Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 4/19

(Certification No.)

Prodotto: *(Product)* **distributed remote Qualified Signature Creation Device (drQSCD) v1.0**

Sviluppato da: *(Developed by)* **I4P-informatikai Kft. (I4P Ltd.)**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(AVA_VAN.5, ALC_FLR.3)

Il Direttore
(Dott.ssa Rita Forsi)
Rita Forsi

Roma, 15 maggio 2019

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

distributed remote Qualified Signature Creation Device (drQSCD) v1.0

OCSI/CERT/SYS/06/2017/RC

Version 1.0

15 May 2019

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	15/05/2019

2 Table of contents

3 Acronyms

AES Advanced Encryption Standard

API Application Programming Interface

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CM Cryptographic Module

CPU Central Processing Unit

DPCM Decreto del Presidente del Consiglio dei Ministri

DTBS/R Data To Be Signed / Representation

EAL Evaluation Assurance Level

ECA External Client Application

eIDAS Electronic IDentification, Authentication and Signature

ETR Evaluation Technical Report

HDD Hard Disk Drive

IT Information Technology

LCA Local Client Application

LCD Liquid Crystal Display

LED Light Emitting Diode

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza (ITSEF)

MPC Multi-Party Computation

MPCA Multi-Party Cryptographic Appliance

MPCM Multi-Party Cryptographic Module

NIS Nota Informativa dello Schema

OCSI Organismo di Certificazione della Sicurezza Informatica

OS	Operating System
PP	Protection Profile
PTRNG	Physical True Random Number Generator
QSCD	Qualified Signature Creation Device
RAD	Reference Authentication Data
RSA	Rivest, Shamir, Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIC	Signer's Interaction Component
SOGIS	Senior Officials Group Information Systems Security
SSA	Server Signing Application
SSH	Secure Shell
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TOTP	Time-based One-Time Password (algorithm)
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
USB	Universal Serial Bus

4 References

4.1 Criteria and regulations

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[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, Official Journal of the European Union L 257, 28 August 2014

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[DEL] “Delivery Documentation: distributed remote Qualified Signature Creation Device (drQSCD)”, version 0.4a, 23 October 2018

[ETR] “drQSCD v1.0” Evaluation Technical Report, v1, 6 March 2019

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, prEN 419 221-5, v0.15, 29 November 2016

[PP-SAM] Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, prEN 419 241-2, v0.16, 11 May 2018

[PRE-CM] “MPCM Preparation Guide”, rev3, 17 January 2019

[PRE-SAM] “MPSAM Preparation Guide”, rev3, 17 January 2019

[ST] “distributed remote Qualified Signature Creation Device (drQSCD)” Security Target, v1.2, 2 May 2019

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA up to EAL4.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “distributed remote Qualified Signature Creation Device (drQSCD) v1.0”, short name “drQSCD v1.0”, developed by I4P-informatikai Kft. (I4P Ltd.).

The TOE is a multi-user, multi-key device, designed to be used as a QSCD to generate qualified electronic signatures and seals according to eIDAS Regulation No 910/2014 [eIDAS] as well as to perform additional supporting cryptographic operations. The TOE is composed by a Cryptographic Module (CM) and a Signature Activation Module (SAM), and is suitable for both Local and Remote use cases.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with AVA_VAN.5 and ALC_FLR.3, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “drQSCD v1.0” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	distributed remote Qualified Signature Creation Device (drQSCD) v1.0
Security Target	“distributed remote Qualified Signature Creation Device (drQSCD)” Security Target, v1.2, 2 May 2019 [ST]
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5 and ALC_FLR.3
Developer	I4P-informatikai Kft. (I4P Ltd.)
Sponsor	I4P-informatikai Kft. (I4P Ltd.)
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 4
PP conformance claim	prEN 419 221-5, v0.15 [PP-CM], prEN 419 241-2, v0.16 [PP-SAM]
Evaluation starting date	11 July 2017
Evaluation ending date	27 March 2019

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE is a multi-user, multi-key device designed to be used as a QSCD to generate qualified electronic signatures and seals according to eIDAS Regulation No 910/2014 [eIDAS] as well as to perform additional supporting cryptographic operations.

For a detailed description of the TOE, consult sect. 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE Architecture

Depending on its configuration, the TOE consists of one or three MPCAs (Multi-Party Cryptographic Appliances). An MPCA comes in the form of a metal, rack mountable box (see Figure 1).

