



## *The Trust Framework for ePassport Extended Access Control*

How the trust infrastructure was designed to meet the needs of access control to advanced biometric data in electronic passports

*Tim Moses  
Director of Advanced Security Technology  
Entrust, Inc.*

March 2010

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© 2010 Entrust Inc. All rights reserved.

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
<b>2</b>	<b>EAC Requirements.....</b>	<b>2</b>
	Resource-constrained relying party.....	2
	No trusted time source .....	2
	Sporadic connectivity.....	2
	User interface .....	2
<b>3</b>	<b>Common Trust Frameworks.....</b>	<b>3</b>
	Two-tier architecture.....	3
	One-tier architecture with public-key revocation .....	4
	One-tier architecture with strong private-key protection.....	4
<b>4</b>	<b>The EAC Framework .....</b>	<b>5</b>
<b>5</b>	<b>EAC Design Choices.....</b>	<b>6</b>
	The credential chain .....	6
	Certificate lifecycle.....	7
	Single Point of Contact (SPOC) .....	8
<b>6</b>	<b>EAC Trust Management.....</b>	<b>9</b>
<b>7</b>	<b>Conclusions.....</b>	<b>15</b>
<b>8</b>	<b>About Entrust .....</b>	<b>15</b>

## 1 Introduction

Increasingly violent international criminal activity is being confronted with greater intelligence-sharing among nations and more accurate and timely tracking of suspects' movements across international borders.

Key to the success of these initiatives is a more reliable travel document; one that is harder to forge than the familiar paper-based passport and one whose holder cannot be so easily impersonated. A beneficial side effect of this development may be greater convenience for travelers who do not pose a threat to national security.

One of the main ways in which new electronic travel documents differ from existing ones is that they can be loaded with digitized biometric data sets, such as fingerprints and iris patterns, that are more difficult to substitute than printed data sets and more difficult to impersonate than facial photographs.

While these data sets can deliver lower false-acceptance rates than facial photographs, their reliability depends crucially upon their being kept secret, since, armed with another person's biometric data set, it can be relatively easy to construct a matching prosthetic and thereby steal their identity.



Unlike some other common credential types, biometric data sets cannot be withdrawn once compromised. So they should only be revealed to systems that can be trusted to handle them properly. Biometric data sets are possibly most vulnerable when the passport falls into criminal hands.

But, other abuses that can occur include: using them for purposes other than the declared purpose, sharing them with others and failing to delete them immediately after use, or ePassports may be inspected by agents other than border-control officials.

For instance, they may be used by law enforcement or banking officials. For this reason, all passport inspection systems in one country are not necessarily treated as equally trustworthy. How can the passport tell whether the passport inspection system that is interrogating can be trusted with its biometric data? This solution is provided by the Extended Access Control (EAC) features of electronic passports.

The familiar passport is passive; it has no dynamic display or user input features. This characteristic must be retained in an electronic replacement, as (at least during a transition period) not all destination countries will have the ability to process a wholly electronic substitute.

So, the same travel document must be capable of being evaluated by a human border agent in the traditional manner and by an electronic inspection system. The user's consent to access information in the passport has traditionally been inferred from the user handing the document over to a trusted agent. This is also the best way to infer the user's consent to access information in an electronic passport.

Issuing states that want to protect their citizens against abuse of their personal information in foreign countries will place restrictions on the release of biometric data sets on a country-by-country and application-by-application basis. So, privilege management must be an integral part of the ePassport trust infrastructure.

Public key infrastructure (PKI) is the technology that has been chosen to establish, maintain and demonstrate the trustworthiness of the systems for releasing and verifying the passport holder's biographical and biometric data sets. This is a well-established technology that has been successfully applied to Internet-scale applications, such as eCommerce on the Web. But, extended access control to electronic passports poses some unique challenges:

- electronic passports have very limited compute resources
- they cannot maintain accurate and fine-grained time
- they (and some passport inspection systems) have only sporadic connectivity to the network
- they do not support direct data input and display

These challenges lead to unique design choices for the underlying trust infrastructure.

