Product Certification Scheme A:

Qualified Electronic Signatures

Product Factsheet for

eIDAS (Electronic Identification and Signatures)

KPMG Certification Body FLCES 006

Enforcement steps:	**Name:**	**Date:**
Created by scheme owner	Philipp Wirth	08.06.2022
Controlled by scheme owner	Reto Grubenmann	15.07.2022
Released by	Reto Grubenmann	15.07.2022

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-20924-01-00

Vaduz, 15.07.2022

Table of Content

1 Introduction

1.1 Product Description

The eIDAS Regulation introduces mutual recognition of electronic IDs and electronic trust services, including electronic signatures. An electronic signature can be defined as data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign. A qualified electronic signature is an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

The purpose of a certificate for electronic signature is to provide an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person. The eIDAS Regulation provides that electronic signatures should not be denied legal effect on the basis that they are in electronic form.

KPMG certification body FLCES 006 aims to assess the conformity of the requirements set forth by the defined regulations, norms and standards in within the client's organizational and technical control framework.

KPMG certification body FLCES 006 is accredited based on DIN ES ISO/IEC 17065 in conjunction with the ISO/IEC 17067 and regulation (EU) 910/2014 including ETSI EN 319 403.

This Product Certification Scheme is part of the Product Certification System of the KPMG Certification Body FLCES 006.

1.2 Major Regulations, Norms and Standards

The following standards and norms are related to eIDAS for this certification scheme:

Norm / Standard	Description	Version
ETSI EN 319 401	Electronic Signatures and Infrastructure (ESI); General Policy Requirements for Trust Service Providers	V2.3.1 (2021-05)
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	V1.3.1 (2021-05)
ETSI EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	V2.4.1 (2021-11)
ETSI EN 319 412-1	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures	V1.4.4 (2021-05)

Norm / Standard	Description	Version
ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons	V2.2.1 (2020-07)
ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements	V2.3.1 (2020-04)
ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic suites for secure electronic signatures	V1.4.2 (2022-02)
DIN EN 419 241-1	Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements	2018-09
IETF RFC 5280	X.509 Internet Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2018-05
IETF RFC 3647	X.509 Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework	2003-11
IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	2013-06

2 Audit Methodology

The audit methodology for the certification scheme is according to Section 3 of the Certification System (Umbrella Document) of the KPMG Certification Body FLCES 006.

3 Requirements for Certified Organization

The following control objectives of norms, standardizations and regulations shall be implemented within the certified organization. The organization shall establish a management system to ensure the “planning, doing, checking and acting” methodology for the continuing improvement of the following functional EN standards.

Regulation / Norm	Mandatory Control Chapters (and sections)
Regulation (EN) No 910/2014 of the European parliament and of the council of 23.07.2014 on electronic identification and trust services for electronic transaction in the internal market and repealing directive 199/92/EC (eIDAS regulation).	Section 4 “Electronic Signatures” (L 257/100)

ETSI EN 319 401 (2021-05)	All chapters
ETSI EN 319 411-1 (2021-05)	All chapters
ETSI EN 319 411-2 (2021-11)	All chapters
ETSI EN 319 412-1(2021-05)	All chapters
ETSI EN 319 412-2 (2020-07)	All chapters
ETSI EN 319 412-5 (2020-04)	All chapters
DIN EN 419 241-1 (2018-09)	All chapters

4 Allocation of Audit Programs and Procedures

The allocation of audit programs and procedures for the certification scheme is according to Section 4 of the Certification System of the KPMG Certification Body FLCES 006.

5 Product certification requirements

The product certification requirements for the certification scheme are according to Section 5 of the Certification System of the KPMG Certification Body FLCES 006. This is a product certification scheme of type 6.

6 Formal Application of Clients

The formal application of clients for product certifications according to this certification scheme are according to Section 6 of the Certification System of the KPMG Certification Body FLCES 006.

7 Responsibilities

Following parties are involved in this product certification with different responsibilities:

- KPMG (Liechtenstein) AG (FLCES 006): Conformity Assessment Body (CAB)
- Deutsche Akkreditierungsstelle GmbH (DAkkS): Accreditation Body
- Amt für Kommunikation (AK) Liechtenstein: Administration of „Trusted List“
- BundesNetzAgentur (BNetzA) Bonn: Member of accreditation commission
- Bundesamt für Sicherheit in der Informationstechnik (BSI)