EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Trust services – Secure move to the cloud of the eIDAS ecosystem

MAY 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use eID@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Evgenia Nikolouzou, Rossen Naydenov (ENISA)

CONTRIBUTORS

Nick Pope, Paloma Llaneza Gonzalez, Inigo Barreira, Michal Tabor, Franziska Granc, Arno Fiedler, Nicholas Dunham

ACKNOWLEDGEMENTS

ENISA would like to thank the members of the ECATS EG (European Competent Authorities for Trust Services Expert Group') who provided valuable comments and feedback to the report and particularly the Austrian Regulatory Authority for Broadcasting and Telecommunications (Ulrich Latzenhofer) and the Spanish supervisory body. Special thanks go to various stakeholders in Europe who provided their response to the survey and/or were interviewed for the purpose of this report.

LEGAL NOTICE

TABLE OF CONTENT

1. INTRODUCTION TO EIDAS, TSPS AND THE CLOUD 8

1.1. eIDAS TRUST SERVICES 8

1.2. STRUCTURE OF THE REPORT 9

1.3. WHAT IS IN THE CLOUD 9

1.3.1. Cloud computing 9
1.3.2. General purpose of cloud platforms 9

1.4. USE OF CLOUD SEVICES IN SUPPORT OF TRUST SERVICES 10

1.4.1. Main cloud service provisions 10

2. GENERAL REQUIREMENTS APPLICABLE TO TSPS AND CSPS 14

2.1. OVERVIEW OF THE REQUIREMENTS FOR TRUST SERVICES 14

2.2. INFORMATION SECURITY REQUIREMENTS OF CLOUD SERVICE 16

2.2.1. ISO standards 16
2.2.2. Cloud Security Alliance STAR self-assessment and certification 18
2.2.3. EU cloud certification scheme 19
2.2.4. EU GDPR 20
2.2.5. NIS 2 Directive 20

3. PROVISION OF SPECIFIC TRUST SERVICES IN THE CLOUD 21

3.1. COMPARISON OF GENERAL CSP STANDARDS WITH GENERAL TSP REQUIREMENTS 21

3.1.1. Information security management 21
3.1.2. Privacy 22
3.1.3. Risk assessment and policy and security requirements 22

3.2. GENERAL CONCLUSIONS 23

3.3. OPERATING TRUST SERVICES IN THE CLOUD 26

3.3.1. Certificate issuance 26
3.3.2. Remote signing service using cloud services 30
3.3.3. Time stamping 30
3.3.4. e-delivery services 32
3.3.5. Signature Preservation services 34
3.3.6. Signature validation 34

3.4. PRACTICAL EXPERIENCES 34

3.5. GENERAL CONCLUSIONS 40

4. EVALUATION OF TRUST SERVICES IN THE CLOUD 41

4.1. ACCREDITATION AND CONFORMITY ASSESSMENT SCHEME UNDER eIDAS 41

4.2. PRACTICAL EXPERIENCES 42

5. CONCLUSIONS 43

6. BIBLIOGRAPHY/REFERENCES 45

6.1. BIBLIOGRAPHY 45

6.2. ENISA PUBLICATIONS 45

6.3. APPLICABLE LEGISLATION/REGULATION 46

7. ANNEX – SURVEY RESULTS 48

7.1. TTUST SERVICE PROVIDERS 48

7.2. CLOUD SERVICE PROVIDERS 49

7.3. PROVIDERS OF SOLUTIONS TO TSPs 52

7.4. NATIONAL AUTHORITIES 53

7.5. CONFORMITY ASSESSMENT BODIES 54

ABBREVIATIONS

CA	Certification Authority
CAB	Conformity Assessment Body
CEN	European Committee for Normalization
CSA	Cloud Security Alliance
CSC	Cloud Service Customer
CSP	Cloud Service Provider
eIDAS	EU regulation on electronic identification and trust services for electronic transactions
EN	European Standard
ERDS	Electronic Registered Delivery Service
ESI	electronic signatures and infrastructures
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI technical specifications
EU	European Union
EUCS	European cybersecurity certification scheme for cloud services
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
IaaS	Infrastructure as a Service
ISMS	information security management system
ISO/IEC	International Organization for Standardisation / International Electrotechnical Commission
NA/SB	national authorities / supervisory bodies
NIS 2	EU directive on measures for a high common level of cybersecurity across the EU
OCSP	Online Certificate Status Protocol
PaaS	Platform as a Service
PII	personally identifiable information
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
REMS	Registered Electronic Mail Service
SB	Supervisory Body
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Universal Time Coordinated

EXECUTIVE SUMMARY

Since Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (hereafter the eIDAS regulation or eIDAS) ([1]) entered into force in July 2016, the EU has offered a trust framework for online and digital transactions in the EU. Qualified trust services (QTS), as defined in the regulation, are the core of the framework establishing trust between businesses, EU Member States and individuals. Not only has eIDAS established trust in the EU, but also opened a new market for trust service providers (TSPs). With over 200 companies listed in the EU trusted list of service providers, the market is developing constantly, changing and adapting to its environment.

Clouds and cloud computing nowadays are a commonly used platform for sharing and storing data. They can be used for many purposes and are often an inherent part of large, small and medium-sized enterprises. The benefits of using clouds are flexibility, cost effectiveness, the easy transfer of data and the availability to extend services as usage grows. In recent years, TSPs have been moving their services to the cloud in order to take advantage of these benefits. Many providers have already moved all or parts of their services to the cloud. Cloud providers have realised their market goals for this transition and conformity assessment bodies (CABs) are investigating the means to audit trust services from the cloud.

This report includes a detailed analysis on the different technical requirements that must be addressed considering the relevant standards. It also gives an overview of practical experiences on the move of trust services to the cloud, based on the results of a survey conducted with over 120 participants. The report finds that there are many existing requirements on the TSP side that can be considered and potentially applied to cloud service providers (CSPs). The two most important standards against which conformance is often assessed by CSPs and which have much in common with the standards for trust services are:

- ISO/IEC 27017: Code of practice for information security controls, based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27001: Information security management systems.

The results of the survey have shown that trust services are moving to the cloud. The findings of the comparison of standards adopted by CSPs and TSPs in the theoretical part of this report show that there are mostly minor disparities. The trust services that stakeholders consider most appropriate to be operated on a cloud are:

- qualified certificates for electronic signature;
- qualified validation for electronic signature;
- qualified certificates for electronic seals;
- provision of revocation status information.

From the audit perspective, the survey results have particularly shown that there is still insecurity and open questions when it comes to auditing the trust services remotely. While there are standards which CABs recognise as supporting compliance audits of TSPs providing services in the cloud (ISO 27017, ISO 27701, EU cloud cyber certification), most CABs think that the terms and conditions of CSPs contain adequate clauses allowing access for auditors to

([1]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv %3AOJ.L_.2014.257.01.0073.01.ENG.

perform TSP assessments. While some impediments from the audit perspective exist, the survey results have shown that CABs can already perform audits on many trust services.

Moving trust services to the cloud must be understood as an ongoing process that has to be followed step by step. While some services – such as the validation of signatures, registered delivery, time stamp or signature preservation – are moved rather quickly, other services – such as the issuance of certificates and remote control over the signing device – require in-depth analysis and preparation. The transition of data to the cloud has to be secure at all times and, in the best case, must remain in the data centre of the TSP. Some services might not be suitable for operation on the cloud. This report gives a detailed overview of the issues to be addressed for such transitions, along with the related challenges and opportunities.

1. INTRODUCTION TO eIDAS, TSPs AND THE CLOUD

1.1. eIDAS TRUST SERVICES

The eIDAS regulation on electronic identification and trust services for electronic transactions in the internal market provides a regulatory environment for the electronic identification of natural and legal persons and a framework for electronic trust services. The regulation repeals Directive 1999/93/EC. Under the eIDAS regulation, it is possible to use trust services and electronic documents as evidence in legal proceedings across all Member States that contribute to their cross-border use.

As of 1 July 2016, all provisions relating to trust services of the eIDAS regulation are directly applicable in the 27 Member States and do not need to be transposed into national law. The eIDAS regulation facilitates seamless digital transactions among individuals and businesses across Member States and establishes a climate of trust when it comes to online and digital transactions in the EU.

One objective of this regulation is to enhance the trust of enterprises and consumers in the internal market and to promote the use of trust services and products. To that end, the regulation introduces the notions of qualified trust service (QTS) and qualified trust service provider (QTSP) with a view to indicating their compliance with the eIDAS high-level security requirements and obligations. A QTSP is a TSP that has been granted a qualified status and is supervised by its national supervisory body (SB).

Therefore, when a TSP intends to start providing QTS, it shall submit to the SB a notification of its intention, together with a conformity assessment report issued by an eIDAS-accredited conformity assessment body (CAB). National accreditation bodies (NAB) contribute to the quality assurance of the whole process by being responsible to accredit a CAB that will perform the conformity assessment audits to the TSP.

In June 2021 the European Commission proposed a revision of the eIDAS regulation (COM/2021/281) ([2]), also known as eIDAS 2.0, which not only suggests the establishment of a European digital identity wallet, but also proposes four new QTS: issuing of electronic attestations of attributes, provision of electronic archiving services, electronic ledgers and management of remote electronic signature and seal creation devices. eIDAS 2.0 is still under development and the requirements of these new services have yet to be defined. This report will focus on the existing technical standards of current eIDAS trust services and will not further consider the proposed new trust services.

In recent years, TSPs have been interested in moving their services to the cloud for the mentioned benefits. Many providers have already moved all or parts of their services to the cloud. Cloud providers have realised their market opportunity for this transition and CABs are investigating means to audit trust services from the cloud. This report considers the issues involved in moving to the cloud, both from a theoretical viewpoint based on a comparison of standards and from a practical viewpoint based on the experiences of stakeholders in this area.

([2]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281.

1.2. STRUCTURE OF THE REPORT

Section 1 of this report introduces the concepts and services provided by TSPs and CSPs. The other sections cover the following topics.

- **Section 2.** An analysis of the provisions of security standards commonly adopted by cloud services compared with the general requirements of standards for trust services.
- **Section 3.** An analysis of the specific requirements of trust services and their components against the ability of cloud services to support those requirements.
- **Section 4.** Consideration of the issues with the evaluation of trust services in the cloud.
- **Section 5.** Conclusion of the report.
- **Annex.** Statistics of the survey.

For this report, a survey for four different stakeholders was conducted. The different questionnaires were sent out to TSPs, CABs, national authorities / supervisory bodies (NA/SBs) and providers of solutions to TSPs. In total there were 128 participants. The results will be referenced throughout this report and analysed in depth in Sections 3 and 4.

1.3. WHAT IS IN THE CLOUD

Since a few years, clouds have been an inherent part of the digital world. Especially in the business sector, clouds are used for many different purposes such as sharing and storing data and developing products and business models. The following will briefly describe the definition of cloud computing and its general purpose.

1.3.1. CLOUD COMPUTING

For the definition of cloud computing, this report refers to ISO/IEC 17788[3], which describes cloud computing as a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand. Thus, cloud services are functions offered through cloud computing and used via a specific interface. In simple terms, cloud computing allows data, services, programs and applications to be accessed on a device-independent basis over the internet.

A cloud service customer (CSC) is a party in a business relationship for the purpose of using cloud services. A CSP is the party which makes cloud services available. A cloud service user is a natural person or a legal entity which acts on behalf of the cloud services customer of cloud services.

The following sections provide further details on the types of cloud services that can be provided and their features. This report indicates the applicability of the different types of cloud services to trust services.

1.3.2. GENERAL PURPOSE OF CLOUD PLATFORMS

There are many benefits in using cloud platforms. Apart from the data storage aspect described above, they offer ways to interact and share data with third parties. The data is accessible from all over the world but, at the same time, data access can be restricted as it would be using hardware-based storage. A big advantage of using cloud services is that the provider takes over the physical security and maintenance of the hardware, which leads to savings in costs and time. In addition, CSPs use a scalable economy model that gives small businesses the opportunity to obtain better IT solutions at lower prices.

[3] At the time of writing, ISO/IEC 17788 was under review and due to be replaced by ISO/IEC 22123-1:2023 and ISO/IEC FDIS 22123-2 in the course of 2023

By using cloud services, significant savings can be made in the hardware and software infrastructure needed to support trust services. Many of the overhead costs in ensuring security are provided. Furthermore, as the infrastructure requirements of a TSP change, the use of shared cloud services can be easily adapted to their changing needs.

The following section explores the common provisions of cloud services and the standards generally adopted by CSPs.

1.4. USE OF CLOUD SERVICES IN SUPPORT OF TRUST SERVICES

This report analyses the potential of moving QTSs to the cloud. In the eIDAS regulation, nine types of QTS are mentioned:

- provision of qualified certificates for electronic signatures;
- provision of qualified certificates for electronic seals;
- provision of qualified certificates for website authentication;
- qualified validation service for qualified electronic signatures;
- qualified validation service for qualified electronic seals;
- qualified preservation service for qualified electronic signatures;
- qualified preservation service for qualified electronic seals;
- qualified time-stamping service;
- qualified electronic registered delivery service (ERDS).

The QTS can be grouped into five main categories:

- issuance of certificates;
- validation of signatures or seals based on those certificates;
- preservation of those signatures or seals;
- time stamps.

ERDS is also performed with the mentioned certificates.

1.4.1. MAIN CLOUD SERVICE PROVISIONS

In order to provide the basis of the analysis of the use of general cloud service platforms, this section provides an outline of the services and associated features commonly provided by CSPs.

This is based on documentation provided online by the major cloud providers offering publicly available services. Other ways of providing cloud services exist, such as private cloud services, hybrid public and private cloud services and community-based cloud services. However, when looking at the move of eIDAS trust services to the cloud, the support for public clouds is considered to be the most appropriate basis for the analysis. This is where most savings can be made and the provisions of the public cloud service are aimed at the general needs of an open community based around open standards, whereas privately operated clouds are aimed at specific security concerns supporting a closed user community with specific security concerns. Furthermore, the majority of respondents to the survey used public cloud services.

