وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Security Guidelines For E-Seals

Version: 1.0

Author: Qatar Public Key Infrastructure Section

Document Classification: PUBLIC

Published Date: July 2018

Q-CERT

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Document Information

Date	Version	Reviewed By
15/07/2018	1.0	Qatar National PKI Team

Content

1. Introduction

This document addresses electronic seals and is one of guide which target to assist parties aiming to use electronic signatures and seals (E-Seals) to understand the subject correctly as-well-as the potential benefits, amongst others, by giving examples of possible application. **The use of E-Seals in the State of Qatar mandate the legal recognition of this technology by the competent authorities. In other way, the use of any e-seal's solutions should be under the approval of the competent authorities.**

2. Legal Mandate

Decree Law No. (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law stipulated the role of the ICT in issuing regulations and decisions to implement the provisions of the enclosed Law.

The Emiri Decree No. 8 of 2016 establishing the Ministry of Transport and Communications and setting the mandate of Ministry of Transport and Communications (hereinafter referred to as "**MOTC**") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology in the State of Qatar.

Article (03) of Emiri Decree No.16 of 2010 stipulates that **Qatar National PKI Section** (under **Cyber Security Division**), as the concerned and the competent authority, to issue regulations and decision on the field of PKI related solutions by proposing and issuing policies and standards and ensuring compliance.

Article (02) of the Bylaw No.01 of 2012 stipulates that Qatar National PKI Section (under Cyber security division), as the concerned and the competent authority, to issue regulations and decision regulating the work of certification service providers pursuant to the Electronic Commerce and Transactions Law by proposing and issuing policies and standards and ensuring compliance.

3. Objective

3.1. Objective of the document

This document proposes a set of **security guidelines on the appropriate use of qualified electronic seals**. The objective of the document is to support relying parties and end users of qualified electronic seal services to securely use these services.

3.2. Scope and Audience

The target audience of the document are the relying parties of qualified electronic seal services. This could comprise government entities, businesses and public administrations.

4. Definitions

The **eIDAS** defines an **electronic seal** (called also **electronic stamp**) as "data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity". A **qualified electronic seal** shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

A **seal** is "generated" by a creator of the seal, possibly "augmented" and "validated" by the receiver of the sealed data (so-called "relying party"), and possibly preserved, in some cases for a long term.

The way these features are used determines the level of strength, assurance and longevity of the qualified seals. In particular, **CSP**s qualified or not, can be called for the qualified seal creation, validation and/or preservation.

Electronic seals are created by an **electronic seal creation device**, which is defined in the **eIDAS** as "a configured software or hardware used to create an electronic seal by means of an '**electronic seal creation data'** (i.e. "a unique data which is used by the creator of the seal to create an electronic seal").

5. E-Seal

Since a few years, it is possible to electronically sign data and to achieve the same effects as when using a hand-written signature. The equivalence with "hand" written signatures works pretty well for human beings, but was difficult to extend to legal persons. However, legal persons (companies, organization, etc.) needed to officialise electronic documents they issued (e-Invoices, e-Statements, e-Bills, e-Receipts**),** in order to ensure the origin of the document. Today electronic Signature supports this need by introducing **electronic seals**, which serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.

E-Seals are technically speaking digital signatures but where the signing key belongs to a legal entity (e.g. a corporation) and often the signature is applied by a business application rather than a human. This is usually achieved through use of a qualified digital certificate that is involved in creation of a digital seal. The unique private key used in the creation of the digital seal ensures non-repudiation: the entity that created the digital seal cannot later deny that it created the seal for that document. If the document is modified after its digital seal was created, the digital seal is not valid for the modified document. This can be checked by anyone with access of the public key corresponding to the private key used in the creation of the digital seal, ensuring the integrity of the sealed document. Besides authenticating the document issued by the legal entity, e-Seals can also be used to authenticate any digital asset of the legal person, such as software code or servers. The important difference between a digital signature and an electronic seal is that the latter is usually created by a legal person while digital signatures are created by a natural person. For the creation of a digital signature, action of the person signing a document or data is required. In contrast, the creation of the digital seals can be automatized and incorporated in processes executed automatically in a digital environment.

6. E-Seal Types

Electronic seals in general shall not be denied legal effect and admissibility as evidence in legal proceedings. Within the electronic seal types, we defines subsets of electronic seals that provide increasing legal predictability up to a level, the qualified electronic seal, that benefits from an automatic presumption of integrity of the data and of correctness of the origin. As showed in figure 1, we recognize three types of E-Seals:

- The **electronic seal** (presented above).
- The **advanced electronic seal (AdESeal)** – which requires security features that ensure it is uniquely linked to the signatory, it is capable of identifying the signatory entity and it is linked to the data in such a manner that any subsequent change of the data is detectable.
- The **qualified electronic seal (QESeal)** – which is an advanced electronic seal which provides additional level of assurance on the identity of the creator of the seal and an enhanced protection and level of assurance on the seal creation. A special device is required for the creation of QESeal (a **qualified seal creation device**, **QSealCD**).

