DIGI- JA
VÄESTÖTIETO-
VIRASTO

CVCA
Certificate Policy
for Extended Access Control to Fingerprint Biometrics on Finland's Electronic Machine Readable Travel Documents

OID: 1.2.246.517.2.10.2

CVCA Certificate Policy
v. 1.1

11.6.2025

1 Introduction 5
1.1 Purpose 5
1.2 Identifiers 6
1.3 Parties 6
1.3.1 Certification Authorities 6
1.3.2 Registration Authority 7
1.3.3 Subscribers 7
1.3.4 Relying Parties 8
1.3.5 Other parties 8
1.4 Certificate Usage 8
1.5 Policy Administration 9
1.6 Definitions and Abbreviations 10
1.6.1 Definitions 10
1.6.2 Abbreviations 11
2 Publication and Data Source Requirements 12
2.1 Publication of and Access to CVCA Information 12
2.1.1 Publication of CVCA information 12
2.1.2 Publication frequency 12
2.1.3 Access to information 12
2.1.4 Data warehouses 12
3 Identification and Authentication 12
3.1 Naming Procedures 12
3.2 Initial Identity Validation 13
CVCA set-up and maintenance 13
DV set-up and maintenance 13
3.2.1 CVCA 13
3.2.2 CVCA to CVCA 13
3.2.3 DV to CVCA 14
3.2.4 IS to DV 14
3.3 Identification and Authentication for Re-key Requests 14
3.3.1 DV to CVCA 14
3.3.2 IS to DV 14
4 Certificate Life-Cycle Operational Requirements 15
4.1 Certificate Applications 15
4.1.1 CVCA 15
4.1.2 DV to CVCA 15
4.1.3 IS to DV 15
4.2 Certificate Applications Processing 15
4.2.1 Certificates issued by CVCA to CVCA 15
4.2.2 Certificates issued by CVCA to DV 15
4.2.3 Certificates issued by DV to IS 16
4.3 Certificate Issuance 16
4.3.1 CVCA-issued certificates 16
4.3.2 DV-issued certificates 16
4.4 Certificate Acceptance 16
4.5 Key Pair and Certificate Security Rules 17

4.6 Certificate Renewal ... 17
4.7 Certificate Re-key ... 17
4.8 Certificate Modification ... 18
4.9 Certificate Revocation and Suspension ... 18
4.10 Certificate Status Services ... 18
4.11 End of Subscription ... 19
4.12 Key Escrow and Recovery ... 19
5 Management, Operational and Physical Controls ... 19
5.1 Physical Controls ... 19
5.2 Procedural Controls and System Access Management ... 20
5.3 Personnel Controls ... 20
5.4 Audit Logging Procedures ... 22
5.5 Records Archival Procedures ... 23
5.6 Key Changeover ... 23
5.7 Compromise and Disaster Recovery ... 24
5.7.1 Incident and compromise handling procedures ... 24
5.7.2 Computing resources, software and/or data corruption ... 24
5.7.3 Entity private key compromise procedures ... 24
5.7.4 Business continuity capabilities after a disaster ... 25
5.8 CVCA or DV Termination ... 25
6 Technical Security Controls ... 25
6.1 Key Pair Generation ... 25
6.2 Private Key Protection and Cryptographic Module Engineering Controls ... 26
6.3 Other Aspects of Key Pair Management ... 26
6.5 Computer Security Controls ... 27
6.6 Life Cycle Security Controls ... 27
6.7 Network Security Controls ... 27
6.8 Time-stamping ... 27
7 Certificate and CRL Profiles ... 27
7.1 Certificate Profile ... 27
7.1.1 CVCA certificate ... 27
7.1.2 DV certificate ... 28
7.1.3 IS certificate ... 28
7.2 CRL Profile ... 29
7.3 OCSP Profile ... 29
8 Compliance Audits and Other Assessments ... 29
8.1 Audit Frequency ... 29
8.1.1 Auditor ... 30
8.1.2 Audit subject matter and coverage ... 30
8.1.3 Measures taken in the event of anomalies ... 30
8.1.4 Provision of information about audits ... 30
9 Other Business and Legal Matters ... 31
9.1 Fees ... 31
9.2 Financial Liability ... 31
9.3 Confidentiality of Business Information ... 31
9.4 Privacy of Personal Information ... 31

9.5 Intellectual Property Rights 31
9.6 Representations and Warranties 31
9.7 Disclaimers of Warranties 31
9.8 Limitations of Liability 32
9.9 Indemnities 32
9.10 Term and Termination 32
9.11 Individual Notices and Communication with Participants 32
9.11.1 Register 32
9.11.2 CVCA Certificate 33
9.11.3 DV Certificate Request 33
9.11.4 DV Certification Receipt Acknowledgement 33
9.11.5 DV Certificate 33
9.11.6 Suspension of CVCA Service 33
9.12 Amendments 33
9.13 Dispute Resolution Procedures 34
9.14 Governing Law 34
9.15 Compliance with Applicable Law 34
9.16 Miscellaneous Provisions 34
9.17 Other Provisions 34
Version 34

1 Introduction

The Certificate Policy (CP) is a description produced by the Certification Authority (CA) regarding the procedures and principles to be followed when issuing certificates.

The Digital and Population Data Services Agency is a Finnish government agency operating under the Finnish Ministry of Finance. It has the statutory duty to issue the certificates necessary for access to fingerprint biometrics recorded on the chips of Finland's Electronic Machine Readable Travel Documents (hereafter 'eMRTD'). The Digital and Population Data Services Agency acts as the Country Verifying Certification Authority (hereafter 'CVCA'). Decisions to grant read access rights to non-Finnish authorities are made by the Finnish Ministry of the Interior.

The goal of this Certificate Policy is to achieve trust and sufficient interoperability between the Country Verifying Certification Authorities (CVCAs) and Document Verifiers (DVs) of different Member States for the EAC-PKI to operate.

This CP is established in accordance with the relevant Commission Decisions on the technical specifications on standards for security features and biometrics in passports and travel documents issued by Member States and in the technical specifications on standards for security features and biometrics in residence permits for third country nationals.

This Certificate Policy only concerns the use of certificates to control access to fingerprint biometrics on Extended Access Control enabled passports and travel documents for the purposes of border control.

