První certifikační autorita, a.s.

Policy

for Issuing Qualified Signatures and Seals

Creation Devices

The Policy for Issuing Qualified Signature / Seal Creation Devices is a public document, which is the property of První certifikační autorita, a.s., and has been prepared as integral part of comprehensive security documentation. No part of this document may be reproduced without the written consent of the copyright holder.

Version 1.0

CONTENT

Table 1 – Document history

Version	Date of release	Approved by	Comments
1.0	25 April 2023	CEO of První certifikační autorita, a.s.	First release.

1 INTRODUCTION

The document Policy for Issuing Qualified Signatures and Seals Creation Devices (further also Policy) is prepared by První certifikační autorita, a. s., (further also as I.CA) and relates to issuing of Qualified Signature / Seal Creation Device service (further also as QSCD and Service).

Requirements concerning QSCD are set out in **Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.**

1.1 Overview

Policy is divided into ten basic chapters and these are briefly introduced in the following list:

- Chapter 1 defines the requirements for QSCD, describes how to publish information;
- Chapter 2 describes the activities related to QSCDs in their acquisition, personalization, handover to end users and also activities of the end user;
- Chapters 3 to 6 describe acquisitions in physical, procedural, personnel and technical security areas;
- Chapter 7 is focused on the audit records issue;
- Chapter 8 defines a set of logged events and their storage;
- Chapter 9 includes business and legal issues;
- Chapter 10 contains list of annexes.

Note: This is English translation of the Policy; Czech version always takes precedence. I.CA attests that the translation is not materially different to the original.

1.2 Policy administration

This Policy is administrated by I.CA.

1.3 Definitions and acronyms

Table 2 – Definitions and acronyms

Term	Explanation
bit	from English binary digit – a binary system digit – the fundamental and the smallest unit of information in digital technologies
CA	Certification authority
Classified Information Protection Act	the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended
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
electronic seal	advanced electronic seal or recognized electronic seal or qualified electronic seal under trust services legislation
electronic signature	electronic signature or advanced electronic signature or qualified electronic signature or recognized electronic signature under valid trust services legislation
key pair	unique data for electronic signature creation together with corresponding data for electronic signature verification
Labour Code	the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended
root certificate	self-signed certificate of certification authority on the top of hierarchical structure of certification authorities
PIN	Personal Identification Number, user authentication code/number
PKI	Public Key Infrastructure
private key	unique data to create electronic signature
public key	unique data to verify electronic signature
PUK	Personal Unlocking Key, authentication code/number for unblocking user's PIN (blocked after three incorrect PIN entries).
QSCD	Qualified Signature / Seal Creation Device
qualified certificate for electronic signature	certificate defined by valid trust service legislation
qualified electronic signature creation device	electronic signature creation device that meets the requirements defined in Attachment 2 to eIDAS
qualified trust service	qualified trust service as defined in eIDAS
RA	registration authority
self-signed certificate	public key certificate signed by private key, forming paired data with that public key
SSCD	Secure Signature Creation Device
Classified Information Protection Act	the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended
trust service legislation	the Czech Republic's legislation related to electronic transaction trust services and the eIDAS Regulation
ZOOÚ	current personal data protection legislation

1.4 Publication of information

The basic addresses (also as the Information Addresses) for obtaining information about První certifikační autorita, a.s., are as follows:

- Registered office:

  První certifikační autorita, a.s.
  Podvinný mlýn 2178/6
  190 00 Praha 9
  The Czech Republic
- Website: http://www.ica.cz;
- Registered offices of the registration authorities.

Electronic address for contact between general public and I.CA is info@ica.cz, data box of I.CA ID is a69fvfb.

Contact addresses mentioned above are published on website or on the registered offices of the registration authorities. Registration authority employees, including contract clients, are also obligated to share this information with public.

2 QUALIFIED SIGNATURE / SEAL CREATION DEVICE

Qualified Signature / Seal Creation Devices issued to the end user by I.CA are plastic cards containing chip with operating system STARCOS 3.7 eIDAS C1 produced by Giesecke & Devrient GmbH, meeting the eIDAS requirements for these specific devices.

Activities related to issuing of QSCDs are performed using a dedicated information system with PKI-based authentication (further System).