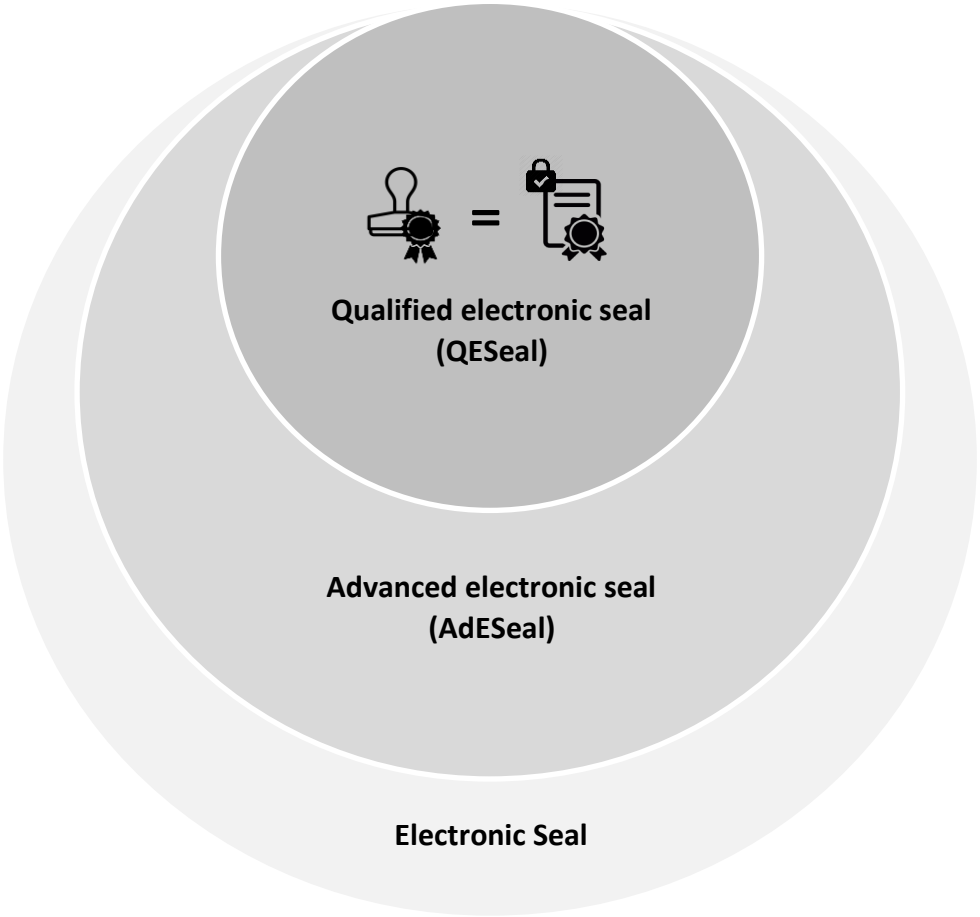

Figure 1: **Types of electronic seals**

7. PKI as technical foundations for (Qualified) E-Seal

Currently, QE-Seals are implemented by means of asymmetric cryptography. With this technology, each seal's owner has a key pair made of a private and a public key (the technology is called public key cryptography) and the electronic seals so produced are called **digital signatures** (not to be confused with 'electronic signatures' that described on others documents).
The signature creation and verification process as follows:

1- The creator of the seal uses the private key to seal (or in technical terms, to digitally sign) a text: The private key is in fact a secret code used by a mathematical function in order to render a data unintelligible (i.e. encrypt data). In the illustration (Figure 2), the data is put in a box closed by the padlock. The private key corresponds to the so-called 'seal creation data'. In the paper world the "private key" concept can be compared to the ring with engraved design used for stamping a seal, that is in theory only reproducible by the owner of the ring, i.e. the creator of the seal.

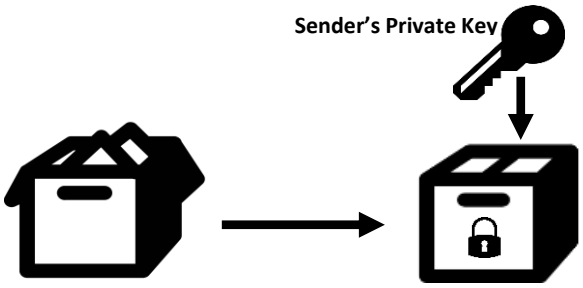

Figure 2: **Digitally signing data with a private key to produce an electronic seal**

2- The verifier (also called relying party) uses the creator of the seal's public key to verify the digital signature: The public key is in fact a code used by the reverse mathematical function to retrieve the initial data from the encrypted data. In figure 3, the data is retrieved from the box using to the public key. In the paper world, the "public key" concept can be compared to an "official" example of a seal that a verifier can compare with a received seal.

