Ministerie van Volksgezondheid,
Welzijn en Sport

Certification Policy

Health CSCA

Version 1.0

Date June 2021

Publisher’s imprint

Directie Informatiebeleid - CIO

Address:
Parnassusplein 5 2511 VX Den Haag

Version	1.0
Organisation	Ministerie van Volksgezondheid, Welzijn en Sport
Author	Policy Authority of the Health CSCA
Number of pages	30

Contents

1 Introduction

The Ministry of Health Welfare and Sport (VWS), Kingdom of the Netherlands, established the Country Signing Certificate Authority for Health purposes (CSCA Health) in 2021.

The purpose of the CSCA Health is to issue Document Signer Certificates (DSCs) within the EU Digital COVID Certificate (DCC) Gateway framework. The DCC framework is established to implement the EU Digital COVID Certificate, which is subject to the provisions laid down in Regulation 2021/953 of 14 June 2021 and its implementing decisions. The Public Key Certificate Governance document (Annex IV to the Commission Implementing Decision), issued by the European Commission, operationalizes Regulation 2021/953, and establishes the trust relationships that apply within the DCC framework.

The CSCA functions as a trust anchor, so that relying parties can use the CSCA certificate to validate the authenticity and integrity of the issued DSCs.

1.1.1 Objective of the Certificate Policy (CP)

This document states the policies of the CSCA Health, to ensure the establishment of a trust relationship between the participants within the DCCG. It includes a description of the requirements for the creation, issuance and revocation of certificates.

The format of this CP conforms as much as possible to the RFC 3647 framework.

1.1.2 Relationship CP and CPS

This CP sets forth the requirements and standards imposed by the PKI and legal context in which it operates. The CP is not subject to confidentiality requirements.

The Certificate Practice Statement (CPS) states how the CSCA and other participants implement procedures and controls to meet the requirements stated in the CP. The CPS is classified Dep.V. and its confidentiality is protected in accordance with its classification.

1.2 Document name and identification

The official name of this document is "Country Signing Certificate Authority for Health purposes – Kingdom of the Netherlands – Certification Policy".

1.3 PKI participants

This section describes the participants and overall operation of the PKI within which this CSCA operates.

The secure and trusted exchange of signature keys for EU digital COVID certificates (DCCs) between participants is realized by the EU Digital COVID Certificate Gateway

(DCCG), which acts as a central repository for the public keys. The trust model of the DCC framework is a PKI. Each Member State maintains one or more Country Signing Certificate Authority (CSCA) certificates, which are relatively long lived. The CSCA issues public key certificates for the national, short lived, Document Signers (i.e. signers for DCCs), which are called Document Signer Certificates (DSCs). The CSCA acts as a trust anchor such that relying parties can use the CSCA certificate to validate the authenticity and integrity of the regularly changing DSC certificates. A DSC is the public key certificate of a Member State's Document Signing Authority (DSA).

1.4 Certificate usage

1.4.1 Acceptable uses

- The CSCA shall only be used to sign and verify DSCs.
- DSCs shall only be used to sign and verify DCCs.

1.4.2 Prohibited uses

- Any use of the CSCA and DSC that is not expressly permitted under §1.4.1 is prohibited.
- Any use of the CSCA and DSC that breaches the provisions of this CP is prohibited.
- The use of production keys for testing purposes is prohibited. The use of testing keys for production purposes is prohibited. This applies to the CSCA and DSAs.

1.5 Policy administration

This policy is administered by the Ministry of VWS, Kingdom of the Netherlands.

A Policy Administrator has been appointed within VWS. The Policy Administrator is responsible for performing operational tasks within the CSCA.

1.6 Acronyms and definitions

1.6.1 Acronyms

Acronyms	**Definition**
BBN2	Baseline security level 2.
BIO	Baseline Informatiebeveiliging Overheid
DCC	EU Digital COVID Certificate. A digital document, signed by the DSA, that contains vaccination, test or recovery information.
DCCG	EU Digital COVID Certificate Gateway
DN	Distinguished Name
DSA	Document Signing Authority (a system that is allowed to sign DCC's) with its DSC private key
DSC	Document Signer Certificate

HSM	Hardware Security Module
MS	Member State
NB_{CSCA}	National Backend Country Signing Certificate Authority
NB_{UP}	National Backend Upload Certificate
PA	Policy Authority
PKCG	Public Key Certificate Governance document (Annex IV of the Commission Implementing Decision)
VOG	Certificate of Conduct, issued by the Dutch Minister of Legal Protection
VWS	(The Ministry of) Health Welfare and Sport (of the Kingdom of the Netherlands)

1.6.2 Definitions

Capitalised terms used in this document which are listed in the table below shall be given the meaning assigned to them in this table.