2.1 Obtaining QSCD from the supplier

Inquiry for QSCD delivery sent by I.CA to the supplier contains:

- Specification of the required quantity;
- Specification of smart card material;
- Specification of printing;
- Requirement that QSCD must be listed in the list of SSCD/QSCD devices of any EU member country with validity period at least two more years;
- Possibly the request for extension of contactless communication interface.

After mutual agreement of smart card final form (design, chip location), the production of the required quantity follows. Finished smart cards are then with the protocol personally accepted at the supplier’s registered office by the I.CA employee, transported to the I.CA storage and registered in the System. A detail description of the procedures performed to obtain QSCDs from a supplier is provided in the internal documentation.

2.2 QSCD chip punching

If a punching for format enabling the placement of the chip part with contacts in a USB token or in small USB readers (so-called punching) is required, the agreed number of smart cards is sent to the processing company through the transport company. Posting is registered to the

System. Processing company make the punching, chips are sent back and acceptance is registered to the System. A detailed description of the procedures related to the performed chip punching from the smart card format is written in the I.CA internal documentation.

2.3 Personalization

Operating procedures performed as part of personalization process are described in detail in internal documentation.

2.3.1 Setting of the request

The authorized I.CA employee defines in the System the customer profile containing the parameters necessary for personalization of QSCD batch. Based on selected customer profile, each QSCD is assigned by unique 16-digit identification number containing the code of this profile in the second four digits. The result is the creation of a personalization file, containing all the necessary information.

2.3.2 QSCD transport to the operating site

The QSCD personalization process itself is performed at the I.CA operating site. Security of this process is described in Chapter 3.1. The authorized I.CA employee will check if the required number of QSCDs is available at the operating site. If there is not required number of QSCDs at the operating site, its transport from I.CA storage must be provided (by the transport company or by employee of I.CA). Transfer is registered in the System.

2.3.3 Implementation

During the personalization, no end user private keys are generated on the QSCD, these are generated by the end user only in the phase of using the QSCD – see in Chapter 2.5.2. The authorized employee of the operating site obtains relevant personalization file from the System (see in Chapter 2.3.1), which will be saved in the personalization device. All information contained in personalization file are stored on the chip, eventually on plastic body of every QSCD (printing), while personalized.

QSCDs are usually personalized without initialization data i.e., PIN and PUK. In this case, end user of QSCD is asked to enter the PIN and PUK when QSCD is used for the first time. In case, when PIN and PUK are generated, these are printed on sheet of paper, where they are sealed with certified security sticker.

Personalized smart cards, where appropriate together with sheets of paper with data sealed by certified security stickers, are transported back to the I.CA storage by transport company or by I.CA employee. Transport is registered in the System.

2.4 Handover to the end user

End user can buy QSCD in e-shop or in RA.

2.4.1 Buying in e-shop I.CA

When buying in e-shop I.CA QSCD is sent to end user by postal delivery service together with acceptance protocol (end user signs it and sends it back by postal delivery service or scanned by e-mail) and QSCD can by personalized (with printing) or not personalized. In both cases QSCD can be:

- Initialized i.e., PIN/PUK are set and together with QSCD and acceptance protocol the letter containing among others PIN/PUK information under security sticker is sent; or
- Not initialized i.e., PIN/PUK are not set and together with QSCD and acceptance protocol installation instructions, where among others the procedure of setting PIN/PUK is described, are sent.

2.4.2 Buying in RA

To enable in-RA purchases the required number of QSCDs is distributed by I.CA employees, on the basis of acceptance protocol, to the registered offices of the registration authorities (registered in System). Here the QSCDs are stored in consignment stock. QSCD is always not personalized (without printing) and can be:

- Initialized i.e., PIN/PUK are set and together with QSCD and acceptance protocol the letter containing among others PIN/PUK information under security sticker is handed over;
- Not initialized i.e., PIN/PUK are not set and together with QSCD and acceptance protocol installation instructions, where among others the procedure of setting PIN/PUK is described, are handed over.

End user, when taking over the QSCD, signs acceptation protocol.