Figure 1 - Physical appearance of an MPCA

In the **Multi-party Configuration**, three identical TOE parts (or MPCAs) operate in a distributed way as a logical whole in order to fulfill the requirements of the Security Target [ST]. If one of the three MPCAs becomes dysfunctional, the other two MPCAs can ensure a limited functionality.

In case of **Standalone Configuration**, the TOE consists of only one MPCA, and that alone fulfills the requirements of the Security Target [ST].

The TOE is composed of two main components inside the physical enclosure of an MPCA which can work together to fulfill different sets of requirements:

- The **Cryptographic Module (CM)** component of the drQSCD is a general-purpose cryptographic module suitable for cryptographic support needed by its legitimate users.

- The **Signature Activation Module (SAM)** component of the drQSCD is a local application deployed within the tamper protected boundary of the drQSCD and implements the Signature Activation Protocol (SAP). It uses the Signature Activation Data (SAD) from a remote signer to activate the corresponding signing key for use in a cryptographic module.

The TOE is suitable for both “Local Signing” and “Remote Server Signing” use cases described in the [PP-CM] Protection Profile.

The “Local” use case (see Figure 2) is aimed at local key owners applying their own electronic signatures or seals. In this use case only the CM functionality of the TOE is used, which performs local cryptographic operations, and associated key management.

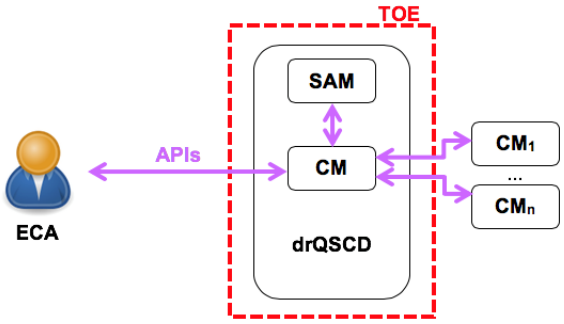

Figure 2 - The TOE in the “Local” use case

These operations can be used by an External Client Application (ECA) to create qualified and non-qualified electronic signatures and electronic seals, as well as to perform additional supporting cryptographic operations, for the local key owner. Examples include TSPs issuing certificates and time-stamps, as well as supporting application services such as e-invoicing and registered e-mail where the service provider uses its own keys to perform a cryptographic function (e.g., sign, encrypt, decrypt).

The “Remote” use case (see Figure 3) is aimed at TSPs supporting requirements for remote signing, or sealing, as specified in [eIDAS]. In this case the inbuilt CM, as well as other external CMs configured to be used (if there are any), and the SAM functionality of the drQSCD together meet the requirements for QSCDs in the context of remote signing, as laid out in Annex II of [eIDAS].

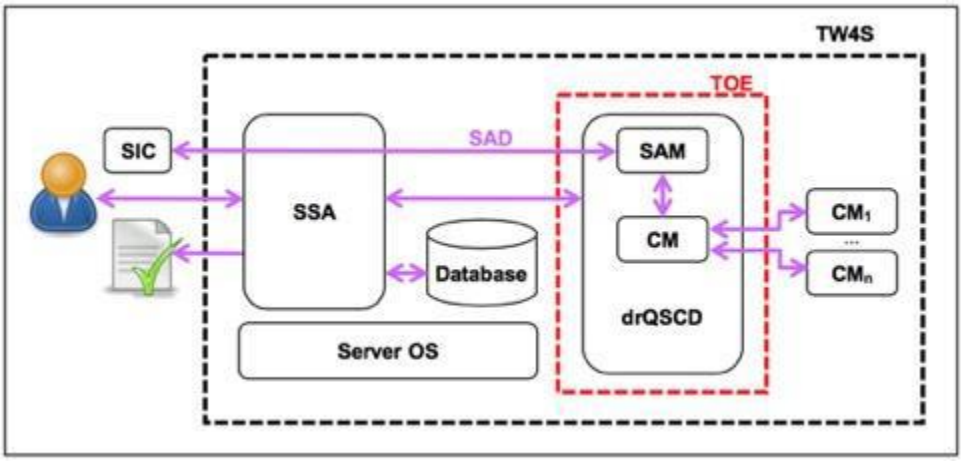

Figure 3 - The TOE in the “Remote” use case

The Signer’s Interaction Component (SIC) is a piece of software and/or hardware, operated on the signer’s environment under its sole control. The Server Signing Application (SSA) uses the drQSCD in order to generate, maintain and use the signing keys.

The CM and SAM components of the TOE provide the following functionalities.