Term	**Definition**
Commission Implementing Decision	'Commission Implementing Decision laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council'
Ministry of VWS	The Ministry of Health Welfare and Sport (VWS), Kingdom of the Netherlands

2 Publication and repository

2.1 Repositories

2.1.1 Dutch National Public Key Directory

The CSCA certificate and its associated CRL shall be made available on the Dutch National Public Key Directory (NPKD): https://www.npkd.nl/csca-health.html
The aforementioned repository is administered by the Judicial Information Service, Kingdom of the Netherlands.

2.1.2 DCCG

The CSCA certificate and its associated CRL shall be made available to the DCCG during the onboarding procedure.
The aforementioned repository is administered by the DCCG operator, and consequently is not under control and oversight of the Ministry of VWS.

2.2 Publication of information

The CP shall be made available on the NPKD.

The CPS shall not be published.

2.3 Time and frequency of publication

The CSCA shall publish certificates following their generation to the repositories listed under §2.1.

2.4 Access controls on repositories

2.4.1 Dutch National Public Key Directory

Information present in this repository is not subject to any confidentiality requirements.

2.4.2 DCCG

Information published by this CSCA to the DCCG is not subject to any confidentiality requirements.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The subject field of certificates must contain a Distinguished Name (DN) in accordance with §5.2 and §5.3 of the PKCG-document for CSCA certificates and DSCs respectively.

3.1.2 Need for meaningful names

Naming used in DSCs is unambiguous.

The Policy Administrator maintains a register of names, and records which legal entities belong to a DSA.

DSCs shall be used only by the legal entities for which they are issued.

3.1.3 Anonymity or pseudonymity of certificate holders

Anonymity or pseudonymity of certificate holders is prohibited.

3.1.4 Rules for interpreting various name forms

The naming convention used by the CSCA and DSC certificates shall comply with the X.500 standard for Distinguished Names (DN).

3.1.5 Uniqueness of names

Only unique names shall be assigned to CSCA certificates and DSC certificates.

3.1.6 Recognition, authentication, and role of trademarks

Not applicable.

3.2 Initial identity validation

3.2.1 Method to prove possession of Private Keys

CSCA: The witnesses present during the key generation ceremony ensure proof of possession of the private key. The attending witnesses and the correct completion of the key generation ceremony are recorded in an audit report.

DSC: An authorised representative of the Document Signing Authority (DSA) shall issue a signing request of its public key to the CSCA. This signing request constitutes proof of possession of the associated private key for the DSC.

3.3 Identification and Authentication for re-key requests

RFC 3647 defines re-keying as "a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key."

3.3.1 Identification and authentication for routine re-key

The procedures set out in §3.2.1 shall apply mutatis mutandis to identification and authentication for routine re-key.

3.3.2 Identification and authentication for re-key after revocation

The procedures set out in §3.2.1 shall apply mutatis mutandis to identification and authentication for re-key after revocation.

3.4 Identification and authentication for revocation request

CSCA: Not applicable.

DSC: A revocation request can only be issued by authorised personnel of the DSA. Acceptable procedures shall be implemented to authenticate the identity claim of DSA personnel issuing a revocation request.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

When a DSA is appointed by the Ministry of VWS, an authorised representative of a DSA is allowed to submit a DSC signing request.

4.1.2 Enrolment process and responsibilities

The following enrolment process shall be implemented by the CSCA Policy Administrator:

- The Policy Administrator shall request identification information from the authorized representative of the DSA.
- The Policy Administrator shall verify if the DSA is authorised to issue a DSC signing request.
- The DSA shall provide proof of possession of the private key. The Policy Administrator shall verify the presented proof of possession.
- The DSA shall agree to the conditions for the key and DSC usage which have been stipulated in this CP.