2.5 Using QSCD by the end user

2.5.1 Installation and initialization of QSCD

After receiving QSCD and before its routine use, following actions must be performed by the end user:

- Installation of the appropriate smart card reader driver. If the corresponding driver is not automatically installed after connecting the USB smart card reader, the installation must be performed manually. It is possible to obtain appropriate driver on the website https://ica.cz/drivers;
- Downloading the current version of the I.CA Secure Store application from the website https://ica.cz/download-application;
- Installation of I.CA Secure Store application. Procedure is described in the current version of installation guide available on website https://ica.cz/download-application;
- If the smart card has been personalized without initialization data, it is necessary to initialize the smart card – i.e., to enter PIN (six to eight digits) and PUK (eight digits).

2.5.2 Using QSCD

After finishing the tasks mentioned in chapter 2.5.1, QSCD is ready for routine usage, including its management. Procedures for administration, key pair generation (public and private key), creating certificate request and certificate installation are described in current user guide on the website https://ica.cz/download-application.

2.6 Check of listing used QSCD in the EU list of SSCD/QSCD devices

Authorized I.CA employee checks monthly the EU list of SSCD/QSCD devices whether the used QSCDs (see beginning of Chapter 2) are still listed. Performance of the check is recorded in I.CA billing system in a table established for that purpose. If there is any change the authorized I.CA employee demonstrably informs the guarantor of certificate issuing and the security manager of I.CA

2.7 Expiration of used QSCD record in the EU list of SSCD/QSCD devices

If the QSCD record in the EU list of SSCD/QSCD devices expires during validity period of the certificate the following procedure as similar to the detection of private key duplicity (the certificate is revoked, end user is offered to buy other QSCD and new certificate is issued free of charge).

3 PHYSICAL CONTROL

3.1 I.CA – operating site

Basic rules for operating site security are described below. Specific physical, procedural and personal countermeasures implemented for operating site security are detailed in internal documentation.

3.1.1 Site location and construction

Processes, related to smart card personalization (see Chapter 2.3.3), are made in operating site buildings, situated in geographically different locations, which are also different from the site of the company headquarters, the business and development sites, the registration authority sites and the points of sale.

Devices intended for QSCD personalization are situated on reserved premises of operating sites. These premises are secured in a manner similar to that required by the Classified Information Protection Act for the ‘Confidential’ category secure areas.

3.1.2 Physical access

Physical access to the place where personalization of QSCD is performed is protected with mechanical and electronic features. Buildings are protected with intrusion alarm system (IAS), alarm receiving center (ARC) and, as may be the case, a special system to monitor movement of persons and vehicles. Details are described in internal documentation.

3.1.3 Power

The supply of electricity is backed up with a UPS (Uninterruptible Power Supply) and a diesel unit.

3.1.4 Water exposures

All Services are so located as to ensure they cannot be flooded with a 100-year flood. Where relevant operating sites have water ingress sensors to detect heating water leakage or rainfall leakage through the roof (as a result of heavy rains).

3.1.5 Fire prevention and protection

The buildings of the operating sites have electronic fire alarm system (FAS) connected to alarm receiving system. Fireproof insulation is installed in the entrance doors with fireproof insert, to the restricted areas in which the Services are situated. Fire extinguishers are fitted in these areas.

3.1.6 Media storage

Smart cards are stored in secure area, where the devices for personalization of this smart cards are placed – see Chapter 3.1.1.

3.2 I.CA storage

If QSCDs are stored in the I.CA storage, these are physically secured areas with access allowed only to authorized I.CA employees. Physical, procedural and personal countermeasures, implemented to secure these areas, are described in internal documents.

4 PROCEDURAL SECURITY

4.1 Trusted roles

Activities related to QSCD personalization are carried out by I.CA employees appointed to trusted roles. These trusted roles and their responsibilities are described in internal documentation.

4.2 Identification and authentication

Employees participating on Service providing and on System operations are equipped by identification and authentication data for those components which are necessary for their jobs.

5 PERSONNEL SECURITY

5.1 Qualification, experience, and clearance requirements

I.CA’s trusted role employees are selected and hired using the following criteria:

- Clean criminal record – statement of criminal conviction records or affirmation is required;

- Bachelor’s or master’s degree in an accredited university program and ICT job experience of three years or longer, or secondary education and ICT job experience of five years or longer, of which at least one-year job experience in the provision of trust services;
- Knowledge in public key infrastructure and information security.

