maintains controls to provide reasonable assurance that:
  - subscriber private keys stored by the TSP remain confidential and maintain their integrity;
  - subscriber private keys archived and escrowed by the TSP remain confidential;
  - subscriber private keys stored by the TSP are completely destroyed at the end of the key pair life cycle.
- The TSP maintains controls to provide reasonable assurance that:
  - EID procurement, preparation and personalisation are securely controlled by the TSP/RA/card bureau;
  - EID Application Data File (ADF) preparation is securely controlled by the TSP(or RA);
  - EID usage is enabled by the TSP/RA/card bureau prior to EID issuance;
  - EID deactivation and reactivation are securely controlled by the TSP/RA;
  - EIDs are securely stored and distributed by the TSP/RA/card bureau;
  - EIDs are securely replaced by the TSP/RA/card bureau;
  - EIDs returned to the TSP/RA/card bureau are securely terminated.
- The TSP maintains controls to provide reasonable assurance that:
  - requirements for protection of subscriber keys are communicated to subscribers and that any subscriber's key management tools provided by the TSP support the requirements of the CA's business practices disclosure.

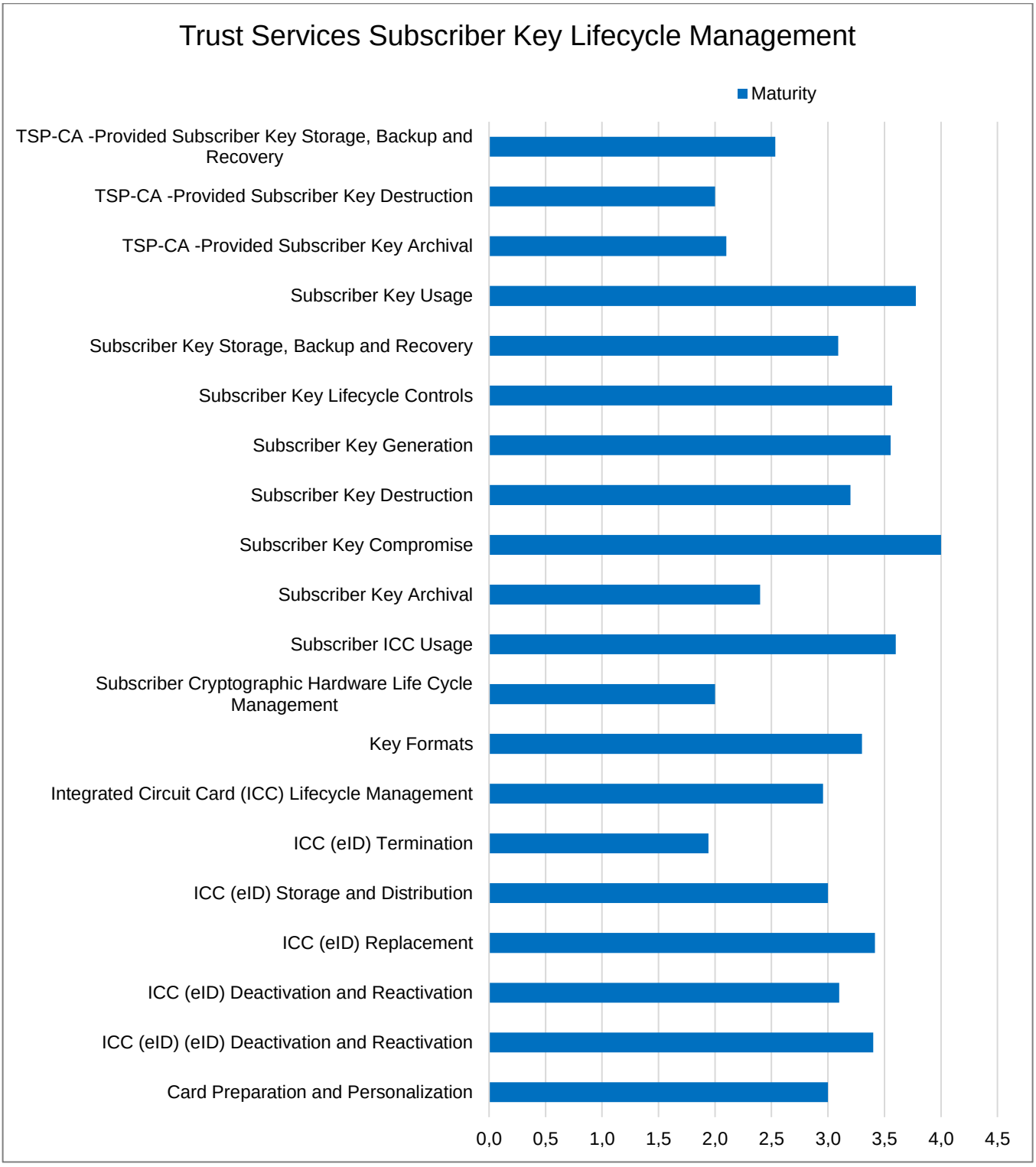
Table 47: Trust services subscriber key lifecycle management control by maturity area