4.2 Certificate application processing

Authorised applications for a DSC signing request shall be processed by the CSCA without undue delay. The CSCA will only process DSC signing requests which comply with §5.3 of the PKCG-document.

4.2.1 Performing identification and authentication functions

Identification and authentication will be performed manually. Appropriate procedures shall be implemented for performing identification and authentication functions.

4.2.2 Approval or rejection of certification applications

The Ministry of VWS is the competent authority that decides on an application.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

- The CSCA shall issue the certificate in a secure environment.
- The CSCA shall not issue certificates that are longer valid than the CSCA certificate itself.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The DSC certificate is deemed accepted by the DSA after it has been uploaded to the DCCG.

4.4.2 Publication of the certificate by the CA

After the CSCA has signed the DSC with its private key, it shall upload the DSC to the DCCG.

4.5 Key pair and certificate usage

4.5.1 DSA responsibilities

- DSAs shall only use DSCs for explicitly authorised purposes (see §1.4.1).
- DSAs shall only use DSCs in accordance with EU Regulation 2021/953 and its implementing decisions (including the Commission Implementing Decision laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council).
- DSCs shall only be used by authorized personnel of the DSA.

4.5.2 Relying party responsibilities

Relying parties are only allowed to use the CSCA certificate for the verification of a signed DSC.

4.6 Certificate renewal

Certificate renewal (whereby a new certificate is issued without changing the participants public key) is not applicable.

4.7 Certificate re-key

When a DSA generates a new key pair, it can apply for the issuance of a new certificate that certifies the new public key (hereinafter 'certificate re-key').

4.7.1 Circumstances for certificate re-key

A DSA can apply for a certificate re-key when a DSC certificate nears expiration or for reasons of private key compromise.

4.7.2 Who may request certificate re-key

Only authorised personnel of the DSA can apply for a certificate re-key.

4.7.3 Processing certificate re-keying requests

A request for a certificate re-key shall be processed without undue delay.

4.7.4 Conduct constituting acceptance of the certificate

The provisions of §4.4.1 shall apply mutatis mutandis to certificate re-keying.

4.7.5 Publication of the re-keyed certificate by the CA

The provisions of §4.4.2 shall apply mutatis mutandis to certificate re-keying.

4.8 Certificate modification

Authorised personnel of a DSA can apply for certificate modification when information in the certificate other than the DSC public key changes. The procedures for certificate re-keying apply, as stipulated in §4.7.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A DSC certificate shall be revoked in cases of (suspected) private key compromise.

4.9.2 Who can request a revocation

Authorised personnel of a DSA can apply for certificate revocation.

The CSCA may at its own discretion decide on certificate revocation when it observes circumstances that justify such a revocation.

4.9.3 Procedure for revocation request

Authorised personnel of a DSA can apply for certificate revocation with the CSCA Policy Administrator through a predetermined secure communications channel. A revocation request must at the minimum specify the following:

- The DSC to be revoked;
- The legal entity for which the DSC has been issued;
- The reason for revocation.

4.9.4 Revocation request grace period

A revocation request must be made without undue delay if a situation arises wherein certificate revocation is necessary. A revocation request grace period is not applicable.

4.9.5 Time within which Certificate Authority must process the revocation request

A request for a certificate revocation shall be processed without undue delay.

4.9.6 Revocation checking requirements for relying parties

- Revoked certificates shall be published through the repositories specified in §2.1.
- Relying Member States should use the CRLs for validation of DSCs.
- DCC validators should not use the CRLs for validation of DSCs, due to privacy concerns.

4.9.7 CRL issuance frequency

The CSCA shall publish its CRL no less frequently than once every six months.

4.9.8 Maximum latency of CRLs

After signing a CRL, it shall be published immediately.

4.9.9 On-line revocation/status checking availability

Online Certificate Status Responder (OCSP) is not allowed and thus not supported. Relying Member States should use the CRLs for validation of DSCs instead.

4.9.10 On-line revocation checking requirements

See §4.9.9.

4.9.11 Other forms of revocation advertisements available

See §4.9.9.

4.9.12 Special requirements regarding key compromise

This CSCA is not responsible and cannot be held liable for the consequences of relying on a certificate placed on the CRL.