1.4.1.1. Types of CSPs

(1) Infrastructure as a service (IaaS) Service offering a virtual computing environment
(2) **Platform as a service (PaaS).** Service offering a platform for developing and running applications on the cloud.
(3) **Software as a service.** Service based on applications located in the cloud.

The major CSPs offer infrastructure as a service (IaaS) services using virtual environments that provide separation between customer software ([4]). They also offer a range of services to support the development of websites and customer applications (PaaS), including Kubernetes. There is a range of different applications that all three types of CSPs support. Finally, CSPs commonly offer file/object storage and relational and other types of databases to support the storage of their customers' data.

Often, CSPs cannot be clearly assigned to one of the abovementioned types. For example, providers of IaaS services often offer development platforms for applications associated with PaaS, along with the isolation provided by virtual environments associated with IaaS. Also, other categories of cloud-based services exist which do not fit neatly into any of these three main classifications, for example cloud services in support of mobile-based applications.

A cloud service may be operated in the following ways:

(1) As a public cloud service, available to any customer.
(2) As a private cloud service, supporting a specific community of users. With a private cloud, greater security and integrity may be maintained by prohibiting use outside the community while sharing the benefits of a cloud service within the user community.
(3) As a hybrid cloud, offering a mixed computing, storage and services environment made up of on-premises infrastructure, private cloud services and a public cloud.
(4) As a multi-cloud, using multiple cloud services from different vendors. This may be done to use different providers for different aspects of a user's service or to use multiple providers as alternatives to provide the same service, in order to avoid reliance on a single provider.

1.4.1.2. Security

All of the major CSPs offer a range of tools to support the security of their services, including:

- identity and access management;
- continuous monitoring of the cloud service to defend against external attacks and ensure compliance with security policy;
- maintenance of audit logs which may be used for monitoring;
- provision of security alerts, event management and incident response;
- network security and firewalls;
- secure web and email services;
- protection of private and other sensitive data, for example using encryption:
  - management of cryptographic keys including certificate management,
  - public key infrastructure (PKI),
  - identity management and authentication services.

Furthermore, most CSPs have settings and configurations defined according to specific frameworks. This way the customer can choose to apply a specific control (e.g. to comply with an ISO standard) and the tool will suggest which settings and policies to implement.

1.4.1.3. Hardware security module and key management

A hardware security module (HSM) is a specialised device used to protect cryptographic keys and support cryptographic functions, such as the creation of digital signatures and encryption. HSMs are commonly placed in a secure data centre, supporting the cryptographic requirements of servers through a local network.

([4]) Further information about cloud services can be found in the ENISA report *Security Aspects in Virtualization*, https://www.enisa.europa.eu/publications/security-aspects-of-virtualization.

HSMs are used for trust services to sign statements (e.g. public key certificates) issued by the TSP.

FIPS 140-2 is an American federal standard for HSMs which is globally accepted as the basis for demonstrating the security of such devices. FIPS 140-2 identifies three levels of security.

- **Level 1.** Requires that production-grade equipment and externally tested algorithms be used.
- **Level 2.** Requires physical tamper-evidence and role-based authentication for hardware.
- **Level 3.** Hardware must feature physical tamper resistance and identity-based authentication.

In Europe, an alternative standard has been defined for HSMs, the European Committee for Normalization (CEN) standard EN 419 221-5. This is extended to support remote signing services in EN 419 241-2.

The major CSPs offer tools for secure management of keys based around HSMs. These are often provided at two levels.

- General purpose key management tools, which can be based on FIPS 140-2 level 2 HSM or even software-managed keys.
- Customer HSM instances, offering full FIPS 140-2 level 3 isolation of keys between customers. This can be done using customer-supplied HSMs which are:
  - remotely managed by the customer but held in cloud service data centres; or
  - 'single-tenant' HSMs, which are operated by the CSP but ensure isolation between use of the HSMs by customers with only a single customer-owned set of keys in the HSM at any one time.

No public cloud service is known to support the EU standard for HSMs (EN 419 221-5), nor is there support for the use of HSMs to support remote signing as defined in EN 419 241-2. Currently, FIPS 140-2 level 3 is accepted but preference is given to EN 419 221-5. For remote signing at the qualified level, EN 419 241-2 is necessary and this is based on the use of EN 419 221-5 HSM.

1.4.1.4. Time synchronisation

Regarding time synchronisation, some CSPs use a recognised Universal Time Coordinated (UTC) source with a satellite/GPS source that is linked to atomic clocks. However, many CSPs do not give a clear statement regarding the synchronisation of time with a recognised UTC time source.

1.4.1.5. Compliance

The major CSPs comply with several different schemes to ensure different aspects of their security. These commonly include the following types of conformity assessment schemes.

- ISO/IEC 27001, to certify security management and the use of generally accepted controls as defined in ISO/IEC 27002.
- ISO/IEC 27017, to certify the application of security controls specifically necessary for building cloud-based services on ISO/IEC 27002.
- ISO/IEC 27018: General code of practice, to provide data protection such as required by the general data protection regulation (GDPR).
- ISO/IEC 27701 privacy extension to ISO/IEC 27001: Information security management and ISO/IEC 27002: Security controls.
- CSA STAR certifications, to meet practices generally considered as required by the cloud providers.

- Other schemes specifically aimed at the GDPR.

According to the results of the survey, 75 % of the CSPs stated that they already provide or plan to provide conformity assessments relating to ISO 27017, ISO 27001 and the European cybersecurity certification scheme for cloud services (EUCS) ([5]).

([5]) For more information on EUCS, visit: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

2. GENERAL REQUIREMENTS APPLICABLE TO TSPs AND CSPs

This section provides an overview of the general requirements for TSPs and analyses the security standards commonly adopted by cloud services.

2.1. OVERVIEW OF THE REQUIREMENTS FOR TRUST SERVICES

TSPs build their systems and services so that security is ensured, as defined in Article 24(2) of the eIDAS regulation. Most TSPs base their safety organisation on the implementation of technical standards defined by the European Telecommunications Standards Institute (ETSI), more specifically as defined in ETSI EN 319 401. For the areas of TSP operations and management, the ETSI EN 319 401 requirements are based on the international standard ISO/IEC 27002: Information security, cybersecurity and privacy protection – information security controls. Policy requirements for specific trust services are also based on requirements defined in ETSI EN 319 401.

Figure 1: TSP policy requirements

As mentioned in Section 1, trust services can be grouped into different categories. The following tables show the requirements that apply for the different categories of trust services according to various ETSI EN standards.

Certificate issuance **All trust services which involve the issuance of public key certificates**
Issuance of qualified and non-qualified certificates for electronic signatures. Issuance of qualified and non-qualified certificates for electronic seals. Issuance of qualified and non-qualified certificates for website authentication. Requirements for the issuance of certificates are specified in ETSI EN 319 411-1: Policy requirements for TSPs issuing certificates and ETSI EN 319 411-2: Policy requirements for TSPs issuing qualified certificates. These standards build on the general requirements for trust services specified in EN 319 401, as described above.

Qualified signature/seal creation device support

The signatory (or creator of the seal) entrusts **qualified signature creation devices** (QSCDs) to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory (or creator of the seal) has sole control over the use of their electronic signature / seal creation data, and that the qualified electronic signature / seal requirements are met by the use of the device (eIDAS regulation recital 51).

As stated in eIDAS recital 52, in order to ensure that such electronic signatures/seals receive the same legal recognition as electronic signature/seals created in an entirely user-managed environment, remote electronic signature service providers should:

(1) apply specific management and administrative security procedures; and
(2) use trustworthy systems and products.

Regarding the first point, eIDAS requires that the remote electronic signature creation environment is managed by a QTSP on behalf of the signatory, even if this type of service is not a QTS per se. The security measures proposed in ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 also apply to QTSPs providing remote QSCD services. Additionally, ETSI released TS 119 431-1 proposing 'Policy and security requirements for TSPs; Part 1: TSP service components operating a remote QSCD/SCDev'.

Concerning the second point, in order to ensure their trustworthiness, systems and products must implement appropriate technical measures to manage the risks posed to their security. Annex II of eIDAS made some of these security measures mandatory and also, pursuant to Articles 30(1) and 39(2) of eIDAS, made the certification against these security measures mandatory. The security framework of such systems and products are provided in CEN EN 419 241-2 and CEN EN 419 221-5.

Time stamps
All trust services issuing qualified and non-qualified time stamps

Time-stamping provision which generates time stamps.
Time-stamping management which monitors and controls the operation of the time.

Requirements for issuing time stamps are specified in ETSI EN 319 421: Policy and security requirements for TSPs issuing time stamps.

This standard builds on the general requirements for trust services specified in EN 319 401, as described in the previous section.

Registered E-delivery services
Delivery of electronic registered mail

Security and policy requirements for this service are specified in ETSI EN 319 521: Policy and security requirements for ERDS providers and ETSI EN 319 531:

Policy and security requirements for registered electronic mail service providers (REMS). Following the guidance in EN 319 401 as the general policy requirements for all types of TSPs, this document sets out general requirements specific for those TSPs providing ERDS and REMS. The general requirements for ERDS are stated in EN 319 521 and then extended for REMS in EN 319 531.

Signature Preservation services **Preservation of electronic signatures, seals or certificates relating to these services**
Requirements for preservation services as specified in TS 119 511: Policy and security requirements for TSPs providing long-term preservation of digital signatures or general data using digital signature techniques. As with other TSP standards, this document makes reference to requirements in EN 319 401 for general requirements for TSPs.

Signature validation **Validation of electronic signatures, electronic seals or electronic time stamps**
Security and policy requirements for signature validation services are specified in ETSI TS 119 441: Policy requirements for TSPs providing signature validation services. As with other TSP standards, this document refers to requirements in EN 319 401 for general requirements for TSPs.

2.2. INFORMATION SECURITY REQUIREMENTS OF CLOUD SERVICES

In a cloud computing environment, the main security assets (data and processes) of CSCs are stored, transmitted and processed by the cloud service. Therefore, CSC information security depends upon the information security of the CSP. Before entering into supplier relationships with cloud services providers, CSCs should be able to assess possible gaps between their own and the providers' information security systems.

2.2.1. ISO STANDARDS

- **ISO/IEC 27001: Information security management systems.** ISO/IEC 27001 provides requirements for an information security management system (ISMS). The standard is supported by several standards in the ISO/IEC 27000 family. Other standards for the security of cloud services, including ISO/IEC 27017 and CSA STAR, are built on ISO 27001

- **ISO/IEC 27002: Information security controls.** This provides a reference set of information security controls and implementation guidance supporting ISO/IEC 27001. ISO/IEC 27002 is a basis for requirements defined for TSPs and in the operation clause of ETSI EN 319 401 and covers all the general areas of security management required for trust services.

- **ISO/IEC 27017: Code of practice for information security controls, based on ISO/IEC 27002 for cloud services.** This standard provides additional cloud-specific implementation

Furthermore, it requires establishing a risk management process and refers to guidance in ISO/IEC 27001 and ISO/IEC 27005. Annex B of the standard presents references on information security risks related to cloud computing.

- **ISO/IEC 27018: Code of practice for protection of personally identifiable information (PII) in public cloud acting as PII processors.** CSPs that process private data of trust service customers need to operate their services in ways that allow both TSPs and CSPs to meet the requirements of the GDPR. The requirements and the way in which the requirements are divided between the CSP and the TSP vary according to legal jurisdictions and the terms of the contract between them. The purpose of the ISO/IEC 27018 standard, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to provide a common set of security controls that can be implemented by a public cloud computing service provider acting as a private data processor. The implementation and maintenance of ISO/IEC 27018 requirements confirm that users of cloud services keep control over the use of their data, have information about their geographic location and that personal data is processed only in accordance with the customer's requirements. However, it does not prevent third-country authorities from accessing the data.

  Compliance with the standard ensures transparency of the rules for the processing, transfer and deletion of personal data stored in cloud databases; customer data will be protected and used only for the purpose approved by the customer. The standard imposes restrictions on the handling of data transmission and storage on memory media. The standard also indicates the appropriate data recovery and restoration processes.

- **ISO/IEC 27701: Privacy information management.** This standard is an extension to the ISO/IEC 27002 controls and is expected to be audited as part of the ISO 27001 certificate. Like ISO/IEC 27018, it is concerned with protecting privacy but directed more at the general management of privacy, rather than controls aimed at PII.

2.2.2. CLOUD SECURITY ALLIANCE STAR SELF-ASSESSMENT AND CERTIFICATION

The Cloud Security Alliance (CSA) STAR (security, trust, assurance and risk) ([6]) programme is dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. It encompasses three levels of assessment (self-assessment, third-party conformity assessment and continuous auditing) and is specifically geared towards supporting and evaluating CSPs for two levels of assurance (STAR Level 1 and STAR Level 2). Third-party conformity assessment is only provided for STAR Level 2. Over 100 CSPs are certified to STAR Level 2, which builds on existing ISO 27001 (or AICPA SOC2 or Chinese equivalents) audits, adding cloud-specific controls. ISO 27017 is intended to businesses moving data to the cloud and/or sharing data in the cloud, including CSPs. STAR is more comprehensive and targeted at CSPs.

STAR is based on a cloud controls matrix, a cybersecurity control framework for cloud computing. It is a spreadsheet that lists 16 domains covering all key aspects of cloud technology. Each domain is broken up into 133 control objectives. It can be used as a tool to systematically assess cloud implementation, by providing guidance on which security controls should be implemented by which actor within the cloud supply chain. The controls framework is aligned to the CSA's security guidance v4 and is currently considered a de facto standard for cloud security assurance and compliance.

The domains covered by the cloud controls matrix are:

- application and interface security;

([6]) https://cloudsecurityalliance.org/star/.

- audit and assurance;
- business continuity management and operational resilience;
- change control and configuration management;
- data security and privacy life cycle management;
- data centre security;
- cryptography, encryption and key management;
- governance, risk management and compliance;
- human resources security;
- identity and access management;
- security infrastructure and virtualisation;
- interoperability and portability;
- universal endpoint management;
- security incident management, e-discovery and cloud forensics;
- supply chain management, transparency and accountability;
- threat and vulnerability management;
- logging and monitoring;
- CSA STAR Level 2 (independent audit).

2.2.3. EU CLOUD CERTIFICATION SCHEME

In December 2020, ENISA published a draft proposal of a European cybersecurity certification scheme for cloud services (EUCS) ([7]). Its aim is to improve the internal market conditions and enhance the level of security for cloud services and the overall infrastructure around them. The scheme addresses CSPs, CSCs and regulatory authorities. The scheme proposes three different assurance levels to describe the level of security required and provided: basic, substantial and high.

The basic level provides limited assurance that the cloud service is built and operated in accordance with the procedures and mechanisms that minimise the known basic threats of incidents and cyberattacks. The aim of the basic level is to ensure that cloud services are designed to meet common service security requirements for non-critical data and systems.

The substantial level ensures, through the CAB's assessment, that the cloud service is built and operated using procedures and mechanisms that minimise known cybersecurity threats and the risk of incidents and cyberattacks by entities with typical skills and resources. An assessment covers whether the CSP has assessed this risk and has implemented appropriate controls that, if operated effectively, minimise this risk and meet the relevant security requirements for a specified period of time. The substantial level should be appropriate for cloud services designed to meet common security requirements for business-critical data and systems.

The high level provides reasonable assurance, again through the CAB's assessment, that the cloud service is built and operated using procedures and mechanisms that minimise the risk of advanced cyberattacks by entities with considerable skills and resources. The audit covers whether the CSP has assessed this risk and has implemented appropriate control measures that effectively minimise the risk and meet the relevant security requirements for a specified period. The high level should be appropriate for cloud services designed to meet specific security requirements for mission-critical data and systems.

All CABs carrying out assessments in the context of EUCS should be accredited to ISO 17065 and meet the additional requirements specified for EUCS. Additional requirements define several profiles corresponding to different roles in conformity assessment. The technical competence requirements related to accreditation are sufficient to perform the basic and

([7]) For more information on EUCS, visit: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

substantial conformity assessments. However, advanced competencies are required to conduct a conformity assessment for the high level.

2.2.4. EU GDPR

Two schemes have been defined for conformity assessment against GDPR-based requirements: the CISPE code of conduct and the EU cloud code of conduct.

Even if a CSP follows the Code of Conduct, an arrangement with the EU or a bilateral contract with a Member State is necessary to ensure GDPR compliance.

Compliance with the CISPE code of conduct ([8]) is verified by independent, external auditors accredited as 'monitoring bodies' by the competent European data protection authority. These bodies strengthen the level of assurance provided by services declared under the code. The code was approved by the European Data Protection Board on 19 May 2021.

The EU cloud code of conduct ([9]) consists of requirements for CSPs that wish to adhere to the code and a governance section that is designed to support the effective and transparent implementation, management and evolution of the code. The code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the code's requirements, either through self-evaluation and self-declaration of compliance and/or through a third-party conformity assessment. The code has been developed to cover GDPR requirements and, following the positive opinion issued by the European Data Protection Board, was officially approved by the Belgian data protection authority in May 2021.

2.2.5. NIS 2 DIRECTIVE

The implications of Directive (EU) 2022/2555 (the NIS 2 directive) ([10]) for trust services are still subject to investigation within ETSI ([11]). However, the use of cloud services in support of trust services could have direct implications for European cybersecurity. In particular, if the provision of cloud services becomes an important part of the supply chain for trust services, this could be relevant to the national cybersecurity strategy under Article 5 of NIS 2 and may need to be considered as part of the EU coordinated risk assessments of critical supply chains.

([8]) Cloud Infrastructure Services Providers in Europe: https://cispe.cloud/code-of-conduct/.
([9]) See: https://eucoc.cloud/en/home.
([10]) https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/.
([11]) See the ETSI work item at: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66935.

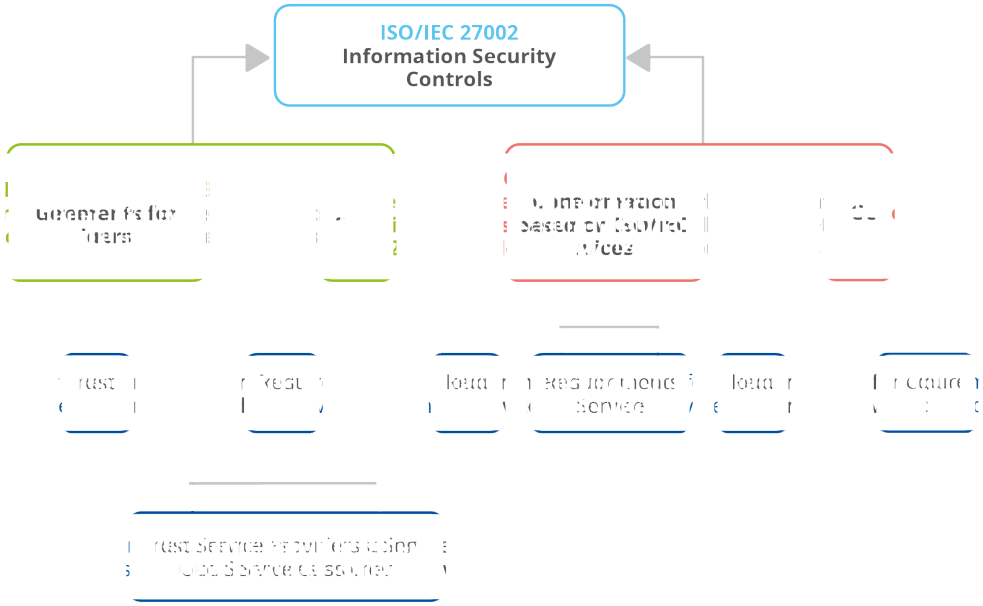
3. PROVISION OF SPECIFIC TRUST SERVICES IN THE CLOUD

This section provides a comparison of the general requirements for trust services (as presented in Section 2) against the ability of cloud services to support those requirements. This analysis is summarised in a table that shows the different responsibilities for TSPs and CSPs. In addition, a more detailed analysis of how to operate trust services in the cloud is given. Therefore, the requirements of each type of trust service are examined to identify where concerns of the provisions of CSPs particularly need to be considered. In a last step, practical examples are given by analysing the results from the survey.

3.1. COMPARISON OF GENERAL CSP STANDARDS WITH GENERAL TSP REQUIREMENTS

Section 3.1.1 describes the ISO/IEC 27017 requirements for CSPs and CSCs. The security model in the standard requires that both parties comply with the requirements. A TSP using CSP services becomes its client, so it should comply with the requirements for cloud service clients and use cloud services that are compliant with the ISO/IEC 27017 standard. As a result, the set of requirements for TSPs using cloud services is a combination of requirements for TSPs and requirements for CSCs.

Figure 4: Requirements for TSPs, CSCs and CSPs



3.1.1. INFORMATION SECURITY MANAGEMENT

There is much in common between the requirements placed by the application of information security management standards for CSPs and those required for TSPs. This is particularly apparent when considering the requirements of ISO/IEC 27017: Code of practice for information security controls, based on ISO/IEC 27002 for cloud services, against the requirements of ETSI

EN 319 401: General policy and security requirements for the provision of trust services. A more detailed depiction can be found in section 3.2 of this report.

Section 3.2 also includes a table specifying the requirements that any TSP/QTSP has to meet according to the eIDAS regulation and the EN 319 401 standard. The following points are covered in the table.

- Domains and specific requirements.
- Who is responsible for implementation. It should be noted that the responsibility towards third parties always lies with the TSP/QTSP and that this section of the table refers to the division of contractual responsibilities between the TSP/QTSP and its supplier.
- Controls usually implemented by the CSP. This column lists the controls that large cloud providers usually have in place. It will depend in each case on the services that the TSP/QTSP has contracted.
- Activities that have to be carried out by the TSP/QTSP, either by parameterising the services provided by the CPS or by implementing its own controls.
- Mapping of controls against ISO/IEC 27002.

3.1.2. PRIVACY

The provision of privacy under the GDPR is not directly addressed by either ISO/IEC 27017 or EN 319 401. However, for cloud services providers it is commonly addressed through ISO/IEC 27018 or the practices specifically aimed at the GDPR.

Generally, compliance with the GDPR is the responsibility of the TSP. However, if private information is held in the cloud, there are implications for the CSP. In general, the information security provisions of CSPs are probably sufficient to meet the requirements of trust services. However, the legal requirements of the placement of private data outside the control of countries not recognising the GDPR need to be considered.

3.1.3. RISK ASSESSMENT AND POLICY AND SECURITY REQUIREMENTS

In Article 19 of the eIDAS regulation, TSPs must take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.

ENISA has developed guidelines for TSPs focusing on a secure framework ([12]), discussing the minimal security levels to be maintained by the TSPs and covering all eIDAS articles where trust and risks were included in the updated version.

(Q)TSPs are required to provide trust services with the appropriate trust within a secure framework and manage all potential risks to minimise and mitigate the impact of having security incidents. This applies to the trust services offered from cloud providers complying with ETSI EN 319 401 and the corresponding policy requirement standard applicable to the trust service.

For the purpose of this document, the risk assessment phases defined in ISO/IEC 27005 are considered valid for assessing cloud providers, because they take the following into account:

- risk identification: scope, assets, threats and vulnerabilities;
- risk analysis: risk level based on impact;
- risk evaluation.

([12]) See: https://www.enisa.europa.eu/publications/tsp1-framework.

CSPs may be reluctant to provide information on the results of their own risk management regime.

3.2. GENERAL CONCLUSIONS

There is significant overlap between the requirements of CSPs following ISO/IEC 27017 and the requirements of TSPs, as both are based around ISO/IEC 27002. If private information is to be placed in the cloud, the implications for legal recognition of any application of privacy controls outside the EU need to be taken into account.

The following table summarises the existing information security management requirements that CSPs and TSPs have to fulfil in order to either provide services for TSP or operate trust services in a cloud. It is important to note that these requirements only address general scenarios. For a detailed report about the specific requirements that have to be met, each use case needs to be examined individually. Not all requirements may be necessary for every use case.

Domains	TSP controls ETSI EN 319 401 referencing ISO/IEC 27002:2013	CSP Controls in ISO/IEC 27017:2015	Common clause reference to ISO 27002:2013
Information security policies	TSP shall implement an information security management system and verify the implementation of ISMS by CSP (ISMS).	CSP shall implement an information security management system and provide relevant information to TSP (ISMS).	5.1.1
	TSP shall take into account cloud services in the information security policy (POLICY).	CSP shall establish a cloud-specific information security policy (POLICY).	5.1.1
Organisation of information security	TSP and CSP shall agree on information security roles and their responsibilities (ROLES).	CSP and TSP shall agree on information security roles and their responsibilities (ROLES).	6.1.1
	TSP shall identify relevant authorities in the context of CSP location (LOCATION).	CSP shall provide information to TSP about locations and countries where data is stored (LOCATION).	6.1.3
Human resources	TSP shall provide training for employees and other involved parties concerning cloud computing: standards, procedures, risk management, systems, networks and legal requirements (AWARENESS).	CSP shall provide training for employees and other involved parties concerning TSP data in the cloud and specific to that data's legal requirements (AWARENESS).	7.2.2
Asset management	TSP shall conduct identification of assets, including where they are maintained (INVENTORY).	CSP shall explicitly identify TSP data and data derived from the cloud (INVENTORY).	8.1.1
	TSP shall label and classify all information stored in the cloud (LABELLING).	CSP shall provide TSP with the capability to label and classify information (LABELLING).	8.2.2
Access control	TSP shall specify requirements for user access to each separate cloud service (ACCESS CONTROL).	-	9.1.2
	-	CSP shall provide TSP with user registration and deregistration capability (ACCESS CONTROL).	9.2.1
	-	CSP shall provide access rights management capability (ACCESS CONTROL).	9.2.2

	TSP shall use sufficient access controls for TSP administrators, e.g. multi-factor (ACCESS CONTROL).	CSP shall provide sufficient access controls for TSP administrators, e.g. multi-factor (ACCESS CONTROL).	9.2.3
	TSP shall verify CSP's management procedure for allocation of secret authentication information (ACCESS CONTROL).	CSP shall provide a management procedure for the allocation of secret authentication information (ACCESS CONTROL).	9.2.4
	TSP shall ensure that access to the services can be restricted (ACCESS CONTROL).	CSP shall provide access controls that allow TSP to restrict access to its services (ACCESS CONTROL).	9.4.1
	TSP shall verify that utility programs do not interfere with service (ACCESS CONTROL).	CSP shall use utility programs strictly limited to authorised personnel and identify all requirements of that program (ACCESS CONTROL).	9.4.4
Cryptography	TSP shall review whether cryptographic protection offered by CSP meets policy requirements (CRYPTOGRAPHY).	CSP shall provide information about cryptography capabilities and assist TSP in implementing its cryptographic protection (CRYPTOGRAPHY).	10.1.1.
	TSP shall identify keys and implement key management for each cloud service (CRYPTOGRAPHY).	-	10.1.2
Physical and environmental security	TSP shall request information from CSP about the secure disposal and reuse of assets (PHYSICAL).	CSP shall provide information to TSP about the secure disposal and reuse of assets (PHYSICAL).	11.2.7
Operations security	TSP shall take into account the impact of any changes made by CSP (OPERATIONS).	CSP shall provide information about changes to TSP (OPERATIONS).	12.1.2
	TSP shall verify that the capacity provided by CSP meets requirements (CAPACITY).	CSP shall provide capacity monitoring and resource-shortage prevention (CAPACITY).	12.1.3
	TSP shall verify that the specification of backup meets expectations (BACKUP).	CSP shall provide a specification of backup to TSP (BACKUP).	12.3.1
	TSP shall define requirements for logging and verify whether CSP meets them (LOGGING).	CSP shall provide logging capabilities to TSP (LOGGING).	12.4.1
	TSP shall verify whether the logging capabilities of CSP are appropriate and all privileged operations delegated to CSP are logged (LOGGING).	-	12.4.3
	TSP shall request information about clock synchronisation (CLOCK).	CSP shall provide information about the clock used for synchronisation and information on how TSP can synchronise local systems (CLOCK).	12.4.4
	nformation about vulnerability management from CSP and identify vulnerabilities on its own site (TECHNICAL [redacted] ITIES).	CSP shall provide information about vulnerability management (TECHNICAL VULNERABILITIES).	12.6.1

System acquisition, development and maintenance	TSP shall determine information security requirements and evaluate whether CSP meets the requirements (INFORMATION SECURITY).	CSP shall provide information about information security capabilities (INFORMATION SECURITY).	14.1.1
	TSP shall request information from CSP about the use of secure development procedures and practices (DEVELOPMENT).	CSP shall provide information to TSP about the use of secure development procedures and practices (DEVELOPMENT).	14.2.1
Supply chain	TSP shall include CSP as a supplier in internal policies (SUPPLIER RELATIONSHIPS).	-	15.1.1
	TSP shall confirm information security roles and responsibilities identified in the service agreement with CSP (SUPPLIER RELATIONSHIPS).	CSP shall specify security measures implemented in the service to avoid misunderstandings (SUPPLIER RELATIONSHIPS).	15.1.2
	-	CSP shall provide supply chain information to TSP and ensure security levels of peer cloud providers (SUPPLIER RELATIONSHIPS.	15.1.3
Incident management	TSP shall verify the allocation of responsibilities for incident management and ensure that it meets requirements (INCIDENT MANAGEMENT).	CSP shall define of allocation of incident management between CSP and TSP and provide documentation to TSP about incident management (INCIDENT MANAGEMENT).	16.1.1
	TSP shall request information from CSP about event reporting (INCIDENT MANAGEMENT).	CSP shall provide information to TSP about event reporting and report events to TSP (INCIDENT MANAGEMENT).	16.1.2
	TSP and CSP shall agree on procedures to respond to evidence requests (INCIDENT MANAGEMENT).	CSP and TSP shall agree on procedures to respond to evidence requests (INCIDENT MANAGEMENT).	16.1.7
Compliance	TSP shall consider the issue of CSP jurisdiction and request compliance evidence from CSP (COMPLIANCE).	CSP shall inform TSP about jurisdiction, identify legal requirements and provide compliance evidence to (COMPLIANCE).	18.1.1
	TSP shall verify the license terms of use in the cloud (COMPLIANCE).	CSP shall establish a process for intellectual property rights complaints (COMPLIANCE).	18.1.2
	TSP shall request information about the protection of the records (COMPLIANCE).	CSP shall provide information about the protection of the records (COMPLIANCE).	18.1.3
	TSP shall verify whether cryptographic controls comply with agreements, legislation and regulations (COMPLIANCE).	SCP shall provide a description of cryptographic controls (COMPLIANCE).	18.1.5
	TSP shall request documented evidence of controls implementation and certification (SECURITY REVIEWS).	SCP shall provide documented evidence to substantiate own claims of implementing an information security system (SECURITY REVIEWS).	18.2.1

As mentioned, the table above is an overview of requirements for TSPs and CSPs when providing trust services in the cloud. It can be understood as a general guideline or checklist that must be considered when intending to offer any kind of trust service in the cloud. The table shows the different responsibilities that TSPs and CSPs have in their roles. However, it does not provide information on the specific requirements that apply for each of the different categories of trust services. It also does not give information on how to audit these services. Both aspects will

be analysed more closely in the following sections of this report. Practical examples from the survey will be presented, in order to compare and confirm the mentioned requirements with assessments of stakeholders in this field.

3.3. OPERATING TRUST SERVICES IN THE CLOUD

The previous section identified the general requirements that apply for the different categories of trust services. The following section provides an analysis of more specific requirements when operating trust services in the cloud. Therefore the respective clauses in the standards that apply will be presented. The section will show where concerns of the provision of CSPs in particular need to be considered. While the table above gave an overall overview of the general requirements and responsibilities for TSPs and CSPs, the following section will also look at specific scenarios for each category of trust services.

3.3.1. CERTIFICATE ISSUANCE

The following section presents the different requirements that apply for the issuance of certificates, depending on the individual scenario.

3.3.1.1. General

Practice statements need to clearly state where use is made of third-party services, such as a CSP. In particular, the TSP practice statement should provide details on whether a CSP is involved in supporting the use and management of certification authority (CA) keys, for example using CSP provided HSM or key management software, and should clearly state how this involves the CSP in supporting key management.

A TSP provides certificates to subscribers and subjects after the subjects' consent to relying parties. Additionally, a TSP is required to provide the terms and conditions regarding the use of the certificate. This could be addressed by the use of CSP cloud storage services and other services using the cloud for data distribution.

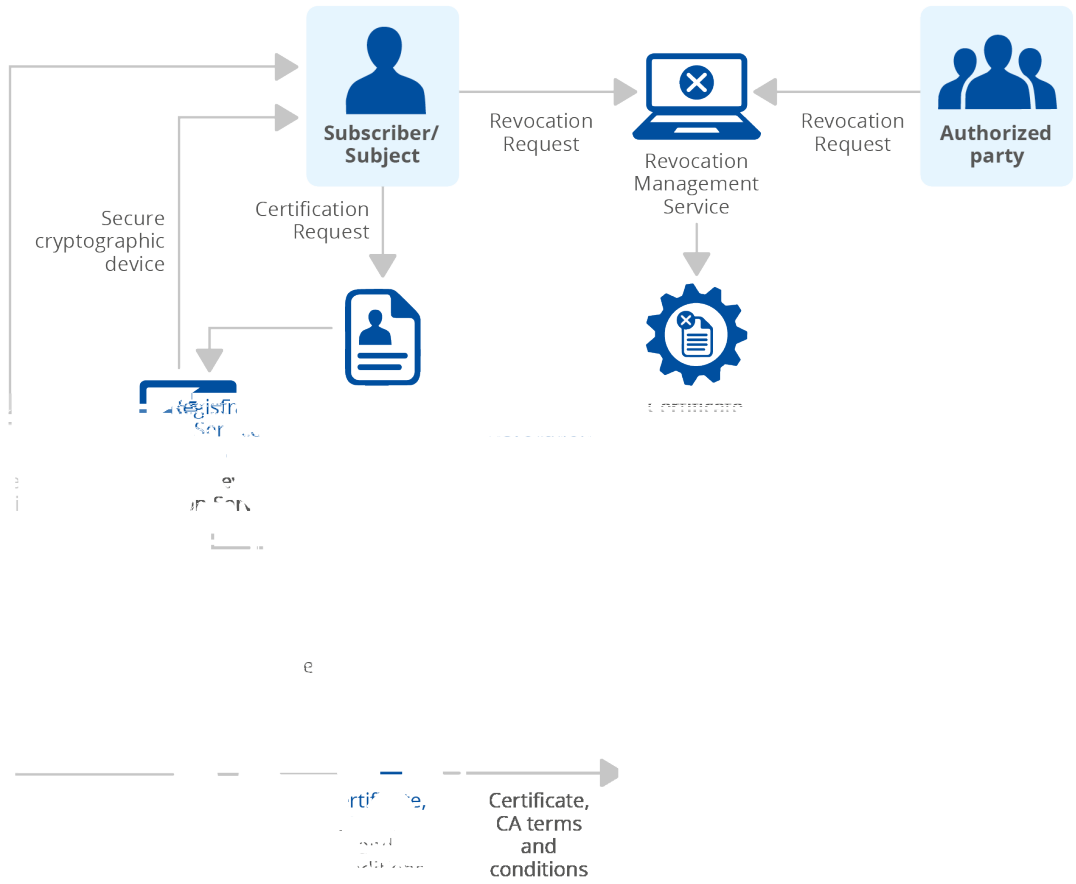
Trust services issuing certificates can be broken down into a number of individual component services, each with their own specific functions and security requirements. The requirements of each component in the cloud is considered in its own right.

EN 319 411-1 clause 6.3 specifies requirements for management of life cycle of certificates: certificate application, issuance, acceptance, usage, renewal, revocation and suspension. Under certain conditions, this could be met by a TSP's own certificate software running on a CSP IaaS platform. EN 319 411-2 clauses 6.4.1–6.4.6 and 6.4.9 specify requirements for QT/13.3 (4 (i)-8 -1.3[(r)3.7 (i)-0.7 e09 Tc o.6 (f)2 (or)17 (4 (i5i)12.7 (n)]TJ0 Tc 0 Tw ( )Tj0.004 Tc -0.002 Tw 8.68 0 Td[(i)-0.7 (nf)15.4 (electronically and this needs to be addressed when a TSPiperates with the use of CSPi4-8.

EN 319 411-1 cla(or)s17 6.u se–64.6 speci fy requirements relating to infrastructure management related to certificate generation and revocation. This infrastructure should operate in an envi fonment that protects services from bei f compromised by unauthorised access to systems or data. It requires entry control fo physicall f protected zones and regi ftration of entrances and exi fs. Clearly defined securit zones must be established for certificate generation and revocation management. Any parts of the premises shared with ot organi sations shall f outside the perimeter of the certi ficate generaton and revocation management services. T standard requires the implementation of physical and envi 7 (r)3.7 (o)13.3 (n)13.3 (m)-3 (ent)15.4 security contr resources. All of these requi fements requi 7 (r)3.7 (e)13.3 (s)-2.7 (p)13.3 (ec)-2.6 (i f)12.3 (a l) (f)2 treatment wh

50 % of T fPs

Figure 5: Different components needed for the provision of issuing certificates



These components or assets are also applicable to cloud providers, as they also use HSMs to manage keys and need to allow access to those keys to specific people or roles who run a specific software following a specific document. That means that the corresponding security requirements and risks assessments that must be performed on local providers are also valid for cloud providers. The assets to be protected are the same as the risks posed in every asset.

An additional important trust service component, which in future revisions of eIDAS could be considered as a trust service itself, is the management of a remote signature / seal creation device (QSCD) which provides the secure basis of remote signing service. In this service, the user's signing key is secured using an HSM under the remote control of an authenticated user to provide a remote QSCD.

- **Registration services.** The registration of customers is an important part of several trust services, notably for TSPs issuing certificates under EN 319 411-1 clause 6.2, and registered electronic delivery services and REMS as defined in clause 5.2 of EN 319 521 and EN 319 531 respectively.

  The registration requirements can be further detailed using TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects. TS 119 461 gives policy and security requirements for trust service components providing identity proofing of trust service subjects. Such identity proofing can be provided by the TSP itself as an integral part of the trust service, or by a specialised identity proofing service provider acting as a subcontractor to the TSP.

Registration requirements could be met by a TSP's own registration software running on a CSP platform (IaaS, PaaS – see Section 1.4.1). Where such services bind an authentication means to the registration, special attention needs to be given to any authentication services provided by the CSP, to ensure that they match the assurance requirements for electronic identification, such as defined in Commission Implementing Regulation (EU) CIR 2015/1502. The functionality of registration services is the responsibility of the TSP.

- **Subject device provision service.** In EN 319 411-1, subject device provisioning is considered to be part of registration and identity proofing, as specified in clause 6.2.2. Provisioning of user signing devices is part of the operation of the registration service under control of the TSP outside the cloud services.

  EN 319 411-2 clause 6.3 gives specific requirements for the issuance of qualified certificates when the QSCD is managed for the subject. In this case, the private key must not be used for signing, except within a QSCD and only under the subject's sole control. Generally, this is the responsibility of the TSP.

  The management of a remote signature / seal creation device (QSCD), while it may be considered as a special case of subject device provisioning, is addressed as a separate trust service below.

- **Certificate generation.** EN 319 411-1 clauses 6.3.1–6.3.8 cover the general requirements for generating certificates, including issuance, renewal, re-key and modification. In addition, when a certificate is issued, it has to be signed by the TSP using a key managed in an HSM in accordance with clauses 6.5.1–6.5.4.

  The requirements covered in EN 319 411-1 clauses 6.3.1–6.3.9 are generally covered by the TSP software.

  EN 319 411-1 clauses 6.5.1–6.5.4 specify requirements relating to key pair generation. The subsequent certification of the public key shall be undertaken in a physically secure environment by personnel in trusted roles. The key pair used for signing certificates shall be created under at least dual control. The number of personnel authorised to carry out CA key pair generation must be kept to a minimum. These requirements cannot be addressed by using a 'shared HSM' provided by the CSP. If a single-tenant HSM is provided by the CSP, checks will need to be made to ensure that these requirements are met, in particular regarding aspects that require at least dual control by trusted personnel. CSPs generally only support FIPS 140-2 level 3 HSMs and preference is given to the European standard EN 419 221-5. The use by CSPs of FIPS 140-2 level 2 HSM is not sufficient for most trust services.

- **Revocation management.** Requirements for revocation (and suspension) management are specified in EN 319 411-1 clause 6.3.9 and EN 319 411-2 clause 6.3.9. The requirements for revocation management in these clauses are generally procedural and can be implemented by the TSP. As long as the CSP provides true separation of uses and secure management of code, this is the responsibility of the TSP.

  EN 319 411-1 clause 6.6 specifies requirements relating to profiles of certificates, certificate revocation lists and Online Certificate Status Protocols (OCSPs). The profile is a matter of configuring the TSP's own certificate software.