Any other I.CA employee taking part in providing Service is accepted using the following criteria:

- Bachelor’s or master’s degree in an accredited university program, or secondary education;
- Basic orientation in public key infrastructure and information security.

5.2 Background check procedures

The sources of information about all I.CA employees are:

- The employees themselves;
- Persons familiar with a particular employee;
- Public sources of information.

Initial information is provided by employees at job interviews, and this information is updated at periodic appraisal interviews with the manager during employment.

5.3 Sanctions for unauthorized actions of employees

If an employee is detected to have been performing unauthorized activity, the employee is subject to the procedure described in internal documentation and governed by the Labour Code (this process does not prevent criminal prosecution if the unauthorized activity exhibits that degree of gravity).

5.4 Independent contractor requirements

I.CA may or must procure some activities from independent contractors. These business relations are regulated in bilateral business contracts. Contractual penalties are applied for a breach of the obligations or duties specified in the said documents, or the contract with the contractor in breach is terminated immediately.

6 TECHNICAL SECURITY

6.1 QSCD

Table 3 – Parameters and evaluation

Card / parameter	Starcos 3.5*	Starcos 3.7**
Chip	Infineon M7820	Infineon SLC52GDA448
EEPROM	do 128 kB	448 kB
Maximum key size	4096 bits/RSA 521 bits/ECC	4096 bits/RSA 384 bits/ECDSA
Smart card certification	Common Criteria EAL 5+, ALC_DVS.2, AVA_VAN.5	Common Criteria EAL 6+, ALC_FLR.1
OS certification	Security function Common Criteria EAL 4+, AVA_VAN.5	Securityx function Common Criteria EAL 4+, AVA_VAN.5

* No longer issued.

** Certified both for qualified electronic signature and qualified electronic seal.

6.2 Computer security

Security level of used components is defined by technical standards.

6.3 Network security

Dedicated System neither personalization devices are not directly accessible from the public Internet and they are among others protected by firewall.

7 AUDIT RECORDS

7.1 Types of events recorded

In the System, there are events coherent with its activity, particularly:

- System startup and shutdown;
- Startup and shutdown of the audit functions;
- Changes of audit parameters;

- Actions taken while audit record repository errors;
- All System access attempts.

The records in audit file are containing following parameters:

- Date and time of event;
- Type of event;
- Identity of the entity, which is responsible for that action.

All audit records are made, kept and processed to the extent as necessary, while preserving the proof of origin and maintaining integrity, availability, confidentiality and time authenticity.

The auditing system is designed and run in a manner ensuring audit data integrity, sufficient space for audit data, automatic non-rewriting of the audit file, user-friendly presentation of audit records, and audit file access limited to the defined users only.

7.2 Retention period of audit log

Unless the relevant legislation provides otherwise, audit records are kept for a minimum of 10 years of the day they are made.

7.3 Protection of audit log

Audit logs are stored in a manner ensuring they are protected against change, stealing and destruction (willful or accidental).

Audit records are stored in two copies. These audit records are saved on a medium each month or more frequently and this medium is kept outside the operating premises of I.CA.

The protection of the aforesaid types of audit records is described in internal documentation.

7.4 Audit log backup procedures

Audit records are backed up similarly to how other electronic information is backed up.

7.5 Audit collection system

The audit record collection system is an internal from the view of information systems.

8 INFORMATION AND DOCUMENTATION STORAGE

Information and documentation storage at I.CA, is in accordance with requirements of the legislation for trust services.

8.1 Types of stored information and documentation

I.CA is storing types of information and documentation mentioned bellow (in electronic or printed version), which are connected with QSCD issuing service, above all:

- Application software, operating and security documentation;
- Records about manipulation with QSCD (for example acceptance, transfer, storage, etc.).

8.2 Information and documentation retention period

Information due to Chapter 8.1 and other documentation are stored in accordance with Chapter 7.2.

Information and documentation archive procedures are described in internal documentation.

8.3 Protection of documentation and information archive

The premises where information and documentation are stored are secured in a manner based on requirements of risk analysis results and the Classified Information Protection Act.

The procedures to protect the stored records are regulated by internal documentation.