4.10 Certificate status services

See §4.9.9.

5 Facilities, Management, and Operational Controls

This section describes physical and operational security controls implemented by the CSCA for the hosting environment of the HSM. The controls are implemented in compliance with BIO, level BBN2.

5.1 Physical security controls

5.1.1 Site location and construction

The following controls apply to site location and construction:

- Physical security shall be designed and implemented for offices, rooms and facilities. (BIO 11.1.3)
- Equipment shall be positioned and protected in such a way as to reduce the risk of external threats and dangers as well as the possibility of unauthorised access. (BIO 11.2.1)

5.1.2 Physical access

The following controls apply to physical access:

- Security zones shall be defined and used to protect areas that contain sensitive or vital information and information processing facilities. (BIO 11.1.1)
- Secured areas shall be protected by appropriate access protection to ensure that only authorised personnel can gain access. (BIO 11.1.2)

5.1.3 Power and air conditioning

The following controls apply to risks related to power and air conditioning:

- Equipment shall be protected against power failures and other disruptions caused by disruptions in utility services. (BIO 11.2.2)
- Power and telecommunication cables used for transmitting data or supporting information services shall be protected against interception, disturbance or damage. (BIO 11.2.3)
- Equipment shall be properly maintained to ensure its continued availability and integrity. (BIO 11.2.4)

5.1.4 Water exposure

The following controls apply to risks related to water exposure:

- Physical protection against natural disasters, malicious attacks or accidents shall be designed and implemented. (BIO 11.1.4)

5.1.5 Fire prevention and protection

The following controls apply to fire prevention and protection:

- Physical protection against natural disasters, malicious attacks or accidents shall be designed and implemented. (BIO 11.1.4)

5.1.6 Media storage

The following controls apply to media storage:

- Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme established by the CSCA. (BIO 8.2.2)
- Procedures for managing removable media shall be implemented in accordance with the classification scheme established by the organisation. (BIO 8.3.1)
- Assets located off-site shall be secured, taking into account the various risks of working off-site. (BIO 11.2.6)

5.1.7 Waste disposal

The following controls apply to risks related to waste disposal:

- Media shall be disposed of in a safe and secure manner when no longer required, according to formal procedures. (BIO 8.3.2)

5.1.8 Off-site backup

The following controls apply to back-ups:

- Back-up copies of information, software and system images shall be created and tested periodically in accordance with an agreed back-up policy. (BIO 12.3.1)
- The backup process shall provide storage of the backup at one location, where an incident at one location cannot result in damage at another. (BIO 12.3.1.4)

5.2 Procedural controls

Principles for the engineering of secure systems shall be established, documented, maintained and applied for all transactions concerning the implementation of information systems. (BIO 14.2.5) The HSM which contains the CSCA private key is designated as a secure system pursuant to this control. This section lays down the principles on the basis of which engineering procedures shall be established.

5.2.1 Trusted roles

Operations that can create security risks in relation to the secure system shall be restricted to personnel with a trusted role. Personnel performing trusted roles have an extraordinary responsibility for the integrity of the secure system. The following functions are trusted roles for the CSCA:

- CSCA Administrator
- Auditor
- Custodian of a smart card

5.2.2 Number of persons required per task

Operations that can create security risks in relation to the secure system shall always be executed by a minimum of two persons.

Dual control shall be enforced on a procedural level for the following operations:
- Generation of the CSCA private key
- CSCA re-key
- Backup of CSCA private key
- Restoring of CSCA private key
- Signing of a DSC certificate
- Signing of a CRL

5.2.3 Identification and authentication for each role

- Identification shall be performed in accordance with the established policy of the CSCA.
- Secret authentication information shall only be provided after successful identification.
- The assignment of secret authentication information should be controlled through a formal management process. (BIO 9.2.4)

5.2.4 Roles requiring separation of duties

- Conflicting duties and responsibilities shall be separated to reduce the possibility of unauthorised or inadvertent modification or misuse of the organisation's assets. (BIO 6.2.1)
- Separation of duties shall be enforced for the roles and tasks described in sections 5.2.1 and 5.2.2 respectively.