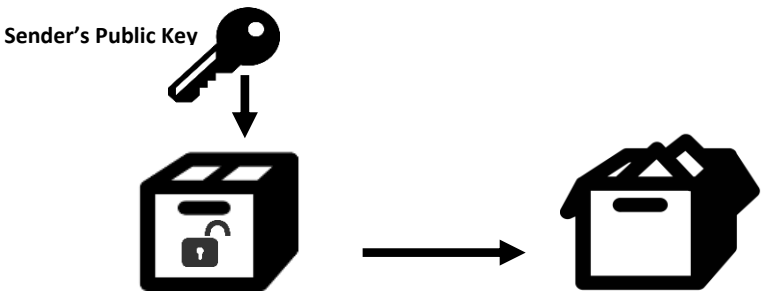

Figure 3: **Verifying a seal**

Of course, there are some technical tricks to ensure that only the person that owns the private key matching the public key is able to create the signature (and a third person would not be able to imitate the creator of the seal's seal):

- It is assumed to be computationally impossible to discover the private key from the knowledge of the public key. Any stakeholder in possession of a public key is able to verify that a signed data has been made by the corresponding private key, without being able to play the role of the creator of the seal since (s) he cannot guess the private key. The size of the key is an important parameter for the security of the algorithm.
- A different unique key pair is allocated to each creator of a seal.
- The creator of the seal shall protect the private key (in the same way as (s) he would not explain to third party how to imitate his seal).

8. The electronic seal process

8.1. Electronic Seal creation workflow

A seal owner, to create a seal in a document, works in a certain environment (e.g. a laptop) to access sealing functionalities made of:

- The seal creation application (e.g. a pdf application residing on the laptop).
- The seal creation device that:
  - Holds the seal creation data (private key).
  - Shall be able to authenticate the creator of the seal (to guarantee his/her control on the private key).
  - Computes the seal (using the sealer's seal creation data).
  - May hold the sealing certificate (or unambiguous references to it).

1- The creator of the seal prepares the document to be sealed (e.g. a PDF file).

2- The application prepares the data to be sealed (i.e. the PDF) in a condensate (called a **hash**) and present it to the secure seal creation device.

3- The seal creation device asks the authorization to the creator of the seal to seal the data, in general, through a windows that pops up on the screen. The creator of the seal authenticates to the device (e.g. (s) he enters a PIN code, or a fingerprint). As explained later on, the seal creation data can be remotely managed (e.g. on a secure server) and there may be more than one persons authorized to activate it in order to create a seal on behalf of an organization.

4- The seal creation device computes the seal and sends the result to the application that integrates the seal into the document.

At this stage, it is important to note that in general, the seal's certificate is provided with the sealed data. This enables the identification of seal owner and the verification of the seal since the public key is immediately available from the certificate.

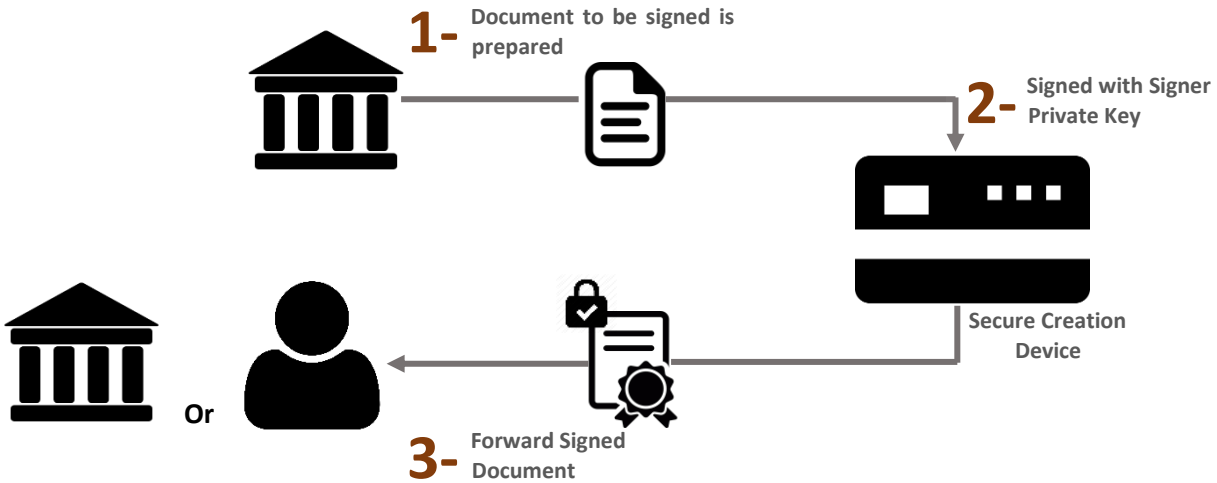

Figure 4: **Electronic Seal creation process**

8.2. Electronic Seal Properties

8.2.1. Security Properties

- **Data integrity**

As mentioned above, the use of public key cryptography to implement ESeal (QE-Seal and AdE-Seal in general) ensures data integrity (i.e. any change in the sealed data after the seal process is detected).

