Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area

Nicolas Buchmann, Christian Rathgeb, Harald Baier and Christoph Busch

da/sec – Biometrics and Internet Security Research Group
Hochschule Darmstadt, Darmstadt, Germany
{firstname.lastname}@h-da.de

Abstract On 14th October 2013 the European Parliament Committee on Industry, Research and Energy (ITRE) paved the way on the regulation and harmonisation for electronic identification, authentication and trust services (eIDAS) between EU member states. This upcoming regulation will ensure mutual recognition and acceptance of electronic identification across borders, which also provides an opportunity to establish trusted electronic transactions in the Single Euro Payments Area (SEPA). The contribution of the presented paper is twofold: on the one hand we discuss the adaption of the upcoming eIDAS standard towards trusted banking transactions and outline resulting security and privacy enhancements; on the other hand we extend the eIDAS standard by biometric authenticated transactions which not only boost user convenience, trust and confidence towards eBanking and eBusiness, but suggest to integrate state-of-the-art privacy compliant biometric technologies into the security ecosystem, which is promoted by both, the European Payment Council (EPC) and the European Banking Union (EBU). As a result we identify eIDAS as highly suitable for banking transactions since it is solely based on security protocols and infrastructure which have been for more than ten years proven secure in the civil aviation domain.

1 Introduction

The European Parliament Committee on Industry, Research and Energy (ITRE) initiated the regulation and harmonisation for electronic identification, authentication and trust services (eIDAS) between EU member states [11]. The eIDAS security protocols and infrastructure are based on standards which have been successfully adapted in the civil aviation organisation for a long time [5,6]. More than a hundred states actively issue ePassports, 54 of which store face and fingerprint biometrics on their ePassports and in total nearly 490 million ePassports have been issued (status: Nov. 2012) [19]. The upcoming EU regulation will ensure mutual recognition and acceptance of electronic identification across borders, which also provides a significant opportunity for trusted electronic transactions in the Single Euro Payments Area (SEPA).

Currently, 33 SEPA countries process over 80 billion electronic payment transactions annually [15]. Therefore a security protocol responsible for protecting such a vast number of transactions has to be based on a standard which

has been proven secure and functional in practice. These pre-conditions apply to the upcoming eIDAS standard, i.e. building a bridge between the upcoming eIDAS standard and SEPA transactions provides a mutual gain for both sectors. On the one hand the ongoing process of the eIDAS regulation is strengthened by new use cases targeted at millions of users (e.g. secure home eBanking and skimming prevention at ATMs). On the other hand SEPA transactions could rely on standards which have been proven secure in another high-security domain.

A study in 2010 [2] identified the harmonisation of the diverse regulatory regimes across Europe as one of the main obstacles for cross-border financial service profit. Despite the fact, that eIDAS is an upcoming standard, which will eliminate the aforementioned obstruction, it will rely on existing infrastructure. Belgium, Estonia, Germany, Italy, Latvia, the Netherlands, Portugal, Romania, and Spain are the EU member states which already operate eID systems, in addition, France, Hungary and Slovakia announced to establish their own eID system in the near future [33]. The harmonisation of these eID systems by the EU with eIDAS yields significant potential and a new level of security for eBanking in the SEPA. Furthermore, incorporation of biometric technologies is conceded to provide protection against phishing, eBanking fraud, as well as identity theft. Additionally, features extracted from biometric characteristics generally exhibit higher entropy than regular numeric PINs applied in current standards.