This National Certificate Policy meets the standards of the Common Certificate Policy. The issuing of certificates by CVCA to domestic DVs is outside the scope of this national Certificate Policy. In this document the CVCA refers to a Finnish national CVCA.

This Certificate Policy is based on the Technical Guideline ‘Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)’, Version 2.21, TR-03110, published by the Bundesamt fur Sicherheit in der Informationstechnik, hereafter referred to as 'TR-EAC', and ‘Common Certificate Policy for the Extended Access Control Infrastructure for Travel and Residence Documents issued by EU Member States’, Version 2.4, TR-03139, published by the Bundesamt fur Sicherheit in der Informationstechnik, hereafter referred to as 'TR-CCP'.

1.1 Purpose

The CVCA has been established to protect sensitive biometric data stored on an eMRTD chip. The CVCA offers the certificate service to parties operating as Document Verifiers (hereafter 'DV'). Confidential personal biometric data on an eMRTD chip can only be accessed if proper certificate chain is introduced to the chip.

For both CVCAs and DVs this Policy offers the same quality as that offered by the Extended Normalised Certificate Policy (NCP+) as defined in ETSI TS 102 042, version 2.4.1.

This Certificate Policy operates within the Public Key Infrastructure described in section 2 “Public Key Infrastructure” of TR-EAC.

1.2 Identifiers

Each Digital and Population Data Services Agency certificate policy document is assigned a unique object identifier (OID).

The title of this Certificate Policy is "CVCA Certificate Policy for Access to Fingerprint Biometrics on Finland's Electronic Machine Readable Travel Documents" and its OID is 1.2.246.517.2.10.2.

This Certificate Policy has been registered by the Digital and Population Data Services Agency.

1.3 Parties

1.3.1 Certification Authorities

Country Verifying Certification Authority The Root Certification Authority (CA) of a national EAC-PKI is called a Country Verifying Certification Authority (CVCA). The public keys of the CVCA are contained in both self-signed CVCA certificates and link CVCA certificates. Both classes are called CVCA certificates. The CVCA determines the access rights to sensitive data stored on domestic eMRTD chips for all DVs (i.e. domestic DVs as well as foreign DVs) by issuing DV certificates entitling to access control attributes.

The CVCA issues certificates to its Certificate Holders (Subscribers). In this document, a Certificate Holder is called a Document Verifier (DV). A DV is an organisational unit that manages inspection systems belonging together.

The duties of the CVCA are to:

- provide certificate and registration services referred to in the Passport Act (671/2006) in accordance with this Certificate Policy;
- identify certificate applicants;
- ensure certificate data content is error-free;
- maintain a high level of privacy protection and good data processing practice in the processing of certificate data;
- issue DV certificates and renew the CVCA certificate.

Document Verifier Certification Authority Finland has only one certification authority at the level of a Document Verifier (DV).

A DV operates a CA to issue certificates for its inspection systems. The inspection system certificates issued by a DV usually inherit both the access rights and the validity period from the underlying DV certificate. However, the Document Verifier may choose to further restrict the access rights or the validity period.

All DV certificates and the new CVCA certificate are signed electronically using a private key corresponding to the public key on the CVCA certificate.

1.3.2 Registration Authority

Country Verifying Registration Authority There is only one RA in Finland. It is operated by Digital and Population Data Services Agency.

The CVRA is responsible for performing identification and authentication of certification requests of Document Verifiers. This means certification applications for subscriber certificates are only allowed by Document Verifiers. In addition, a CVRA initiates the issuance of certificates to Document Verifiers and validates the process of revoking and renewing certificates issued by the CVCA.

For the purposes of the remainder of this document, the CVRA is assumed to be part of the CVCA and only the term CVCA is used.

The CVCA and DV certificates of the state of Finland are registered by the Digital and Population Data Services Agency.

The registration of the CVCA certificate and DV certificates take place in compliance with the procedure described in section 4.2 below.

- The Registration Authority acts by order of and at the responsibility of the CVCA.
- The Registration Authority complies with the CVCA's Certificate Policy.
- The Registration Authority identifies certificate applicants in accordance with this Certificate Policy. The Registration Authority complies with the registration-related procedures agreed with the CVCA.

Document Verifier RA DVRAs are responsible for performing identification and authentication of certification requests of Inspection Systems. In addition, a DV initiates the issuance of certificates to Inspection Systems and validates the process of revoking and renewing certificates.

For the purposes of the remainder of this document, the DVRA is assumed to be part of the DV and only the term DV will be used. There is only one DVRA in Finland. It is operated by Digital and Population Data Services Agency.

1.3.3 Subscribers

Subscribers under this Policy are Document Verifiers (DV) and Inspection Systems (IS).

For the purpose of this Certificate Policy an Inspection System is defined as the infrastructure, hardware and software required to obtain certificates from a Member States DV, store and manage those certificates, and to obtain fingerprint biometrics from eMRTDs' using those certificates, including mechanisms controlling access to the inspection systems.

The CVCA and DV certificates in accordance with this Certificate Policy are issued to the state of Finland, which is represented by the Digital and Population Data Services Agency. A DV certificate may also be issued to a non-Finnish authority, as decided by PKI coordination. The Ministry of the Interior grants authorisation. PKI coordination (POHA-Migri) notifies authorisation.

CVCA certificate and DV certificate applicants comply with the CVCA's Certificate Policy.

1.3.4 Relying Parties

A Relying Party is an organisation or system that relies on the certificate data.

Relying Parties must check the integrity of the certificate's trust chain (see section 1.4 below for trust chain definitions).

1.3.5 Other parties

a) The Ministry of the Interior, issues the necessary permits to non-Finnish authorities.
b) The Directorate-General for Justice, Freedom and Security of the European Commission, which is responsible for maintaining the list of CVCA and DV contact data at Member State level.

1.4 Certificate Usage

The CVCA key pairs and certificates are used as follows:

a) The CVCA Private Key is used:

- to sign Finnish and foreign DV certificates;
- to sign a new CVCA certificate
- to sign the first request for a DV certificate sent to foreign CVCAs.

b) CVCA-issued certificates are used:

- to verify signatures of Finnish or foreign DV
- to verify signatures of Finnish CVCA link certificates

DV key pairs and certificates are used as follows:

a) The DV private key is used:

- to sign IS certificates
- to apply for a DV certificate from national or foreign CVCAs

b) the DV certificate is used:

- to verify IS signature certificates

Certificate trust chains

a) CVCA – to previous CVCA certificate
b) DV – CVCA certificate and another country's accepted CVCA certificate
c) IS – DV certificate, CVCA certificate and another country's accepted CVCA certificate
d) eMRTD – relies on the CVCA, its DV and IS certificates.

