Entrust®

A Trust Infrastructure for ePassports

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

+1-888-690-2424
entrust.com

Table of contents

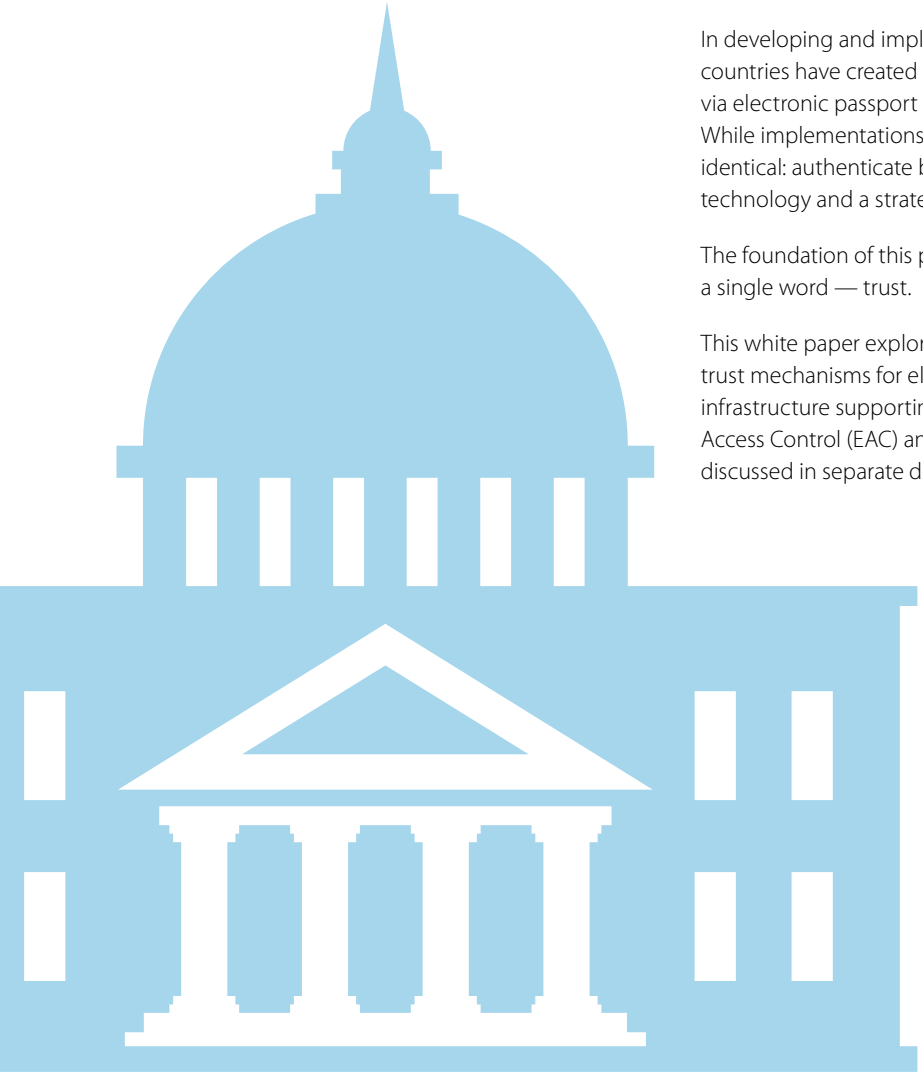
Entrust®

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 approached, 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.

Birth of an idea

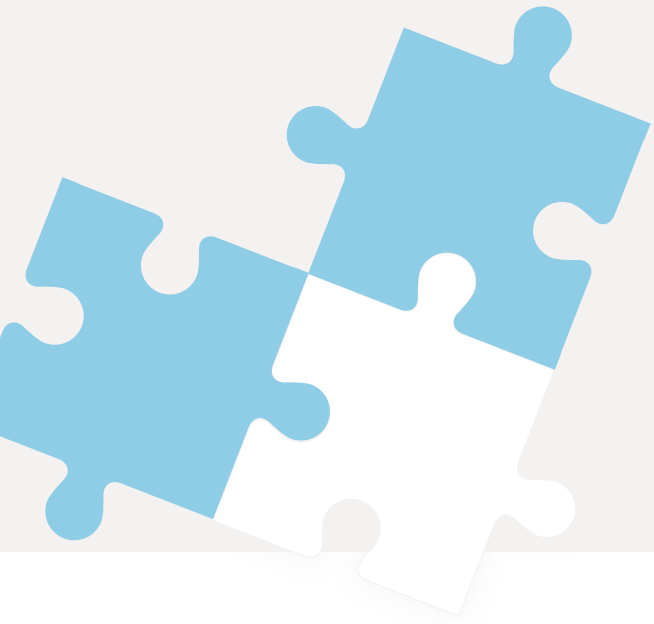
It was May of 1975. Those "in the know" had come to understand just how big an impact personal computers and data networks were going to have on our professional and domestic lives, and that existing security solutions were totally inadequate for the job they would be called upon to do.

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.

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, issued by trusted certification authorities (CA) 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 CA 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.

ePassports

"… an ePassport, containing an RFID chip and a certificate, can prove the binding between the biometric and identity information that it contains."

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.