The **CM functionality** includes but is not limited to:

- generating, storing, using, backing up, restoring and destructing symmetric and asymmetric cryptographic keys;
- ensuring the security (confidentiality and integrity) of symmetric keys and asymmetric private keys, and pre-generated primes for RSA key pairs;
- creating qualified electronic signatures and electronic seals;
- performing additional supporting cryptographic operations, such as creation of non-qualified electronic signatures and seals, verification of electronic signatures and seals, cryptographic hash function, keyed-hash message authentication, AES encryption and decryption, symmetric and asymmetric encryption and decryption, key derivation, TOTP one-time-passwords verification;
- supporting of authentication of client applications or authorised users of secret keys, and support of authentication for electronic identification, as identified by [eIDAS];
- allowing the key owners to use TOTP when activating their keys.

The drQSCD can also be configured to generate, store and activate signer's keys in one or more external CMs for speed enhancement or legacy reasons.

The **SAM functionality** includes but is not limited to:

- authenticating the remote signer based on two authentication factors;
- authorising the signature operation,
- activating the signing key within the internal CM functionality (and the external CM if configured).

The SAM functionality of the TOE ensures that the remote signer has sole control of his signature keys for qualified signatures, according to Annex II of [eIDAS].

In case of Multi-Party Configuration, the **MPC functionality** includes but is not limited to:

- generation of RSA key pairs (and the pre-generated primes for them) in a distributed way;
- creation of electronic signatures, using a multi-step signing method;
- decryption of encrypted messages, using a multi-step decrypting method;
- authentication of the end users in a distributed way.

The drQSCD ensures the consistency among the MPCAs (e.g., their databases, internal states).

7.3.1.1 Roles & Available Functions

The CM functionality of the TOE maintains the following roles, associating users with roles:

- *Administrator*: a privileged subject who can perform CM specific management operations, through a local console or the externally available CMAPI, including the following:
    - creating a new account with security attributes for an Administrator (creating the initial Administrator requires entering an installation code);
    - exporting the public component of an RSA key;
    - unblocking access to a blocked key;
    - modifying attributes of keys;
    - audit data export/deletion;
    - backup and restore functions (restore function is under dual control).
- *Key User*: a normal, unprivileged subject who can invoke operations on a key according to the authorisation requirements for the key.
- *Local Client Application* (LCA): application running inside the physical boundary of the MPCA.
- *External Client Application* (ECA): application communicating remotely with one of the MPCA through a network connection.

The SAM functionality of the TOE maintains the following roles:

- *Privileged User*: a user who can perform SAM specific operations, through a local console or the externally available SAMAPI, including the following:
    - creating a new account with security attributes for a Signer;
    - maintaining a Signer's account;
    - creating a new account with security attributes for a Privileged User;
    - creating and modifying the SAM configuration data record and SAM configuration file;
    - Backup and Restore functions;
    - Signer Key Pair Generation.
- *Signer*: a user who communicates remotely with the SAM and is able to perform the following operations:
    - requesting a new RSA key pair generation and assigning it to his/her account;

- establishing or modifying the key Authorisation Data for his/her key;
- signing (utilizing his/her signing key in the CM, transmitting the required data, including the unique user ID, two different authentication factors, the key ID, the key Authorisation Data and one or more DTBS/R);
- maintaining his/her own Signer's account.

7.3.1.2 Authentication and Authorisation

The CM component of the TOE uses a common method for identification and authentication in case of each role: a unique user identifier (sent by the user during authentication) and a static password. The password is checked against the RAD (salted, hashed and encrypted password) stored in the user's account as a security attribute.

The CM blocks the account after a predefined number of consecutive failed authentication attempts, where these administrator configurable numbers can be different for each role.

Before using a secret key in a cryptographic operation, an authorisation or a re-authorisation as a user of the key is always required. The CM blocks the secret key after a predefined number of consecutive failed authorisation attempts.

For the Privileged Users, the SAM component of the TOE uses the same identification and authentication method as the CM: a unique user identifier and a password. For the Signers, the SAM requires two different authentication factors: a password (knowledge-based factor) and a TOTP (possession-based factor). The SAM ensures that all user have only one role, consequently a signer can't be a privileged user.

The SAM blocks the account after a predefined number of consecutive failed authentication attempts. When a signer account has been locked the SAM also suspends the usage of all signing keys of the Signer.