Certificate trust chains can be used when reading fingerprints on an eMRTD and only when verifying a person's identity when the person's biometric data is directly accessible.

These procedures are described in:

- Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals;
- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States; and
- Article 13(1) of Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

An exception to this, however, is an IS used to personalize an eMRTD when testing the functioning of biometric data in conjunction with eMRTD production. The Common Certificate Policy does not apply to its own quality control.

1.5 Policy Administration

Any questions regarding this Certificate Policy may be sent to the following address:

Digital and Population Data Services Agency
Certificate Services
P.O. Box 123
FI-00531 Helsinki
FINLAND

vptuotanto@dvv.fi
Phone: +358 295 536 000
Fax: +358 295 535 555

Any questions regarding the Certificate Policy will be answered by the Certificate Service Unit of the Digital and Population Data Services Agency.

1.6 Definitions and Abbreviations

1.6.1 Definitions

1. Certification Authority – an entity that issues certificates;

2. Certificate Revocation List – a list of revoked certificates;

3. Certificate Policy – a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirement;

4. Certificate Practice Statement – a statement of the practice that a certification authority employs in issuing, managing, revoking and renewing or re-keying certificates;

5. Common Certificate Policy – the outline Certificate Policy published by the Commission which sets the minimum requirements that must be met by Member States' National Certificate Policies in order to be included in the EAC-PKI;

6. Common Criteria - Common Criteria for Information Technology Security Evaluation; the title of a set of documents describing a particular set of IT security evaluation criteria;

7. Extended Access Control Public Key Infrastructure – the infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilising Extended Access Control;

8. Document Signer – the entity signing the original document, in this case the organisation that issues the eMRTD;

9. Document Verifier – an entity within the EAC-PKI that requests certificates from CVCAs and, on the basis of those certificates, issues certificates to Inspection Systems;

10. Evaluation Assurance Level – a numeric grade assigned to an IT system or product following the completion of a Common Criteria security evaluation;

11. Inspection System – the operational system that reads fingerprint biometrics from eMRTDs;

12. International Civil Aviation Organisation – a UN organisation tasked with fostering the planning and development of international air transport. In this role it sets international standards for eMRTDs;

13. Key Ceremony - a procedure whereby a key pair is generated using a cryptographic module and where the public key is certified;

14. Link Certificate – link certificates ensure business continuity without exchanging a new trusted self-signed root CVCA certificate out-of-band;

15. Machine Readable Travel Document – an international travel document containing eye- and machine-readable data;

16. National Certificate Policy – a Member State's Certificate Policy for management of the process of issuing and receiving certificates to and from other Member States;

17. Object Identifier – a unique numerical sequence allowing a document to be identified;

18. Public Part of the Certification Practice Statement – a subset of the provisions of a complete CPS that is made public by a CA;

19. Registration Authority – an entity that establishes enrolment procedures for certificate applicants, performs identification and authentication of certificate applicants, initiates or passes along revocation requests for certificates, and approves applications for renewal or re-keying certificates on behalf of a CA;

20. Trusted Certification Path – a chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of one or more CVCA certificates, link certificates as appropriate, a DV certificate and the IS certificate.

1.6.2 Abbreviations

CA	Certification Authority
CAR	Certification Authority Reference
CC	Common Criteria
CHR	Certification Holder Reference
CP	Certificate Policy
CCP	Common Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CSPKI	Country Signing Public Key Infrastructure
CVRA	Country Verifying Registration Authority
CVCA	Country Verifying Certification Authority
DV	Document Verifier
EAC-PKI	Extended Access Control Public Key Infrastructure
ECDSA	Elliptic Curve Digital Signature Algorithm
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ICAO	International Civil Aviation Organisation
IS	Inspection System
ISO	International Organization for Standardization
eMRTD	Electronic Machine-Readable Travel Document
OCSP	Online Certificate Status Protocol
OID	Object Identifier
RA	Registration Authority
SHA	Secure Hash Algorithm

2 Publication and Data Source Requirements

The European Commission is responsible for maintaining a list of contact details for CVCAs and DVs at the European level. The content and integrity of this list is preserved by diplomatic means. The corresponding information is available on the website of the Directorate General for Justice, Freedom and Security (DG-JLS) of the European Commission.

2.1 Publication of and Access to CVCA Information

2.1.1 Publication of CVCA information

The Certification Authority publishes the Certificate Policy, which is a public document.

2.1.2 Publication frequency

The CVCA certificate and DV certificate are not published in a public directory.

2.1.3 Access to information

The CVCA certificate and DV certificate are not published in a directory.

2.1.4 Data warehouses

Confidential data of the certificate system are stored in the CVCA's own, confidential data warehouse. CVCA data are archived in accordance with up-to-date archiving regulations.

3 Identification and Authentication

3.1 Naming Procedures

As defined in section C.1 of TR-EAC, the Certification Authority Reference (CAR) is used to identify the public key to be used to verify the signature of the certification authority (CVCA or DV).

The Certificate Authority Reference is equal to the Certificate Holder Reference (CHR) in the corresponding certificate of the certification authority (CVCA Link Certificate or DV Certificate).

The Certificate Holder Reference (CHR) identifies the public key of the certificate holder. It is composed of the following concatenated elements:

1) the ISO 3166-1 ALPHA-2 country code of the certificate holder’s country;
2) a mnemonic that represents the certificate holder;
3) a numeric or alphanumeric sequence number.

The CVCA certificate and DV certificate data provide unique identification of the certificate holder.

3.2 Initial Identity Validation

CVCA set-up and maintenance

The Digital and Population Data Services Agency sets up the Finnish CVCA and maintains it so that it can issue DV certificates for Finnish and foreign DVs for the purpose of reading fingerprint data stored on Finnish eMRTDs.

The Digital and Population Data Services Agency sets up the Finnish CVCA by generating a CVCA certificate for itself. The Digital and Population Data Services Agency maintains the Finnish CVCA certificate by renewing it in compliance with the schedule agreed with the National Police Board, and Finnish Immigration Service.