## 2 EAC Requirements

As mentioned, ePassport systems must be designed to accommodate a number of unique constraints.

### **Resource-constrained relying party**

In the EAC framework, the relying party software executes on an RFID chip, physically embedded in the passport document. This is a severely constrained compute platform not capable of much flexibility in terms of the algorithms and protocols that it supports. This constraint demands that any credential chain that the passport has to validate be based throughout on a single class of cryptographic algorithm. Because of its inherent efficiency, elliptic-curve cryptography is best suited to protecting information in this setting.

### **No trusted time source**

In its basic form, the ePassport does not contain a real-time clock. In some security protocols a real-time clock is required as a countermeasure against protocol replay attacks. But, a secure random number generator can be used instead. Although ePassport RFID chips lack a battery-backed, real-time clock, they can obtain a trusted, lower-bound estimate of the current time from the latest effective date of any valid certificate they encounter that was issued by a certification authority in their own country.

### **Sporadic connectivity**

Fixed ports of entry, such as airports and road-crossings, often have good, continuous connectivity with the network. However, cross-border trains, large ships and remote land-borders also have to be supported, and these may have unreliable or sporadic connectivity.

### **User interface**

Usually, when a human operator interacts with a secure information system, a human-computer interface is provided to activate private credentials, indicate the result of authentication and authorize release of personal information.

It might have been possible to give ePassports a suitable human-computer interface. But, a single document must be acceptable both in countries that have tooled up to accept ePassports

and in countries that have not yet done so — hence the decision to simply embed an RFID chip in an otherwise-conventional passport booklet.

Nevertheless, the user's consent must be obtained before personal information can be released. Otherwise, the passport is vulnerable to "skimming" — whereby a rogue inspection system interrogates the passport and extracts its contents without the passport holder's knowledge.

The holder's consent is inferred when the passport inspection system demonstrates to the passport chip its knowledge of the passport's printed contents, obtained from the optical machine-readable zone, which (in normal use) can only be obtained if the user hands over the document, thereby implying consent.

A beneficial side-effect of this procedure is the derivation of an encryption key which is used to encrypt subsequent wireless communications between the passport and the inspection system in order to prevent eavesdropping.

### 3 Common Trust Frameworks

The cost of validating the identity and authority of a subject for the purpose of issuing a credential is relatively high. And, circumstances that may invalidate the information encapsulated in a credential — a lost or stolen private key, for example — arise unpredictably.

These two considerations must be balanced when choosing a suitable credential lifetime; too short a lifetime leads to prohibitive cost of issuance, and too long a lifetime throws the trustworthiness of the credential, as it approaches the end of its life, into doubt.

There are three mainstream approaches to striking the right balance between these two considerations:

- the two-tier architecture
- the one-tier architecture with public-key revocation
- the one-tier architecture with strong private-key protection

#### **Two-tier architecture**

In architectures such as Kerberos and the various Identity 2.0 frameworks, the proper balance is struck by means of a two-tier architecture, in which a primary credential, such as a username/password combination, is issued to the subject.

The architecture includes an intermediary, called a Ticket Granting Server (TGS) or Identity Provider (IdP), which verifies the primary credential and issues a secondary credential, called a ticket or token. It is this secondary credential that is relied upon directly by the relying party.

The primary credential is long-lived. But, the ticket or token has a very short lifespan. The TGS or IdP must participate in the issuance of the token. So, this provides an opportunity for an administrator to effectively invalidate credentials when circumstances demand.

While the cost of issuing the primary credential may be high, the cost of issuing a ticket is trivial. So, the overall cost can be contained.

Relying parties are spared the task of confirming the continued validity of the primary credential. But reliable connectivity is required to deliver the tokens, so these solutions have found acceptance mainly in distributed computing environments. Federated variants of these architectures are not widespread, although there are efforts to use Identity 2.0 frameworks in federated applications.

### **One-tier architecture with public-key revocation**

The common X.509 trust model is a one-tier architecture. Relatively long-lived credentials are issued, with the capability to revoke them, if necessary. This approach allows the issuance cost to be amortized over an extended period of time, while maintaining trustworthiness by withdrawing credentials if and when they become invalid. Additional cost is incurred only for relatively rare revocation events.

This approach imposes two requirements on the relying party: first, reliable connectivity for retrieving revocation information and, secondly, a source of reliable time, so that it can check that the retrieved revocation information is fresh.

Federated variants of this architecture are in widespread use; perhaps the most ubiquitous example is Secure Sockets Layer (SSL) for the Web.

Client software for the Web runs on comparatively powerful platforms. This makes it practical for clients to handle several classes of cryptographic algorithm with various key sizes when processing a credential chain. This, in turn, allows for stronger keys with longer lifetimes in the upper layers of the key hierarchy. Ensuring that lower-layer certificates comply with the crypto policy of the root authority is managed by contractual agreement, not technical controls.

### **One-tier architecture with strong private-key protection**

The final type of architecture is one-tier, with credentials that cannot be revoked. Instead, elements of the system apply strong protection measures to their private keys, including tamper-resistant enclosures, physical security and automated deletion. Because of the challenge associated with balancing the cost of issuance with the ongoing trustworthiness requirement, there are few examples of this type of solution.

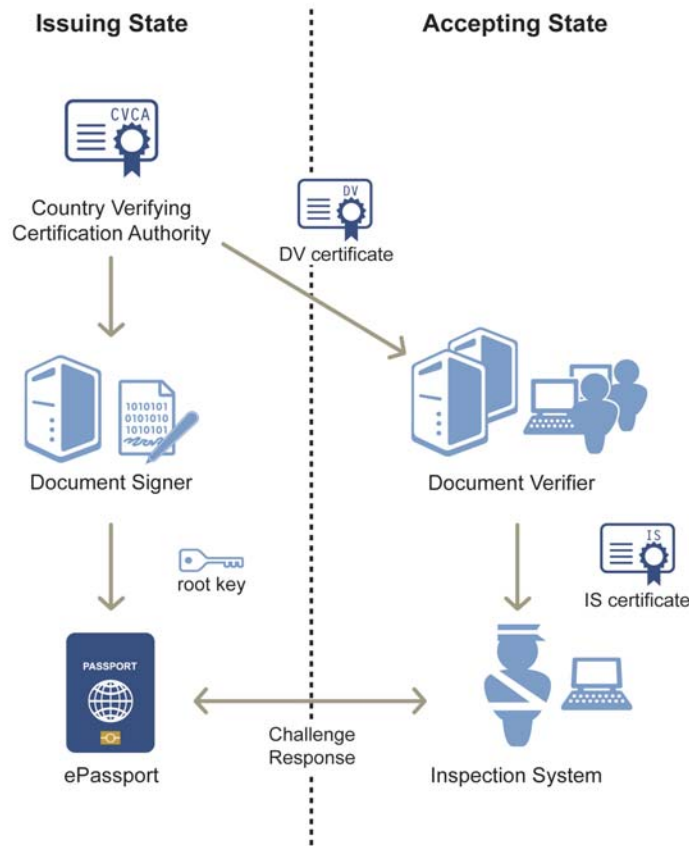
It is, however, the best approach for the EAC application. The absence of continuous connectivity and a reliable, fine-grained time source make the alternatives impractical. And the cost of repeated issuance can be defrayed by using automated renewal processes.

In order to achieve the necessary strong protection of the inspection system's private key, it may be housed in a separate system component with strong physical, procedural, computer and network safeguards. The terminals used by inspectors can then connect to it over a virtual private network.

## 4 The EAC Framework

The principal entities in the EAC architecture are shown in Figure 1. Naturally, many (if not all) countries will act in the role of both ePassport issuer and ePassport acceptor.

These countries will operate all the components of the architecture, including: a Country Verifying Certification Authority, Document Verifier CAs, Document Signers and Inspection Systems. The diagram, however, just shows one issuing state that issues ePassports and one accepting state that accepts ePassports.