- **Certificate revocation status service.** EN 319 411-1 clause 6.3.10 specifies requirements for providing information on the revocation status of certificates, using certificate revocation lists or OCSPs. In addition, when issuing information on certificate status, this has to be signed by the TSP using a key managed in an HSM in accordance with clauses 6.5.1–6.5.4.

ETSI EN 319 411-2 in section 6.3.10 also adds additional requirements for qualified certificates which are eIDAS compliant.

The requirements specified in EN 319 411-1 clause 6.3.10 are generally procedural and can be implemented by the TSP. As long as the CSP provides true separation of uses and secure management of code, this is a responsibility of the TSP.

The requirements for managing the TSP keys in accordance with clauses 6.5.1–6.5.4 cannot be addressed by using a shared HSM provided by the CSP. This requires at least an HSM provided by the TSP, hosted by the CSP and with remote HSM management. If a single-tenant HSM is provided by the CSP, checks will need to be made to ensure that these requirements are met, in particular regarding aspects that require at least dual control by trusted personnel.

3.3.1.3. TSP issuing certificates – general conclusions

Most of the aspects of these policy requirements are likely to be met by CSPs, particularly those offering a virtual infrastructure (IaaS – see Section 1.4.1). Nevertheless, before this can be confirmed, detailed checks on provisions of a particular CSP against the EN 319 411-1 and EN 319 411-2 policy requirements are required. The use of cryptographic services and HSMs require particular attention. The assurance of dual control of the management of the TSP signing keys held in an HSM is a particular concern. This is best met using a TSP-provided HSM, where the keys are managed remotely by the TSP personnel. Detailed investigation of the provision of some CSPs called single-tenant HSMs is necessary to see whether this provides the appropriate level of control of the TSP's signing keys.

3.3.2. REMOTE SIGNING SERVICE USING CLOUD SERVICES

Two critical elements of the remote signing service are: (i) the use of a specialised HSM, which ensures that the use of the signing key is, with a high level of confidentiality, under the control of the signatory; and (ii) the means used for authentication and identification of the signer. For the signing device to be considered as a remote QSCD, the signature activation module in the specialised secure devices (e.g. an HSM) has to be certified under EN 419 241-2 and EN 419 221-5. This device has to be under the direct control of the TSP. Thus, it is not considered that this service could be provided by a CSP, unless very special arrangements are made to give the TSP sole control of the specialised HSM device.

The authentication and identification means are required to meet the requirements specified in Implementing Regulation (EU) 2015/1502 at a 'substantial' or 'high' level. Thus, unless the CSP can demonstrate that their authentication meets these requirements, specific steps have to be taken by the TSP to meet this regulatory requirement.

3.3.3. TIME STAMPING

EN 319 421 clause 5 specifies requirements related to a time stamp policy called 'best practices time-stamp policy for TSAs issuing time stamps'. This policy is supported by public key certificates. The policies and general requirements deal mainly with matters relating to TSP management of policies outside the scope of a CSP. A time-stamping service provider is required to manage their own practice statement. The general requirements for policy management are outside the scope of the CSP. The certification practice statement needs to cover the practice statement requirements defined in EN 319 401 and identify the obligations of all external organisations supporting the TSP services, including the applicable policies and practices.

EN 319 421 clauses 7.6.2 and 7.6.3 specify requirements relating to time-stamping unit (TSU) key generation and key protection. Provision of time-stamping services requires the use of HSMs with keys generated by trusted personnel under dual control. If a single-tenant HSM is

provided by the CSP, checks will need to be made to ensure these requirements are met, in particular regarding aspects that require at least dual control by trusted personnel.

EN 319 421 clause

appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP. On top of general controls, EN 319 421 specifies requirements to record all relevant information concerning all events relating to the life cycles of TSU keys and TSU certificates. Additionally, all events relating to the synchronisation of a TSU's clock to UTC and the detection of loss of synchronisation is required to be logged. If a CSP provides services related to securing event logs, this requires special treatment in relevant policies and agreements.

EN 319 421 clause 7.13 specifies requirements relating to business continuity. The TSA disaster recovery plan should include a violation or suspected violation of TSU private signing keys or loss of TSU clock calibration that may have affected the issued time stamps. In the event of compromise or suspected compromise or loss of calibration when issuing a time stamp, the TSA must provide all subscribers and relying parties with a description of the compromise. This includes specific requirements for handling compromises, which would be managed by the TSP.

EN 319 421 clause 7.14 specifies requirements relating to termination of the service. The TSA is required to revoke the TSU's certificates. Specific requirements for revocation of certificates can be a matter for the TSP.

3.3.4. E-DELIVERY SERVICES

EN 319 521 clause 4 specifies requirements relating to general provisions on policies and practices, which build on EN 319 401 (general requirements for trust service practices and policies). The practice statement and policy are managed by the TSP and hence outside the scope of the CSP. However, the practice statement needs to clearly state where use is made of third-party services such as a CSP. The ERDS practice statement includes a description of how the ERDS provision ensures the security of transmission against any risk of loss, theft, damage or any unauthorised alterations, and that it needs to involve the CSP if applicable.

EN 319 521 clause 5.1 specifies requirements relating to content integrity and confidentiality, including the use of digital signatures or other mechanisms to protect content. The TSP protects the integrity of user content and associated metadata in transmissions, especially when exchanged with the sender/recipient or between distributed ERDS system components, and in storage. This should be generally met by security and privacy controls of the CSP, although checks will be needed against the specific requirements.

EN 319 521 clause 5.2 specifies requirements relating to user Identification and authentication. This generally concerns identity checks on the ERDS/REMS user and user authentication. If the identification of the recipient for the qualified service is based on an internal process, the TSP conducts the whole process in a secured and controlled environment; the TSP gathers and protects all evidence of identification and consignment or handover process. This is mainly covered by the TSP software, hardware and procedures, but specific checks will be necessary according to provision by the CSP of the environment and protection of evidence.

EN 319 521 clause 5.3 specifies requirements relating to time reference. In the case of a qualified service, a qualified time stamp must be used, which is a matter for the TSP. Otherwise, no specific requirements on time synchronisation are stated for non-qualified services.

EN 319 521 clause 5.4 specifies requirements relating to events and evidence and specifies the information to be recorded relating to events, which is a matter for the TSP. It also requires the CSP to maintain confidentiality, integrity and availability logs, which are important for checking the CSP against privacy and security controls (see also EN 319 421 clause 7.10).

EN 319 521 clause 5.5 specifies requirements relating to interoperability. This is a matter for the TSP-provided software.

EN 319 521 clause 6 specifies requirements relating to risk assessment and follows the requirements of EN 319 401.

EN 319 521 clauses 7.1–7.4 specify requirements relating to organisation, human resources, asset management and access control. These requirements are covered by general EN 319 401 requirements, with the addition of specific TSP procedures.

EN 319 521 clause 7.5 specifies requirements relating to cryptographic controls. It requires the use of a secure cryptographic device but does not require the use of a certified HSM. If CSP cryptographic services are used, these will need to be checked against the specific requirements. In particular, there is a requirement for dual control of trusted persons for backup, storage and recovery of the service provider's private signing keys.

EN 319 521 clause 7.6 specifies requirements relating to physical and environmental security and addresses physical access control, natural disaster protection, fire safety factors, failure of supporting utilities, structure collapse, plumbing leaks, protection against theft, breaking and entering and disaster recovery. The TSP is required to implement controls to protect against equipment, information, media and software relating to the provision of the ERDS being taken off-site without authorisation. Additionally, the TSP is required to protect facility housing system resources, the system resources themselves and the facilities used to support their operation. All this must be covered by CSP practices and certifications but may require additional checking.

EN 319 521 clause 7.7 specifies requirements relating to operational security and follows the requirements of EN 319 401.

EN 319 521 clause 7.8 specifies requirements relating to network security, which follow the requirements of EN 319 401. In addition, the clause requires projections of future capacity requirements to ensure that adequate processing power and storage are available. The TSP is also required to use state-of-the-art protocols and algorithms for encryption on the transport layer level. Additional requirements would need to be checked but are expected to be addressed by general CSP provisions.

EN 319 521 clause 7.9 specifies requirements relating to incident management and follows the requirements of EN 319 401.

EN 319 521 clause 7.10 specifies requirements relating to collection of evidence. The TSP is required to log all security events, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts. The TSP is also required to define at least a 2-year retention period for security logs. Specific requirements are the responsibility of the TSP, but CSP practices may require additional checking.

EN 319 521 clause 7.11 specifies requirements relating to business continuity and follows the requirements of EN 319 401. There are specific requirements for backup and storage in safe places that are suitable to allow the TSP to quickly return to operations in case of incidents/disasters. The TSP is required to provide adequate recovery facilities to ensure that all essential information and software can be recovered following a disaster or media failure and to set up regular tests to ensure that the facilities meet the requirements of business continuity plans. If a CSP is involved in providing facilities enabling business continuity, the CSP practices may require additional checking.

EN 319 521 clause 7.12 specifies requirements relating to termination plans and follows the requirements of EN 319 401. Additional requirements to keep the collected evidence for the national statutory time may need to be implemented by the TSP software.

Most of the aspects of these policy requirements are likely to be met by CSPs, particularly those offering a virtual infrastructure (IaaS). Nevertheless, before this can be confirmed, detailed checks on provisions of a particular CSP against the EN 319 521 policy requirements are required. The use of cryptographic services and HSMs requires particular attention, but the standard does not impose any requirements on the certification of HSMs.

3.3.5. SIGNATURE PRESERVATION SERVICES

ETSI TS 119 511 clauses 5 and 6 specify requirements for risk analysis and management of the policies and practices of TSPs. These are outside the scope of the CSP.

Much of ETSI TS 119 441-clause 7 (other than clause 7.5 on cryptographic controls) includes general requirements on the operation of the validation service, building on EN 319 401. This would be generally covered by the CSP's practices and certifications, but checks would be necessary against the requirements of the TSP, as applied to the validation services.

EN 319 421 clause 7.5 on cryptographic controls provides requirements for the time-stamping authority that is used in support of preservation services. Thus, the assessment given in Section 3.3.3 applies to this aspect of preservation services. In the case that the preservation service signs preservation evidence, as with other TSP cryptographic services issuing signed data, these requirements cannot be addressed by using a shared HSM provided by the CSP. If a single-tenant HSM is provided by the CSP, checks will need to be made to ensure these requirements are met, especially regarding aspects that require at least dual control by trusted personnel.

3.3.6. SIGNATURE VALIDATION

ETSI TS 119 441 clauses 5 and 6 specify requirements for risk analysis and management of the policies and practices of TSPs. These are outside the scope of the CSP.

Much of ETSI TS 119 441 clause 7 (other than clause 7.5 on cryptographic controls) include general requirements on the operation of the validation service, building on EN 319 401. This would be generally covered by the CSPs practices and certifications, but checks would be necessary against the requirements of the TSP as applied to the validation services.

ETSI TS 119 441 clause 7.5 includes similar requirements on the cryptographic controls applied to the signing of validation reports. As with other TSP cryptographic services issuing signed data, these requirements cannot be addressed by using a shared HSM provided by the CSP. This requires at least an HSM provided by the TSP, hosted by the CSP and with remote HSM management. If a single-tenant HSM is provided by the CSP, checks will need to be made to ensure these requirements are met, regarding aspects that require at least dual control by trusted personnel.

The technical requirements in ETSI TS 119 441 clause 8 specify requirements on the operation of the validation service in a correct manner, aligned with the referenced standards. Provided that the CSP provides true separation of uses and secure management of code, this is just a concern of the TSP.

Survey details
Participation of over 120 stakeholders from over 29 countries in the EU and globally.

50 % of the TSPs that participated in the survey already operate or plan to operate at least parts of their trust services in the cloud.

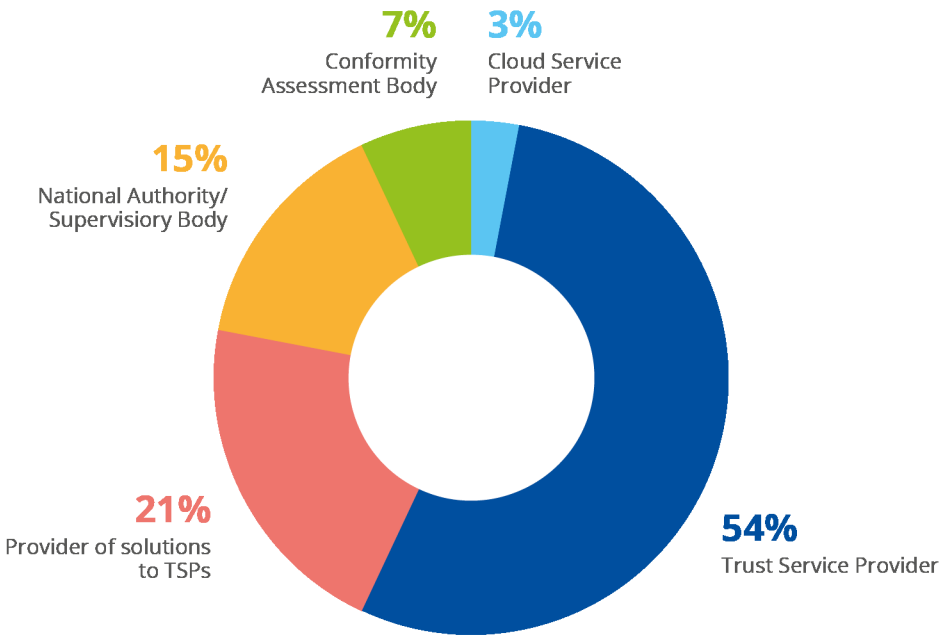
3.4. PRACTICAL EXPERIENCES

The previous sections analysed multiple standards for the move of trust services to the cloud. A detailed overview was given on the requirements that both sides (TSP and CSP) have to fulfil in order to implement the services on a cloud platform. The following section presents practical experiences and considerations of TSPs, CSPs, NA/SBs, CABs and providers of solutions to TSPs regarding the transition of trust services to the cloud. The findings come from a survey that was conducted during the creation of this report, with over 120 participants from over 29 countries in the EU and globally.