DV set-up and maintenance

The Digital and Population Data Services Agency sets up and maintains the Finnish Document Verifier (DV) system, enabling it to issue IS certificates for national use by the Finnish Police, Finnish Immigration Service, and the Finnish Border Guard to read fingerprint data stored on eMRTDs in Finland. The DV also administers the keys required to read fingerprint or iris data on Finnish and foreign eMRTDs.

3.2.1 CVCA

The Digital and Population Data Services Agency is responsible for CVCA authentication and CVCA identity definition.

3.2.2 CVCA to CVCA

CVCAs must establish each other's identity before sending requests for DV certificates. This takes place under the supervision of the European Commission.

The CVCA submits the following information to the European Commission:

a) the Certificate Policy;
b) the Public Key of the CVCA certificate.

The European Commission conveys this information to CVCAs.

The European Commission is informed of any changes to the above-mentioned information.

3.2.3 DV to CVCA

When submitting its registration details for the first time, a foreign DV submits the registration details to the CVCA using a mutually agreed reliable channel.

The following registration details are submitted:

a) the public part of the DV's Certificate Practice Statement;
b) the latest Certificate of Conformity with the National Certificate Policy for the DV;
c) a list of the organisations using Inspection Systems subscribing to the DV;
d) a Certificate Request as specified in section C.2. of TR-EAC. This Certificate Request includes an Outer Signature, as defined in section C.2.6. of TR-EAC, signed by the DV's supervising CVCA.

In the event of a non-trivial change to any of the above, the DV submit details of the change to the CVCA to allow it to make an assessment as to whether a new Initial Identity Validation is required.

3.2.4 IS to DV

DVs have a proper mechanism in place to identify an authenticated inspection system. When the initial key material is generated and the Certificate Request is compiled, staff authorised by the DV are physically present. The first IS requests must be created manually and forwarded by signed email.

3.3 Identification and Authentication for Re-key Requests

Identification and authentication for Re-key Requests are specified in section C.2. of TR-EAC.

3.3.1 DV to CVCA

The CVCA ensures the validity of the request by confirming that:

a) the request is formatted in accordance with section C.2. of TR-EAC;
b) the CVCA of the DV’s Member State continues to list the DV as valid;
c) the DV’s Certificate of Conformity is valid;
d) the outer signature of the request is created with a key which is valid with respect to a certificate of that DV, issued by the CVCA.

3.3.2 IS to DV

The DV only issues a certificate once it has confirmed that:

a) the Inspection System remains registered as operational;
b) the Inspection System is not listed as stolen/missing.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Applications

4.1.1 CVCA

The Digital and Population Data Services Agency is responsible for CVCA creation.

4.1.2 DV to CVCA

Following successful Initial Identity Validation as per 3.2.3 above, DV Certificate Application is carried out in accordance with section C.2. "Certificate Requests" and section 2.2 "Document Verifiers" of TR-EAC.

4.1.3 IS to DV

Inspection Systems submits Certificate Applications upon completion of successful Initial Identity Validation as per 3.2.4 above.

4.2 Certificate Applications Processing

4.2.1 Certificates issued by CVCA to CVCA

A CVCA only issues a self-signed CVCA certificate or a link certificate to a former CVCA certificate during the key ceremony that complies with its own National Certificate Policy. The CVCA checks that a certificate request is authorised and valid (see section 4.1.1 above).

The CVCA certificate applicant confirms the accuracy of the information provided with its signature and accepts the CVCA certificate creation.

4.2.2 Certificates issued by CVCA to DV

A CVCA only issues a certificate to a DV that is complying with its own (the DV's) National Certificate Policy that is, at a minimum, in accordance with this Certificate Policy, and whose usage (governmental and non-governmental) of fingerprint biometrics in the Travel Document is in conformance with section 1.4 of this document.

The CVCA checks that the certificate request is valid.

The CVCA acknowledges the certificate request upon its receipt.

The DV certificate applicant confirms the accuracy of the information provided with its signature and accept the DV certificate creation.

The CVCA MUST process the certificate request within a timeframe of 7 days according to the Common Certificate Policy (TR-CCP).

In the event that a CVCA system is non-operational for more than this time frame, it MUST inform all subscribing domestic DVs and foreign Member State CVCAs no later than 7 days before the loss of service, if planned, and as soon as is reasonably possible in the event of an unplanned loss of service (TR-CCP).

4.2.3 Certificates issued by DV to IS

A DV only issues a certificate to an IS that is complying with its own National Certificate Policy and that is using the certificates in accordance with section 1.4 of this document.

The DV checks that the certificate request is valid prior to issuing a certificate.

4.3 Certificate Issuance

4.3.1 CVCA-issued certificates

The CVCA takes measures against the forgery of certificates and ensures that the procedures of issuing the certificate are securely linked to the associated registration, certificate renewal or re-key, including the provision of any subject generated public key.

Certificates are generated and issued in accordance with section C. "Certificates" of TR-EAC.

4.3.2 DV-issued certificates

The DV ensures that it issues certificates securely to maintain their authenticity. The DV takes measures against the forgery of certificates and ensure that the procedures of issuing the certificate are securely linked to the associated registration, certificate renewal or re-key, including the provision of any subject generated public key.

Certificates are generated and issued in accordance with section C. "Certificates" of TR-EAC.

4.4 Certificate Acceptance

CVCA self-signed certificates are accepted by the entity responsible for the CVCA after its creation at the end of the key ceremony.

A DV or IS are deemed to have accepted a certificate upon its receipt.

4.5 Key Pair and Certificate Security Rules

The CVCA, DVs and ISs fulfil the following requirements as appropriate:

- ensure that accurate and complete information is submitted to the CVCA/DV in accordance with the requirements of this policy, particularly with regard to registration;
- the key pair is only used in accordance with the limitations imposed by this Certificate Policy;
- ensure there is no unauthorised use of the private key;
- make sure keys are generated in accordance with TR-EAC;
- only use private keys for signing or decrypting within a secure cryptographic device as described in section 6.2.
- notify a CVCA/DV without any reasonable delay if any of the following occur up to the end of the validity period indicated in the certificate:
  - a private key has been lost, stolen, potentially compromised; or
  - control over the private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or
  - inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject;
- following compromise, the use of a private key is immediately and permanently discontinued;
- in the case of being informed that a CVCA's or DV's Private Key has been compromised and certificates signed by these Private Keys should not be relied upon.