5.3 Personnel controls

5.3.1 Qualifications, experience and clearance requirements

A trusted role shall only be assigned to an officer who has proven competence in the field relevant to his duties.

5.3.2 Background check procedure

The CSCA shall have an established screening policy. A VOG shall be requested upon commencement of employment or upon a change of position. (BIO 7.1.1.1)

5.3.3 Training requirements and procedures

All employees and, where relevant, contractors shall receive appropriate awareness training and regular refresher training in the organisation's policies and procedures, as relevant to their functions. (BIO 7.2.2)

5.3.4 Retraining frequency and requirements

All employees and, where relevant, contractors shall receive appropriate awareness training and regular refresher training in the organisation's policies and procedures, as relevant to their functions. (BIO 7.2.2)

5.3.5 Sanctions for unauthorised actions

There shall be a formal and communicated disciplinary procedure to take action against employees who have committed a breach of information security. (BIO 7.2.3)

5.3.6 Independent contractor controls

The CSCA shall require all contractors to apply information security in accordance with the organisation's established policies and procedures. (BIO 7.2.1)
The rules for internal personnel of the CSCA apply inter alia to independent contractors.

5.3.7 Documentation supplied to personnel

All employees (internal and external) shall be made aware of their responsibilities regarding information security when they are appointed or when their jobs change. The regulations and instructions that apply to them with regard to information security shall be easily accessible. (BIO 7.1.2.1)

5.4 Audit logging procedure

5.4.1 Types of events recorded

- Event logs that record user activities, exceptions and information security events shall be created, kept and regularly reviewed. (BIO 12.4.1)
- Activities of system administrators and operators shall be logged and the logs shall be protected and regularly reviewed. (BIO 12.4.3)

5.4.2 Frequency for processing and archiving audit logs

For the purpose of the log analysis, the retention period of the logging shall be determined on the basis of a documented risk assessment. Within this period, the availability of the log information shall be guaranteed. (BIO 12.4.2.2)

5.4.3 Retention period for audit logs

For the purpose of the log analysis, the retention period of the logging shall be determined on the basis of aa documented risk assessment. Within this period, the availability of the log information shall be guaranteed. (BIO 12.4.2.2)

5.4.4 Protection of audit log

Logging facilities and information contained in log files shall be protected against falsification and unauthorised access. (BIO 12.4.2)

5.4.5 Audit log backup procedures

A back-up policy shall be in place in which the requirements for preservation and protection are defined and established. (BIO 12.3.1.1)

5.4.6 Audit log accumulation system

Logging facilities and information contained in log files shall be protected against falsification and unauthorised access. (BIO 12.4.2)

5.4.7 Notification to event-causing subject

Notifications shall not be provided to the event-causing subject.

5.4.8 Vulnerability assessments

Information systems shall be checked annually for technical compliance with security standards and risks with regard to actual security and be reported to the Policy Authority. (BIO 18.2.3.1)

5.5 Records archival

5.5.1 Types of records archived

The CSCA shall maintain an archive, which contains records sufficient to establish the proper operation of the CSCA and the validity of certificates issued by the CSCA (including revoked and expired certificates).

5.5.2 Retention period for archive

The retention period for records in the archive is 10 years after the initial creation of the record.

5.5.3 Protection of archive

- Registrations shall be protected against loss, destruction, falsification, unauthorised access and unauthorised disclosure in accordance with legal, regulatory, contractual and business requirements. (BIO 18.1.3)
- The contents of the archive shall be released only when legally required under the law of the Kingdom of the Netherlands.

5.5.4 Archive backup procedures

A back-up policy shall be in place in which the requirements for preservation and protection are defined and established. (BIO 12.3.1.1)

5.5.5 Requirements for time-stamping of records

- Issued certificates and CRLs shall contain time and date information.
- A log entry shall contain at least the date and time of the event.

5.6 Key changeover

- CSCA keys shall be re-keyed every 3 years (or earlier, if appropriate) in compliance with §4 of the PKCG-document. The CSCA public key shall be provided to the DCCG operator after re-keying.
- Unexpired older CSCA private keys shall be used to sign CRLs until all certificates signed by the unexpired older private key have expired.

5.7 Compromise and disaster recovery

The controls in this section apply to compromise and disaster recovery.