**Figure 1: EAC Framework**

The function of the Country Verifying Certification Authority (CVCA) is to authorize foreign and domestic Document Verifier (DV) certification authorities by issuing DV certificates. DVs, in turn, authorize Inspection Systems (IS) to examine the contents of ePassports by issuing IS certificates.

The CVCA public signature-verification key is embedded in ePassports by the Document Signer, which is also responsible for signing the contents of ePassports. The IS demonstrates its authority to view passport contents by means of a challenge/response exchange with the ePassport involving a random challenge generated by the passport and the signature-verification certificate of the IS.

## 5 EAC Design Choices

The constraints of the EAC environment have led to the following design choices.

### The credential chain

The same algorithm and parameters are used throughout the credential chain. The relying party's crypto policy is determined by the Issuing CVCA. It accepts only certificates protected with the same algorithm and key parameters as expressed in its root certificate.

The Issuing CVCA can update that policy at any time by means of a link certificate (i.e., a certificate whose issuer and subject are the same, but whose subject key is different from the key with which it was signed). After successfully validating a link certificate, the ePassport adopts the key it contains as its new root and the crypto policy of that key as its new crypto policy.

There are two benefits to this approach. First, the CVCA knows the cryptographic capabilities of its own passports. So, it ensures that passports are not confronted with cryptographic algorithms and algorithm parameters that they are not capable of processing. It also ensures that the cryptographic strength of protection employed throughout the certificate chain can be enforced by the Issuing CVCA using technical means.

One implication of this choice is that DVs and ISs must generate and maintain keys that conform to the crypto policies of each country whose passports they wish to accept, even as these policies change over time.

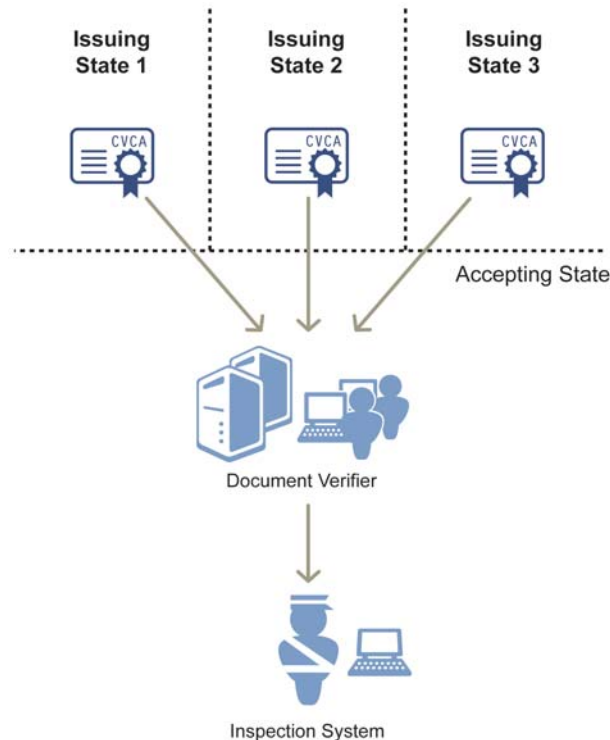
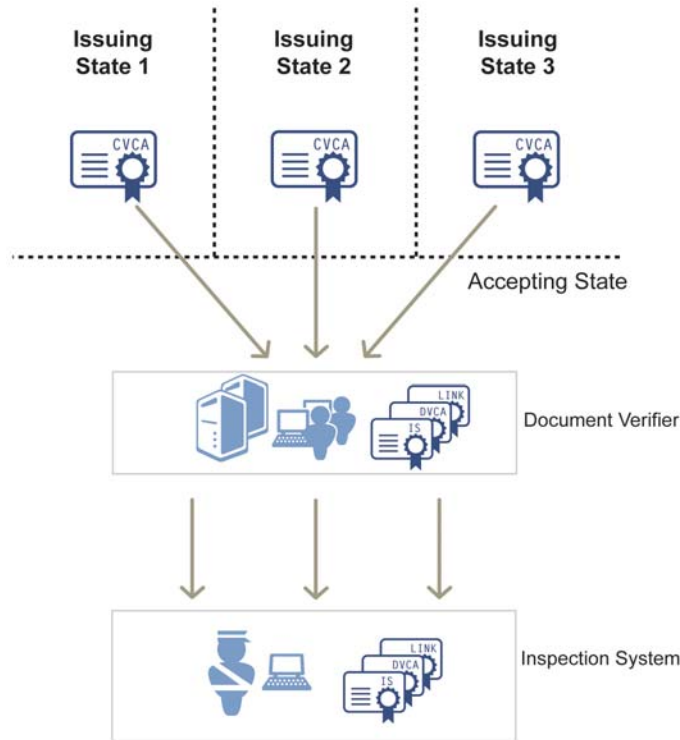


