Increased use of biometrics in the ePassport lifecycle also comes with increased privacy concerns over the storage and exchange of biometric data. This white paper shows how FIDELITY addresses these concerns with private database query techniques and template protection mechanisms.

— the FIDELITY WP8 team

A proper identity document issuance process is key to stop identity fraud. First of all, the issuing country has to make sure that it is issuing the identity document to the intended person. Secondly, it needs to ensure that people cannot create multiple identities, possibly in different countries, which could be used to collect illicit social benefits, apply for asylum in multiple EU Member States or even be exploited by criminals to avoid prosecution.

To create a strong link between the identity and the person, biometrics are typically used. These can also be used to verify that the person applying for an identity document is not already known under another identity, i.e., by performing a Duplicate Enrolment Check (DEC).

Protecting EU citizens' identities is a balancing act between the means to fight identity fraud and respecting citizens' privacy.

This white paper targets the use of privacy preserving biometrics during duplicate enrolment checking. Within the FIDELITY project, the DEC concept has been considered to its fullest extent, i.e., a cross-Member States' DEC, where an EU Member State forwards information from an applicant to check whether this applicant is already registered in another EU Member State.
Duplicate Enrolment Check

Duplicate Enrolment Checking (DEC) is typically performed when a person applies for an identity document. The goal of DEC is to distinguishing between a genuine application for an identity document and a fraudulent attempt to become registered under different identities (e.g. different names).

During the application process for an identity document, a biometric sample (fingerprint) is collected from the person applying. DEC relies on a central or distributed biometric database to find potential matches with the collected biometric sample. In case of a match, DEC produces a positive output – which may be later on reviewed by a human expert to confirm the duplicate enrolment.

Next to the biometric database, DEC often benefits from an identity database which is linked to the biometric database. In this case, if DEC produces a match, i.e., at least one registered biometric data is close to the captured biometric data, the corresponding identity data can be checked.

However such solutions are not without risks to the citizen’s privacy. There are already different data protection authorities in Europe questioning the proportionality of such solution with respect to the purpose. Moreover, this issue is amplified by the scale of the risks related to the existence of an accurate and complete identity record of citizens with various personal data included. The fact that often several biometric samples (for instance several fingerprints) are needed to ensure a high accuracy level in DEC increases the issue raised by those authorities. One threat is that the database would be used for other purposes (commonly referred to as “function creep”), in particular for identification of suspects under police investigation.

Within the FIDELITY project, the DEC concept has been considered to its fullest extent, i.e., a cross-Member States’ DEC, where an EU Member State forwards information from an applicant to check whether this applicant is already registered in another EU Member State. This will ensure that the same person cannot use multiple identities among different EU Member States. This means that one has to consider data protection constraints not only on the database itself, but also on the queries made to the database, since these possibly transmit personal data to a foreign country.
Private queries

There are a myriad of techniques to ensure that databases only leak minimal information when performing queries, here referred to as private queries. Private queries can have different goals: prevent the database from learning the exact query and/or limit the amount of information revealed by the database.

When making queries to a biometric database, the main goal is to perform a comparison between a given sample and the stored templates. Hence, the database does not necessarily need to know what sample is being queried for and the reply to the query might only require information on the presence or absence of a match, without additional details.

A simple but powerful way of achieving a private query technique is a database with weak links. As an example, consider storing identity data combined with fingerprint data. Instead of directly storing the link between an identity and the corresponding fingerprint, individuals are grouped at random into sets of a sufficiently large size and only the link between a set of identities and a set of fingerprints is stored. This ensures that biometric data are not uniquely linkable to identity data. This way, database queries can be used to detect impersonations but do not allow for direct identification of individuals. This technique can be used for DEC by searching the biometric data for a match with the biometric sample and at the same time searching the identity database for a match with the person's identity. Depending on the outcome of both searches one can detect several fraud scenarios. For example, in case of a match in both databases, but in unlinked sets, this indicates that the applicant is already known under a different identity.

Two other solutions for private queries were developed in the FIDELITY project: the GSHADE and the PRC+biometrics protocol. Both of these make use of cryptographic techniques to hide information on both the query and the query result. Weak links do not hide any information in the query.
Template protection

Template Protection Schemes (TPS) store a protected sample or template instead of the clear data. A TPS should be such that it is impossible to retrieve the original sample (e.g., face, fingerprint, iris) or template. It should also be impossible to link subjects across different services. A TPS should, despite the security features, still be useful for biometric comparison. In this way template protection limits the functionality of the data to certain specific functions, such as comparison, and thus limits the abuse potential.

