



## ***A Trust Infrastructure for ePassports***

Building reliable, timely and cost-effective trust links for electronic travel document verification

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

January 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

1	Trust in government .....	1
2	Birth of an idea .....	2
3	The missing piece .....	2
4	ePassports .....	3
5	Bootstrapping trust.....	5
6	Importance of the CPS.....	6
7	Role of the ICAO.....	7
8	About Entrust .....	8

## 1 Trust in government

Citizens, no matter in what part of the world, seek a certain level of trust from their government in the protection of their personal identities and information. Whether it's driver's or professional licenses, birth certificates, taxpayer ID numbers or other personally identifiable information (PII), citizens rely on governments to safeguard their information and keep it from being used for malicious purposes.

In turn, governments initiate standards, create regulations and issue mandates that aim to protect this information and help secure assets. By layering security technologies across different applications and resources, governments are managing their processes and leveraging a variety of technologies in order to create secure environments.

By using this layered approach, governments avoid single points of failure and voids in their defenses. Strategies may differ by government entity. Each, however, demands interoperability to promote synergy, efficiency, security and cost-effectiveness.

In developing and implementing a government-focused security model, many countries have created systems of trust to protect borders and citizen information via electronic passport technology — more commonly known as ePassports. While implementations may vary across the globe, the primary objective is identical: authenticate both citizens and the validity of ePassports through technology and a strategic, secure infrastructure.

The foundation of this process must be, regardless of technology, defined by a single word — trust.

This white paper explores the development of reliable, timely and cost-effective trust mechanisms for electronic travel documents. It addresses the trust infrastructure supporting Basic Access control (BAC) for ePassports. Extended Access Control (EAC) and protection of biometric data are explained and discussed in separate documents.

## 2 Birth of an idea

It was May of 1975. Those “in the know” had come to understand just how big an impact personal computers and data networks were going to have on our professional and domestic lives, and that existing security solutions were totally inadequate for the job they would be called upon to do.

Whit Diffie had been wrestling with this question — struggling to develop a solution for close to a decade — when a solution came to him in a moment of insight. On an otherwise unremarkable day, the answer suddenly revealed itself to him: by separating the encryption and decryption keys in such a way that disclosure of one did not reveal any information about the other, it would be possible to secure information for someone that you had never met or corresponded with before.

In a further insight, he realized that such a system would allow an individual to identify him- or herself to a total stranger. The solutions and products that have flowed from Diffie’s discovery have entered into everyday use and overcome one of the biggest hurdles to the success of the Internet.

## 3 The missing piece

Twenty years later, Netscape built software into its Web browser that exploited Diffie’s discovery. But, its usefulness was limited: a significant piece of the puzzle was still missing. A trusted third party was required to authenticate and certify identities. Public-key certificates provided the answer.

Many felt that the liability attaching to a certificate issuer would make it impossibly expensive to operate in practice. Michael Baum at VeriSign pondered this question and developed a framework that overcame the objection, making it cost-effective for a utility to operate the certification service. The solution involved a standard contract between a certification authority (CA) and its relying parties called a certification practice statement, or CPS.

This solution essentially laid out the steps by which a certification authority would authenticate its subscribers, and allowed it to limit its liability to just those losses that resulted from a failure to adhere to those practices, but not for any other reason. The legal and technical security communities then collaborated to define exactly what it meant to operate a certification authority. Since that time, the CPS has become a fixture of systems in which statements by authorities are relied upon by arms-length partners.



The trust infrastructure defined by these pioneers is now in routine use for all styles of e-commerce, including online banking and e-government. And, recently, attention has turned to how best to apply the same techniques to improve the security of travel documents, such as passports.

## 4 ePassports

A great deal has been written about the use of RFID chips, certificates and biometrics for travel documents. But, the question of a suitable trust infrastructure for the ePassport application has not received the same level of attention. When it comes to travel documents, we are at the same stage that eCommerce was during the mid-'90s.

It is well understood how an ePassport, containing an RFID chip and a certificate, can prove the binding between the biometric and identity information that it contains; or how a passport inspection station can use a certificate to prove its bona fides to an electronic passport when asking it to reveal the holder's personal data.