7.3.1.3 Cryptographic Support

The CM component of the TOE ensures the security of its keys for their whole lifecycle. The generic key lifecycle includes the methods by which a key may arrive in the drQSCD (import, generation or restore from backup), resulting in binding of a set of attributes to the key, storage of the key, and finally the ways in which a stored key may then be processed (export, use in a cryptographic function, backup, destruction).

The SAM component of the TOE does not perform cryptographic operations for its users: in particular, it does not generate/store/destruct, export/import, backup/restore, or use user key.

The SAM invokes the internal CM (or the external CM if configured) with appropriate parameters whenever a cryptographic operation for the Signer is required.

The SAM uses different infrastructural keys to protect its stored files and database records, and data transmitted or received via communication channels.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 7.1 of the Security Target [ST]. The most significant aspects are summarized below:

- **Roles, Authentication and Authorisation (CM and SAM)**: for a description of these functions see sect. 7.3.1.1 and sect. 7.3.1.2.

- **Security management (CM)**: The CM Administrator is able to unblock a blocked user account or a blocked key, specify alternative initial value for the “Key Usage” security attribute (“General” or “Signing”), export and delete the local audit and Errorlog file, backup and restore of the CM’s TSF state. The Key User is able to modify the attributes of his/her key.

- **Security management (SAM)**: The SAM implements the following management functions: Signer management, Privileged User management, configuration management, backup and restore functions.

- **Key Security (CM)**: The CM implements the following security functions related to the whole lifecycle of the keys:

    - key import;
    - key generation;
    - key restore from backup;
    - binding of a set of attributes to the key;
    - storage of the key;
    - key export;
    - key usage;
    - key backup;
    - key destruction.

- **Key Security (SAM)**: The SAM does not perform distributed cryptographic operations with Key User’s key and does not delete Key User’s key. The SAM invokes the CM with appropriate parameters whenever a distributed cryptographic operation or a key deletion is required. At the same time SAM performs non-distributed cryptographic operations with infrastructural keys.

- **Access and information flow control (CM)**: The CM enforces the following Security Function Policies:

    - *Key Basics*: Import of secret keys are not allowed. Export of secret key is allowed only for non-Assigned keys with Export Flag=“yes”. Public keys will

always be exported with integrity protection of their key value and attributes. Unblocking access to a key will not allow any subject other than those authorised to access the key at the time when it was blocked. No subject will be allowed to access the plaintext value of any secret key directly or to access intermediate values in any operation that uses a secret key.

  - *Key Usage*: The “Unprotected Flag” and “Operational Flag” key attributes can be changed only by the Key User. The Authorisation Data can be changed only by the Key User. Only subjects with current authorisation for a specific secret key are allowed to carry out operations using the plaintext value of that key. Only cryptographic functions permitted by the secret key’ s Key Usage attribute shall be carried out using the secret key.

  - *Backup*: Only Administrator are able to perform the backup or restore function (restore function is under dual control). All backups are signed and encrypted. Consequently, any backup preserves their integrity and confidentiality.

- **Access and information flow control (SAM)**: The SAM enforces the following additional SFPs:

  - *Privileged User Creation*: Only a Privileged User is able to create a new Privileged User’s account.

  - *Signer Creation*: Only a Privileged User can create a new Signer account.

  - *Signer Maintenance*: Only a Privileged User or the owner Signer is able to delete a key identifier and a public key from a Signer’s account.

  - *Supply DTBS/R*: Only an authorised Privileged User is able to supply the DTBS/R on behalf of the Signer.

  - *Signer Key Pair Generation*: Only a Signer can request a new RSA key pair generation and assign it to his/her account. Only a Privileged User can generate a new RSA key pair and assig it to a Signer’s account.

  - *Signing*: Only a Signer can instruct the SAM to perform a signature operation with his/her own key.

  - *SAM Maintenance*: Only a Privileged User can carry out the SAM Maintenance related commands, transmitting information to the SAM to manage roles and configuration.

  - *Signer*: The order of “Signer” related commands is regulated and controlled.

  - *Privileged User*: The order of “Privileged User” related commands is regulated and controlled.

- **Data protection (CM)**: The CM ensures the security of its TSF data, including the following:

  - *Self-tests*: to demonstrate the correct operation of the TSF.

  - *Secure failure*: the capability to preserve a secure state when the different types of failures occur.
  - *Tamper protection*: tamper detecting and tamper response capabilities.