Key pair and certificate usage take place as indicated by the certificate issuer (CVCA or DV) in the Certificate Holder Authorisation Field of the Certificate.

DVs and ISs only use the private key corresponding to the received DV and IS certificate for the following purposes only:

- the purpose as described in section 1.4 "Certificate Usage" of this Certificate Policy;
- in accordance with the content of the issued certificates.

4.6 Certificate Renewal

Certificate renewal is not allowed.

4.7 Certificate Re-key

Certificate re-key is understood to mean the issue of another certificate to the certificate holder during which the following data is always be changed:

a) the serial number of the certificate;
b) the start date of certificate validity;

c) the end date of certificate validity;
d) the public key of the certificate holder.

During the issuance of a re-keyed certificate no other data given in the certificate is changed.

Certificate re-key only takes place where:

a) a DV or IS certificate is about to expire;
b) a DV certificate is revoked;
c) an IS key is compromised;
d) a DV/IS certificate requires modification due to changes in the DV/IS attributes.

In cases where a DV certificate is about to expire (see 4.7 a above), section C.2. "Certificate Requests" of TR-EAC are complied with.

In cases where a DV certificate is revoked, expired or requires modification (see 4.7 b, c and d above), re-keying is equal to the procedures followed when a DV applies for a DV certificate for the first time.

In the case where an IS private key is compromised or has expired, re-keying take place in a manner equal to the procedure followed when an IS applies for an IS certificate for the first time.

The CVCA/DV ensures that requests for certificates issued to a previously registered DV/IS are complete, accurate and duly authorised. The CVCA/DV then:

a) checks the existence and validity of the certificate to be re-keyed and checks that the information used to verify the identity and attributes of the DV/IS is still valid;

b) issues a new certificate based on verification of the subject’s signature on the request only if the cryptographic security of that signature key is still sufficient for the new certificate’s validity period and no indications exist that the key used to generate the subject’s signature on the request has been compromised.

4.8 Certificate Modification

See section 4.7 "Certificate Re-Key" of this document.

4.9 Certificate Revocation and Suspension

Certificate Revocation and Suspension are not applicable.

4.10 Certificate Status Services

Certificate Status Services are not applicable.

4.11 End of Subscription

End of Subscription is not applicable.

4.12 Key Escrow and Recovery

Key Escrow and Recovery are not applicable.

5 Management, Operational and Physical Controls

5.1 Physical Controls

CVCA and DV ensure that they operate their services in a secure environment. This includes:

a) site location and construction: the CVCA/DV services are operated in a physically protected area.

The CVCA systems are located in high-security data centres and comply with the security guidelines and regulations issued for computer centres.

b) physical access: Access to the CVCA/DV are controlled and audited. Only authorised persons have physical access to the CVCA/DV environment.

Access to premises where certificate system production duties take place are controlled. Both authorised and unauthorised access are detected by the access control system. Access to data centre premises requires identification where the person is identified, his/her access rights checked, and the events registered. Data centre premises are guarded around the clock.

c) media storage: the storage media is protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).

Data is stored in high-security premises with access control. A high level of privacy protection and good data processing practice are maintained in data storage.

d) waste disposal: Procedures for the disposal of waste are implemented in order to avoid unauthorised use, access, or disclosure of sensitive data.

A high level of privacy protection and good data processing practice are maintained in data destruction.

e) Off-site backup: An off-site backup system for critical data is installed.
Hardware solutions are implemented in accordance with good data management practice to make sure that, in the event of system failure, a back-up system can be activated without compromising the confidentiality, integrity or availability of data in the system.

Access to and servicing of spare parts of important hardware are secured.

5.2 Procedural Controls and System Access Management

Procedural controls are implemented, especially the separation of duties by implementing a two-person principle for critical tasks.

CVCA, DV and IS ensure that system access to any EAC-PKI device is limited to individuals who are properly authorised on a need-to-know basis. In particular, the following requirements apply:

a) Controls (e.g. firewalls) are implemented to protect the CV internal network domains from external network domains accessible by third parties.

b) Sensitive data is protected against unauthorised access or modification.

c) Sensitive data is protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.

d) CVCA, DV and IS ensure effective administration of users' (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access.

e) The CVCA, DV and IS ensure that access to information and application system functions is restricted to authorised staff and that the EAC-PKI systems provide sufficient computer security controls for the separation of trusted roles, including the separation of security administrator and operation functions. Particularly, the use of system utility programs is restricted and strictly controlled. Access is restricted, only allowing access to resources as necessary for carrying out the role(s) allocated to a user.

f) CVCA, DV and IS personnel is successfully identified and authenticated before using EAC-PKI applications related to certificate management or access to eMRTDs.

g) CVCA, DV and IS personnel are accountable for their activities, for example by retaining event logs as defined in section 5.4 below.

h) Sensitive data is protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorised users.

5.3 Personnel Controls

All EAC-PKI systems (CVCA, DV and IS systems) are operated by qualified and experienced staff. In particular, the following requirements hold:

a) Each CVCA, DV and IS employ a sufficient number of personnel who possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

The Digital and Population Data Services Agency pays particular attention to the reliability of both its own personnel and that of technical suppliers and registration authorities as well as the skills needed in the performance of tasks.

b) Personnel undergoes domestic security screening appropriate to the role(s) they are carrying out.

The Digital and Population Data Services Agency obtains a basic background check on its own personnel and the personnel of technical suppliers who work in the certificate environment.

c) Appropriate disciplinary sanctions are applied to personnel violating CVCA, DV or IS policies or procedures.

The personnel of the Digital and Population Data Services Agency perform their duties under the legal liability of a public servant for their official acts in office and in accordance with the Digital and Population Data Services Agency's internal guidelines. Provisions regarding the status of public servants are laid down under the Act on Public Officials in Central Government 750/1994. The activities of technical suppliers are monitored on the basis of existing security agreements and operational audits.

d) Security roles and responsibilities, as specified in the system's security policy, are documented in job descriptions. Trusted roles, on which the security of the system's operations is dependent, are clearly identified.

Duties, obligations and powers are specified in the Digital and Population Data Services Agency's Rules of Procedure and each employee's job description.

e) All personnel (both temporary and permanent) have job descriptions defined from the viewpoint of separation of duties and least privilege.