But, in each case, the relying party must have first been provisioned with a faithful copy of the public key of the certificate issuer and accepted the suitability of its practices for the purpose for which its certificate will be relied upon. This is the job of the trust infrastructure.



Perhaps the most straightforward part of the problem addressed by the trust infrastructure is the authentic delivery of public keys from one domain to another. Because they are "public" keys, their confidentiality does not require protection. However, the receiving domain does need assurance that the key is genuine, has not been modified in transit and is approved for the purpose.

Although, technically, read access to public keys does not have to be restricted, it is worth noting that some authorities do restrict read access. This allows them to disavow responsibility for losses incurred by unauthorized relying parties.

Two solutions to the key-distribution problem for the ePassport application have been described. The first distributes the keys by way of the diplomatic bag of the originating country. The second uses a threshold scheme based on lists of certificates obtained from other countries that already rely on them.

The first of these solutions is an attempt to leverage an existing mechanism that was developed a century ago to protect the confidentiality of symmetric keys delivered to government representatives located in foreign, and possibly hostile, countries. Unfortunately, it does not adapt perfectly to the ePassport problem. It is a cumbersome mechanism, introducing unacceptable delay in the distribution process. More suitable solutions exist.

The list of certificates in the second solution is known as a "master list." The list is signed by the country that compiled it using a syntax that is similar to that of a cross-certificate. However, the semantics, while not formally stated anywhere, are quite different.

The presence of a country's certificate on such a list is taken to mean that the list issuer associates the public key in the certificate with the country identified as the subject of the certificate. No information about the basis for, and duration of, that association are included.

While it might be questionable for a passport-accepting country to rely on certificates from just one such list, if a passport-issuing country's certificate can be found on lists from several countries, then the risk of reliance may drop to an acceptable level. This approach may be of particular interest to countries that lack the resources needed to perform their own direct import and evaluation of foreign certificates.

The master list approach involves the delegation of a highly sensitive function to a set of foreign governments; something that likely won't be acceptable to all passport-accepting countries. Furthermore, it relies on the willingness of some passport-accepting countries that have undertaken the effort required to import and evaluate issuing countries' certificates to publish the results of their evaluation.

The master list syntax was recently standardized and approved by both the International Organization for Standardization (ISO) and the International Civil Aviation Organization (ICAO). But, it will be several years before its success can be evaluated. And, unlike the diplomatic bag solution, master lists do not provide a solution to the "bootstrap" problem.

## 5 Bootstrapping trust

Every trust infrastructure must solve the “bootstrap” problem. Before one can validate a public-key certificate for another entity, a trusted public key for the certificate issuer must already be in place. The most common solution to this circularity is that an initial key is embedded in a software distribution. This can work well for software publishers. But, other types of entities don't enjoy this luxury. For them, an out-of-band exchange is required.

Public keys are not amenable to distribution by any other than electronic means; they are large and unstructured strings (typically more than 400 characters in length). But techniques exist for extracting a “thumbprint” of less than 30 characters that uniquely corresponds to the public key for verification purposes.

A thumbprint can be distributed by trustworthy channels other than electronic ones (e.g., IVR, fax, letter mail or official publication) as well as by electronic means (e.g., e-mail or the Web).

Once a genuine thumbprint has been exchanged, the corresponding public key can be distributed via any convenient but untrusted channel, such as e-mail or the Web, and reliably verified by the recipient. In this way, trust can be bootstrapped and a larger set of keys can then be validated automatically.

The security of an out-of-band exchange can be substantially improved by using multiple channels and recommending that receiving parties verify the thumbprint by means of more than one channel. In this way, an adversary must subvert multiple channels simultaneously in order to compromise the overall system. A central authority is required to facilitate the bootstrap operation, and the ICAO is a suitable body to perform this function for the ePassport application.



## 6 Importance of the CPS

As mentioned, it is not sufficient for the relying party to assure itself that the public key is a genuine copy of the issuer's key. It is also critical to understand the way in which the public and private keys have been and will be managed throughout every stage of their lifecycles; information contained in the issuer's CPS.

