KeyOne

eMRTD Solutions

Safelayer.com

Document Reference: K1_EMRTD

Product Release: 4.0.16S1R1

CONTENTS

CHAPTER 1

eMRTD Overview

An eMRTD (electronic Machine Readable Travel Document) is a travel document containing identification data that can be validated by reader terminals. To ensure the interoperability between nations when identifying people at border controls, two main eMRTD standards have been defined: ICAO eMRTD and EAC eMRTD.

As outlined in Figure 1-1, these standards define both PKI entities and communication protocols.

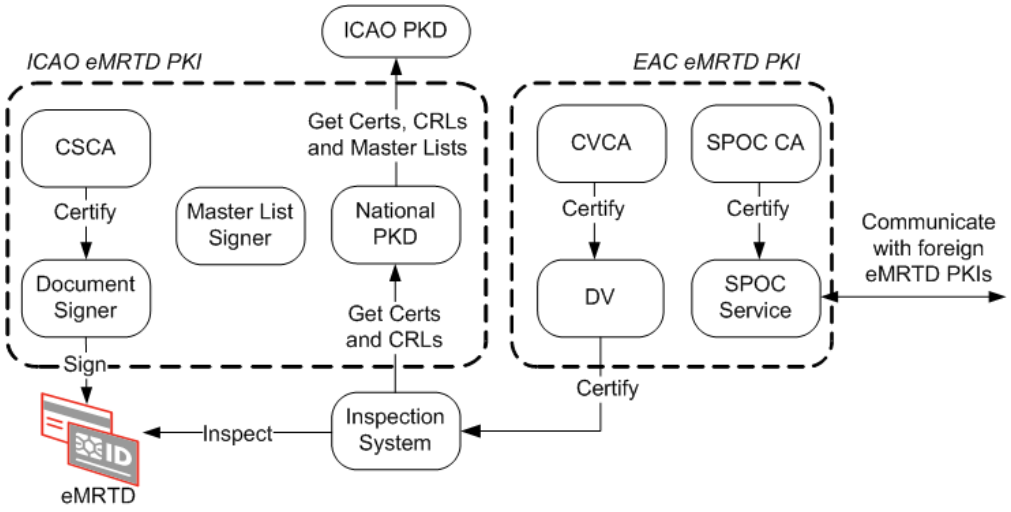

Figure 1-1. eMRTD PKI entities.

ICAO eMRTD

The International Civil Aviation Organization (ICAO) created an international standard for the first generation of ePassports. This standard is known as ICAO eMRTD and entails storing personal and basic biometric data on an RFID chip.

Note
See Doc 9303, Machine Readable Travel Documents for advanced details on first generation standards.

ICAO standard ensures both the authenticity and originality of eMRTDs. This is done by signing the personal and biometric data held on the eMRTD chip.

For issuing national eMRTDs, the personal and biometric data of the holder is signed by a national **Document Signer** (DS) using a certificate issued by the national **Country Signing Certification Authority** (CSCA). Thus, the CSCA operates as the root CA of the national ICAO PKI and certifies the national Document Signers. The personal and biometric data and the signature are stored in the chip of the eMRTD.

To read the personal data on an eMRTD, a national or foreign **Inspection System** (IS) must perform a set of security operations.

First of all, since the IS reads the data stored in the eMRTD's chip by Radio Frequency ID (RFID), the IS establishes a secure channel to prevent unauthorized accesses (eavesdropping) of the data stored in the chip. The IS optically scans the Machine Readable Zone (MRZ) of the eMRTD and, using the **Basic Access Control** (BAC) protocol, derives a session key from the MRZ to establish a secure (encrypted) communication with the eMRTD's chip.

Secondly, the IS ensures the integrity (i.e., to detect illegal modifications) of the data on the eMRTD's chip. To do this, the IS, using the **Passive Authentication** (PA) protocol, verifies the signature generated by the DS that is stored in the eMRTD's chip. The IS validates the signature using the following material: the certificate used by the DS to sign the data, the certificate of the CSCA that issued the DS certificate and a fresh CRL to check the validity status of the DS certificate. To obtain this cryptographic material, the IS usually contacts the **National Public Key Directory** (NPKD).

Lastly, the IS verifies the originality of the data (i.e., it checks for eMRTD cloning) where the eMRTD's chip supports this feature. Using the **Active Authentication** (AA) protocol, the IS sends a signature challenge to the eMRTD. The chip signs the received data using the private key in its cryptographic chip.

EAC eMRTD

The European Union adopted Extended Access Control (EAC) standard for the second generation of eMRTD. These MRTD offer improved security mechanisms against the fraudulent use of the personal data stored on the eMRTD's chip.

Note
See Advanced Security Mechanisms for Machine Readable Travel Documents (BSI TR-03110) *for advanced details on second generation standards.*

The objective of Extended Access Control is to protect the authenticity, originality, and confidentiality of the biometric data stored on eMRTD chips. This is done by adding the capability of authenticating (national and foreign) Inspection Systems (IS) trying to access the

data in the chip to the eMRTD's chip. Each **Inspection System** is provided with card-verifiable (CV) certificates for this purpose.

Each state manages one **Country Verifying CA** (CVCA) that issues CV certificates to **Document Verifiers** (DV). The CVCA typically delegates registration responsibilities to an associated **Country Verifying RA** (the CVRA).

In turn, each national DV acts as a subordinate CA that issues CV certificates to national Inspection Systems (IS). ISs are the end-entities of the PKI and hold certified keys for authenticating with MRTD chips. A DV must be certified by both

- the national CVCA and
- the foreign CVCAs of all states whose eMRTD wants to inspect via the Inspection Systems in its domain.

Each state manages one **Single Point Of Contact** (SPOC) that handles communication between national CVCA and DVs with counterparts in other states.

Note

See Country Verifying Certification Authority Key Management Protocol for SPOC (Česká Technická Norma ČSN 36 9791) *for advanced details about SPOC.*

When issuing a CV certificate to a DV, the CVCA of state *S* can grant the DV access rights to sensitive information stored in the eMRTD of nationals of state *S* (these access rights are included in the CV certificate).

The DV, in turn, issues certificates to all its ISs for each state (possibly further restricting the access rights). All DVs and ISs need to hold multiple certified key pairs, one per state.

To inspect the eMRTD of a national of state *S*, an IS authenticates against the chip by presenting its CV certificate for state S's certificate hierarchy and the corresponding certificate chain. The chip validates the IS certificate and grants the IS access rights to sensitive data according to the information in the certificate. The chip can validate the certificate chain because it knows the public key of state *S*'s CVCA (this public key was inserted in the chip at the eMRTD personalization phase).

As a result of this requirement, each IS needs to generate and use multiple key pairs stored in a secure device, such as an HSM, for authenticating against the eMRTDs of the different states. In turn, the ISs need to access the cryptographic material (CSCA certificates, DS certificates and CRLs of all states) stored in the national PKD to verify the integrity and authenticity of the eMRTD's data.

CHAPTER 2

KeyOne eMRTD Solutions Overview

The KeyOne family of PKI products comprises the solutions required for deploying the eMRTD standards introduced in *eMRTD Overview*, page 4.

As outlined in the following sections, these solutions facilitate the easy integration of all services.

KeyOne Solutions for ICAO eMRTD

The KeyOne product family provides the solutions required for deploying an ICAO eMRTD infrastructure (*Figure 2-1*). See the following chapters for a detailed description of each solution.

- *Country Signing CA*, page 10.
- *Document Signer*, page 12.
- *National Public Key Directory*, page 14.
- *CSCA Master List Signer*, page 17.

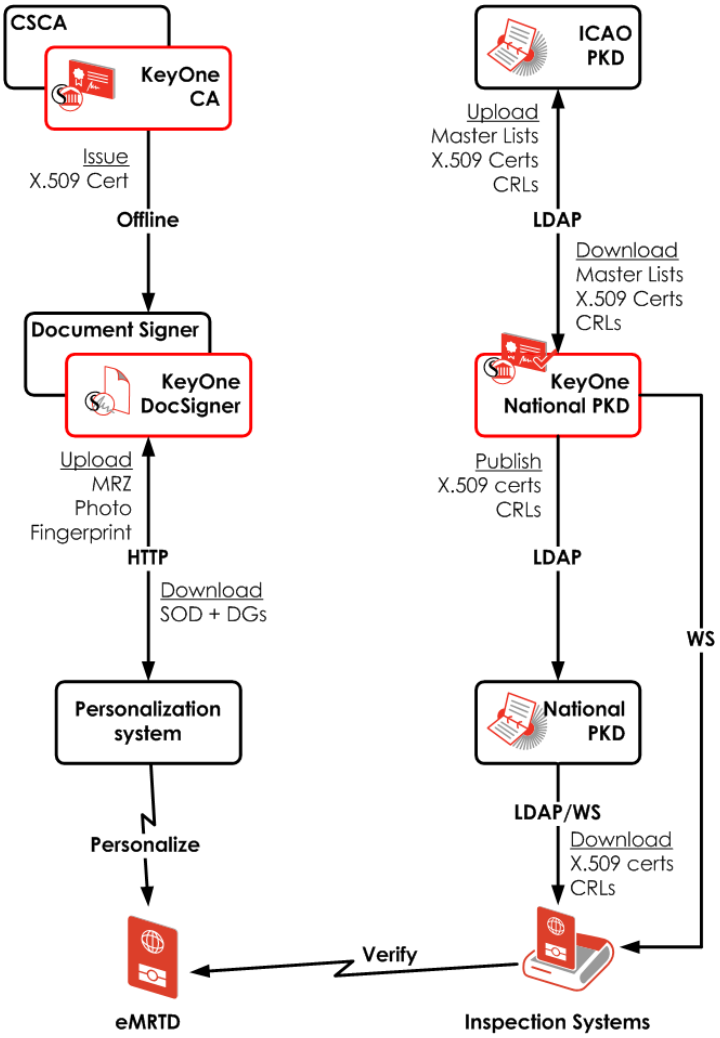

Figure 2-1. KeyOne solutions for an ICAO eMRTD infrastructure.

KeyOne Solutions for EAC eMRTD

The KeyOne product family provides the solutions required for deploying an EAC eMRTD infrastructure (*Figure 2-2*). See the following chapters for a detailed description of each solution.

- *Country Verifying* CA, page 19.
- *Country Verifying* RA, page 26.
- *Single Point* of Contact, page 31.
- *Document Verifier*, page 34.

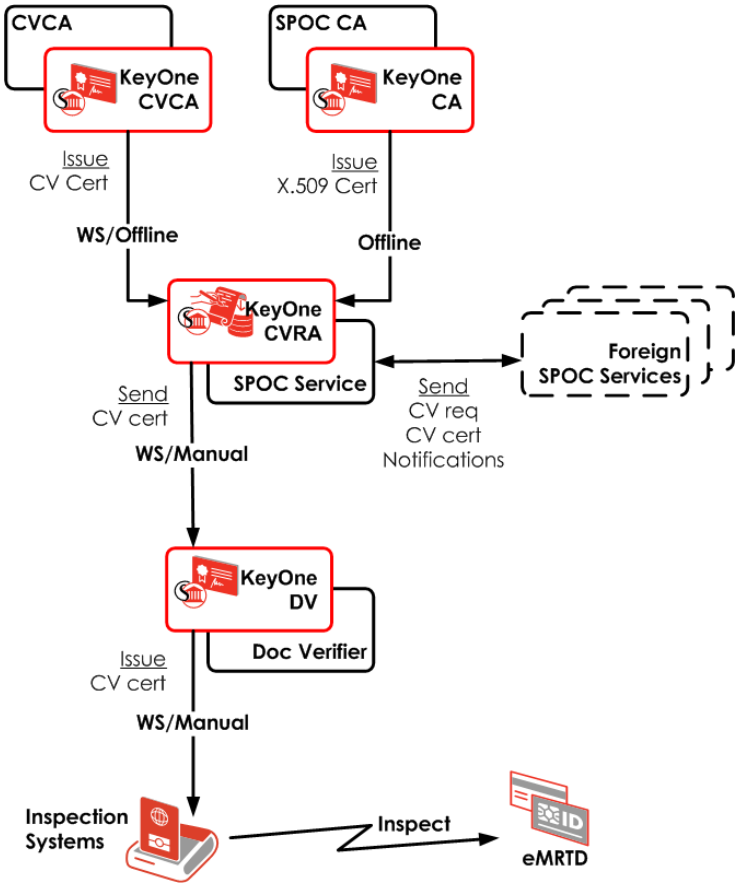

Figure 2-2. KeyOne solutions for an EAC eMRTD infrastructure.

CHAPTER 3

Country Signing CA

This chapter introduces the main functions of a Country Signing CA and describes the KeyOne solution for implementing them.

What is a Country Signing CA?

In an ICAO eMRTD PKI, a Country Signing CA (CSCA) is the root Certification Authority (CA) that:

- Issues certificates for national Document Signers, Master List Signers and Defect List Signers.
- Issues Certificate Revocation Lists (CRL) that report the validity status of the issued certificates.

KeyOne's CSCA

KeyOne CA is the native Certification Authority of the KeyOne family. This application fully supports the functionality required for it to be deployed as a CSCA.

As explained in the Safelayer documentation, KeyOne CA can be customized via a complete set of add-ins and a graphically-configurable workflow. For example, KeyOne CA supports advanced features such as:

- Automated publication of the issued certificates and CRLs.
- Notifications via mail (e.g., certificate expiry).
- A complete set of online Web services (with SOAP/XML and REST/JSON interfaces).

These features facilitate straightforward integration as described in the following sections.

Integration with National Document Signers

When operating as a CSCA, KeyOne CA issues certificates for the national Document Signers, which entails:

1. The Document Signer to be certified generating a X.509 certificate request batch.
2. KeyOne CA processing the batch and issuing the corresponding certificates in a response batch.
3. The Document Signer processing the response batch and enabling the included certificates.

Eventual revocation of these certificates is reported by the CRLs issued by the same CSCA.

Note

See Document Signer*, page 12, for a description of the KeyOne eMRTD Document Signer solution.*

Integration with Public Key Directories

Certificates and CRLs issued by each CSCA must be published in public key directories. KeyOne CA fully supports the certificate and CRL publication operations typically required of a CSCA.

For example, KeyOne CA can automatically publish the issued certificates and CRLs in the LDAP directory of either the ICAO PKD or the national PKD (NPKD).

Note

See National Public Key Directory*, page 14, for a description of the* KeyOne eMRTD National PKD *solution for PKD management.*

CHAPTER 4

Document Signer

This chapter introduces the main functions of a Document Signer and describes the KeyOne solution for implementing them.

What is a Document Signer?

In an ICAO eMRTD PKI, a Document Signer is an entity that signs the personal and biometric data stored in the eMRTD's chip.

Each eMRTD contains identification data on the document's owner (e.g., name, photograph, fingerprint) distributed in **Data Groups**. Once signed by an eMRTD Document Signer, this data is returned as a **Document Security Object**.

KeyOne eMRTD Document Signer

KeyOne eMRTD Document Signer implements all the functionality of a Document Signer. KeyOne eMRTD Document Signer main strengths are:

- *Integration with eMRTD Issuing Systems*
- *Support for Multiple Signature Owners*

Integration with eMRTD Issuing Systems

KeyOne eMRTD Document Signer has two online services for processing different request formats:

- The **DocSigner** service signs the owner's data received in Data Groups (binary message).
- The **DocSigner XML** service signs the owner's data received in an XML message.

Support for Multiple Signature Owners

KeyOne eMRTD Document Signer supports the following deployments:

- Multiple KeyOne eMRTD Document Signer applications are deployed and each of them signs eMRTD with its own key (certified by the national CSCA).
- A single KeyOne eMRTD Document Signer signs eMRTD with the same key but on behalf of different authorized entities (e.g., on behalf of different embassies of the same state).

CHAPTER 5

National Public Key Directory

This chapter introduces the main functions of a national Public Key Directory and describes the KeyOne solution for implementing them.

What is a National Public Key Directory?

In order to validate an eMRTD of state *S* (via Passive Authentication), the Inspection System needs the following material:

- The certificate used by the Document Signer of state *S* to sign the eMRTD.
- The certificate used by the CSCA of state *S* to issue the Document Signer certificate.
- The last CRL issued by the CSCA of state *S*.

However, the ICAO PKD does not provide the certificates and CRLs for all states, and direct requests from each Inspection System would be highly inefficient.

Therefore, it is preferable to deploy a **National PKD** that provides certificates and CRLs to national Inspection Systems. These certificates and CRLs are obtained from the following sources:

- ICAO PKD.
- Out-of-band communication (e.g., diplomatic exchange, direct communication with the national CSCA).

KeyOne eMRTD National PKD

KeyOne eMRTD National PKD operates as a broker for the National PKD. This application performs the operations described in the following sections.

Obtaining Data

KeyOne eMRTD National PKD provides automatic online updating of the certificates and CRLs managed by the ICAO PKI. This material is obtained by from different sources:

- The ICAO PKD, from which KeyOne eMRTD National PKD downloads foreign CSCA certificates, DS certificates, Certificate Revocation Lists andMaster lists.
- The national CSCA, from which KeyOne eMRTD National PKD obtains national CSCA certificates, DS certificates and CRLs.
- The national Defect List Signer, from which KeyOne eMRTD National PKD obtains national Defect Lists.
- Out-of-band communication (e.g., diplomatic exchange), via which KeyOne eMRTD National PKD can obtain certificates, CRLs, Master Lists and Defect Lists from a foreign state.

Note
Data download procedures can be executed either manually or automatically.

Data Approval

CSCA certificates can be approved either manually or automatically.

When a link CSCA certificate—signed by an already-approved CSCA certificate—is available, both the link CSCA certificate and the root CSCA certificate are automatically approved by KeyOne eMRTD National PKD.

Note
When renewing a CSCA certificate, a new CSCA root certificate is issued. Optionally, a certificate with the same public key of the new root is signed by the previous root certificate. This certificate ensures the authenticity of the new one and is referred as ***link certificate****.*

When no link certificate is available, the Registration Approver must explicitly approve an obtained CSCA certificate. To facilitate this decision, KeyOne eMRTD National PKD displays the Master Lists that include the CSCA certificate.

Note
A Master List is a list of CSCA certificates trusted by a state and signed by a certificate issued by the national CSCA of this state.

Once a CSCA certificate is approved, all CRLs and DV certificates issued using this CSCA certificate are automatically approved. Thus, KeyOne eMRTD National PKD regularly provides trusted updates of CSCA certificates, DS certificates and CRLs.

Data Publication

KeyOne eMRTD National PKD can publish approved material in different repositories.

Note
Data publication procedures can be executed either manually or automatically.

Data Publication in the National PKD

KeyOne eMRTD National PKD regularly publishes the following approved data in the National PKD:

- DS certificates
- CSCA CRLs
- CSCA root certificates
- CSCA link certificates
- CSCA Master Lists
- Defect Lists

Data Upload to the ICAO PKD

KeyOne eMRTD National PKD can upload the following material to the ICAO PKD:

- National CSCA Master Lists issued by the application
- CSCA CRLs issued by the national country signing CA
- DS certificates issued by the national country signing CA

Note
CSCA root certificates are not automatically uploaded because ICAO PKD only supports out-of-band publication of these certificates.

Web Service for Inspection Systems

Although Inspection Systems can access the national PKD to obtain the certificates and CRLs, KeyOne eMRTD National PKD provides a Web service (with SOAP/XML and REST/JSON interfaces) for distributing the data needed by Inspection Systems to validate the eMRTD's biometric data (Passive Authentication).

This Web service allows Inspection Systems to access the cryptographic material without needing LDAP or Active Directory client. By using just a SOAP or REST client, Inspection Systems can retrieve the required data for validating national and foreign eMRTD.

CHAPTER 6

CSCA Master List Signer

This chapter introduces the functions of a CSCA Master List signer and describes the KeyOne solution for implementing them.

What is a CSCA Master List Signer?

A CSCA Master List is a list of CSCA certificates trusted by a state, i.e., a list of CSCA root or link certificates:

- Not expired
- Approved by the national PKI.

The CSCA Master List Signer of a state is the entity that signs national CSCA Master Lists to ensure their authenticity.

Note
CSCA Master Lists must be signed with a certificate issued by the national Country Signing CA.

KeyOne's CSCA Master List Signer

As explained in *National Public Key Directory*, page 14, the KeyOne eMRTD National PKD application:

- Compiles validation material.
- Approves CSCA certificates.

It centralizes all the data required to build CSCA Master Lists. KeyOne eMRTD National PKD is the KeyOne solution for issuing, signing and publishing CSCA Master Lists.

CSCA Master List issuing

In KeyOne eMRTD National PKD, CSCA Master List can be signed and issued

- On-demand, via a graphical wizard.
- Automatically, via programmed tasks.

CSCA Master Lists Publication

KeyOne eMRTD National PKD's publication functionality entails the publication of the issued CSCA Master Lists in the ICAO PKD.

As with CSCA Master List issuing, this operation can be performed either manually or automatically.

CHAPTER 7

Country Verifying CA

This chapter introduces the main functions of a Country Verifying CA and describes the KeyOne solution for implementing them.

What is a Country Verifying CA?

In an EAC eMRTD PKI, a Country Verifying CA (CVCA) is a root Certification Authority that:

- Issues and renews CV certificates for national and foreign Document Verifiers.
- Authenticates initial certificate requests sent by national Document Verifiers to foreign CVCAs.
- Authorizes or unauthorizes Document Verifiers. When a Document Verifier is unauthorized, all its requests are discarded by the CVCA (even if properly authenticated).

KeyOne's Country Verifying CA

When extended with the **eMRTD Country Verifying CA** add-in, **KeyOne CA** implements all the functionality required of a Country Verifying CA. KeyOne's CVCA's main strengths are:

- *CVCA Key Management*
- *CV Certificate Profiles*
- *Document Verifier Enrollment*
- *Key Renewal Management*
- *Support for X.509* Keys

Note
Although KeyOne eMRTD Country Verifying CA is intended to operate in online mode, Web service capabilities could easily be disabled if it were considered necessary.

CVCA Key Management

KeyOne eMRTD Country Verifying CA holds a key pair with an associated CV certificate. One of the first tasks of the KeyOne eMRTD Country Verifying CA's Security Officer is to configure the properties of this key pair and certificate:

- CVCA country code and mnemonic.
- Cryptographic algorithms.
- Domain parameters (where the ECDSA is used).
- Initial key pair sequence number.
- Certificate validity period.

The Security Officer triggers the generation of the key pair and the CV certificate in line with the configured properties. The first certificate of the CVCA is always self-signed. The certificate is submitted to the European Commission for distribution to other states.

The CVCA private key is generated and protected by a Hardware Security Module, which must be configured when the KeyOne system of the CVCA is initialized.

Note

The generated key must be activated for the CVCA to become operative (as discussed later).

CV Certificate Profiles

The characteristics of the issued DV certificates (e.g., validity period, access rights to eMRTD sensitive data) are defined by the CVCA Security Officer via the CV certificate profiles. These are similar to the X.509 certificate profiles included in the KeyOne CA certification policies but are based on a different set of rules.

As with X.509 certificate profiles, a CV certificate profile includes rules for performing certain checks on the certificate request (e.g., checking that the cryptographic algorithms and the domain parameters in the request match the CVCA's). If one of these checks fails, the request is rejected.

The Security Officer can define any number of CV certificate profiles. Each profile is given a unique name. When issuing a certificate to a Document Verifier, the Registration Officer chooses one of the configured profiles.

CV certificate profiles are also used to define the data to be included in the CVCA self-signed certificate and some options for the generation of the CV link certificate (such as the inclusion or exclusion of the EC domain parameters where applicable).

Document Verifier Enrollment

KeyOne eMRTD Country Verifying CA provides the following DV enrolment operations.

Note

These operations can be integrated with the functionality of KeyOne eMRTD Country Verifying RA. This application provides a stateful and client-oriented system for request approval. This means that KeyOne eMRTD Country Verifying RA centralizes all information on request processing, making the management of the approval process easier.

Process an initial DV certificate request (non-authenticated)

The application processes the first CV certificate request from a DV when the request is non-authenticated (this happens mainly for national DVs). Explicit approval of the request by the Registration Officer is required.

Process an initial DV certificate request (authenticated)

The application processes the first CV certificate request from a foreign DV when the request has been authenticated by the respective CVCA. The Security Officer must have previously imported the current certificate of the foreign CVCA (a self-signed or a link certificate) as a trusted certificate.

Process a DV certificate renewal request

The application processes an authenticated CV certificate request from a DV previously certified by the CVCA. The CV certificate profile that was used to issue the previous certificate to that DV is proposed by default to the Registration Officer.

Authenticate a DV certificate request

The application authenticates the initial CV certificate request from a national DV before it is submitted to the CVCA of another state. This is part of the initial registration process of a DV in a foreign CVCA.

Revoke an issued DV certificate

The application discards non-recognized DV certificates. Discarding a certificate already delivered to the respective DV causes the rejection of subsequent authenticated requests from that DV signed with the revoked certificate.

Key Renewal Management

The rekeying ceremony of a CVCA entails the generation of both a new key pair and a CV link certificate.

Note

The CV link certificate is signed by the previous CVCA key, which allows the rest of the PKI components and the state's MRTD chips to automatically verify and accept the renewed CVCA certificate as a new trust point.

KeyOne does not enforce that the new key be immediately activated for DV certification purposes. During the time when the new key has been generated but not yet activated, DV certificates are signed with the old (current) key.

To manage this transition period, the Security Officer of KeyOne eMRTD Country Verifying CA can configure the following rekeying parameters:

- *Next key activation period*
- *Renewal start period*

Both parameters control when the respective notifications appear in the key management to-do list along with the appropriate actions to be taken. Configuring these periods is optional, although the Security Officer can force the renewal and activation of the key at any moment.

Next key activation period

The next key activation period is the moment, expressed as the period left until the current CV certificate expires, in which the new certified key can be activated.

A criterion for choosing the key activation period is the concept of maximum distribution time. The new key should start being used with sufficient time in advance so that all entities lower down in the hierarchy (DVs and Inspection Systems) can be re-certified before the current CVCA certificate expires.

The key activation period should be equal or greater than the validity period of the DV certificates issued by the CVCA (this period is configured in the CV certificate profiles). Following this rule avoids generating certificates with a validity period exceeding the expiration date of the signing certificate.

Note

*In case of this latter situation, the behavior is dictated by the **Adjust expiration date to CA** rule in the CV certificate profiles. The possible actions are issuing an error, truncating the resulting DV expiration date to the CVCA expiration date or truncating only if both dates are sufficiently near. This rule also allows extending the resulting DV expiration date to make it coincide with the CVCA expiration date, as per a configurable maximum adjustment period.*

Renewal start period

The renewal start period is the moment, expressed as the period left until the current CV certificate expires, in which the rekeying process can be started.

The renewal start period is normally chosen once a decision has been made on the key activation period. One possibility is to define the renewal start period as the key activation period plus an estimate of the maximum time the CVCA rekeying ceremony will last.

- Where it is necessary to submit the new CVCA certificate to the European Commission before starting to issue DV certificates with the new key, the renewal start period must also take into account the estimated maximum time that this process will require.
- Alternatively, the renewal start period and the key activation period can be set to the same value (the maximum distribution time). In this case, the key activation period can be left empty, meaning that the new certified key can be activated as soon as it is generated.

Support for X.509 Keys

Since the full functionality of KeyOne CA is available, the CVCA can also be set up to issue X.509 certificates. This allows the CVCA to issue X.509 service and infrastructure certificates required by other PKI components lower down in the hierarchy (typically, the associated CVRA and national Document Verifiers), without the need for an additional CA for that purpose.

In this case, and in addition to the CV-certified key pair, the CVCA needs X.509-certified key pairs for the following purposes:

- X.509 certificate signing
- KeyOne batch signing

Important
The CVCA key is not X.509 certified and therefore cannot be used for the above-mentioned purposes; different key pairs need to be set up.

CHAPTER 8

SPOC CA

This chapter introduces the functions of a SPOC CA and describes the KeyOne solution for implementing them.

What is a SPOC CA?

When communicating with foreign states, each SPOC endpoint requires TLS certificates for client and server operation. Thus, in an EAC eMRTD PKI, the SPOC CA is the Certification Authority (CA) that:

- Issues X.509 SSL/TLS certificates for the national SPOC endpoint.
- Generates Certificate Revocation Lists that report the validity status of the issued certificates.

Depending on the selected deployment, these certificates and CRLs can be issued by:

- A single root SPOC CA.
- An intermediate SPOC CA certified by the root SPOC CA.

Both deployments can be implemented by KeyOne solutions.

Note
See Single Point *of Contact, page 31, for a description of the* KeyOne's SPOC *solution.*

KeyOne's SPOC CA

KeyOne CA is the native Certification Authority of the KeyOne family. When extended with the KeyOne CRL Authority add-in, this application fully supports the functionality required for it to be deployed as either a root SPOC or intermediate SPOC CA for:

- Issuing SPOC TLS client certificates.
- Issuing SPOC TLS server certificates.

- Issuing and publishing CRLs that report the validity status of the issued certificates.

Note

The KeyOne CA workflow facilitates the straightforward configuring of certificate and CRL automated publication.

CHAPTER 9

Country Verifying RA

This chapter introduces the main functions of a Country Verifying RA and describes the KeyOne solution for implementing them.

What is a Country Verifying RA?

To read the sensitive data of a foreign eMRTD, a national Inspection System must hold a certificate with the following validation chain:

- **Root CA**: CVCA of foreign state.
- **Subordinate Issuing CA**: national Document Verifier.

Therefore, a national CVCA must:

- Issue certificates for the Document Verifiers of all states allowed to inspect national eMRTD.
- Frequently renew the issued DV certificates because their validity is quite short (e.g., the EAC standard recommends a maximum validity of 3 months).

In this context, a Country Validation RA is a Registration Authority to which the CVCA can delegate the registration of the frequently-received certification and renewal requests.

Note

See Country Verifying *CA, page 19, and* Document Verifier*, page 34, for a description of the KeyOne solutions for deploying CVCAs and Document Verifiers.*

KeyOne eMRTD Country Verifying RA

KeyOne eMRTD Country Verifying RA operates as a gateway for the certification of national and foreign Document Verifiers. The main strengths of KeyOne eMRTD Country Verifying RA are:

- *Online and Offline Integration*
- *Built-in SPOC Endpoint*
- *DV Certificate Profiles*
- *Support for Different Registration Scenarios*
- *Manual and Automatic Request Processing*

Online and Offline Integration

KeyOne eMRTD Country Verifying RA supports full online integration with national and foreign entities (*Figure 9-1*):

- Communication with the national CVCA and the national Document Verifiers is performed either online (via Web services) or offline (via file exchange). When communicating online, KeyOne eMRTD Country Verifying RA operates as a client for the KeyOne eMRTD Country Verifying CA's Web service and as a server for national Document Verifiers.
- Communication with foreign CVCAs and Document Verifiers is performed either online (via the SPOC protocol) or offline (via diplomatic exchange).

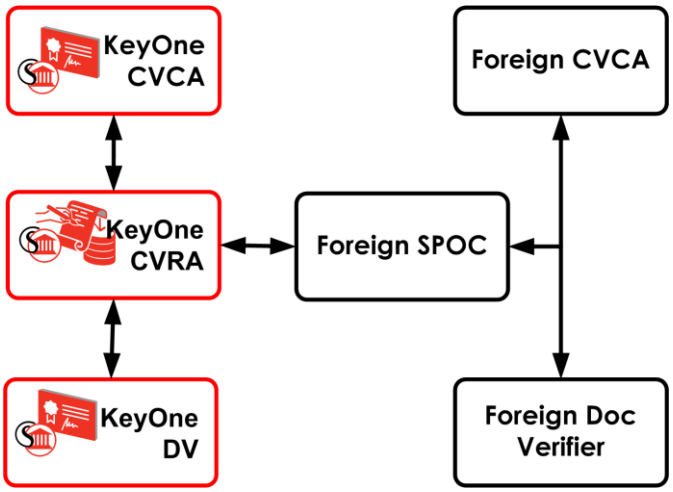

Figure 9-1. KeyOne eMRTD Country Verifying RA integration.

Built-in SPOC Endpoint

In the KeyOne EAC PKI, both the SPOC client and server are integrated in the KeyOne eMRTD Country Verifying RA application. Therefore, when processing certification requests, communication with foreign states is performed directly from KeyOne eMRTD Country Verifying RA.

Note

See Single Point *of Contact, page 31, for a description of KeyOne's SPOC integrated solution.*

DV Certificate Profiles

When the national CVCA certifies a DV, the issued certificate has access to the privileges on national eMRTD. When this DV certifies an Inspection System, the issued certificate inherits all or some of the access privileges granted to the DV certificate. Therefore, the CVCA manages the privileges granted to each DV. For example, certificates issued for national Document Verifiers can hold higher access privileges than certificates issued for foreign Document Verifiers.

The management of DV certificate privileges can be delegated by the CVCA to KeyOne eMRTD Country Verifying RA. When registering a Document Verifier, the Registration Officer of KeyOne eMRTD Country Verifying RA selects a specific certificate profile that determines the properties of the certificates issued by the national CVCA for this DV (e.g., access privileges, certificate validity).

Support for Different Registration Scenarios

KeyOne eMRTD Country Verifying RA supports all the registration scenarios in an EAC eMRTD PKI:

- *Registering a DV Request for the National CVCA*
- *Registering a DV Request for a Foreign CVCA*

Note

In KeyOne eMRTD Country Verifying RA, each Document Verifier is associated to a CV certification profile configured in the CVCA.

Registering a DV Request for the National CVCA

When a national or foreign Document Verifier is certified by the national CVCA, the KeyOne eMRTD Country Verifying RA application:

1 Receives the DV certificate request from the national or foreign DV.

2 Processes the request (as explained in following section *Manual and Automatic Request Processing*, page *29*).

3 Routes the request to the national CVCA.

4 Receives the issued certificate from the national CVCA.

5 Returns the certificate to the national or foreign DV that requested it.

Registering a DV Request for a Foreign CVCA

When a national Document Verifier is certified by a foreign CVCA, the KeyOne eMRTD Country Verifying RA application:

1 Receives the certificate request from the national DV.

2 Processes the request (as explained in following section *Manual and Automatic Request Processing*, page 29).

3 Routes the request to the SPOC endpoint of the foreign state.

4 Receives the issued certificate from the SPOC endpoint of the foreign state.

5 Delivers the certificate to the requesting national DV.

This approach means that national Document Verifiers do not communicate directly with foreign CVCAs and, therefore:

- Frees Document Verifiers of transport-related issues on the certification protocol between states.
- Facilitates management of exceptional situations by providing a unique inter-state communication point.

Manual and Automatic Request Processing

DV Certification requests received by KeyOne eMRTD Country Verifying RA can be processed either manually or automatically as described in the following sections.

Manual Approval of Initial DV Requests (Non-Authenticated)

Initial DV requests addressed by national or foreign Document Verifiers to the national CVCA only need to be approved by the Registration Officer before they are sent to the national CVCA. By contrast, initial DV requests addressed by national Document Verifiers to a foreign CVCA must be authenticated and processed as follows:

1 The Registration Officer of KeyOne eMRTD Country Verifying RA approves the request.

2 KeyOne eMRTD Country Verifying RA sends the request to the national CVCA.

3 The national CVCA authenticates (i.e. countersigns) the request.

4 The authenticated request is sent back to KeyOne eMRTD Country Verifying RA.

5 KeyOne eMRTD Country Verifying RA forwards the authenticated request to the SPOC endpoint of the foreign state.

Important
Non-authenticated requests must be obtained from a trusted source (e.g., diplomatic exchange).

Automatic Processing of Authenticated DV Requests

The EAC standard defines the following types of authenticated DV requests:

- DV renewal requests, which are authenticated by the previous DV certificate.
- Initial DV requests from a foreign state, which are authenticated by the respective foreign CVCA.

Once received by KeyOne eMRTD Country Verifying RA, both types of DV requests are automatically approved and forwarded to the corresponding CVCA.

CHAPTER 10

Single Point of Contact

This chapter introduces the Single Point of Contact (SPOC) and describes the KeyOne solution for implementing it.

What is the Single Point of Contact?

In an EAC eMRTD PKI, the Single Point of Contact (SPOC) is the unique endpoint for online communication with foreign states. This point of contact must be implemented as a Web service with a standard SOAP/XML interface. Communication between SPOC endpoints is performed via the SPOC protocol (secured via SSL/TLS).

Note

The Web service protocol outlined here meets the requirement of the "ČSN 36 9791 Country Verifying Certification Authority Key Management Protocol for SPOC" document, published on 1 December 2009.

The national SPOC sends the following requests to foreign SPOC endpoints:

- **National DV Certification Requests**. When a national DV needs to be certified by a foreign CVCA, the national SPOC forwards the request to the SPOC endpoint of the corresponding foreign state.
- **National CVCA Certificates**. The first certificate of the national CVCA is distributed out-of-band to the foreign states (e.g., via diplomatic exchange), whereas renewed CVCA certificates are distributed by the national SPOC.
- **Notifications**. The national SPOC notifies the foreign SPOC servers of some operational issues in the national EAC eMRTD PKI (e.g., CVCA service suspension, a compromised DV key).
- **Foreign DV Certificates**. When the national CVCA certifies a foreign DV, the issued certificate is sent to the SPOC server of the foreign states.

The national SPOC receives the following requests from foreign SPOC endpoints:

- **Foreign DV Certification Requests**. When a foreign DV must be certified by the national CVCA, the foreign SPOC sends the request to the national SPOC.

- **CVCA Certificates**. When a foreign CVCA certificate is renewed, the foreign state distributes the new CVCA certificate to the other SPOC endpoints in requests.
- **Notifications**. Some operational issues in the foreign EAC eMRTD PKIs (e.g., CVCA service suspension, a compromised DV key) are reported in requests to the other SPOC endpoints.
- **National DV Certificates**. When a foreign CVCA certifies a national DV, the issued certificate is sent to the national SPOC in a request.

KeyOne's SPOC

KeyOne eMRTD Country Verifying RA implements both the SPOC client and server for automated operations and notifications between states. Its main strengths are:

- *Support of multiple CVCAs per State*
- *Manual and Automatic Request Sending*
- *Synchronous and Asynchronous Operation*

Note

To test other SPOC implementations and its interoperability, Safelayer offers a complete SPOC system at http://labs.safelayer.com. Please email us at spoc@safelayer.com to register and get more details.

Support of multiple CVCAs per State

KeyOne eMRTD Country Verifying RA supports that national or foreign States having multiple CVCAs, i.e. different CVCAs for e-passport issuing and for e-residence permit issuing.

KeyOne eMRTD Country Verifying RA acts as the only interface for communication between national and foreign eMRTD PKIs.

Manual and Automatic Request Sending

From the KeyOne eMRTD Country Verifying RA, all kind of requests can be sent manually to foreign SPOC servers.

Furthermore, requests related to the KeyOne eMRTD Country Verifying RA's operation as a Registration Authority can be automatically sent to foreign SPOC endpoints:

- DV Certification Requests of national Document Verifiers for foreign CVCAs.
- DV Certificate Issuing requests for distributing certificates asynchronously issued by the national CVCA for foreign Document Verifiers.

Synchronous and Asynchronous Operation

KeyOne's SPOC can be configured for either synchronous or asynchronous request processing.

When the national CVCA operates online, KeyOne's SPOC can be configured for sending synchronous responses for received requests. For example, when KeyOne eMRTD Country Verifying RA receives a DV certification request from a foreign SPOC, it:

1 Sends the request to the Web service of the national CVCA.

2 Receives the issued certificate.

3 Responds to the foreign SPOC with the issued DV certificate.

If the national CVCA operates offline, KeyOne's SPOC must be configured for sending asynchronous responses for received requests. For example, when receiving a DV certification request from a foreign SPOC, KeyOne eMRTD Country Verifying RA. For example, when receiving a DV certification request from a foreign SPOC, KeyOne eMRTD Country Verifying RA:

1 Responds to the foreign SPOC with an operation confirmation.

2 Sends the request to the national CVCA.

3 Waits for the issued certificate.

4 Receives the issued certificate from the national CVCA

5 Sends the issued DV certificate to the foreign SPOC.

Note

Asynchronous messages can be managed in KeyOne eMRTD Country Verifying RA either manually (via to-do lists) or automatically (via programmed automatisms).

Document Verifier

This chapter introduces the main functions of a Document Verifier and describes the KeyOne solution for implementing them.

What is a Document Verifier?

In an EAC eMRTD PKI, a Document Verifier is the subordinate Certification Authority that issues certificates for national Inspection Systems.

Document Verifiers are in turn certified by the CSCAs of all the nations whose eMRTD can be read by national Inspection Systems.

Thus, before reading the data of a foreign eMRTD, an Inspection System must authenticate by presenting a certificate:

- Issued by the national Document Verifier.
- Signed using a key certified by the CVCA of the foreign state.

Note
See Country Verifying *CA, page 19, for a description of the KeyOne's CVCA solution.*

KeyOne Document Verifier

When extended with **eMRTD Document Verifier** add-in, add-in, **KeyOne CA** implements all the functionality of a Document Verifier. This product has both CA and RA functions (thus combining the role of a DVCA and a DVRA), which entails:

- Managing multiple key pairs for IS certification, one per recognized state.
- Enrolling national Inspection Systems in the domain of the DV.
- Issuing and renewing CV certificates for Inspection Systems.
- Providing a Web service (with SOAP/XML and REST/JOSN interfaces) for online IS certification.
- Discarding registered Inspection Systems and issued IS certificates.

To perform these operations, KeyOne's Document Verifier provides advanced features, which include:

- *State Management*
- *Local and Remote IS Registration*
- *CV Certificate Profile Management*
- *Automatic Rekeying*
- *Rekeying Error Management*
- *X.509 Key Management*

State Management

The Security Officer of KeyOne's Document Verifier manages the states for which the DV is currently certified (and for which Inspection Systems under the DV can be certified). Thus, when a new state is added:

1 The Security Officer imports the CVCA certificate by explicitly accepting it as a trusted CV certificate.

2 The application automatically creates a new DV logical key for that state and sets up the respective key generation options (according to the cryptographic algorithms used by the state's CVCA).

3 Once the new state has been registered and configured, keys and certificate requests for the configured states are automatically generated and sent to the CVRA.

Note
See Country Verifying *RA, page 26, for a description of the* KeyOne eMRTD Country Verifying *RA solution.*

Local and Remote IS Registration

The Registration Officer of KeyOne's Document Verifier can manage Inspection System registration:

- Locally (from the GUI of KeyOne Document Verifier).
- Remotely (via a SOAP or REST request to the IS certification services of KeyOne Document Verifier).

The following table details the execution modes supported for each IS management operation.

Operation	*Local*	*Remote*
Register	√	
Revoke (i.e. discard for further renewals)	√	
Process an initial certificate request (non-authenticated)	√	√

Operation	*Local*	*Remote*
Process an certificate renewal request	√	√

CV Certificate Profile Management

The characteristics of the certificates issued for the Inspection System (e.g., validity period, access rights to eMRTD sensitive data) are defined by the Security Officer by means of CV certificate profiles. The Security Officer can define any number of profiles (each profile is given a unique name).

When processing an IS certification request, KeyOne Document Verifier applies the profile previously assigned to this type of request. Each CV certificate profile can be assigned to:

- A registered IS (and applied to all CV certificate requests from that IS).
- A certifying state (and applied to all IS requests for this state).
- An `<Inspection System,Certifying State>` pair (and applied to all requests from a given IS for a given state).

All assignation modes are supported by both *Local and Remote IS Registration* procedures.

Note
CV certificate profiles are also used to define the data to be included in the DV certificate request for each state (e.g., DV mnemonic, initial key pair sequence number).

Automatic Rekeying

Because CV certificates issued for the DV have very short validity periods, KeyOne's Document Verifier provides an automatic rekeying capability.

Note
For cases in which manual rekeying is preferred or required, to-do list-based key management from the KeyOne administration application is also possible.

The automatic rekeying process works as follows:

1 When the configured **Renewal start period** is reached, the DV automatically generates a new key pair and an authenticated CV certificate request (conforming to the EAC cryptographic algorithms of the respective state) with an incremented key pair sequence number.

2 The CV certificate request is automatically obtained by the (national) CVRA by invoking one of the DV Web services.

3 The CVRA automatically sends the request to the foreign state's CVCA or keeps it for inclusion in the next batch to be processed by the national CVCA. (In both cases, explicit approval of the request by a Registration Approver is not necessary as the request is self-authenticating.)

4 When the CV certificate issued by the (national or foreign) CVCA is received, the CVRA automatically sends it to the DV via another Web service invocation.

5 The DV automatically validates the received CV certificate (and possibly a new CVCA link certificate) and stores it. At this point, the old certified key is still being used by the DV to issue Inspection System certificates.

6 When the configured **Next key activation period** is reached, the DV automatically activates the new (certified) key for Inspection System certification.

Note

While the new DV key is generated but still not certified or activated, IS certificates are signed with the old (current) key. Once the new key is activated, the old key is no longer used (but the old certificate is still usable for IS certificate validation purposes).

Figure 11-1 illustrates the DV key-renewing process.

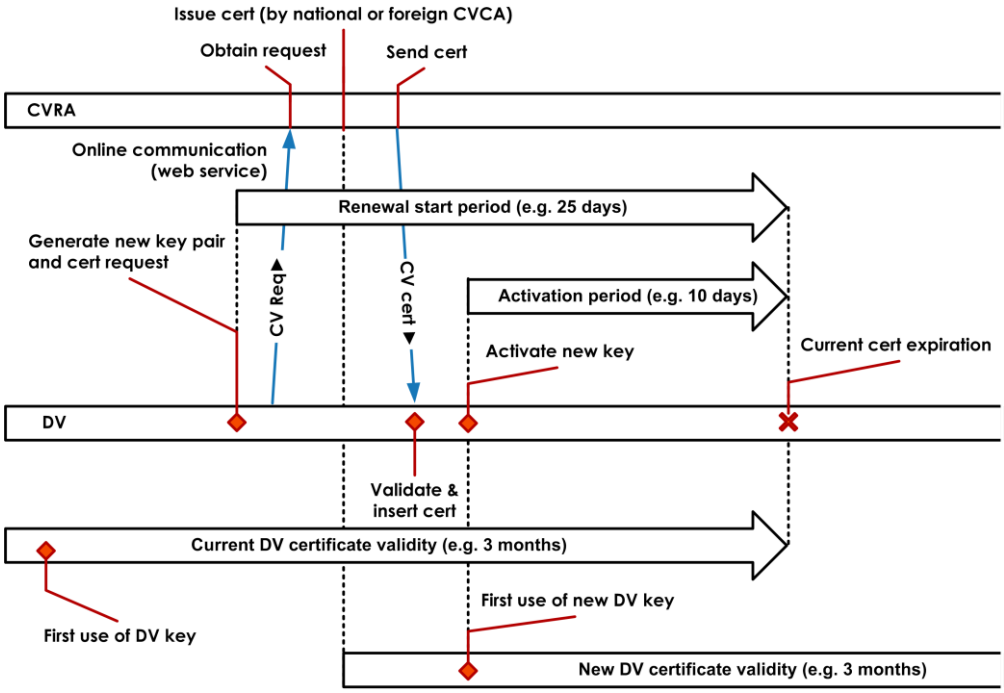

Figure 11-1. DV key-renewing process.

Rekeying Error Management

During *Automatic Rekeying*, the following issues cause an alert to be displayed in the application to-do list:

- The new DV key is not generated before the **Renewal start period**.
- The CV certificate request cannot be sent to the CVRA.
- The CV certificate is not received by the DV before the **Maximum renewal period**.

X.509 Key Management

Since KeyOne CA's full functionality is available, the DV can also be set up to issue X.509 certificates. This allows the DV to issue X.509 infrastructure certificates required by other PKI components lower down in the hierarchy without requiring an additional CA for issuing them. For example, the DV can issue the SSL/TLS client authentication certificates needed by the Inspection Systems to connect to the certification Web service.

In this case, and in addition to the (multiple) CV-certified key pairs, the DV needs X.509-certified key pairs for:

- X.509 certificate signing.
- KeyOne batch signing.

The respective X.509 certificates are commonly issued by the national CVCA (although they could alternatively be issued by any other X.509 CA).

Besides the above-mentioned keys, the DV needs to hold an SSL/TLS server authentication key for the Web services responder and other common KeyOne services. The corresponding X.509 certificate is typically self-issued by the same DV (if it has been set up as an X.509 CA).

Edificio Valrealty C/ Basauri, 17 Edificio B Pl. Baja Izq. Of. B 28023 Madrid (SPAIN) Tel.: +34 91 7080480 Fax: +34 91 3076652
World Trade Center (Edif. S-4), Moll de Barcelona S/N 08039 Barcelona (SPAIN) Tel.: +34 93 5088090 Fax: +34 93 5088091