Duties, obligations and powers are specified in the Digital and Population Data Services Agency's Rules of Procedure and each employee's job description.

f) Personnel follow administrative and management procedures and processes that are in line with the Procedural Controls described in 5.2 above.

g) All CVCA, DV and IS personnel in trusted roles are free from conflicting interests that might prejudice the impartiality of the system's operations.

Personnel recruitment take place making sure personnel's skills are in compliance with the requirements set by their duties and that the background check carried out on them did not reveal anything that might create a conflict of interests between their duties and the service provision.

h) Personnel with access to private keys within the EAC PKI is formally appointed to trusted roles by a member of senior management responsible for security of the IS.

i) The CVCA, DVs and ISs do not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel have no access to the trusted functions until any necessary checks are completed.

5.4 Audit Logging Procedures

Each CVCA, DV and IS implement appropriate logging procedures to analyse and recognise any proper and improper use of its system within the EAC PKI.

The CVCA, DVs and ISs ensure that all relevant information concerning a certificate is recorded for an appropriate period of time, at a minimum to ensure compliance with audit requirements as described in section 8 "Compliance Audit and Other Assessment" below.

The CVCA and DVs ensure the following:

a) The confidentiality and integrity of current and archived records concerning certificates are maintained.

b) Records concerning certificates are completely and confidentially archived.

c) The precise time of significant environmental, key management and certificate management events are recorded.

d) All events relating to the life-cycle of keys are logged.

e) All events relating to the life-cycle of certificates are logged.

f) All events relating to registration are logged.

g) All requests and reports relating to revocation, as well as the resulting actions, are logged.

h) The specific events and data to be logged are documented.

i) Events are logged in a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the time period they are required to be held.

ISs maintain a log including the following:

a) The logging of the key management part of the Inspection System take place in such a way that the responsible DV can detect misuse of the system and apply appropriate countermeasures.

b) Protection against modification or deletion of logs is in place.

c) Records are kept to enable the auditor to confirm that misuse can be detected.

5.5 Records Archival Procedures

Each CVCA, DV, and IS implement appropriate records archival procedures for its system within the EAC-PKI. Procedures ensure the integrity, authenticity and confidentiality of the data.

The archives are created in a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

Access to archives is restricted to authorised operators only.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media is defined by the archive site.

Inspection Systems do not log or transmit fingerprints obtained from eMRTDs. These biometrics are deleted immediately after finishing the comparison process between fingerprints acquired from of the bearer and fingerprints read from the eMRTD.

The provisions of the Archives Act (831/1994) applies as general legal provisions governing archiving. The right to access information are determined in accordance with the Act on the Openness of Government Activities (621/1999).

Archived information is retained in accordance with the provisions that apply to the authority acting as the CVCA. Public keys are retained for ten (10) years following their expiry.

5.6 Key Changeover

The CVCA and DVs ensure that keys are generated in controlled circumstances and in accordance with the procedures defined in Section 5.2 "Management, Operational and Physical Controls" above.

Full self-signed certificates plus link certificates are provided by the CVCA

5.7 Compromise and Disaster Recovery

The CVCA takes reasonable measures to ensure that service continuity is maintained, including:

a) measures to minimise the impact of disruption to power services;

b) measures to minimise the impact of events such as flooding or fire;

c) measures to minimise the impact of the loss of availability of key staff.

5.7.1 Incident and compromise handling procedures

Each CVCA, DV and IS ensures in the event of a disaster, including compromise of the participant's private key, that operations are restored as soon as possible. In particular, the following requirements hold:

1. Each CVCA, DV and IS define and maintain a continuity plan followed in case of a disaster (see also section 5.7.4 below).

2. CVCA and DV systems data necessary to resume CVCA and DV operations are backed up and stored in safe places suitable to allow the CVCA and DV to rapidly resume operations in case of an incident/disaster.

3. Back-up and restore functions are performed by the relevant trusted roles.

4. The EAC-PKI business continuity plan (or disaster recovery plan) address the compromise or suspected compromise of a private key as a disaster, and the planned processes are in place (see also section 5.7.3 below).

5.7.2 Computing resources, software and/or data corruption

If a private CVCA key is unusable for non-critical reasons, the procedure described in section 5.6 above are followed.

5.7.3 Entity private key compromise procedures

A Document Verifier inform immediately all CVCAs that have issued certificates for this DV about DV or IS private key compromise or misuse.

If an Inspection System is lost or stolen, the responsible Document Verifier informs all CVCAs that have issued certificates for this DV about the corresponding incident as soon as possible but not later than the next certificate request.

Information is accessible through a mutually agreed reliable channel.

5.7.4 Business continuity capabilities after a disaster

The Digital and Population Data Services Agency has a Business Continuity Plan to secure its functions.

5.8 CVCA or DV Termination

In the event of a CVCA terminating its operations, the CVCA acts as follows:

- notify all CVCAs, with which it is registered, of the termination;
- notify all CVCAs, with which it is registered, of the CVCA, if any, which will be taking over responsibility for national DVs;
- notify all DVs which it supplies with certificates of the termination;
- notify all DVs which it supplies with certificates of the CVCA, if any, which will be issuing certificates in its place;
- any replacement CVCA continue to provide certificates for eMRTDs issued under the original CVCA;
- the CVCA destroys, or withdraw from use, its private keys;
- the CVCA takes care of data archiving and otherwise comply with the provisions of the Archives Act (831/1994) regarding data archiving.

In the event of a DV terminating its operations, it notifies its CVCA which will then notify all CVCAs issuing certificates to that DV.

6 Technical Security Controls

6.1 Key Pair Generation

The CVCA and DVs ensure that CA keys are generated in controlled circumstances according to section 5 "Management, Procedural and Physical Controls" of this document.

Key pairs are generated and stored in security modules in accordance with FIPS 140-2 class 3 or FIPS 140-3 class 3. Private keys are read and write protected.

Before the expiration of a CVCA or DV signing key, the CVCA or DV generates a new certificate-signing key pair and apply all necessary actions to avoid disruption to the operations of any CVCA, DV or IS which may rely on that key. The new key is generated and distributed in accordance with TR-EAC and this policy.

The CVCA and DVs ensure that the integrity and authentication of their public keys and any associated parameters are maintained during distribution to DVs and ISs.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

In accordance with the Common Certificate Policy, private keys are stored and used in security modules that comply with either FIPS 140-2 Class 3 or FIPS 140-3 Class 3. Private keys are read and write-protected.