5.7.1 Incident and compromise handling procedures

Responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents. (BIO 16.1.1)

5.7.2 Recovery procedures if computing resources, software and/or data are corrupted

- Information security incidents shall be responded to in accordance with documented procedures. (BIO 16.1.5)
- The CSCA shall maintain a means to recover the private key if computing resources, software and/or data are corrupted.

5.7.3 Recovery procedures after key compromise

- Information security incidents shall be responded to in accordance with documented procedures. (BIO 16.1.5)
- The CSCA shall establish a procedure applicable in the event of key compromise.

5.7.4 Business continuity capabilities after a disaster

The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of information security continuity during an adverse situation. (17.1.2)
The CSCA shall maintain a means to recover the private key after a disaster.

In case all copies of the private key are destroyed, already issued DSCs shall remain valid. The CSCA shall then generate a new private key in a key ceremony.

5.8 CA Termination

If the CSCA terminates operation, the DCCG operator shall be informed without undue delay.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

- The CSCA key pair generation shall be documented.
- The CSCA key pair generation must be performed using HSMs that provide the required cryptographic strength of the generated keys. The system shall prevent loss, disclosure or unauthorised use of the generated keys.
- The HSM used for key pair generation and storage shall meet the relevant requirements of the BIO.
- The CSCA key pair generation shall be witnessed and attested by an external auditor as part of a key ceremony.

6.1.2 Public key delivery to certificate issuer

- The DSA is responsible for secure key pair generation in compliance with the Commission Implementing Decision.
- DSA private keys shall not be provided by the CSCA.
- The DSA shall deliver the DSC public key to the CSCA for certification through a secure channel.

6.1.3 Public key delivery to relying parties

The CSCA public key shall only be provided to relying parties through a secure channel. Relying parties shall only rely on public keys that are provided through one of the following official channels:

- DCCG
- NPKD, insofar as communication is secured with HTTPS.

6.1.4 Key sizes

Key sizes and algorithms must comply with Annex I, §3.2.2 and Annex IV, §5.1 of the Commission Implementing Decision. No other algorithms or key sizes are permitted. The key must represent a valid point on the NIST P-256 elliptic curve.

The following table contains the current applicable key sizes:

Authority	**Key size (ECC)**
CSCA	256 bit
DSA	256 bit

6.1.5 Public key parameters generation and quality checking

The following parameters and algorithms shall be supported:

Authority	Algorithm and parameters	Hash function
CSCA	EC-DSA, NIST P-256 curve	SHA-2 with an output length of ≥ 256 Bit
DSA	EC-DSA, NIST P-256 curve	SHA-2 with an output length of ≥ 256 Bit

6.1.6 Key usage purposes

- The CSCA shall use its private keys for DSC and CRL signing.
- The DSA shall use its private keys for DCC signing.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards & control

Cryptographic modules must meet the relevant requirements of the BIO.

6.2.2 Private key multi-person control

The usage of the CSCA private key shall require procedural dual control (see §5.2.2.).

6.2.3 Private key escrow

Not applicable.

6.2.4 Private key backup

The CSCA private key shall be backed-up under multi-person control in accordance with an n out of m scheme.

6.2.5 Private key archival

The CSCA shall maintain an archive of all certificates.

6.2.6 Private key transfer into or from a cryptographic module

For the CSCA and DSA private keys, the following applies:
- The private keys shall be generated and remain in the HSM.
- The private keys shall never be transferred (temporarily or permanently) in software for any purpose.

6.2.7 Private key storage on a cryptographic module

For the CSCA and DSA private keys, the following applies:

- Private keys must be stored on a HSM which meets the relevant requirements from the BIO, in encrypted form.

6.2.8 Activating private keys

The CSCA private key shall be activated by authorised personnel of the main stakeholders by supplying their activation data. Activation data shall be stored on a smart card and shall require completion of authentication using a PIN.

6.2.9 Deactivating private keys

The CSCA private keys may be deactivated by authorised personnel of the main stakeholders by removing their smart card.

6.2.10 Destroying private keys

The CSCA private keys shall only be destroyed after a decision to that effect by the Ministry of VWS.

6.2.11 Cryptographic module capabilities

For the CSCA and DSA private keys, the following applies:

- Private keys must be stored on a HSM which shall meet the relevant requirements of the BIO, in encrypted form.