Figure 2: Branching Credential Chain

So, the IS must assemble, and present to the passport, a certificate chain that terminates in the passport's own CVCA certificate and that uses the same crypto-security policy throughout. While it is possible for a key to have multiple "upstream" certificates in branching credential chains (as shown in Figure 2), IS keys are uniquely matched to the Issuing CVCA and there will be separate unbranching credential chains to each country's root (see Figure 3).



**Figure 3: Unbranching Credential Chain**

### Certificate lifecycle

Sporadic connectivity and the lack of a real-time clock in the RFID chip make revocation impractical; one of the compensating measures is the use of short-lived DV and IS certificates. Hence, there is a need for automated processing of frequent certificate renewal requests. DV certificates must be replaced no later than their expiry time minus the validity period of their downstream IS certificates.

For example, if a DV certificate has a validity period of three months, and it issues certificates to ISs with a validity period of one month, then the DV certificate must be replaced at least one month before it expires. And, in order to accommodate potential delays in the request processing, replacement should be initiated even earlier.

A logical consequence of this requirement is that downstream certificates must always have a shorter validity period than certificates upstream in the chain. Once a component has successfully replaced its key, it can curtail use of that key, even though it may not have expired yet.

## Single Point of Contact (SPOC)

As the number of issuing states and accepting states increases, so does the number of individual relationships between DVs and CVCA. Given the short validity periods of DV and IS certificates, lifecycle management between issuing and accepting states quickly becomes unmanageable.

Within the European Union, the concept of a Single Point of Contact (SPOC) and associated key management protocol has been standardized for certificate lifecycle operations between CVCA in issuing states and foreign DVs in accepting states. The SPOC standard is not relevant to communication between DVs and CVCA within a single state.

Each state sets up a single SPOC that acts as its communication hub with foreign states. Prior to certificate lifecycle message exchange, each SPOC must register with SPOCs in other states that it intends to communicate with. All inter-SPOC key management messages are authenticated using traditional X.509-based SSL/TLS. Therefore, as part of the initial registration process, the SPOC's certification authority for its SSL certificates must also be registered, establishing initial trust between SPOCs.

Each SPOC gathers certificate requests from its domestic DVs, forwards them to foreign SPOCs for handling by the intended CVCA and delivers responses received from foreign SPOCs to the requesting domestic DVs. The same SPOC collects incoming requests from foreign SPOCs, delivers them to the domestic CVCA for handling, and forwards responses to the requesting SPOCs for delivery to the requesting DV.

Because SPOCs are formally registered with one another and trust established through that registration process, certificate requests received from registered SPOCs (and the named requesting DV) are considered valid by the receiving SPOC. There is no need to establish validity through other means such as having initial requests countersigned by the accepting state CVCA.

However, it is important to remember that the SPOC specification is relevant only to international communications between issuing and accepting states. Communication among the EAC entities within a single state (e.g., DV-SPOC, CVCA-SPOC, DV-CVCA) are not covered by the SPOC protocol. Therefore, other means must be used to ensure that all requests received by the SPOC from DVs are really from currently valid and authorized DVs.