The motivation for template protection schemes is to reduce the gain for an adversary attacking the biometric database. By not storing biometric samples in a recoverable way, a compromised database cannot be used to create spoofs (e.g. a gummy finger) to impersonate citizens in the database. The database is also protected against unauthorised modification, making it harder for an attacker to modify the database. A possible attack would be replacing in the database a fingerprint of an existing citizen with the fingerprint of an accomplice, after which the accomplice can impersonate the citizen.

TPS categories

Biometric cryptosystems are also referred to as helper-data-based techniques since some public information is stored in the system database. They usually need a key to create the template and depending on the way the helper data are obtained, we have key binding and key generation techniques.

Feature transformation (or cancellable biometrics) apply a transformation to the template. We distinguish biometric salting, where the transformation is invertible and defined by a key; and non-invertible transformations, which do not require a key and are always one-way functions. Non-invertible transformations are typically the most difficult to construct.

Designing a template protection scheme that is secure but still allows for accuracy for fuzzy matching (two biometric samples of the same person are never identical) is challenging. In order to improve the accuracy, multiple modalities can be used. This typically requires a fusion mechanism, which combines the biometric comparison algorithms for all the modalities. In this case also the template protection mechanism needs to be extended to multiple modalities, taking into account the fusion.

In the FIDELITY project eight different template protection schemes were developed and/or analysed, not counting several variants. The template protection schemes are based on several different underlying techniques and belong to different categories, some of them requiring a key. The development of these schemes was the result of an iterative process, including a security analysis that also showed vulnerabilities in multiple existing schemes. Concerning the different modalities, FIDELITY template protection schemes are available for fingerprints, irises and face.
Towards DEC solutions

When specifying an architecture for DEC a balance has to be struck between several design criteria. There are operational requirements in terms of speed, accuracy and in general the overall performance of the system. There also requirements in terms of protecting the sensitive data stored in the system. Such protection measures can include limiting access to the DEC system, limiting information release, not storing certain information, hiding query data... The balance between operational and privacy requirements becomes especially difficult when more detailed comparisons should be performed by an expert (e.g., to determine if there is actual fraud), which require access to raw data.

Regarding the security/privacy objectives a clear distinction can be made between native and cross-Member State usage. In the case of native access, both the client and the database server fall under the same authority and legislation. Cross-MS access implies that a foreign country accesses a remote database. In this case only limited guarantees, both technical and legal, can be given regarding the security of the client system. This distinction also has implications regarding the level of privacy. For native access, the database can release more information to the client and allow more complex queries.

When a foreign country accesses a biometric database, it is reasonable to assume that the information released might be handled in an unknown, possibly insecure manner. Therefore the information released by the database should be minimized, possibly only releasing a single bit of information on a match or non-match and leaving the detailed handling to an offline, manual process that can include additional verifications.

For accuracy it is often required to store multiple modalities. By using a combination of private query techniques and template protection schemes a system can be built that satisfies operational and privacy requirements for both native and cross-Member State DEC. FIDELITY provides several key technologies to build such a system. For native DEC a weak link scheme might suffice as we do not need to hide query information. This also still allows manual verification as the biometric is stored in plain, but limits the identifying capabilities. For cross-Member State a stronger private querying mechanism should be used that also hides query information. An interesting way of achieving this is a query in the form of a protected template which is matched with the plain biometric information in the database. The resulting information is a smaller data set of possible matches, on which one can use for example the GSHADE protocol for performing more detailed comparisons while still respecting privacy. By combining the right template protection schemes with weak links and other private query techniques, one can create a functional DEC system that respects privacy. Despite still being at a research stage, the future possibility to improve the balance between security and privacy is a nice perspective for further investigations.
FIDELITY achievements

- Novel private database query techniques, to protect privacy of queries and/or answers.
- Template protection: new schemes and security analysis of existing schemes
- Combine private queries and protected templates to improve privacy in DEC.
- Differentiated requirements for Native and Cross-Member State DEC.
Further reading

Scientific publications


Contributors

We would like to thank the following people for their contributions to this document and to the development of the FIDELITY privacy preserving biometrics and DEC solutions: Aysajan Abidin, Julien Bringer, Christoph Busch, Moazzam Butt, Raffaele Cappelli, Hervé Chabanne, Matteo Ferrara, Olaf Henniger, Jens Hermans, Victor Leyva, Guoqiang Li, Davide Maltoni, Edlira Martiri, Constance Morel, Bart Mennink, Alexander Nouak, Andreas Pashalidis, Alain Patey, Roel Peeters, Ramachandra Raghavendra, Christian Rathgeb, Bian Yang and all other contributors to the FIDELITY WP8 technology. This document includes synthetic fingerprint images generated by the University of Bologna.