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and	Answered as Optimized	No. of total questions	Maturity
Card Preparation and Personalisation	5	0	0	15	5	5	30	**3.0**
ICC (eID) (eID) Deactivation and Reactivation	1	0	0	3	2	0	5	**3.4**
ICC (eID) Deactivation and Reactivation	6	0	0	10	8	0	20	**3.1**
ICC (eID) Replacement	1	0	0	5	4	2	12	**3.4**
ICC (eID) Storage and Distribution	3	0	0	9	3	3	18	**3.0**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and	Answered as Optimized	No. of total questions	Maturity
ICC (eID) Termination	5	0	0	7	3	0	17	**1.9**
Integrated Circuit Card (ICC) Lifecycle Management	5	0	1	10	4	4	23	**3.0**
Key Formats	15	0	8	32	30	15	93	**3.3**
Subscriber Cryptographic Hardware Life Cycle Management	3	0	0	2	1	0	5	**2.0**
Subscriber ICC Usage	1	0	0	14	9	6	30	**3.6**
Subscriber Key Archival	6	0	0	2	2	2	10	**2.4**
Subscriber Key Compromise	0	0	0	2	2	2	6	**4.0**
Subscriber Key Destruction	4	0	0	2	4	2	10	**3.2**
Subscriber Key Generation	2	0	0	4	8	4	18	**3.6**
Subscriber Key Lifecycle Controls	2	0	0	9	10	8	30	**3.6**
Subscriber Key Storage, Backup and Recovery	7	0	0	6	5	6	22	**3.1**
Subscriber Key Usage	1	0	0	5	7	5	18	**3.8**
TSP-CA -Provided Subscriber Key Archival	7	0	0	1	2	2	10	**2.1**
TSP-CA -Provided Subscriber Key Destruction	6	0	0	2	2	2	12	**2.0**
TSP-CA -Provided Subscriber Key Storage, Backup and Recovery	11	0	0	7	5	7	30	**2.5**

Source: Developed by EU4Digital Facility

Figure 12: Trust services subscriber key lifecycle management control by maturity area



Source: Developed by EU4Digital Facility

8.4 Trust Services Certificate Lifecycle Management

This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that Subscriber information was properly authenticated. It specifically measures if:

- The TSP maintains controls to provide reasonable assurance that subscribers are accurately identified in accordance with the CA's disclosed business practices; subscribers' domain names and IP addresses are accurately validated in accordance with the CA's disclosed business practices; and subscribers' certificate requests are accurate, authorised and complete.
- The TSP maintains controls to provide reasonable assurance that certificate renewal requests are accurate, authorised and complete.
- The TSP maintains controls to provide reasonable assurance that certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorised and complete.
- The TSP maintains controls to provide reasonable assurance that certificates are generated and issued in accordance with the CA's disclosed business practices.
- The TSP maintains controls to provide reasonable assurance that, upon issuance, complete and accurate certificates are available to subscribers and relying parties in accordance with the CA's disclosed business practices.
- The TSP maintains controls to provide reasonable assurance that certificates are revoked, based on authorised and validated certificate revocation requests within the time frame in accordance with the CA's disclosed business practices.
- The TSP maintains controls to provide reasonable assurance that certificates are suspended based on authorised and validated certificate suspension requests within the time frame in accordance with the CA's disclosed business practices.
- The TSP maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including Certificate Revocation Lists and other certificate status mechanisms) is made available to relevant entities (Subscribers and Relying Parties or their agents) in accordance with the CA's disclosed business practices.