There are several options to accomplish this task, one being a CVCA countersignature on initial requests sent from a DV to the SPOC for communication to foreign SPOCs. Also, messages need to be protected within the state boundary during transmission. Several options are available for that also, one being SSL/TLS.

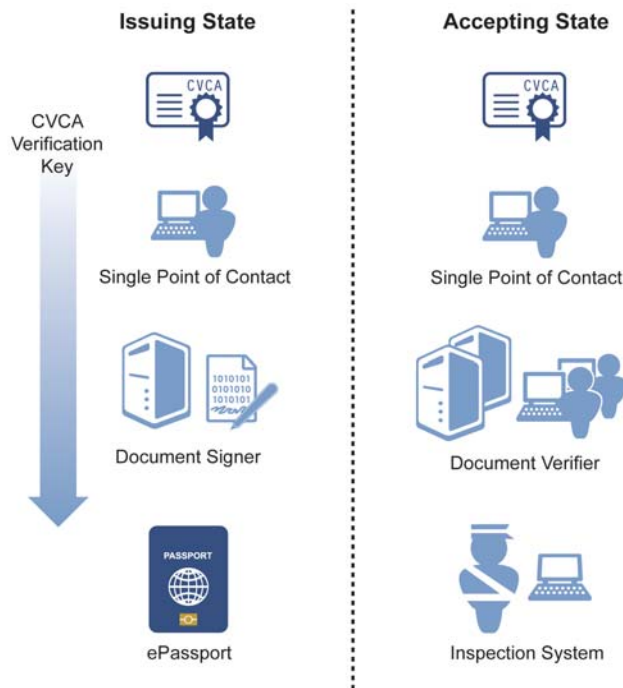
There also needs to be a policy management authority within the state that enables the management of all domestic entities and ensuring the domestic SPOC is updated with respect to the current valid and active set of entities and the foreign states with which each is authorized to communicate.

## 6 EAC Trust Management

The EAC trust model was shown in Figure 1 in Section 4. Note that protocol exchanges between elements located in the same country will be governed by national standards. But, those that cross international boundaries will be governed by international standards. International efforts are currently at a more advanced stage of development than most national efforts.

The trust infrastructure is established by the following steps.

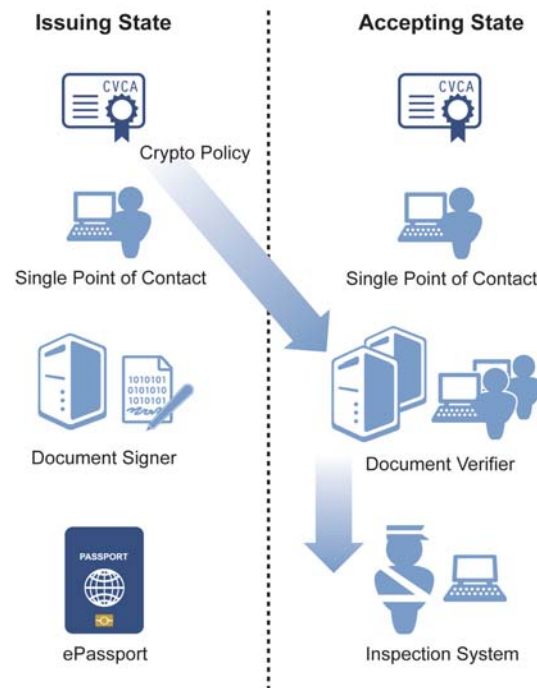
1. The issuing CVCA signature-verification key and its associated parameters are injected into the ePassport by the Document Signer at the time of passport issuance.



2. The issuing and accepting SPOCs register with each other, providing contact information, SPOC service URLs, SPOC CA root certificate and SPOC root CA certificate policy.



3. The accepting DV and accepting IS discover the crypto policy of the issuing CVCA. These change infrequently, so the International Civil Aviation Authority (ICAO) directory can intermediate in this process. The DV and IS must download the crypto policy each time they renew their own keys in case it has changed in the previous period. The crypto policy also could be extracted from the issuing state's CVCA verification certificate, obtained via the accepting state's CVCA.