8.4 Requirements for time stamp usage for information and documentation retention

If time stamps are used, they are qualified electronic time stamps issued by I.CA.

8.5 Information and documentation archive backup procedures

Information and documentation archive backup procedures are described in an internal documentation.

8.6 Archive information and documentation collection system

Records are stored at a place designated by COO of I.CA.

Internal documentation regulates how both electronic and printed records are prepared for storage and stored. Records are kept of collecting the records.

8.7 Procedures to obtain and verify information and documentation

Stored information and records are placed at sites designated therefore and are accessible to:

- I.CA employees if they need to have such an access for their job;
- Authorized supervising and inspection entities and law enforcement authorities if required by legislation.

A written record is made of any such permitted access.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 QSCD issuance fees

The fees for QSCD issuance are given in the current price list, which is available on the web information address of I.CA.

9.1.2 Other fee establishments (incl. refunds)

I.CA is authorized to set a different QSCD issuance fee for individually concluded contracts.

9.2 Financial responsibility

9.2.1 Insurance coverage

I.CA represents it holds a business risk insurance policy that covers financial damage.

I.CA has drawn an employee liability insurance policy for each employee, with a scope of coverage as determined by the company's board of directors.

9.2.2 Other assets and assurances

I.CA represents it has available financial resources and other financial assurances sufficient for providing the Services given the risk of a liability for damage claim.

See the Annual Report of První certifikační autorita, a.s., published in Commercial Register for detailed information on the company's assets.

9.3 Confidentiality of business information

9.3.1 Account of confidential information

I.CA's confidential information covers any information other than public information and other than that published in the manner pursuant to Chapter 1.4, including:

- I.CA's business information;
- Any internal information and documentation;
- Any personal data.

9.3.2 Information not within the scope of confidential information

Public information is only the information designated as public and published in the manner pursuant to Chapter 1.4.

9.3.3 Responsibility for protection of confidential information

I.CA employee who comes in contact with confidential information may not disclose the same to a third party without consent of CEO of I.CA.

9.4 Privacy of personal information

9.4.1 Privacy plan

I.CA protects personal data and other non-public information in accordance with the relevant legislation, that is ZOOÚ and GDPR in particular.

9.4.2 Information treated as private

Personal information is common personal data subject to protection in the sense of legal norms.

I.CA employees or the entities defined by valid legislation that come into contact with personal data must maintain confidentiality of these data and the security controls the disclosure of which would put the security of these data at risk. The confidentiality duty survives the termination of employment or other similar relationship, or the completion of pertinent work.

9.4.3 Information not deemed private

Any information outside the scope of relevant legislation, is not considered as confidential.

9.4.4 Responsibility to protect private information

CEO of I.CA is responsible for the protection of personal data.

9.4.5 Notice and consent to use private information

I.CA deals with the notifying of personal data use and consents to personal data processing in accordance with the relevant legislation.

9.4.6 Disclosure pursuant to judicial or administrative process

I.CA discloses personal data for judicial or administrative purpose in accordance with the relevant legislation, all personal data are subject to protection within the meaning of applicable legislation.

9.4.7 Other information disclosure circumstances

I.CA provides access to personal data strictly as regulated in relevant legislation.

9.5 Intellectual property rights

This Policy, all related documents, the website content and the procedures facilitating the operation of the systems providing trust services are copyrighted by První certifikační autorita, a.s., and are important know-how thereof.

9.6 Amendments

9.6.1 Amending procedure

This procedure is a controlled process described in an internal documentation

9.6.2 Amending notification procedure

The release of a new document version is always notified as published information (see Chapter 1.4).

9.7 Governing law

The business of První certifikační autorita, a.s., is governed by the laws of the Czech Republic.

9.8 Compliance with applicable law

The QSCD issuing is in compliance with legislative requirements of the Czech Republic and EU and also with relevant international standards.

9.9 Force Majeure

I.CA may not be held liable for breaching its obligations if it is a result of force majeure, such as major natural disaster, major disaster caused by human activity, strike or civil unrest always followed by the declaration of a situation of emergency, or the declaration of a state threat to the state or a state of war, or communication failure.

10 ANNEX

1. Instructions_for_installation.pdf