# Entrust®

# Protecting biometric data with Extended Access Control

Securing biometric datasets in electronic identification documents

+1-888-690-2424

entrust.com

# Table
## of contents

**Entrust**®

# Sensitivity
## of biometric datasets

"… people should only allow their biometric samples to be gathered by systems that can be trusted …"

Biometric datasets represent very sensitive personally identifiable information (PII). When used to authenticate a subject's transactions and travel, they could be misused to track the subject's actions and movements. In the case of fingerprints, biometric datasets could even be used to falsely incriminate the subject in a physical crime.

In addition to these privacy concerns — which are taken more seriously in some parts of the world than others — there exists an important realization for anyone who relies on biometric data: if biometric datasets fall into criminal hands, they could be used to impersonate the subject, and thereby allow criminals to evade safeguards intended to identify and apprehend them.

As a result of this threat, people should only allow their biometric samples to be gathered by systems that can be trusted to handle them properly (e.g., using the datasets only for the declared purpose, destroying them immediately after use, etc.). And, for maximum reliability, they should only be used in closely supervised settings. If these precautions are not taken, biometric samples can lose their effectiveness as a means of authentication.

# Extended access control

"An innovation in the security of machine-readable travel documents ..."

Much work remains to be done to devise acceptable ways of controlling the use, storage and communication of personally identifiable information. However, the European Union has been proactive in standardizing a scheme for controlling the release of biometric datasets from their citizens' ePassports and other electronic identity documents.

An innovation in the security of machine-readable travel documents (MRTD), Extended Access Control (EAC) has been adopted and deployed by the EU, as well as by some countries outside the EU.

EAC is based on public-key technology and uses card-verifiable (CV) certificates, which are issued to document-readers and are very similar to X.509 certificates. In addition to identity information, they also contain privilege information, indicating the types of personally identifiable information that the reader can be trusted to receive. These privileges can be controlled by the passport holder's own passport authority. CV certificates have to be evaluated by the ID card prior to the release of sensitive data.

Unlike X.509 certificates, CV certificates use a syntax that is more amenable to processing by platforms — such as smartcards and ePassports — that have access to very limited computing resources.

EAC doesn't support a certificate revocation scheme, due partly to problems of reliable and timely communication over large distances and with remote locations, as well as the absence of a real-time clock on the relying party platform (i.e., the card or ePassport).

Consequently, if a document-reader were to fall into criminal hands, it would not be possible to centrally withdraw its privilege to access personally identifiable information, including biometric datasets on an ePassport.

ICAO and ISO are working on standards for the next generation of electronic passport, with EAC expected to play a key role. The next-generation passport will support writing to the chip after the passport has been issued, enabling electronic travel records, electronic visa and additional biometrics to be added and to be read from these passports. EAC will enable authentication and access control to ensure that only authorized terminals read and/or write to these next generation passports.

# Safeguarding ePassport contents

"Some experts have suggested that short-lived certificates mitigate … vulnerabilities …"

Some experts have suggested that short-lived certificates mitigate the vulnerabilities that would otherwise be addressed by a revocation scheme. But this point of view doesn't stand up to scrutiny. Because the relying party platform does not contain a real-time clock, it is not capable of detecting any change of status with time.

In point of fact, identity documents can estimate a lower-bound to the time by looking at the effective date of any trusted certificates that they have occasion to process. But, there are limits to the efficacy of this solution.

Picture the scenario shown in Figure 1. An ePassport was last used on May 15, then stolen on May 19 (its internal lower-bound estimate of time is frozen at May 15). An active card-reader was stolen on May 25. Its certificate chain remains valid for the time at which it was last connected to the network.

If the passport were to be presented to the stolen card-reader, then it would update its estimate of the date to the day on which the reader was stolen and grant it access to its biometric datasets.

Criminals behind the theft could then create a prosthetic from the biometric dataset and, in combination with the stolen passport, impersonate its holder. This capability would persist until the expiration of the passport.

| | ePassport used to re-enter home country | ePassport stolen | Reader stolen | Stolen ePassport presented to stolen reader |
|---|---|---|---|---|
| Date according to reader certificate | MAY 15 | MAY 19 | MAY 25 | MAY 25 |
| Date according to ePassport | MAY 15 | MAY 15 | MAY 15 | MAY 25 |
| Actual date | MAY 15 | MAY 19 | MAY 25 | MAY 30 |

Figure 1: ePassport estimates date based on reader certificate

Of course, the ePassport system implements other safeguards that compensate for any failure of EAC. So, the scenario laid out above is not likely to lead directly to a security breach. It does, however, represent a failure of the EAC feature.

The absence of a battery and, therefore, a real-time clock, internal to the identity document makes both revocation and short-life certificates ineffective safeguards against loss of control over the reader's private key. The main safeguard designed to compensate for this deficiency is strong confidentiality protection of the reader's private key; instead of revoking the public key, the private key must be placed beyond unauthorized use.

# Protecting
## the private key

*"For portable inspection systems, tamper-resistance technology must be used …"*

It may be quite straightforward to protect the confidentiality of a private key in a device operated at a large port of entry. One solution is to house the cryptographic functions and private keys away from the immigration desk, in a protected facility, with communication between the reader and the protected facility carried over a private network. But problems may still arise when the devices containing the private keys are shipped for redeployment, repair or destruction.

Readers are also required to operate at remote land-based border crossings and to be taken out to small airplanes and yachts. Such systems cannot benefit from being housed and operated in a secure physical facility; they are much more vulnerable to theft or loss. For portable inspection systems, tamper-resistance technology must be used, with keys being automatically overwritten after a short period of disuse.

The inspection system's private keys must be generated, used and destroyed entirely within either a tamper-resistant enclosure or a secure facility. In the case of an enclosure, in order to protect against loss or theft, effective tamper-detection measures must cause overwriting of the private key in the event of power or temperature out-of-range, as well as detected attempts to open the unit. As a back-up safeguard, units that do not connect with the management system for a period of time should overwrite the key.

# Conclusion

*"The requirements for Extended Access Control dictate a unique public key infrastructure."*

While extremely valuable for strong authentication, biometric datasets contain sensitive personally identifiable information that criminal organization could leverage to commit fraud, impersonate identities or gain unauthorized access into ePassport-protected countries.

Extended Access Control technology helps protect these invaluable biometric datasets from being stolen and used for malicious gain.

The requirements for Extended Access Control dictate a unique public key infrastructure (PKI) design; one that does not include revocation of public keys. Strong protection for the confidentiality of the reader's private key must be relied upon instead. This is a more brittle solution than public-key revocation, because there is no way to recover when it goes wrong. However, with careful system design, sufficiently reliable and secure solutions can be created.

# 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** | **Headquarters** | **Sales** |
|---|---|---|
| Website: entrust.com | Three Lincoln Centre | North America: |
| Employees: 359 | 5430 LBJ Freeway, | +1-888-690-2424 |
| Customers: 5,000 | Suite 1250 | EMEA: +44 (0) 118 953 3000 |
| Offices: 10 globally | Dallas, TX 75240 USA | Email: entrust@entrust.com |