وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Guidelines for Virtual Smart Cards

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

A standard solution to store and use PKI certificates is cryptographic hardware tokens and smartcards since they are the most effective way to guarantee sole control over the private key. However, experience has shown that this solution is heavy for both card holders and CSPs when it comes to:

- **Life cycle management**: since the user needs to authenticate and get a smartcard from the registration authority prior to generating his key pair and certificate, also replacing a lost or damaged card can cause delays for users.
- **Cost**: since smart cards and tokens introduce an extra cost to PKI deployments requiring the inclusion of card management systems, printers and qualified staff. The extra deployment cost has to be charged on final users
- **Ease of use:** Having his physical card and reader at all times, having to install drivers and middleware are challenges for non-technical users.
- **Mobile usability:** Only desktop has been targeted so far by smartcard and cryptographic tokens, which means a laptop has to be carried at all time in order to perform even basic documents signing.

Another solution is to use virtual smartcards but without losing in term of non-repudiation since the user is not holding his private key anymore but it is stored somewhere by a trust party in a distant server.

This document provides an overview of the VSC technology, its legal sanctity and guidance for decision makers and system integrators in the state of Qatar to evaluate and deploy the right solution for virtual smartcards.

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. Virtual Smart Card (VSC)

Unlike physical smart card when the card is held by the user, the VSC concept is when the private key and certificate are stored and activated remotely.

A VSC is a service provided by a trust party to ease the distribution and use of PKI certificates and could be used for same key usages as a physical smart card.

Anything related to soft tokens are not considered VSC and will not be subject of this document including:

- Platform related key stores (JKS, PFS/PKCS12)
- Operating system or browser cryptographic providers

Soft tokens differ from VSC by the fact that there is no guarantee to avoid private key duplication.

4. Key usages

4.1. VSC use on e-signature

The main key usage of VSC is on remote signature. It's is a different approach that uses a central HSM to store the user keys and process the electronic signature in the server side. For physical protection of the signature keys, the keys are generated and used within the secure tamper protected boundaries of an HSM. To match this highly secure environment, in TS 419 241, it is required that the authorization for activating the signature keys is also carried out inside the HSM. This is illustrated below with arrows from the user device to the HSM.

The protocol (that is used to provide a secure signature authorization and activation process from the user device to the server and HSM) is known as the Signature Activation Protocol (SAP). The purpose of the protocol is to allow the signatory to activate the signing key in the HSM and generate a signature.

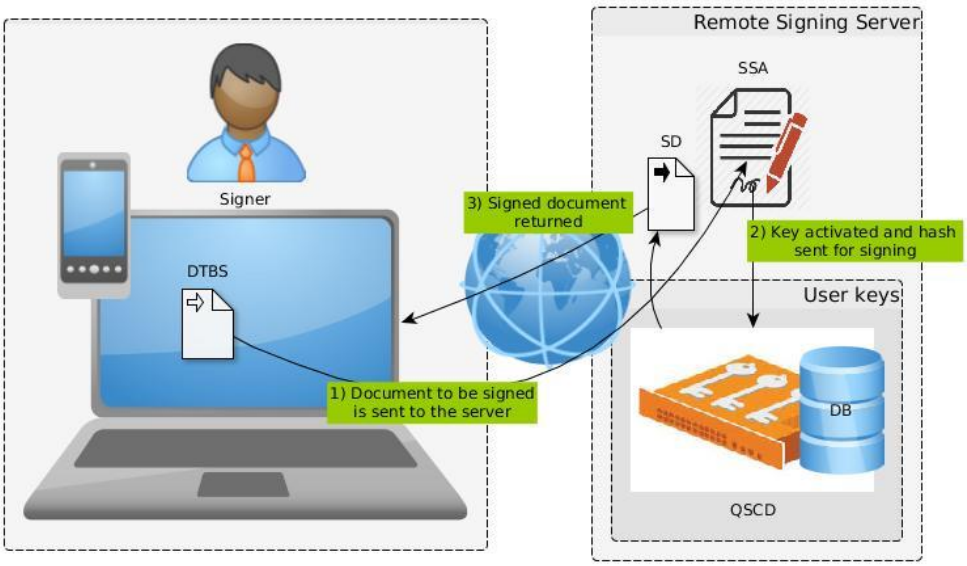

Illustration 1: Simplified remote signing

4.1.1. Difference with hardware smart cards

For an **electronic signature to be considered as a qualified electronic signature**, it must meet two main requirements, the most important ones are:

- The signatory must be linked and uniquely identified to the signature.
- The data used to create the signature must be under the sole control of the signatory. Which means the signer is responsible for his SCD, and the signature has to be created locally either using a local signing application or an applet provided by a remote server. The deployment of a server to assist the creation and verification of electronic signatures is not mandatory but can be useful providing additional services like authentication and WYSIWYS assistant and plugins.

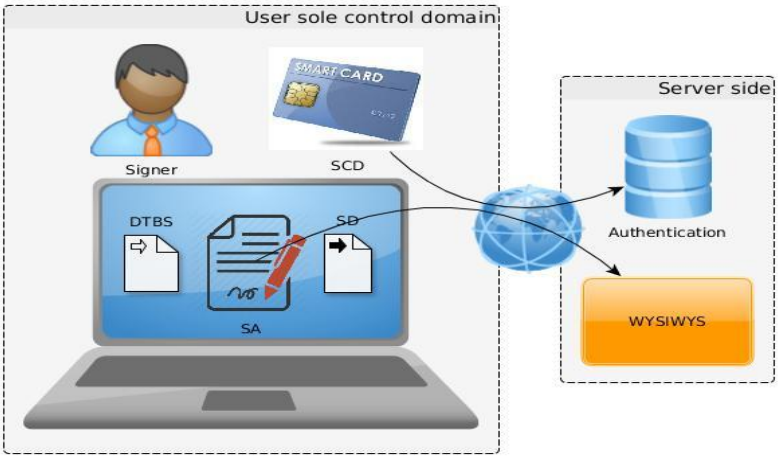

Illustration 2: Electronic signature using a physical smart card

4.2. Authentication

The only available way to implement Virtual Smart Cards for authentication is using the Trusted Platform Module (**TPM**, also known as **ISO/IEC 11889**) which is a dedicated microcontroller playing the role of a secure crypto processor.