The survey results have shown that there is a high interest in operating trust services in the cloud. 50 % of the TSPs who participated in the survey already operate or plan to operate at least parts of their trust services in the cloud. This number clearly shows that TSPs are moving their services to the cloud. In comparison, only 12 % stated that they do not consider it at all. This trend is also reflected in the responses from the NA/SBs: 39 % of them have stated that they have direct experience with TSPs operating their services on a cloud. From the perspective of NA/SBs, the use of trust services on a cloud has already been adopted to a large extent. 11 % stated that TSPs have asked them to consider TSPs using cloud services. 15 % of the NA/SBs do not see the move of trust services to the cloud as a requirement or do not consider it practical.

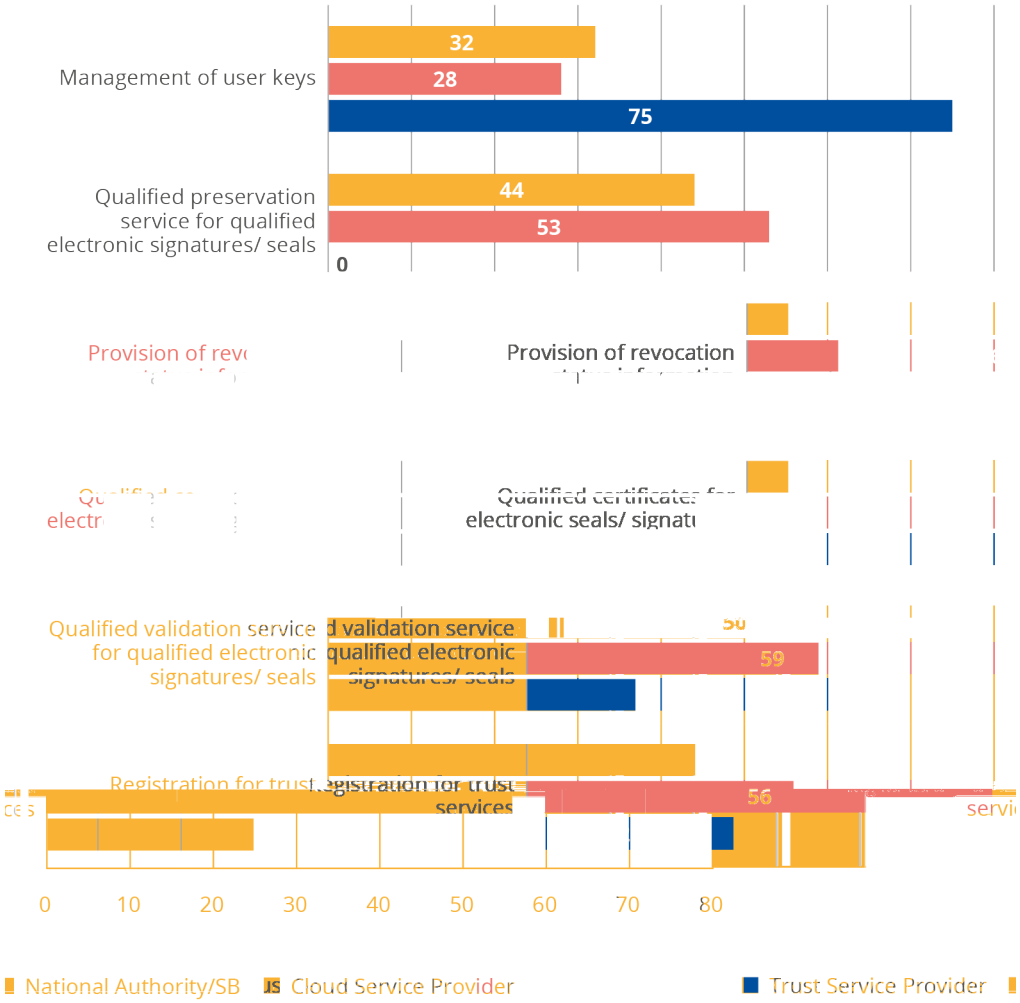
In the following section, a detailed analysis of the survey results will be given. TSPs and solution providers to TSPs were the most represented stakeholder group in the survey results. Together they made up more 75 % of the respondents. For the analysis of the results this has no impact, as each stakeholder received their respective survey. In total, five different questionnaires were created. The results were analysed individually and put into context where appropriate, as the following section will show.

Figure 6: Types of stakeholders that participated in the survey



All stakeholders were asked which trust services could in their opinion be operated on the cloud. TSPs and technical solution providers had different response options due to their differing offer in services. Furthermore, the CABs were asked about the possibility of an audit of the services, which will be further discussed in Section 4. The following table shows the services that were mostly chosen by TSPs, NA/SBs and CSPs.

Figure 7: Trust services that are mostly considered to be operated on a cloud platform by TSPs, NA/SBs and CSPs



The figure shows that there are some differences among the TSPs, NA/SBs and CSPs. The revocation status information and the preservation of seals and signatures were not considered at all by CSPs. The survey also contained many more response options that were selected in lower percentages.

It is noticeable that services such as time stamping or e-delivery are not among the most chosen services. As explained in earlier sections, the necessary requirements and standards to operate these services on the cloud already exist. However, when comparing the overall services offered by TSPs according to the EU trusted list, neither of them are usually in the portfolio of trust services.

We can say that the results reflect the current landscape of services that TSPs usually offer. The management of user keys is the service mostly chosen by CSPs, whereas NA/SBs consider this less likely to be operated on the cloud. Apart from the management of user keys, qualified time stamps, qualified electronic signatures and validation services were each chosen equally by 50 % of the providers that participated in the survey.

As mentioned above, the services offered by technical solution providers differ from those offered by TSPs, which is why the results will be presented in a separate figure. The survey showed that 48 % of the solution providers to TSPs already provide solutions for trust services

on a cloud platform and another 24 % plan to do so. In comparison, 16 % stated that they do not consider providing solutions for TSPs on a cloud platform. All results can be found in the Annex of this report.

The figure below shows the solutions or parts of solutions that could be placed on a cloud platform.

Figure 8: Solutions mostly chosen to be operated on a cloud platform by technical solution providers

When asked about the specific elements of the solutions that could be placed in the cloud, event logs, data, backups and access control were the most selected responses. With regards to trust services, the providers were asked to state the PKI-related parts of their solution that could be placed in the cloud. Signature validation and a shared PKI service were selected most often. Apart from that, time stamping, signature creation, revocation and certificate issuance and renewal were the most chosen services. This assessment is consistent with the responses from the trust services and NA/SBs.

In Section 1, the main cloud service provisions were described. The following figure illustrates the preferred type of cloud by TSPs.

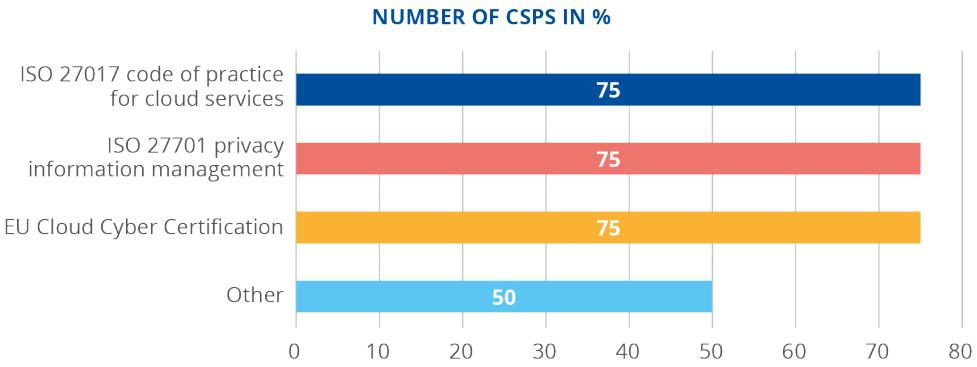
Figure 9: Preferred type of cloud by TSPs

require a localised HSM under the control of a TSP. Thus, when it comes to the type of cloud that is preferred by TSPs, many of them chose a hybrid solution of public and local clouds.

Some CSPs see perceived regulatory obstacles for cloud services from Member States. Most CSPs support international certifications, which in their view are better suited to ensure customer and CSP security needs.

The following figure illustrates the adoption of the main standards by CSPs identified in Section 2.3. The 'Other' option includes global and regional certifications. The numbers show the percentages of CSPs stating that they had adopted or planned to adopt the respective standards.

Figure 10: Security and privacy standards that CSPs have adopted or plan to adopt in the future



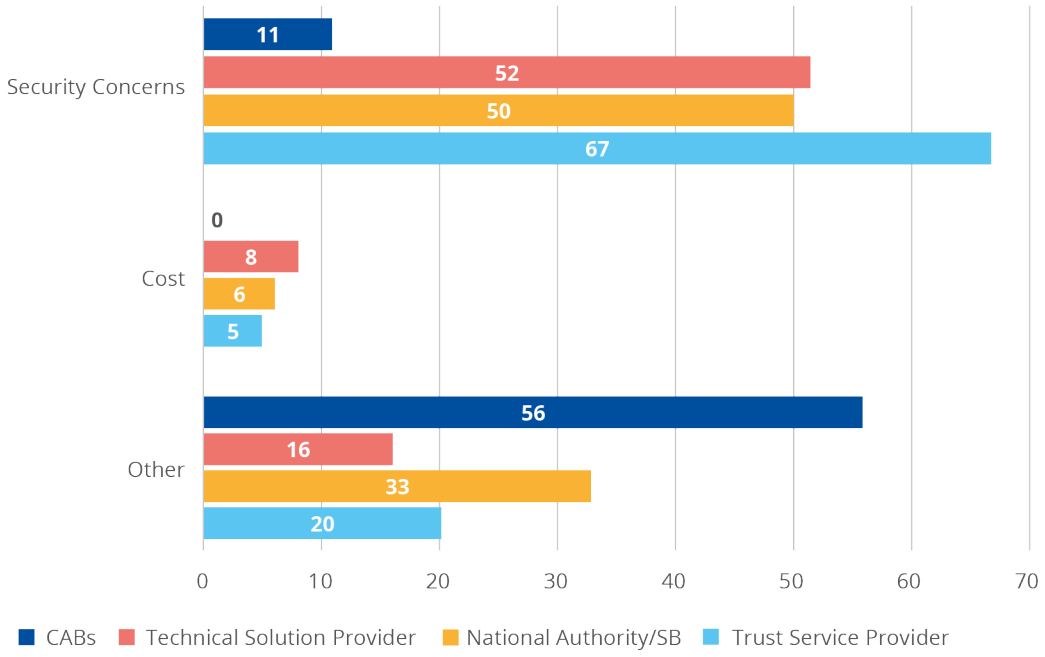
Before having a closer look at the benefits of moving trust services to the cloud, the impediments that were mentioned by the survey participants will be presented. When implementing eIDAS trust services in a cloud or when intending to do so, compliance with EU standards in particular is crucial. CSPs that have implemented the transition have experienced a lack of appropriately conformity-assessed CSPs. Fulfilling the requirements of ETSI EN 319 401 is a core precondition. This result goes along with the earlier sections describing requirements for CSPs. One of the main reasons as to why coherence with EU standards is so important is the set of auditing requirements. In Section 4, further details on the evaluation of trust services in the cloud will be given.

Apart from the audit, the security requirements of the CSPs might not match those of some Member States (such as Italy). Typical cloud providers offer 'basic' security whereas TSPs need 'high' levels to fulfil eIDAS requirements. Apart from the defined security requirements, other measures that go along with the security concept of the providers might differ, which can lead to a lack in transparency, for example regarding the geographic positioning of services and related data centres.

The considerations and possible impediments that have been stated by solution providers mainly refer to the risk of non-EU entities accessing data and processes that are operated in a cloud. The lack of standardisation for clouds could lead to privacy and security-related problems.

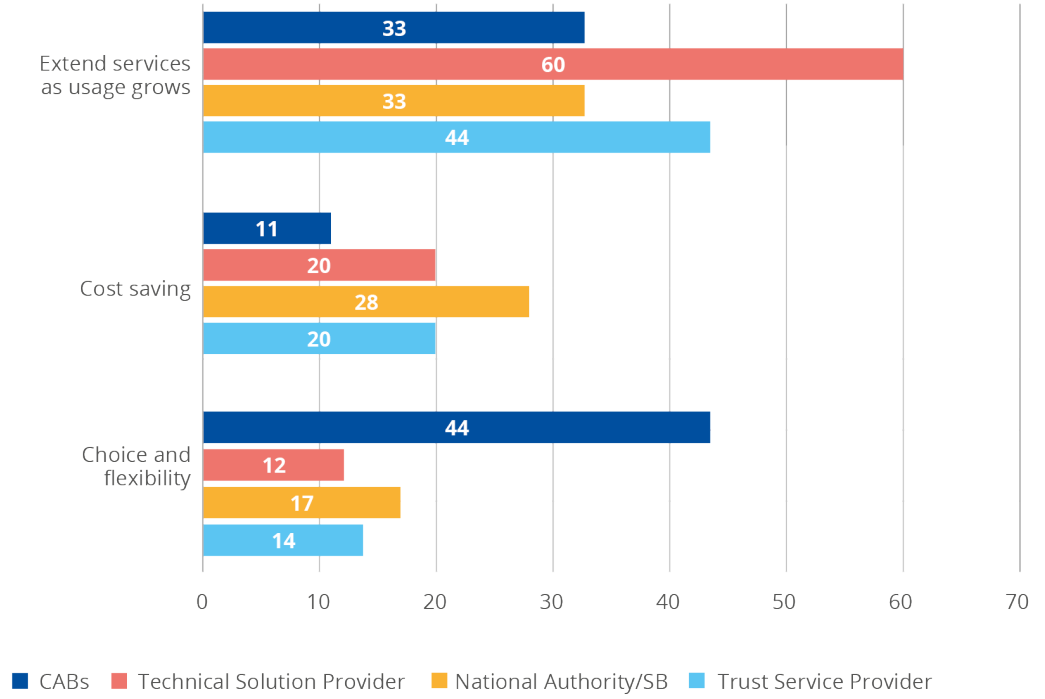
From the perspective of NA/SBs, the increase in complexity, the loss of control of information (user information, privacy, GDPR) and a potential lack of knowledge about how to handle these trust services were all stated as possible impediments or reasons to not use trust services operated in the cloud. However, its practical use is recognised.