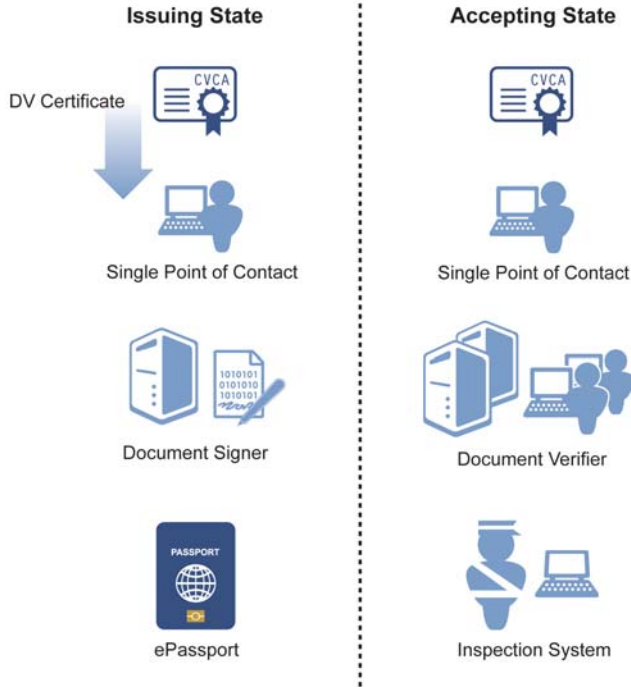
4. The accepting DV generates a signature key pair using parameters dictated by the issuing CVCA's crypto policy. It creates a certificate request message, addressed to the issuing CVCA and submits it to the accepting SPOC for transfer. This will be a relatively frequent operation (on the order of a small number of weeks). So, reliance on the intermediation of the ICAO public-key directory is not practical. This step should be repeated no later than the expiry time of the current certificate minus the validity period of downstream IS certificates minus the maximum processing delay of the issuing CVCA.



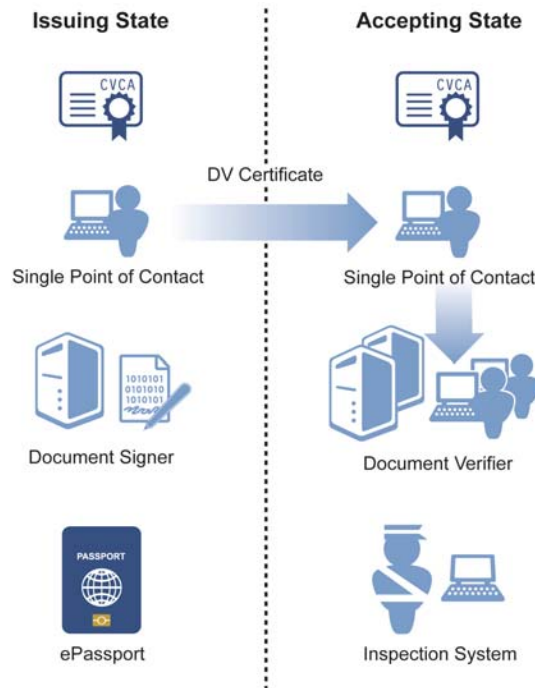
5. The accepting SPOC ensures that the request is from a valid DV and sends the request to the issuing SPOC, which forwards it to the issuing CVCA.