- **Data origin authentication**

The use of public key cryptography to implement E-Seal (QE-Seal and AdE-Seal in general) guaranties the proof of origin of the sealed data since only the person in possession of the private key can be at the point of origin of data sealed with the corresponding public key. For QE-Seal, in addition, there is a high level of assurance on the identity of the person owning private key.

8.2.2. Functional Properties

- **Non-repudiation of sealing**

As mentioned above, the use of public key cryptography to implement ESeal (QESeal and AdESeal in general) provides for non-repudiation of having sealed.

- **Secure identification of the creator of the seal**

The qualified digital certificate ensures the identification of the creator of the seal with a very high level of assurance, due to the controls of the CSP on one hand, but also due to the requirements on the content of the creator of the seal's certificate (See Appendix II). It shall be noted that the eIDAS strongly encourages Trust service providers issuing qualified certificates for electronic seals "to implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided".

APPENDIX I

ACRONYMS

ETSI: European Telecommunications Standards Institute

eIDAS: Electronic IDentification, Authentication and trust Services

PKI: Public Key Infrastructure

QESeal: Qualified Electronic Seal

AdSeal: Advanced Electronic Seal

QSealCD: Qualified seal creation device

SCD: Seal creation device

CSP: Certification Service Provider

APPENDIX II

REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:

1) An indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal.
2) A set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:
    - For a legal entity: Name, where applicable, CR number as stated in the official records.
    - For a natural person: the person's name, ID Card Number.
3) At least the name of the creator of the seal and, where applicable, registration number as stated in the official records.
4) Electronic seal validation data, which corresponds to the electronic seal creation data.
5) Details of the beginning and end of the certificate's period of validity.
6) The certificate identity code, which must be unique for the qualified trust service provider.
7) The advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider.
8) The location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (7) is available free of charge.
9) The location of the services that can be used to enquire as to the validity status of the qualified certificate.
10) Where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

APPENDIX III

DIGITAL SEAL FOR NON-ELECTRONIC DOCUMENTS

The digital seal is a mechanism that allows to verify (in parts or as a whole) the authenticity and integrity of non-electronic documents automatically by cryptographic means using optical document readers only. The digital seal is a two-dimensional bar code printed on the document and comprises digitally signed data for checking the authenticity of the document and the integrity of relevant document contents, e.g. text or images, as well as optionally additional biometric features of the document holder in case of travel or identity documents. The purpose of the digital seal is to provide a cryptographic protection of the authenticity and integrity for non-electronic documents.

Printing and optical reading of integral parts of the non-electronic documents, of course, is prone to inaccuracy. Error tolerant techniques, which enable correcting tolerable deviations while reading and decoding document information, should therefore be applied in using the digital seal.

In general, the generation of a digital seal encompasses the following steps:

1) Create digital reference data assigned to the document (and if applicable biometric data of the document holder) which shall be stored in the digital seal for enabling an automatic verification.
2) Add auxiliary data if needed and necessary information on signature methods and algorithms used to protect the stored data.
3) Digitally sign the reference data and the auxiliary data to protect the document information stored in the digital seal and to prove the integrity and authenticity of the document information.
4) Encode the information (reference and auxiliary data, digital signature) in a machine-readable bar code.
5) Attach (print) the coded information to (on) the document.

APPENDIX IV

APPROVAL PROCESS

Any government entities, businesses and public administrations wishing to deploy and use E-Seals should have the prior approval of the E-Seal solution by **Qatar National PKI Section.** The approval process consist on:

1- Download the application form QPKI Website (www.qpki.gov.qa).
2- Fill and sign the application form.
3- Attach the necessary documents beside the solution.
4- Send a scanned copy of the application form and documents to the following email address to csppmaqatar@qcert.org

APPENDIX V

REFERENCES

- [**eIDAS**] Regulation No 910/2014; On electronic identification and trust services for electronic transactions, July 2014.
- **[ETSI]** EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, August 2017.
- [**ETSI**] TS 119 172-1; Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents, July 2015.
- [**ETSI**] EN 319 412-5; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements, December 2015.
- [**ENISA**] Security guidelines on the appropriate use of qualified electronic seals, December 2016.