Figure 11: Impediments mentioned by TSPs, TSP solution providers, NA/SBs and CABs



While there are still some hurdles and open questions regarding trust services in the cloud, the numbers clearly show a trend towards this transition. There are several benefits in providing trust services or components in the cloud. The flexibility of choice of the platform is one of them. This implies greater scalability and adaptation to changing environments. Another benefit is the cost-saving aspect that results in flexibility. A TSP can easily change to another CSP. Another big advantage of using cloud services is the set of recovery services and backup systems that can work from the same CSP or from another CSP. Changes in structure, system or languages are thus implemented quicker and more safely.

Figure 12: Benefits mentioned by TSPs, TSP solution providers, NA/SBs and CABs



All of these benefits can lead to an extension of services, as there is growth in usage. Moving trust services to the cloud can thus help achieve business objectives and play an important role in their success.

3.5. GENERAL CONCLUSIONS

Most of the aspects of the policy requirements for the trust services considered in this section are likely to be met by CSPs, particularly those offering a virtual infrastructure (IaaS – see Section 1.4.1). Nevertheless, before this can be confirmed, detailed checks on provisions of a particular CSP against the specific policy requirements of the particular trust services to be supported are required.

The use of cryptographic services and HSMs requires particular attention. The assurance of dual control of the management of the TSP signing keys held in an HSM is a particular concern. This is best met using a TSP-provided HSM, where the keys are managed remotely by the TSP personnel. Detailed investigation of the provision of some CSPs called single-tenant HSMs is necessary to see whether this provides the appropriate level of control of the TSP signing keys. CSPs generally only support FIPS 140-2 level 3 HSMs and preference is given to the European standard EN 419 221-5. The use by CSPs of FIPS 140-2 level 2 HSM is not sufficient for most trust services.

Certificate generation and revocation management services, and time-stamping services are required to use security zones and to be physically isolated from any other organisation's services. It remains to be seen whether the same security isolation can be achieved using virtual platforms provided by cloud services.

4. EVALUATION OF TRUST SERVICES IN THE CLOUD

This section considers the issues with the evaluation and audit of trust services in the cloud.

4.1. ACCREDITATION AND CONFORMITY ASSESSMENT SCHEME UNDER eIDAS

A key policy choice made by the eIDAS regulation is that in order to be granted a qualified status by a national supervisory authority, TSPs must first demonstrate that they and the QTSs they plan to provide meet the functional requirements of the regulation. This implies that TSPs and the QTSs they intend to provide need to undergo a specific process and receive approval from a competent national SB to attest to their conformity with the requirements. If successful, this process leads to their inclusion in the national trusted list attesting their qualified status.

As part of this process, the prospective QTSP/QTS must be audited by an eIDAS-accredited CAB to confirm, through a conformity assessment (audit) report, that they meet the requirements of the eIDAS regulation. The CAB needs to be accredited by an NAB in line with Regulation (EU) 765/2008, based on a suitable eIDAS conformity assessment scheme and the CAB's competence for assessing the compliance QTSPs and the QTSs they provide (hereafter QTSPs/QTSs) with the eIDAS requirements.

89 % of the CABs stated that the terms and conditions of CSPs do not contain adequate clauses allowing access for auditors to perform TSP assessments.

The requirements on the CAB and the conformity assessment report referred to in Articles 20(1) and 21(1) are further specified by Article 3(18) of the eIDAS regulation. Article 20(1) of the eIDAS regulation requires that 'the purpose of the audit shall be to confirm that the [QTSP] and the [QTS] provided by them fulfil the requirements laid down in this Regulation.' Consequently, the resulting conformity assessment report must include a formal conformity statement confirming, when applicable, that the audited QTSP/QTS meets all of the applicable requirements of the eIDAS regulation.

The accreditation of the CAB under eIDAS must ensure that the conformity assessment activities used by such an independent body are such that there is a justifiable trust that the QTSPs/QTSs meet the requirements laid down in the eIDAS regulation.

Neither the business nor the technical model can be imposed upon the QTSPs, nor a specific standard to be followed for the QTS it provides. (Q)TSP/(Q)TS have to demonstrate their compliance (building upon standards if it is deemed appropriate) with the requirements of the eIDAS regulation, while the SB cannot refuse to grant the qualified status solely on the grounds that the proposed model does not comply with a given standard or a given business or technical model. However, in practical terms, supervisory and accreditation authorities have built the scheme on the ETSI standards referred to above.

When using cloud services in support of a trust service the overall conformity assessment of the trust service(s) is the responsibility of the trust service provider. Inevitably there will be aspects of the trust service, such as management of the operation of the trust service by trusted personnel, which will not be met by the CSP. It is the responsibility of the TSP to provide its auditor with evidence that it meets all the operational and technical requirements of the trust service. This will require the TSP to provide evidence that requirements of the services of the CSP, on which the TSP depends, are met for example by the CSP through certifications with more detailed information as considered necessary by the auditor.

4.2. PRACTICAL EXPERIENCES

A significant number of TSPs – not only CAs but also qualified certified electronic delivery or time-stamping services – are migrating to or establishing their services directly in the cloud. The level of integration with CSPs varies, but in general the service is hosted and operated from the cloud by the provider's staff on their premises.

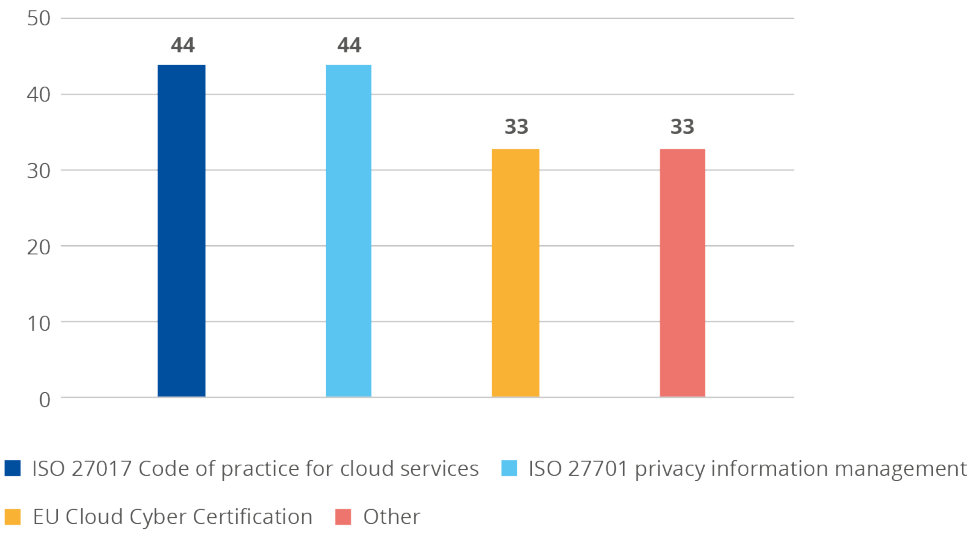
This poses a number of challenges in implementing TSPs requirements and in auditing them when they provide the trust service from the cloud. Some of the main problems encountered in carrying out the compliance assessment are shown below.

- Inability to access data centres to assess physical security and other location-related aspects. Large CSPs do not allow entry to CAB auditors or those appointed by the providers themselves for various reasons, including business secrecy, impossibility of handling such a large number of audits, location of data centres in another jurisdiction and virtualisation of the service.
- Difficulty in accessing the CSP audit reports, which makes it impossible to verify the work done by other auditors with other scopes and the total or partial overlap with the scope of the trusted service.
- Difficulty in determining the contractual responsibility for the implementation of each of the requirements and therefore in the review during the evaluation, always bearing in mind that the responsibility for compliance with all the requirements always lies with the TSP.

To solve these issues, a Spanish CAB has initiated a project with a CSP to identify the responsibility for each control, i.e. to determine whether the controls implemented by the provider on other accredited schemes fully or partially overlap with those required of the TSP and its service(s). Using this information, it is possible to establish an audit time with greater precision, to improve the analysis of the evaluation of the TSPs hosted by that CSP and to reduce the time required to request and evaluate documents.

However, there is still the problem that the assessment of the controls that the TSP has contractually outsourced to the cloud provider can only be done in a documentary manner, which reduces the quality of the audit. This problem needs to be addressed.

Figure 13: Standards CABs recognise as supporting compliance audits of TSPs providing services in the cloud (%)



Other standards

There is a limitation about the recognition of other standards in the sense of accepting them instead of performing an own assessment. It would be helpful to get clear normative and legal regulations supporting the reuse of assessments/audit results/certifications of other parties.

5. CONCLUSIONS

The current report has examined the potential of moving trust services as defined in the eIDAS regulation to the cloud. The applied method focused on analysing existing standards and the technical requirements which have to be addressed for such movement to occur. In this report, the current landscape of technical EU requirements that include a possibility for a move of trust services to the cloud was presented and the survey results showed that there is interest from TSPs to provide services from a cloud and from cloud providers to offer a platform for such service. However, each specific case requires a detailed analysis to meet security and privacy needs, as the individual requirements and the processes of offering trust services on the cloud also highly depend on the CSPs and their requirements and capabilities.

The assessments of this report are based on the assumption that CSPs already follow the mentioned standards (e.g. ISO/IEC 27001 and ISO/IEC 27002). Above all, there are existing EU regulations that cloud services providers need to comply with, especially regarding privacy issues and the GDPR, where private data is held in the cloud. Looking at these requirements, it can be stated that a requirement for moving trust services to the cloud is that the cloud services are provided from within the EU. The implications of the application of NIS 2 to trust services which operate on the cloud require further study.

This report has identified the role of the HSM and the control over it as important aspects to be addressed when planning to move trust services to the cloud. To ensure security, it is indispensable that the TSP retains the control over the keys held in the HSM and their use in signing. There are some cloud providers (even big global players) that allow the TSP to install their own HSM and retain control over the keys. Others allow only temporary control over the keys, which is called ‘temporary tenants’ or ‘multi-tenants’. From the perspective of the HSM provider, the provision of key attestations, the knowledge of the cryptographic capacity and when its limits are reached and the backup of data when using a remote HSM need to be addressed. Preference is given to the use of HSMs certified under European standards EN 419 221-5 and EN 419 241-2.

Certain aspects of trust services are required by existing standards to use security zones and to be physically isolated from any other organisation's services. It remains to be seen whether the same security isolation can be achieved using virtual platforms provided by cloud services.

From the audit perspective, the survey results have particularly shown that there is still insecurity and open questions when it comes to auditing trust services remotely. While there are standards which CABs recognise as supporting compliance audits of TSPs providing services in the cloud (ISO 27017, ISO 27701, EU cloud cyber certification), most CABs think that the terms and conditions of CSPs contain adequate clauses allowing access for auditors to perform TSP assessments. Auditing TSPs that offer their services on a cloud requires the cooperation of CSPs. This can take the form of physical access to the cloud service premises to perform the compliance assessment of the TSP’s requirements, remote access to its system or the provision of all necessary documentation for the TSP’s evaluation. However, the latter was evaluated by the CABs who answered the survey as insufficient when generic cloud service is used in support of a TSP. While some impediments from the audit perspective exist, the survey results have shown that CABs can already perform audits on many trust services. It is important to note that CABs carrying out assessments in the context of EUCS should be accredited to ISO 17065 and meet the additional requirements specified for EUCS.

All in all, moving trust services to the cloud must be understood as an ongoing process that has to be followed on a step-by-step basis. While some services – such as the validation of signatures, delivery, time stamp or preservation – are moved rather quickly, other services – such as the issuance of certificates and remote control over the signing device – require in-depth analysis and preparation. This also applies to the different components of trust services. Either way, during the time of the move, the communication between the CSP and the data centre needs to be secured and protected from attacks. The transition of data to the cloud has to be secured at all times and, in the best case, remain in the data centre of the TSP. Some services might not be suitable for operating on the cloud.

There are multiple benefits to moving trust services to the cloud. The main ones identified in this report are the ability to extend services, cost savings and more choice and flexibility in choosing the platform. 50 % of the TSPs who participated in the survey already operate or plan to operate at least parts of their trust services in the cloud. This number clearly shows that TSPs are moving their services to the cloud. This development is ongoing and we can expect more TSPs to move their services to the cloud. This report has given a detailed overview of the issues to be addressed for such a transition, including the related challenges and opportunities.

6. BIBLIOGRAPHY/ REFERENCES

6.1. BIBLIOGRAPHY

- Rison, A., '13 effective security controls for ISO 27001 compliance', Azure blog and updates, Microsoft Azure, 2016, https://azure.microsoft.com/de-de/blog/13-effective-security-controls-for-iso-27001-compliance.
- CSA, 'Security guidance for critical areas of focus in cloud computing v4.0', Cloud Security Alliance, Working Group Security Guidance, 2017, https://cloudsecurityalliance.org/research/guidance/.
- Skoutaris, E., 'What is the Cloud Controls Matrix (CCM)?', Cloud Security Alliance, blog article, 2020, https://cloudsecurityalliance.org/blog/2020/10/16/what-is-the-cloud-controls-matrix-ccm.
- Huang, J. and Nicol, D. M., 'Trust mechanisms for cloud computing', *Journal of Cloud Computing: Advances, Systems and Applications*, Vol. 2, No 9, 2013.
- Vdovenko, K., 'Cloud as a key to trust with public services', Accenture Insights, 2022, https://www.accenture.com/fi-en/blogs/insight/cloud-as-a-key-to-trust-with-public-services.
- Taleb, N. and Mohamed, E. A., 'Cloud computing trends: A literature review', *Academic Journal of Interdisciplinary Studies*, Vol. 9, No 1, 2020.
- Samani, R., Honan, B. and Reavis, J., *CSA Guide to Cloud Computing – Implementing cloud privacy and security*, Syngress, 2014, https://doi.org/10.1016/B978-0-12-420125-5.01001-3.
- Diogenes, Y. and Shinder, T., *Microsoft Azure Security Center, 2nd Edition*, Microsoft Press, 2019.

6.2. ENISA PUBLICATIONS

ID	Description
ENISA Threat Landscape	ENISA, *ENISA Threat Landscape 2022*, 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
ENISA Threat Landscape	ENISA, *ENISA Threat Landscape 2021*, 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
Cloud Services Scheme	ENISA, *EUCS – Cloud services scheme*, EUCS candidate scheme, 2022, https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.
Trust Services Security incidents	ENISA, *Trust Services Security Incidents 2021 – Annual report*, 2021, https://www.enisa.europa.eu/publications/trust-services-security-incidents-2021.
Cloud Computing	ENISA, *Cloud Computing – Benefits, risks and recommendations for information security*, 2009, https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

6.3. APPLICABLE LEGISLATION/REGULATION

ID	Description
ETSI EN 319 401	ETSI EN 319 401 – V2.3.1 (2021-05) Electronic signatures and infrastructures (ESI); General policy requirements for TSPs
ETSI EN 319 411-1	ETSI EN 319 411-1 – V1.3.1 (2021-05) ESI; Policy and security requirements for TSPs issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	ETSI EN 319 411-2 – V2.3.1. (2021-05) ESI; Policy and security requirements for TSPs; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI EN 319 421	ETSI EN 319 421 ESI; Policy and security requirements for TSPs issuing time stamps
ETSI EN 319 422	ETSI EN 319 422 – V1.1.1 (2016-03) ESI; Time-stamping protocol and time-stamp token profiles
ETSI EN 319 513	ETSI EN 319 531 – V1.1.1 (2019-01) ESI; Policy and security requirements for REMS providers
ETSI TS 119 441	ETSI TS 119 441 – V1.1.1 (2018-08) ESI; Policy requirements for TSPs providing signature validation services
GDPR	General data protection regulation (Regulation (EU) 2016/679)
ISO/IEC 27017	ISO/IEC 27017:2015 Information technology; Security techniques; Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	ISO/IEC 27018:2019 Information technology; Security techniques;

	Code of practice for protection of PII in public clouds acting as PII processors
ISO/IEC 27001	ISO/IEC 27001 and related standards Information security management
ISO/IEC 27002	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection; Information security controls
ISO/IEC 17788	ISO/IEC 17788:2014 Information technology; Cloud computing; Overview and vocabulary
NIS 2	The NIS2 directive (Directive (EU) 2022/2555)

7. ANNEX – SURVEY RESULTS

7.1. TRUST SEVICE PROVIDERS

How much do you consider the use of general-purpose cloud platforms as being appropriate to your trust services (select the most relevant)?

Answer	Ratio
We already operate all our trust services on a cloud platform	15 %
We already operate parts of our trust services on a cloud platform	20 %
We plan to operate all our trust services on a cloud platform	1 %
We plan to operate parts of our trust services on a cloud platform	14 %
We might consider operating all our trust services on a cloud platform	9 %
We might consider operating parts of our trust services on a cloud platform	29 %
We don't consider use of a cloud platform appropriate to our trust services	12 %
Other	0 %
No answer	0 %

What cloud platform(s) do you or are you considering using in support of all or parts of your trust service (select all that apply)?

Answer	Ratio
Amazon Web Services	48 %
Microsoft Azure	44 %
Google Cloud Platform	21 %
Other international cloud provider(s)	11 %
Local cloud provider(s)	30 %
None	21 %
No answer	0 %

Please identify which trust services or components you consider could operate on a cloud platform (select all that apply).

Answer	Ratio
Qualified certificates for electronic signatures	56 %
Qualified certificates for electronic seals	55 %
Qualified validation service for qualified electronic signatures	53 %
Qualified preservation service for qualified electronic signatures	47 %
Qualified validation service for qualified electronic seals	47 %
Qualified preservation service for qualified electronic seals	41 %
Qualified certificates for website authentication	32 %
Qualified time stamps	44 %
Qualified electronic registered delivery service	33 %
Registration for trust services	44 %
Management of user keys	32 %
Generation of certificates, timestamps or other trust statements	39 %
Revocation management	47 %
Management of TSP signing keys	20 %
Provision of revocation status information (e.g. OCSP)	54 %
Management of user devices (e.g. smart card)	17 %
Other	14 %
None	12 %
No answer	0 %

7.2. CLOUD SERVICE PROVIDERS

How much do you consider your cloud platform as being appropriate to supporting trust services (select the most relevant)?

Answer	Ratio
We already support a range of trust services on our cloud platform	0 %
We already support parts of trust services on our cloud platform	100 %
We plan to support a range of trust services on our cloud platform	0 %
We plan to support parts of trust services on our cloud platform	0 %

We might consider supporting parts of trust services on our cloud platform	0 %
We don't consider supporting trust services on our cloud platform	0 %
Other	0 %
No answer	0 %

Do you consider your cloud services as appropriate for supporting all or part of trust services supporting PKI or identity-related services (select all that apply)?

Answer	Ratio
All PKI services	25 %
Qualified certificates for electronic signatures	50 %
Qualified certificates for electronic seals	50 %
Qualified validation service for qualified electronic signatures	50 %
Qualified preservation service for qualified electronic signatures	0 %
Qualified validation service for qualified electronic seals	25 %
Qualified preservation service for qualified electronic seals	0 %
Qualified certificates for website authentication	25 %
Qualified time stamps	50 %
Qualified electronic registered delivery service	25 %
Registration for trust services	25 %
Management of user keys	75 %
Generation of certificates, time stamps, or other trust statements	25 %
Revocation management	25 %
Management of TSP signing keys	0 %
Provision of revocation status information (e.g. OCSP)	0 %
Management of user devices (e.g. smart card)	25 %
Other trust services or components	25 %
Regulated banking services	25 %
Other regulated services	25 %
None	0 %
No Answer	0 %

Does your service include security-related services such as user key management and cryptographic functions (e.g. using an HSM)?

Answer	Ratio

Yes	75 %
No	25 %
No answer	0 %

What security and privacy certifications does your cloud service provide or plan to provide in the near future?

Answer	Ratio
ISO 27017: Code of practice for cloud services	75 %
ISO 27701: Privacy information management	75 %
EU cloud cyber certification	75 %
Other certification(s)	50 %
No answer	0 %

Do you provide your services to TSPs from specific locations/facilities?

Answer	Ratio
Yes	25%
No	75%
No Answer	0%

If yes, where and with whom?

Answer	Ratio
Within the EU	25%
Globally	25%
Specifically in the following non-EU country or countries	0%
We share information within our organization just inside the EU	0%
We share information across all or some of the following locations	0%
No Answer	75%

If customers have elements of the trust service requirements that may be supported by the cloud but are not currently certified, is it possible for independent audit checks to be carried out to confirm that any additional requirements are met by any of the following (select all that apply):

Answer	Ratio
Using an external auditor appointed by the customer?	25 %

Using an accredited auditor (e.g. accredited against ISO 17065 or ISO 17021)?	75 %
Using an auditor appointed by a national regulatory/competent authority?	25 %
Through detailed reports from an auditor appointed by yourself as the cloud service provider?	25 %
Through detailed reports provided to clarify areas of uncertainty regarding existing certification?	0 %
Other	25 %
No answer	0 %

7.3. PROVIDERS OF SOLUTIONS TO TSPs

How much do you consider the use of general-purpose cloud platforms as being appropriate to the solutions you provide to support parts of trust services (select the most relevant)?

Answer	Ratio
We already provide solutions for trust services on a cloud platform	48 %
We plan to provide solutions for trust services on a cloud platform	24 %
We might consider providing solutions for trust services on a cloud platform	12 %
We don't consider providing solutions for trust services on a cloud platform	16 %
Other	0 %
No answer	0 %

Would you consider that all or parts of your solution could possibly be placed in the cloud (select all that apply)?

Answer	Ratio
ID proofing	60 %
HSM/shared secure key storage	36 %
PKI-related software	60 %
Electronic identities	60 %
Remote signing	72 %
Document workflow	44 %
Other	16 %
No answer	0 %

Please identify any PKI-related parts of your solution that could possibly be placed in the cloud (select all that apply).

Answer	Ratio
Shared PKI service	48 %
Certificate issuance/renewal	44 %
Revocation management	44 %
OCSP	40 %
RA	36 %
Time stamping	44 %
Signature creation	44 %
Signature validation	52 %
Other PKI	24 %
No answer	40 %

What elements of your solution(s) could be placed in the cloud (select all that apply)?

Answer	Ratio
Policy	68 %
Data	72 %
Segregation of duties	48 %
Keys	44 %
Event logs	80 %
Backups	72 %
Private data	44 %
Access control	68 %
Network security	44 %
Media handling	36 %
Other	8 %
No answer	0 %

7.4. NATIONAL AUTHORITIES

How much consideration has been given to the use of cloud services by TSPs to support all or part of their service (select the most relevant)?

Answer	Ratio

We have direct experience with TSPs use of the cloud	39 %
It is something that TSPs have asked us to consider	11 %
It is something that we would promote	6 %
It is something that we are investigating	28 %
We don't currently see this as a requirement	11 %
We don't see this as a practical	6 %
No answer	0 %

In your view, which trust services or trust service component could be placed in the cloud (select all that apply)?

Answer	Ratio
Qualified certificates for electronic signatures	44 %
Qualified certificates for electronic seals	44 %
Qualified validation service for qualified electronic signatures	56 %
Qualified preservation service for qualified electronic signatures	56 %
Qualified validation service for qualified electronic seals	61 %
Qualified preservation service for qualified electronic seals	50 %
Qualified certificates for website authentication	39 %
Qualified time stamps	50 %
Qualified electronic registered delivery service	44 %
Registration for trust services	56 %
Management of user keys	28 %
Generation of certificates, time stamps, or other trust statements	44 %
Revocation management	39 %
Management of TSP signing keys	28 %
Provision of revocation status information (e.g. OCSP)	61 %
Management of user devices (e.g. smart card)	44 %
Other	22 %
No answer	0 %

7.5. Conformity assessment bodies

What requirements do you use as the basis of your audits (select all that apply)?

Answer	Ratio

eIDAS regulation	100 %
WebTrust	11 %
ETSI standard relating to the trust service being audited	89 %
Other	22 %
No answer	0 %

What additional standards do you recognise as supporting compliance audits of TSPs providing services in the cloud?

Answer	Ratio
ISO 27017: Code of practice for cloud services	44 %
ISO 27701: Privacy information management	44 %
EU cloud cyber certification	33 %
Other	33 %
No answer	0 %

Do you think that the documentary review sufficient when generic cloud service is used in support of TSP?

Answer	Ratio
Yes	11 %
No	89 %
No answer	0 %

In your opinion, do the terms and conditions of cloud service providers contain adequate clauses allowing access for auditors to perform TSP assessments?

Answer	Ratio
Yes	11 %
No	89 %
No answer	0 %

In your opinion, with the existing limitations, is it possible to carry out an adequate TSP compliance assessment when hosted wholly or partly on a cloud service?

Answer	Ratio
Yes	33 %
No	67 %

No answer	0 %

Could you perform an audit on a TSP or TSP component in the cloud for any of the following (select all that apply)?

Answer	Ratio
Qualified certificates for electronic signatures	56 %
Qualified certificates for electronic seals	56 %
Qualified validation service for qualified electronic signatures	56 %
Qualified preservation service for qualified electronic signatures	56 %
Qualified validation service for qualified electronic seals	56 %
Qualified preservation service for qualified electronic seals	44 %
Qualified certificates for website authentication	56 %
Qualified time stamps	56 %
Qualified electronic registered delivery service	33 %
Registration for trust services	33 %
Management of user keys	33 %
Generation of certificates, time stamps, or other trust statements	33 %
Revocation management	33 %
Management of TSP signing keys	22 %
Provision of revocation status information (e.g. OCSP)	33 %
Management of user devices (e.g. smart card)	22 %
Other	22 %
None	22 %
No Answer	0 %

If you have performed any audit on a TSP that makes use of a general-purpose cloud service, what are your experiences (select all that apply)?

Answer	Ratio
We have been allowed physical access to the cloud service premises to perform the compliance assessment of the TSP's requirements outsourced to the cloud provider	11 %
We have been allowed remote access to its systems to perform the compliance assessment of the TSP	0 %
The cloud service provider has provided us or our customers with all necessary documentation for the TSP's evaluation	33 %
Other	56 %

No answer	0 %

What information has been provided?

Answer	Ratio
Security processes and procedures	22 %
Periodic security reports	11 %
Security incident reports	11 %
Supply chain information	22 %
Penetration testing	11 %
Other schemes full audit reports (ISO 27000, Spanish ENS, C5, critical infrastructure compliance, etc.)	22 %
Risk analysis	22 %
GDPR reports	22 %
Other	0 %
No answer	67 %

TP-08-22-346-EN-N

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-619-9
doi: 10.2824/246732