Communications
Regulatory Authority
State of Qatar

هيئة تنظيم
الاتصالات
دولة قطر

Technical Specifications on the requirements applicable to advanced electronic signatures and advanced electronic seals, adopted pursuant to Articles 40.2 and 46.2. of the CSP Regulation

Version 1.0

25 February 2024

1. ARTICLE 1 – Definitions

1.1. The terms, words, and phrases used in these technical specifications shall have the same meaning as are ascribed to them in the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 as amended or repealed and the Regulation of Certification Service Providers issued under the Communications Regulatory Authority President Decision No. [X] of, unless these specifications expressly provides for otherwise. For the purposes of these technical specifications, the following terms and words shall have the meanings ascribed to them below:

1.2. The terms listed below have the corresponding meanings:

State	State of Qatar.
The Authority	The Communications Regulatory Authority (CRA).
“Law"	the Electronic Commerce and Transactions Law promulgated by Decree Law No. 16 of 2010 or any amendment or law which repeals and replaces such law;
“CSPs Regulation”	Regulation on the Licensing and the Work of Certification Service Providers of 2024

2. ARTICLE 2 – General requirements

2.1. Pursuant to Articles 40.2 and 46.2. of the Regulation, advanced electronic signatures and advanced electronic seals shall be created in accordance with one or more of the following standardized formats:

- CAdES baseline signatures as specified in [ETSI EN 319 122-1];
- XAdES baseline signatures as specified in [ETSI EN 319 132-1];
- PAdES baseline signatures as specified in [ETSI EN 319 142-1];
- JAdES baseline signatures as specified in [ETSI TS 119 182-1];
- Associated Signature Containers ASiC-S and ASiC-E as specified in [ETSI EN 319 162-1].

3. ARTICLE 3 – Cryptographic requirements

3.1. The cryptographic suites and the cryptographic key lengths and parameters used for the creation of advanced electronic signatures and advanced electronic seals shall be capable to resist to cryptographic attacks during the validity period of the data to which they are applied and, when applicable, of the associated certificate, whichever is the longer.

3.2. The cryptographic suites and the cryptographic key lengths and parameters shall conform to the latest version of the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [SOG-IS Crypto WG].

4. ANNEX I – References

ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3 as listed below:

Reference	Title
[ETSI EN 319 122-1]	ETSI EN 319 122-1 V1.3.1 (2023-06): Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: "Building blocks and CAdES baseline signatures".
[ETSI EN 319 132-1]	ETSI EN 319 132-1 V1.2.1 (2022-02): Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
[ETSI EN 319 142-1]	ETSI EN 319 142-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
[ETSI EN 319 162-1]	ETSI EN 319 162-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: "Building blocks and ASiC baseline containers".
[ETSI TS 119 182-1]	ETSI TS 119 182-1 V1.1.1 (2021-03): Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
[SOG-IS Crypto WG]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms (https://www.sogis.eu/uk/supporting_doc_en.html)