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 todisavow 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 through bilateral means. Originally, this meant through use of a diplomatic bag of the originating country.

More recently, electronic forms of bilateral exchange have been introduced, including download from the CA website, email exchange, etc. The second uses a threshold scheme based on lists of certificates obtained from other countries that already rely on them.

The diplomatic bag form of bilateral exchange was 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. Electronic bilateral exchange is more efficient and economic, but requires individual exchange directly with each country.

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, not as a recommendation that others place trust in that 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.

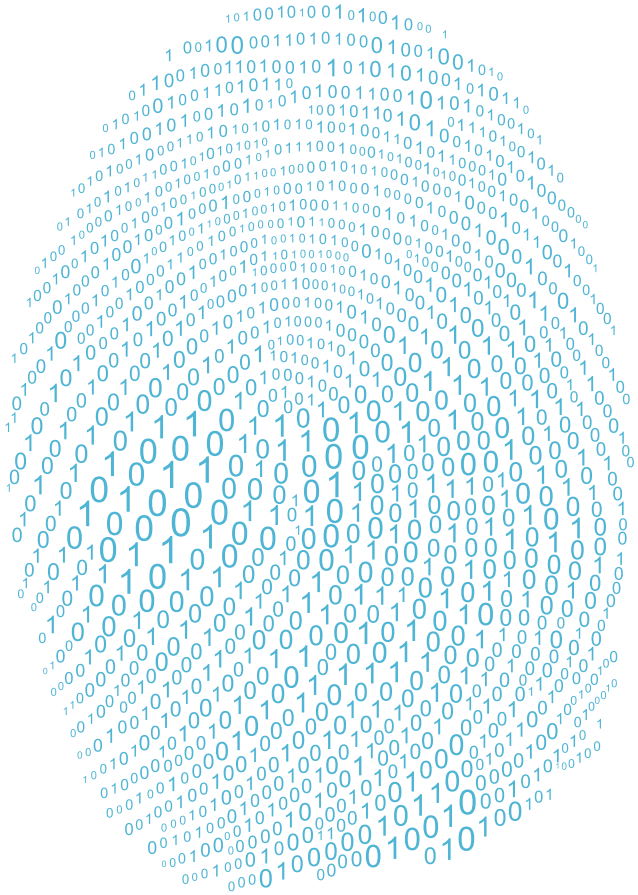
The master list approach involves the delegation of a highly sensitive function to a set of foreign governments; something that likely won't be acceptable to all passport-accepting countries.

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. A centralized master list, published by ICAO rather than individual countries might help make the issuer certificates more readily available.

The master list concept and specification was approved by ICAO in 2009 and a few countries have published lists. And, unlike the diplomatic bag solution, master lists, as well as the other technologies used for bilateral exchange, do not provide a solution to the "bootstrap" problem.

Bootstrapping trust

"Before one can validate a public-key certificate for another entity, a trusted public key for the certificate issuer must already be in place."



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., email 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 email 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.

Passport
PKI infrastructure

The PKI infrastructure for the ePassport BAC application is a relatively simple one compared to other open applications such as the Web.

Each country operates a single CA, referred to as their Country Signing CA (CSCA). That CA issues certificates to Document Signers (DS), Master List Signers (MLS) and possibly other entities. The CA also issues a periodic Certificate Revocation List (CRL) indicating whether any current certificates they issued have been revoked.

A Document Signer digitally signs a copy of the data stored on the passport chip so that its authenticity and integrity can be verified.

In addition to distribution of the CSCA certificate and bootstrapping trust, border control, or other entities verifying the electronic data on the passport RFID chip, needs to obtain the Document Signer certificate and CRL associated with that passport.

The DS certificate is included directly on the chip of every passport with which it is associated. The CRL can be obtained from one or more publication sources. The CSCA includes pointer(s) to the relevant CRL in each certificate it issues.

Using the trusted public key of the CSCA, the digital signatures on the DS certificate and the CRL can be verified and the revocation status of the DS certificate verified. Assuming success, the DS public key can be used to verify its digital signature on the signed object on the passport chip.

Assuming that is successful, the relying party, typically border control, can be assured that the electronic data has not been tampered with since the signature was created and that the signature was created by a DS associated with the trusted CSCA of the passport issuer.

The First Generation: Basic Access Control
The initial generation of ePassports uses Basic Access Control (BAC), which features passive and optional active authentication, and is in production in many parts of the world. This functionality, based on X.509 PKI (CSCA), provides verification that the document was signed by the legitimate issuing authority and the data stored on the chip has not been changed since issuance.

The Evolution: Extended Access Control
Countries are now evolving their ePassport programs to a second-generation framework that includes capabilities for Extended Access Control (EAC). Through terminal and chip authentication, EAC aims to increase the security of MRTDs through enhanced protection of biometric data (e.g., iris scan and/or fingerprint) stored on the contactless chip in the ePassport.

Entrust and you

"More than ever, Entrust understands your organization's security pain points."

Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Now, as part of Datacard Group, Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards.

For more information about Entrust solutions, call **+1 888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Company Facts
Website: entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway,
Suite 1250
Dallas, TX 75240 USA

Sales
North America:
+1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

Twitter Facebook Youtube LinkedIn Google+ RSS

Entrust®

23267/8-14