- **Data protection (SAM)**: The SAM is implemented as a local application within the same physical boundary as the CM. Consequently, the CM provides its security services also for protecting the SAM.
- **Audit (CM and SAM)**: The CM and the SAM audit all security related events. Every audit record includes a reliable time stamp, subject identity (if applicable), identifier of the related CM or SAM and a human readable descriptive string about the related event.
- **Communication protection (CM)**: The CM implements and enforces:
  - a secure channel based on TLS protocol, for communication with ECAs;
  - a secure channel based on TLS protocol, for communication with Administrator, through SSA;
  - a secure channel based on SSH protocol, for communication with Administrators, using the console command interface in the provided limited shell;
  - a direct channel for communication with Administrators, using the console command interface with a physical keyboard;
  - a secure channel based on TLS protocol, for internal communication among MPCAs.
- **Communication protection (SAM)**: The SAM implements and enforces:
  - a secure channel based on TLS protocol, for communication with Privileged Users, through the SSA;
  - a secure channel based on SSH protocol, for communication with Privileged Users, using the console command interface in the provided limited shell;
  - a secure channel based on the proprietary SAP protocol;
  - a direct channel for communication with Privileged Users, using the console command interface with a physical keyboard.
- **Distributed structure**: In case of multi-party configuration, this security function based on the distributed structure of the drQSCD ensures the following:
  - distributed cryptography;
  - secret sharing;
  - consistency protection;

- fault tolerance.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage of the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims strict conformance to the following Protection Profiles:

- Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, prEN 419 221-5, v0.15, 29 November 2016 [PP-CM]

- Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, prEN 419 241-2, v0.16, 11 May 2018 [PP-SAM]

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Considering that the Security Target claims strict conformance to the Protection Profiles prEN 419 221-5 [PP-CM] and prEN 419 241-2 [PP-SAM], all the SFRs from such PPs are also included, with the exception of the following SFRs from [PP-SAM]:

- FCS_RNG.1. (according to Application Note 40 of [PP-SAM])

- FPT_PHP.1 and FPT_PHP.3 (according to Application Note 67 of [PP-SAM])

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 6 March 2019 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 27 March 2019. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operating environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "drQSCD v1.0" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with AVA_VAN.5 and ALC_FLR.3, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with AVA_VAN.5 and ALC_FLR.3.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass

Assurance classes and components		Verdict
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Systematic flaw remediation	*ALC_FLR.3*	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Advanced methodical vulnerability analysis	AVA_VAN.5	Pass

Table 1 – Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product “drQSCD v1.0” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the [ST] are respected.

This Certification Report is valid for the TOE in the evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([DEL], [PRE-CM], [PRE-SAM]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

The delivery steps and the procedures that are necessary to maintain security when distributing the TOE to the consumer are described in sect. 4 of [DEL].

The protection applied corresponds to the nature of the product (software and hardware). The following procedures ensure the security during the delivery steps:

- The TOE is moved into its shipment box, sealed using security tape and labelled.
- Contracted distribution service ships the TOE to the customer, who checks the tamper evident seals on the shipment box.
- If the box was not tampered, the customer unpacks and checks the tamper evident seals and cables on the TOE.
- If the TOE was not physically tampered, the customer starts the TOE and checks the cryptographic checksum and the serial number on the screen. The serial number and cryptographic checksum are received earlier via e-mail.
- Customer fills the acceptance checklist, signs it and sends it back to I4P, were the customer gets registered for guarantee and flaw remediation.
- If any of the tamper seals, serial numbers and cryptographic checksum control show a tamper event, the TOE should be sent back to I4P for inspection.

9.2 Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- “MPCM Preparation Guide”, rev3, 17 January 2019 [PRE-CM]
- “MPSAM Preparation Guide”, rev3, 17 January 2019 [PRE-SAM]

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “distributed remote Qualified Signature Creation Device (drQSCD) v1.0”, developed by I4P-informatikai Kft. (I4P Ltd.).

The TOE is referenced in the Security Target [ST] as “drQSCD version 1.0”.

The evaluated configuration of the TOE includes the following items:

- one or three MPCAs;
- guides, which provide information on the evaluated configuration and refers the reader to the relevant product guides to enable her/him to install and operate the TOE correctly.