The CVCA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorisations to perform sensitive CVCA key operations (such as creation, back-up, restore, destruction and use).

A DV implements technical and procedural mechanisms that require the participation of multiple trusted individual authorisations to perform sensitive DV key operations (such as creation, back-up, restore and destruction). The DV implements the trusted role authentication process with the DV HSM to allow DV key usage.

IS key operations (such as creation, back-up, restore, destruction and use) are restricted to authorised personnel appointed to this role.

When outside the signature-creation device, private signing keys are protected in a way that ensures the same level of protection as provided by the signature creation device.

If private keys are backed up, they are stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorised to carry out this function are kept to a minimum.

Backup copies of the private signing keys are subject to the same or greater level of security as keys currently in use.

Where keys are stored in a dedicated key processing hardware module, access controls are in place to ensure keys are not accessible outside the hardware module.

Private signing keys are not used beyond the end of their lifecycle, and all copies of the key are destroyed or put beyond use at the end of their life.

The security of cryptographic devices is ensured throughout their lifecycle, including ensuring that certificate and revocation status signing cryptographic hardware is not tampered with during shipment or storage, functions correctly when in operation and any private keys stored on the equipment are destroyed upon device retirement.

6.3 Other Aspects of Key Pair Management

CVCA certificates remain valid for three (3) years.

DV certificates remain valid for three (3) months.

IS certificates remain valid for one (1) month.

Maximum values are used for certificates. The CVCA may also issue certificates for a shorter period of validity. IS certificate validity depends on DV certificate validity. For example, if a DV certificate has 14 days left, an IS certificate will also be valid for 14 days. See also section 5.5 "Records Archival Procedures" above.

The activation data of the private keys are securely stored on authentication cards in possession of employees in trusted roles. Employees in trusted roles protect their authentication cards from loss and misuse and keep their activation code secret.

6.5 Computer Security Controls

The CVCA, DVs and ISs comply with the procedures for computer security controls described in section 5 "Management, Operational and Physical Controls" above.

6.6 Life Cycle Security Controls

The trustworthy devices used by CVCA, DVs and ISs are protected against modification.

The Digital and Population Data Services Agency maintains a security classification regarding service objects and systems, their securing, prioritisation, and minimum maintenance level, taking security factors into consideration.

6.7 Network Security Controls

The CVCA and DVs complies with the procedures for network security controls described in section 5 "Management, Operational and Physical Controls" above.

6.8 Time-stamping

Time-Stamping is not applicable.

7 Certificate and CRL Profiles

7.1 Certificate Profile

CV Certificates are as specified in section C. "CV Certificates" of TR-EAC.

7.1.1 CVCA certificate

The CVCA certificate is issued by the CVCA.

The CVCA keys are 256-bit ECDSA keys and the signature hash function is SHA-256.
Certification Authority Reference:

Country Code:	FI
Holder Mnemonic:	CVCA
Sequence number:	FI001…FI002 (alphanumeric series)

Certificate Holder Reference:

Country Code:	FI
Holder Mnemonic:	CVCA
Sequence number:	FI001…FI002 (alphanumeric series)

Validity = three (3) years

7.1.2 DV certificate

DV certificates are issued by the CVCA.

The DV keys are 256-bit ECDSA keys and the signature hash function is SHA-256.

BrainBool256 and Sha256 may not be used in other countries, so IS and DV certificates may differ from Finnish ones in terms of cryptographic curves, RSA, and so on.

Certification Authority Reference:

Country Code:	FI
Holder Mnemonic:	CVCA
Sequence number:	FI001…FI002 (alphanumeric series)

Certificate Holder Reference:

Country Code:	FI
Holder Mnemonic:	DV
Sequence number:	FI001…FI002 (alphanumeric series)

Validity = three (3) months

7.1.3 IS certificate

IS certificates are issued by a DV.

The IS keys are 256-bit ECDSA keys and the signature hash function is SHA-256.

BrainBool256 and Sha256 may not be used in other countries, so IS and DV certificates may differ from Finnish ones in terms of cryptographic curves, RSA, and so on.

Certification Authority Reference:

Country Code:	FI
Holder Mnemonic:	DV

Sequence number:	XX001…XX002 (alphanumeric series, XX is the country code of CVCA)

Certificate Holder Reference:

Country Code:	FI
Holder Mnemonic:	PASPR01 / PASPR02
Sequence number:	XX001…XX002 (alphanumeric series, XX is the country code of CVCA)

Validity = three (3) months

7.2 CRL Profile

CRL profile is not applicable.

7.3 OCSP Profile

OCSP profile is not applicable.

8 Compliance Audits and Other Assessments

A DV may only claim conformance with this Certificate Policy if it is able to show it is conformant with a National Certificate Policy that meets the standards set in this document. Other CVCAs must assess whether the National Certificate Policy is compliant with this Certificate Policy prior to issuing certificates to a DV operating under that policy. In the event of a dispute, arbitration takes place under the supervision of the European Commission.

Activities of the CVCA and a DV may be audited by the National Police Board in accordance with the agreement concluded between the Digital and Population Data Services Agency and the National Police Board.

The Digital and Population Data Services Agency inspects and audits the premises, equipment and activities of its technical suppliers as appropriate.

8.1 Audit Frequency

The Digital and Population Data Services Agency audits the activities of its technical suppliers every three years, or more frequently if necessary.

The Schengen evaluation takes place every five years.

8.1.1 Auditor

The Digital and Population Data Services Agency's information security audit is conducted by the Digital and Population Data Services Agency's certificate personnel and an external auditor specialised in the auditing of technical suppliers related to certificate services. The external auditor is an accredited auditor.

8.1.2 Audit subject matter and coverage

The audit subject matter is determined on the basis of the ISO 27001 Information Security Management Standard, the Digital and Population Data Services Agency's Information Security Policy or technical supply agreements. Full audits take place at least once every three years. The auditor also conducts annual assessments of whether activities meet policy requirements.

The information security aspects audited are confidentiality, integrity and availability. The audit assesses the policy and application instructions against the functioning of the entire certificate organisation and system. The Digital and Population Data Services Agency monitors the conformity of application instructions with the Certificate Policy.

In addition to administrative security, the audits also take service providers into consideration.

8.1.3 Measures taken in the event of anomalies

Any anomalies detected are recorded in the audit report and measures in response are taken in accordance with legislation, the ISO 27001 Information Security Management Standard and existing supply agreements.

8.1.4 Provision of information about audits

Information about audit results is provided in accordance with legislation, the ISO 27001 Information Security Management Standard, the Digital and Population Data Services Agency's Information Security Policy and existing supply agreements. Intended for internal use, the detailed fixed-form audit result is confidential and no details of it is published. The fixed-form reports are drawn up separately for use outside the organisation. Certificates of Conformity are also to DVs by the auditor.

The Digital and Population Data Services Agency informs the National Police Board about audit results.

In the event that an audit indicates that a DV is not conforming to its National Certificate Policy, the DV notifies all CVCAs from which it receives certificates.

9 Other Business and Legal Matters

9.1 Fees

Fees are not applicable.

9.2 Financial Liability

Liability is determined on the basis of the agreements applied, as applicable, in accordance with the provisions of the Damages Act (412/1974).

9.3 Confidentiality of Business Information

This Certificate Policy is a public document.

9.4 Privacy of Personal Information

ISs may not log or transmit fingerprint biometrics obtained from eMRTDs. These biometrics are deleted immediately after finishing the comparison process between the fingerprint biometric collected by the IS from the bearer and the fingerprint biometric read from the eMRTD.

Privacy and data protection issues are determined in accordance with the provisions of the Data Protection Act (1050/2018) and EU protection of natural persons with regard to the processing of personal data and on the free movement of such data (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)

9.5 Intellectual Property Rights

The Digital and Population Data Services Agency holds all ownership rights and copyrights to the CVCA certificate and DV certificates and related documentation in accordance with the supply agreements signed.

9.6 Representations and Warranties

Representations and warranties are not applicable.

9.7 Disclaimers of Warranties

Disclaimers of warranties are not applicable.

9.8 Limitations of Liability

The provisions of the agreements applicable apply to liabilities and limitations of liability.

The Digital and Population Data Services Agency is not liable for any loss or damage arising from the disclosure of the private key of the CVCA certificate or a DV certificate unless such disclosure is attributable to direct action by the Digital and Population Data Services Agency.

The Digital and Population Data Services Agency is not liable for any indirect or consequential loss or damage suffered by a party relying upon the CVCA certificate or a DV certificate or other contractual partner of the CVCA certificate or a DV certificate holder.

The Digital and Population Data Services Agency is not liable for the functioning of public communication connections or information network nor for the usage of the CVCA certificate or a DV certificate being disabled due to non-functioning of hardware or software used by the CVCA certificate or a DV certificate holder or a Relying Party nor for the usage of the CVCA certificate or a DV certificate against its purpose.

9.9 Indemnities

Liability for indemnities is determined on the basis of the agreements applicable, as applicable, the provisions of the Damages Act 412/1974.

9.10 Term and Termination

Term and Termination are in accordance with the regulations and agreements applicable.

9.11 Individual Notices and Communication with Participants

All key management tasks are carried out by robust communication channels. Such communications are carried out by email at a minimum, although other additional online or offline communication channels may be mutually agreed.

In the event of a disruption to the CVCA's normal communication channels, the CVCA notifies subscribing DVs of an alternate channel by which Certificate Requests can be submitted. This takes place in a timeframe that minimises the risk of current certificates expiring.

Email messages must conform to the following format.

9.11.1 Register

Subject:	Register
Body:	URLs to be used to contact this state
Attachments:	none

9.11.2 CVCA Certificate

Subject:	CVCA Certificate
Body:	Unspecified
Attachments:	CVCA Link Certificate(s)

9.11.3 DV Certificate Request

Subject:	DV Certification Request
Body:	Unspecified
Attachments:	Certificate Request(s)

9.11.4 DV Certification Receipt Acknowledgement

Subject:	DV Certification Request Receipt Acknowledgement
Body:	Unspecified
Attachments:	Certificate Request(s)

9.11.5 DV Certificate

Subject:	[Reply to] DV Certification Request
Body:	If a DV certificate is not to be issued, the reason why.
Attachments:	DV Certificate (if at least one is issued)

9.11.6 Suspension of CVCA Service

Subject:	{Nation States} CVCA Suspension
Body:	Details of start and end date of CVCA service suspension
Attachments:	Unspecified

9.12 Amendments

The Certificate Policy is accepted by the Digital and Population Data Services Agency. Amendments to this document are made following a mutual decision by the Digital and Population Data Services Agency and the National Police Board.

The Digital and Population Data Services Agency performs document version management and archive all certificate policies. Typographic corrections and changes in contact details may be made immediately.

1. Amendments to any item of this Certificate Policy may be made following a notice of future amendments to main substance given 90 days before their entry into force.

2. Items that the Digital and Population Data Services Agency does not regard as having a significant impact on the certificate holder and Relying Parties may be amended without prior notice.

3. The CP OID is changed if it is determined that a change in the CP modifies the level of trust provided by the CP.

9.13 Dispute Resolution Procedures

When issuing certificates, the Digital and Population Data Services Agency ensures the compliance of the CVCA certificate and DV certificates with the requirements set in this Certificate Policy. Any disputes are settled in accordance with Finnish law.

9.14 Governing Law

Provisions regarding the status of the Digital and Population Data Services Agency are laid down in the Act on the Population Information System and the certificate services of the Digital and Population Data Services Agency (661/2009).

Liability for damages related to the provision of services described in this Certificate Policy are, as applicable, determined in accordance with the provisions of the Damages Act (412/1974).

9.15 Compliance with Applicable Law

The CVCA and DV certificates issued in accordance with this Certificate Policy meet the requirements set in the Passport Act (671/2006).

9.16 Miscellaneous Provisions

Miscellaneous provisions are not applicable.

9.17 Other Provisions

Other provisions are not applicable.

Version

CVCA Certificate Policy for Extended Access Control to Fingerprint Biometrics on Finland's Electronic Machine Readable Travel Documents v.1.1

CVCA Certificate Policy
v. 1.1

11.6.2025

Version	Date	Description / changes
v 1.0	31.10.2010	Accepted version 1.0.
v 1.1	11.6.2025	Agency’s name changed, TR-03110 references updated, TR-03139 reference added, and law references updated. The National Police Board of Finland’s comments applied.