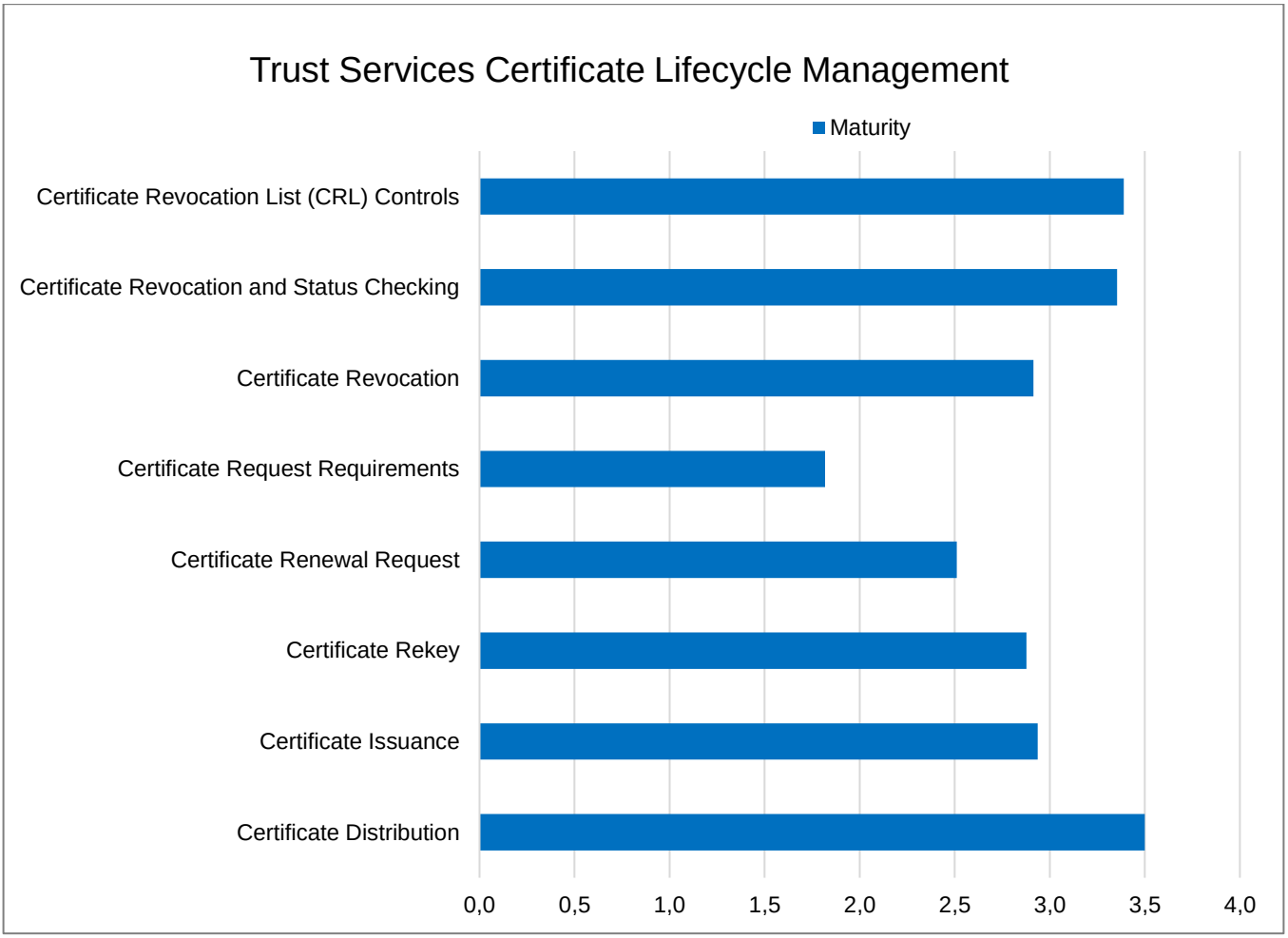
Table 48: Trust services certificate lifecycle management controls by maturity area

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	No. of total questions	Maturity
Certificate Distribution	0	0	5	10	10	5	30	**3.5**
Certificate Issuance	9	0	1	18	13	6	47	**2.9**
Certificate Rekey	24	0	3	38	16	15	90	**2.9**
Certificate Renewal Request	35	0	0	33	18	16	100	**2.5**
Certificate Request Requirements	5	0	0	4	2	0	11	**1.8**
Certificate Revocation	12	0	11	13	17	8	58	**2.9**
Certificate Revocation and Status Checking	2	0	7	17	14	8	48	**3.4**
Certificate Revocation List (CRL) Controls	7	0	6	38	29	16	95	**3.4**
Certificate Suspension	40	0	1	7	22	12	70	**2.4**

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and Measured	Answered as Optimized	No. of total questions	Maturity
Identification and Authentication	1	0	0	9	5	3	18	**3.4**

Source: Developed by EU4Digital Facility

Figure 13: Trust services certificate lifecycle management controls by maturity area



Source: Developed by EU4Digital Facility

8.5 Trust Services Cross Certificate Lifecycle Management

This maturity area measures the effective controls maintained by TSP to provide reasonable assurance that subordinate CAs and cross certificate requests are accurate, authenticated and approved. It specifically measures if the TSP maintains controls to provide reasonable assurance that:

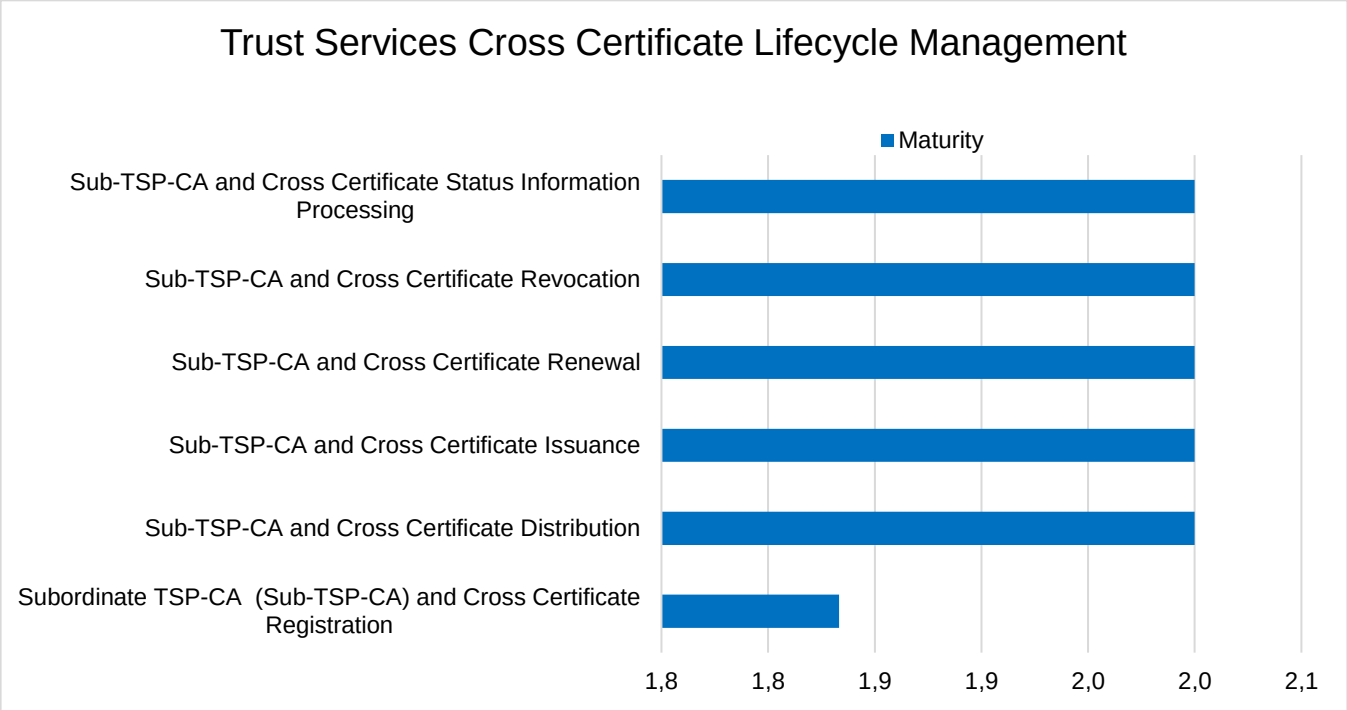
- subordinate TSP and cross certificate requests are accurate, authenticated and approved;
- subordinate TSP and cross certificate replacement (renewal and rekey) requests are accurate, authorised, complete;
- new, renewed and rekeyed Subordinate TSP and cross certificates are generated and issued in accordance with the TSP's disclosed business practices;
- upon issuance, complete and accurate Subordinate TSP and cross certificates are available to relevant entities (Subscribers and Relying Parties) in accordance with the TSP's disclosed business practices;
- subordinate TSP and cross certificates are revoked based on authorised and validated certificate revocation requests; and timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the TSP's disclosed business practices.

Table 49: Trust services cross certificate lifecycle management controls by maturity area

Maturity Area	N/A	Answered as Ad-Hoc	Answered as Managed	Answered as Defined	Answered as Defined and	Answered as Optimize	No. of total questions	Maturity
Subordinate TSP-CA (Sub-TSP-CA) and Cross Certificate Registration	9	0	3	0	3	3	18	**1.8**
Sub-TSP-CA and Cross Certificate Distribution	3	0	0	1	1	1	6	**2.0**
Sub-TSP-CA and Cross Certificate Issuance	3	0	0	1	1	1	6	**2.0**
Sub-TSP-CA and Cross Certificate Renewal	12	0	0	4	4	4	24	**2.0**
Sub-TSP-CA and Cross Certificate Revocation	6	0	0	2	2	2	12	**2.0**
Sub-TSP-CA and Cross Certificate Status Information Processing	3	0	0	1	1	1	6	**2.0**

Source: Developed by EU4Digital Facility

Figure 14: Trust services cross certificate lifecycle management controls by maturity area



Source: Developed by EU4Digital Facility