The CA has to ensure manufacturer certificate chain validation, thus provide at least a medium to high attestation level.

PS: There is no standard yet on the topic.

APPENDIX I

ACRONYMS

ETSI: European Telecommunications Standards Institute
eIDAS: Electronic IDentification, Authentication and trust Services
DTBS: Data To Be Signed
HSM: Hardware Security Module
QSCD: Qualified Signature Creation Device
SA: Signing Application
SAD: Signature Activation Data
SSA: Signing Server Application
SCD: Signature Creation Data
SD: Signed Data
TPM: Trusted Platform Module
VSC: Virtual Smart Card

APPENDIX II

Qualified remote signature

- **Requirements for implementation**

Qualified remote signatures are possible and each provider willing to implement remote signing has to fulfill these requirements:

- The solution should implement a specially certified Signature Activation Module (SAM), which ensures "sole control"
- A Cryptographic hardware security module EAL4+ certified according to ETSI EN 419 221-5 and ETSI EN 419 241-2 protection profiles should serve as the signing device for the solution.
- The provider should fulfill a Qualified Trust Service Provider audit and certification (ETSI EN 319 401 or equivalent)

- **How does it works**

Unlike the classic signature when signing private key is being stored in a cryptographic card or token and held by the user, the remote signing key is stored in a database held by the trust party.

The key is protected encrypted using a hardware security module.

The user holds only the activation data that makes him the only person who is able to authorize the signing transaction; this principle is called ***"Sole Control"***.

Once the user authorizes the signature, the key is decrypted within the hardware security module and removed after the signing operation takes place.

APPENDIX III

SOLE CONTROL LEVELS

- **Level 1**

This is the basic level of sole control which relies on the trust party and signature environment only.

It does not rely on Signature activation data to activate the signature creation data but only on authentications, policies etc to "Guarantee" the sole control over signing data.

This does not however meet the requirements of qualified signature.

- **Level 2** (Illustration 3)

For qualified signatures, it is recommended to use level 2. This level requires a solid signature activation protocol (SAP) that serves to provide a secure signature authorization and activation process from the user device to the server and HSM.

This signature activation data must be designed in a way that binds information about:

- The signatory.
- The document to be signed (DTBS).
- The private key unique identifier.

The requirements for the SAP are typical for a cryptographic protocol: Confidentiality and integrity of transmitted data must be guaranteed and it must be resistant to attacks like MIM, replay etc.

Sole control level 2 is required for qualified electronic signature.

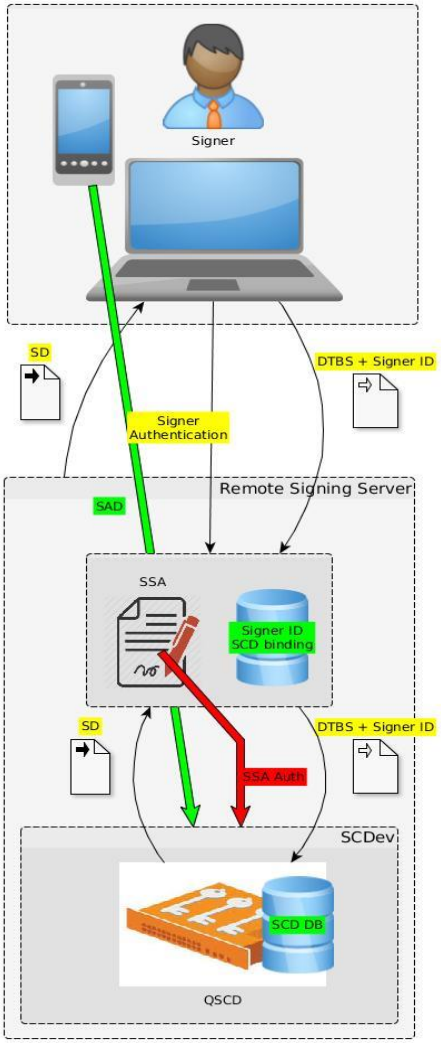

Illustration3: Sole Control Level 2

APPENDIX IV

REFERENCES

- [**eIDAS**] 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. [ONLINE] Available at: https://eur-lex.europa.eu/legal-ontent/EN/TXT/?uri=CELEX:32014R0910. [Accessed 11 June 2018].

- **[Cryptomathic] Cryptomatic. 2018. Signer Overview | Cryptomathic**. [ONLINE] Available at: https://www.cryptomathic.com/products/authentication-signing/signer-centralised-digital-signatures. [Accessed 10 June 2018].

- **[Ascertia] eIDAS Remote Qualified Signatures | SigningHub.com™. 2018. eIDAS Remote Qualified Signatures | SigningHub.com™**. [ONLINE] Available at: https://www.signinghub.com/eidas-remote-signing/. [Accessed 10 June 2018].

- **[MICROSOFT]Justinha. 2018. Virtual Smart Card Overview (Windows 10) | Microsoft Docs**. [ONLINE] Available at: https://docs.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-overview. [Accessed 10 June 2018].

- **[ETSI] ETSI EN 319 401** V2.2.0 (2017-08)**, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers**