Federal Office
for Information Security

Website Authentication, Electronic Signatures and Electronic Seals

Fulfilling the eIDAS requirements for providers of qualified certificates with BSI Technical Guidelines

6. May 2016

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

1 Introduction

On 17th September 2014, the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS regulation) entered into force.

The eIDAS regulation establishes a legal framework for the cross border use of electronic identification and trust services. As part of this legal framework, the eIDAS regulation introduces qualified certificates for website authentication, electronic signatures and electronic seals.

The eIDAS regulation defines technical requirements for providers of qualified certificates. In addition, the eIDAS regulation comprises operational requirements for them and the supervision of such providers by a supervisory body of a EU Member State in order to enhance reliability of these providers an to enhance trust in this category of certificates.

This document maps the technical and organisational security requirements of the eIDAS regulation for qualified certificates to the requirements of the Technical Guideline BSI TR-03145-1 “Secure CA operation, Part 1 - Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high'” and shows that the requirements for qualified trust service providers issuing qualified certificates are met by a certification according to this Technical Guideline, which includes an ISO/IEC 27001 certification of the trust service.

The requirements on the certificate profiles for qualified certificates for electronic signatures defined in **Article 28(1)**, electronic seals defined in **Article 38(1)** and website authentication defined in **Article 45(1)** of the eIDAS regulation are covered by:

- ETSI EN 319 412-1 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles;Part 1: Overview and common data structures”;
- ETSI EN 319 412-2 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles;Part 2: Certificate profile for certificates issued to natural persons”;
- ETSI EN 319 412-3 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- ETSI EN 319 412-4 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates”.

2 Mapping

eIDAS Regulation requirements	BSI requirements
Article 5(1): Processing of personal data shall be carried out in accordance with Directive 95/46/EC.	**ISO/IEC 27001 A.18.1** requires “All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.”
Article 13(2): Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.	**TR-03145-1 clause 5.2** “Dissemination of 'Terms and Conditions'” requires “Diss.Obj.1The CA needs to define limits of certificate usage and the duties of the subscribers and relying parties to make clear in what kind of scope the subscribers are trustworthy. Additionally, the CA needs to declare its liability towards involved parties, i.e. subscribers and relying parties, covering the services the CA offers in key- and certificate management as well as related services (i.e. the validation service) for the PKI. Therefore the CA shall disseminate its current 'Terms and Conditions' to subscribers and relying parties.”
Article 15: Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.	**ISO/IEC 27001 A.18.1** requires “All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.”
Article 19(1): Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.	**TR-03145-1 clause 6.1** requires the implementation of an Information Security Management System including the certification of the ISMS by an independent ISO/IEC 27001 auditor. The audit shall include the ISMS and the requirements of TR-03145. The **TR-03145** defines requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', which includes all processes and resources of a CA needed for the Certificate life-cycle. **ISO/IEC 27001 A.16** demands: “Information security events shall be reported through appropriate management channels as quickly as possible.”
Article 19(2): Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection	**ISO/IEC 27001 A.16** demands:“Information security events shall be reported through appropriate management channels as quickly as possible.” **ISO/IEC 27001 A.6.1** requires “Appropriate contacts with relevant authorities shall be

eIDAS Regulation requirements	BSI requirements
authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.	maintained."
Article 20(1): Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.	**TR-03145-1 Clause 6.1** requires a certification according to BSI TR-03145 includes an ISO 27001 certification and therefore requires a full audit every 36 months and re-assessment audits every 12 months.
Article 24(1): When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued. The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law: (a) by the physical presence of the natural person or of an authorised representative of the legal person; or (b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or (c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.	**TR-03145-1 clause 5.3** "Identification and Registration" requires the following: "IR.Req.7: The CA shall verify the information identifying the applicants and the physical existence directly or indirectly using appropriate measures in accordance with the national law. The physical address or other appropriate attributes for contact shall be verified. The CA shall define clearly the set of information identifying the applicant. ... If the subject differs from the subscriber, additional information shall be provided and checked. In case of a physical person associated with a legal person, this association shall be verified."
Article 24(2): A qualified trust service provider providing qualified trust services shall: (a) inform the supervisory body of any change in the provision of its qualified trust services and an	**ISO/IEC 27001 A.16** demands:"Information security events shall be reported through