All MPCAs include the following items:

- a metal, rack mountable box with external power supply unit;
- physical interfaces of the MPCA:
    - network interfaces (3 Ethernet Interfaces using TCP/IP);
    - 2 USB interfaces for local console administration and backup purposes;
    - display connector for a local display;
    - power connector;
    - chargeable battery holder and battery health LED;
    - Power/Reset and Tamper/Confirm buttons;
    - LED indicators;
    - LCD display for version information.
- the internal hardware:
    - motherboard and CPU from the OS’s certified list;
    - HDDs that maintain the MPCA’s software and data (files and data records);
    - a Tamper Detection Module that automatically deletes sensitive information and shut downs the appliance when trying to open the appliance;
    - different tamper sensors;
    - PTRNG that provides true random seed for different cryptographic operations (e.g., key generations).
- the internal software:

- the hardened OS (based on the CC certified Red Hat Enterprise Linux, Version 7.1);
- limited shell;
- Multi-Party Cryptographic Module (in case of multi-party configuration, the three MPCAs jointly provide the CM functionality);
- Signature Activation Module local client application (in case of multi-party configuration, the three SAM LCAs jointly provide the SAM functionality);
- OpenSSL FIPS Object module v2.0.16, the FIPS 140-2 validated version of OpenSSL.

For more details, please refer to sect. 1.4 of the Security Target [ST] and to sect. 2 of [DEL].

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL4, augmented with AVA_VAN.5 and ALC_FLR.3, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage and level of detail;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

For the execution of the testing activities the Developer provided the TOE to the Evaluators in the following two configurations:

- three physical MPCAs for independent tests and vulnerability assessment;
- one virtual vMPCA for repeating the Developer tests.

The Evaluators installed the TOE applying the installation procedure described in [PRE-CM] and [PRE-SAM] (“Setting up the system”) which provide detailed information about the minimum system requirements for secure installation of the TOE and the installation steps.

After the installation, the Evaluators checked the status of the TOE and verified that it was installed properly and in a known state.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer performed manual and automated tests to verify the functionality of the TOE. The tests cover all security functions and aspects of the TSF.

The Developer used the following test suites and tools:

- Maven
- Java
- Red Hat Linux

The Developer performed extensive testing on the TOE, at subsystem, module and module interface level. The tests are performed by the Developer through execution of test scripts using an automated and distributed system. Test tools and scripts are extensively used to verify that the tests return expected values.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements SFR and the TSFI described in the functional specification.

All parameter choices, also for the module interface level, have been addressed at least once. All the cryptographic operations with keys of all key sizes have been tested at least once. All boundary cases identified have been tested explicitly. The near-boundary conditions have been covered probabilistically.

11.2.3 Test results

The Evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the Developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the Evaluators

Therefore, the Evaluators have designed independent testing to verify the correctness of the TSFI.

The Evaluators focused on the following aspects of the TOE security functions/TSFI when selecting the Developer test cases to repeat:

- Test permissions to sign by running the sign command with correct and incorrect parameters, with one and more proprietary keys, and with different users in the Admin and User roles.
- Test MPCM's decrypt function with good and bad input parameters, with particular emphasis on padding. Encryption is done with OpenSSL.
- Test the `mpc_passwd` command with correct and incorrect parameters.
- Test `login` command with correct and incorrect parameters and passwords.

The Evaluators verified the actual test results and found that they were consistent with the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE configurations already used for the functional tests activities, verifying that the test configurations were consistent with the version of the TOE under evaluation.

In a first phase, the Evaluators looked for possible vulnerabilities in publicly available books and articles which relate to the threats documented in the Security Target [ST]. Then the Evaluators compared the information found with the possible threats of the TOE, identifying some potential vulnerabilities applicable to the TOE in its intended environment.

In the second step, the evaluator looked for all the vulnerabilities on the Internet which are related to types of products similar to the TOE. Browsing the Internet, the Evaluators used

keywords (versions of vulnerable software components) to select the best hits, and particularly investigated specialist publications, research papers, and conference proceedings on professional sites.

The Evaluators also examined the TOE with a commercial vulnerability scanner software.

The Evaluators then performed an advanced methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

The Evaluators' analysis focused on the following aspects, identifying several potential vulnerabilities:

- session management;
- command management and input validation of API interfaces;
- roles management;
- escape from limited shell;
- SSH vulnerabilities;
- backup/restore function.

The Evaluators analysed in detail the potential vulnerabilities identified in the previous steps to verify their effective exploitability in the TOE operating environment.

Based on the potential vulnerabilities identified in the previous analysis, the Evaluators devised several attack scenarios and penetration tests to try to exploit these vulnerabilities in the TOE's operational environment, considering an High attack potential.

At the end of all the penetration testing sessions, the Evaluators could conclude that no attack scenario with potential High or lower can be completed successfully in the operating environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively. They have not identified residual vulnerabilities, i.e., vulnerabilities that could be exploited only by an attacker with attack potential beyond High.