6.3 Other aspects of key pair management

6.3.1 Public key archival

For the CSCA and DSA public keys, the following applies:

- The public key shall be archived as part of the archival process.

6.3.2 Certificate operational periods and key pair usage periods

The table below shows key-pair usage periods and maximum certificate lifetime:

Key/certificate	**Maximum validity period**
CSCA	20 years
DSC	11 years

The following key-pair usage periods are used in consideration of timely renewal:

Key/certificate	**Maximum usage period**
CSCA	3 years
DSC	7 months

6.4 Activation data

Not applicable.

6.5 Computer security controls

For the CSCA and the management of the CSCA measures are in place for:
- cryptographic controls,
- physical and environmental security,
- operation security, and
- network security,

in accordance with ISO 27001 and the requirements for Trust Service Providers given by the European Telecommunications and Standards Institute (ETSI).

6.6 Life cycle technical controls

6.6.1 System development controls

- Principles for the engineering of secure systems shall be established, documented, maintained and applied for all transactions concerning the implementation of information systems. (BIO 14.2.5) The HSM which protects the CSCA private key is designated as a secure system pursuant to this control.
- To control the installation of software on operational software on operational systems, procedures shall be implemented. (BIO 12.5.1)
- Changes to systems within the development lifecycle shall be controlled through the use of formal change management procedures. (BIO 14.2.2)

6.6.2 Security management controls

For the CSCA and DSA, the following applies:
- An information security management system (ISMS) shall be in place, that can be shown to cover the entire PDCA cycle in a structured manner.

6.6.3 Life cycle security controls

Not applicable.

6.7 Network security controls

The CSCA shall be hosted in a secure and isolated network environment.

6.8 Time-stamping

Not applicable.

7 Certificate, CRL and OCSP Profile

7.1 Certificate profile

For the CSCA certificate and DSC, the following applies:

- The certificate profile is defined in Annex I, §3.2.2 and Annex IV, §5.1 of the Commission Implementing Decision.
- The certificate shall comply with the X.509v3 standard for certificates as defined in IETF RFC 5280.

7.2 CRL profile

The CRLs shall comply with the X.509v2 standard for CRLs as defined in IETF RFC 5280.

7.3 OCSP profile

For the CSCA certificate and DSC, the following applies:

- OCSP is not allowed and thus not supported.
- Relying parties shall not use OCSP.

8 Compliance audit

8.1 Frequency and circumstances of assessment

For the CSCA and DSA, the following applies:

- The hosting environment of the HSMs shall be subject to periodic compliance audits. These audits shall be conducted no less frequently than once every 2 years.
- The Ministry of VWS has the discretionary authority to require ad hoc compliance audits.

8.2 Identity/qualifications of assessor

The auditor must have sufficient experience in auditing certificate authorities.

8.3 Topics covered by assessment

The audit shall verify if the CSCA complies with the requirements specified in this CP and the associated CPS.

8.4 Actions taken as a result of deficiency

If a deficiency is found, corrective action will be taken immediately.

8.5 Communication of results

The results of the audit will be available exclusively to the Ministry of VWS.

9 Other Business and Legal Matters

9.1 Confidentiality of business information

9.1.1 Scope of confidential information

Information subject to the requirement of confidentiality shall be given an appropriate level of classification. The information classification scheme of VIRBI 2013 applies.

9.1.2 Responsibility to protect confidential information

Classified information is protected in accordance with the provisions of VIRBI 2013.

9.2 Privacy of personal information

The CSCA does not handle personal information in the context of this PKI.

9.3 Limitations of liability

By using the CSCA as a trust anchor, the PKI participant agrees to the following conditions: The Kingdom of the Netherlands cannot be held liable for any damage resulting from the use of the CSCA in any way whatsoever.

9.4 Term and termination

This CP is valid as from the date of entry in force. The CP is valid for the period of time that the PKI is used or until this CP is replaced by a newer version, whichever comes first.

9.5 Amendments

The PA will review the CP and make changes if deemed necessary. Newer versions are marked with a higher version number.

9.6 Governing law

Dutch law shall apply.

9.7 Force majeure

See §9.3.