eIDAS Regulation requirements	BSI requirements
intention to cease those activities;	appropriate management channels as quickly as possible." **ISO/IEC 27001 A.6.1** requires "Appropriate contacts with relevant authorities shall be maintained."
(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;	**TR-03145-1 clause 6.8** "Trustworthy Personnel"demands the following: "TwP.Req.1: The CA shall employ sufficient personnel who possess expert knowledge, experience and qualifications necessary for the offered services and appropriate to the job function." and **TR-03145-1 clause 6.15** "Requirements for subcontractors" requires: "SubC.Obj.1: The requirements for subcontractors shall be fulfilled to uphold the security standard as provided by the CA itself." and **ISO/IEC 27001 Annex A.7.2.2** : "All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function."
(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;	**ISO/IEC 27001 A.18.1** requires "All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization."
(d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;	**TR-03145-1 clauses 5.2 and 6.2** require the following: "DissTC.Req.4: The 'Terms and Conditions' acceptance by the subscriber shall be checked during the registration process of the subscriber and every time a new version is published." "CP.Req.6: The CP shall specify the scope and applicability of the PKI as well as the key- and certificate management life-cycle processes of the CA completely, comprehensively and adequate to the security level 'high'. The following aspects shall be covered at a minimum: ... limitations concerning subscribers of the PKI (e.g. company or administration specific PKIs) application context of the PKI description of subscriber registration procedures including specification of registration data, requirements for data transmission, and description of verification procedures of the RA subscriber obligations (e.g. requirements on subscriber key stores and application environment) ... CP update procedures"

eIDAS Regulation requirements	BSI requirements
(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;	**TR-03145-1 clause 6.9** "Hardened IT systems and networks supporting logging and monitoring" require amongst other things: "IT.Req.4: The CA servers used for certificate generation shall be hardened. This covers configuration and setting of utilized hardware and software components (i.e. operating systems, CA server software or firewall components)."
(f) use trustworthy systems to store data provided to it, in a verifiable form so that: (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii) only authorised persons can make entries and changes to the stored data, (iii) the data can be checked for authenticity;	**TR-03145-1 clause 5.6** "Dissemination of trusted certificates" requires: "DissCert.Req.2: The CA shall ensure that certificates are only retrieved with consent of an authenticated subscriber. This consent can e.g. be given by accepting the 'Terms and Conditions' by the subscriber." while **TR-03145-1 clause 6.9** claims: "IT.Req.9: The CA shall protect sensitive data against unauthorized access or modification (encryption and integrity measures), specifically when connected to non-secure networks." **TR-03145-1 clause 6.10** "Archiving and tracking" demands logging of registration and certificate issuance events and protection of the integrity of the databases.
(g) take appropriate measures against forgery and theft of data;	**TR-03145-1 clause 6.9** "Hardened IT systems and networks supporting logging and monitoring" requires amongst other things: "IT.Req.9: The CA shall protect sensitive data against unauthorized access or modification (encryption and integrity measures), specifically when connected to non-secure networks. ..."
(h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;	**TR-03145-1 clause 6.14** "CA termination"demands: "CT.Obj.1: In case of a CA termination, required obligations and liability of the CA shall be preserved by a successor instance for a transition period or a secure termination of all services shall be guaranteed."
(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);	**TR-03145-1 clause 6.14** "CA termination" in combination with **TR-03145-1 clause 6.2** CP.Req.6: The CP shall specify the scope and applicability of the PKI ...The following aspects shall be covered at a minimum:... •CA termination" cover this eIDAS regulation requirement.
(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;	**ISO/IEC 27001 A.18.1** requires "All relevant legislative statutory, regulatory, contractual

eIDAS Regulation requirements	BSI requirements
	requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization."
(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.	**TR-03145-1 clause 6.10** "Archiving and tracking" requires the following: "ArchC.Req.1: The CA shall ensure that a complete set of information concerning a certificate is archived. This set shall be clearly and a priory defined, containing the information relevant for the certificate and be stored for an appropriate time."
Article 24(3): If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.	**TR-03145-1 clause 5.7** "Revocation and suspension" demands: "RM.Req.6: The CA shall maintain the revocation list in a timely manner (cf. 6.11). The complete Revocation and suspension process (i.e. the delay between a revocation request or report and the availability of the revocation status information to all relying parties) should be at most [assignment: *number of minutes*]."
Article 24(4): With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.	**TR-03145-1 clause 6.11** "Maintained revocation status" requires: "MRS.Req.2: The CA shall ensure that the maintained revocation information are accessible continuously to the relying parties and up to date." and **TR-03145-1 clause 6.10** "Archiving and tracking" demands: "ArchC.Req.1: The CA shall ensure that a complete set of information concerning a certificate is archived. This set shall be clearly and a priory defined, containing the information relevant for the certificate and be stored for an appropriate time."