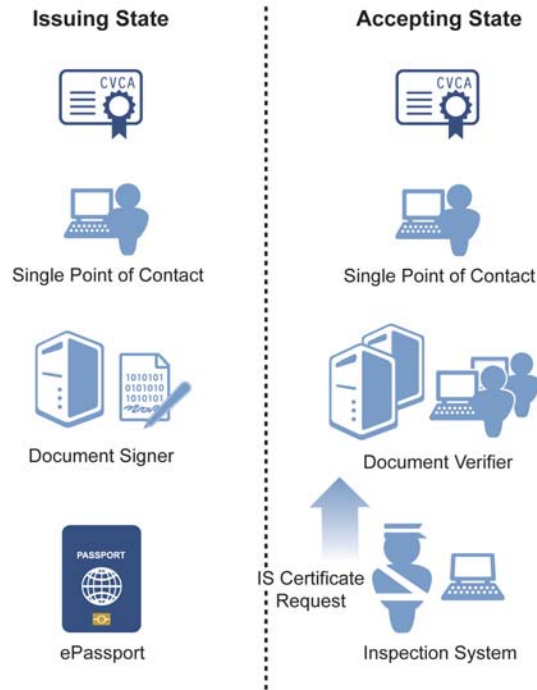
6. The issuing CVCA evaluates the request. And, if it approves, it creates a certificate in conformance with its own certificate and crypto policy (including maximum validity period). It then returns the certificate to the issuing SPOC for transfer along with a sequence of link certificates covering the validity period of the oldest extant passport. For a 10-year passport with CVCA keys updated every three years, this amounts to four link certificates.



7. The issuing SPOC returns the response to the accepting SPOC for transfer to the accepting DV.



8. The accepting IS creates a signature key pair using parameters dictated by the issuing CVCA's crypto policy. It submits a certificate request to the accepting DV. This step should be repeated prior to expiry of the current certificate.



9. The accepting DV evaluates the certificate request. And, if it approves, it creates a certificate in conformance with the issuing CVCA crypto policy and returns it to the accepting IS along with the corresponding CVCA signature-verification key and the sequence of link certificates.



Upon completion of the setup procedure, separately with each issuing state, the accepting IS has certificate chains that conform to the crypto policy of each issuing state and are compatible with the root key embedded in the ePassports of those states.

Each issuing CVCA may have a different crypto policy. So, the IS must maintain a separate chain for each issuing state. The issuing CVCA can update its crypto policy at any time by issuing a link certificate. Upon encountering a link certificate, the ePassport should adopt the crypto policy expressed in its subject key.

This procedure is executed upon initial setup and, perhaps, periodically thereafter. If the accepting state uses CVCA countersignatures as a way to indicate to the accepting SPOC that an initial request is coming from a valid DV, that countersignature stays with the request.

However, the issuing CVCA and issuing SPOC are not required to verify the signature. Once the accepting SPOC is registered with the issuing SPOC, all requests from the accepting SPOC are deemed by the issuing state to be on behalf of valid DVs. Interim renewals are not countersigned by the accepting CVCA, but are instead signed by the DV using its current key. DV certificates expire relatively frequently, so normal renewal requests are not ordinarily evaluated manually.

Inspection Systems may also operate under the issuing jurisdiction to check passports presented by travelers upon return to their home state, or for carriers to check passengers against “no fly” lists. In such cases, the issuing CVCA does not have to counter-sign the DV certificate request. Instead, it simply processes the certificate request received directly from its subordinate DV and issues a DV certificate.

## 7 Conclusions

The unique characteristics of the ePassport computing platform, particularly its limited resources (e.g., lack of a real-time clock and user interface; sporadic network connectivity), have determined the design of the EAC trust infrastructure. These characteristics have disqualified the more familiar trust infrastructure designs and led to the choice of a single-tier infrastructure that places strong reliance on private-key protection.

The use of trusted SPOC entities and the associated key management protocol simplifies the communication requirements for DVs and CVCA in issuing and accepting states.

However, standards do not cover the establishment and management of trusted services among the EAC entities within a given state. Measures must be taken to ensure that only currently valid entities communicate with other states through the SPOC and that the domestic communication infrastructure is as secure as the international one.

The potential number of keys and the relative brevity of their lifetimes argue for automated key management. But, periodic intervention by administrators would be advisable in order to ensure continuing trustworthiness.

## 8 About Entrust

Entrust provides identity-based security solutions that empower enterprises, consumers, citizens and Web sites in more than 4,000 organizations spanning 60 countries. Entrust's identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail [entrust@entrust.com](mailto:entrust@entrust.com) or visit [www.entrust.com](http://www.entrust.com).