If the originating country does a poor job of distributing its public key or protecting its private key, or a poor job of confirming the correspondence between the biometric and identifying information of its citizens, then the fact that the signature can be confirmed is of little value. Therefore, standards are required by which countries operate their trust infrastructures and confirm that they adhere to those standards.

In an ideal world, every country on the globe that issues ePassports would manage their trust infrastructures in a common way — and to a common standard. But, this is too much to expect, given the wide gap that exists in available resources, attractiveness of the target and consequences of a failure. Nevertheless, a relying country must be able to evaluate the degree of assurance offered by another country's travel documents.

In the commercial world, it is common to use independent IT auditors for this purpose. Governments more commonly employ independent internal departments to audit their own operations. Regardless of whoever performs the audit, standard criteria are needed as guidance.

Relying countries are likely to guard their autonomy when it comes to accepting identity documents from other countries. In general, they are not likely to accept, without careful consideration, an audit performed by another body. However, standard audit criteria would provide a basis for evaluating these audit reports.

## 7 Role of the ICAO

Modern information systems, such as the Internet, avoid dependence on centralized real-time functions. This makes them resilient and fosters competition, which leads to improved quality and reduced cost. They do, however, employ centralized functions for policy setting and for ensuring the uniqueness of names and locators.

The same principles can be applied to the ePassport trust infrastructure. ICAO already sets standards for nations that issue and rely on passports. So, it would be a natural extension of this role for it to establish criteria for auditing certificate issuers.

In order for an audit to be meaningfully interpreted by a relying country, it must be conducted according to a transparent standard, covering aspects such as team structure, professional qualifications, sample size, etc.

ICAO is in a position to set the required standard and accredit audit bodies according to the standard. And, as a side effect of this function, ICAO will be able to authenticate the source of the audit reports it receives from its accredited auditors.



Also, as the auditor inevitably has an intimate relationship with the issuers that it has audited, it can be relied upon to deliver the issuer's thumbprint to ICAO. The thumbprint and location of the issuer's public key could be included in the audit report. Then ICAO could sign the audit reports to indicate that they were produced by an accredited auditor. A relying party, equipped with ICAO's thumbprint, can then authenticate the audit report, evaluate its contents and locate, import and verify the foreign issuer's public key.

This solution eliminates the need for centralized real-time functions, respects the autonomy of individual countries and leverages existing and natural relationships to provide tools for quickly and cost-effectively locating, importing and trusting public keys from foreign governments.

In summary, existing proposals for distributing authentic public keys in the ePassport application are not well suited to deliver the speed and transparency required of a modern trust management infrastructure for arms-length partners. However, tools developed for the commercial world can be readily adapted to the needs of governments to identify citizens of foreign countries.

## 8 About Entrust

Entrust has been a trusted advisor to many countries as they pursue ePassport projects. Our software is currently in production use in a number of countries issuing a high volume of ePassports including the United States, United Kingdom, Singapore, Slovenia and New Zealand.

Countries are beginning to evolve their ePassport programs to include capabilities for recently standardized Extended Access Control (EAC). Entrust's participation in related standards bodies and consulting with our customers have enabled early implementation of EAC solutions.

With flexible solutions for Basic Access Control (BAC) passive authentication (CSCA PKI) already widely deployed, Entrust has also released security solutions to meet the certificate management requirements of Extended Access Control (CVCA PKI). By implementing the Entrust platform, customers can begin with BAC and layer in new capabilities for EAC, as well as additional functionality such as secure e-mail for transporting root certificates or other critical communications.

Entrust provides trusted solutions that secure digital identities and information for enterprises and governments in 2,000 organizations spanning 60 countries. Offering trusted security for less, Entrust solutions represent the right balance between affordability, expertise and service. These include SSL, strong authentication, fraud detection, digital certificates and PKI. For information, call 888-690-2424, e-mail [entrust@entrust.com](mailto:entrust@entrust.com) or visit [www.entrust.com](http://www.entrust.com).