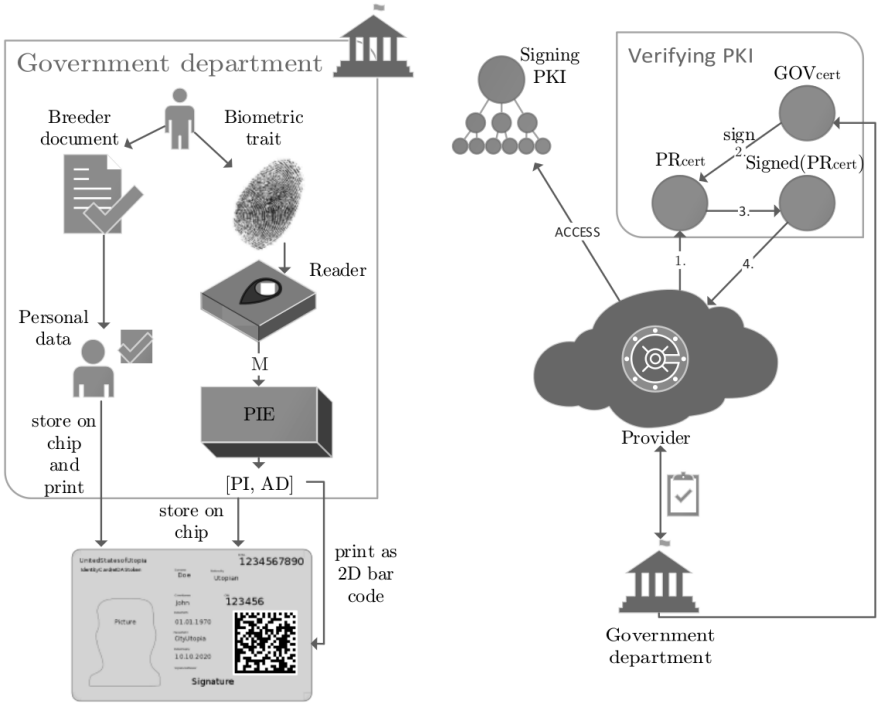
The contribution of the presented paper is twofold: (1) we discuss the adaption of the upcoming eIDAS standard towards trusted banking transactions and outline resulting security and privacy enhancements; (2) the first extension of the eIDAS standard regarding privacy compliant biometric authenticated transactions is given, which enhances user convenience, trust and confidence towards eBanking and eBusiness.In contrast to the very limited amount of existing proposals on the integration of biometrics into trusted banking transactions, e.g. [16], the proposed system fully relies on standardised and provable secure protocols, infrastructure, and technologies, which is vital for any kind of banking transaction application.

This paper is organised as follows: Section 2 presents the proposed overall system. Section 3 summarises the state-of-the-art of privacy compliant biometric technologies and discusses the entropy of common biometric characteristics. To augment the eIDAS standard by biometric authentication we extend the well-established PACE protocol to the BioPACE protocol in Section 4. Section 5 introduces the used security protocols and infrastructure. Section 6 evaluates the overall security and privacy properties of the proposed system. Finally, conclusions are drawn and future perspectives are given in Section 7.

2 System Architecture

The proposed system comprises four constituting processes, which are schematically depicted as part of Figure 1 and Figure 2, and combines three key components, (1) electronic identification, authentication and trust services (eIDAS) which are currently harmonised by the EU, (2) biometric template protection, (3) and the BioPACE protocol. These three components together provide a trus-

ted service with electronic identification and biometric authenticated transactions (see: section 6).



(a) eIDAS token issuing and enrolment. (b) eIDAS provider activation.

Figure 1: Wrap-up of (a) token issuing, enrolment, and (b) provider activation.

2.1 System hardware requirements

A user needs a specific set of hardware in order to use an eIDAS-enabled eBanking application. The vast majority of users will most likely possess a subset of the required hardware. The primary device can either be a notebook, smartphone or tablet with a browser and Internet access. This user device, which is assumed to be free of any kind of malware, additionally needs a camera which is common for all three mentioned device families. An eIDAS token can either be contact based or contactless, but due to easier handling and less abrasion, most eIDAS tokens will be contactless. In case of smartphones or tablets Near Field Communication (NFC) is necessary in order to communicate with a contactless eIDAS token. Focusing on notebooks the user most likely needs an external eIDAS token reader or a notebook with NFC support. To capture the user's biometric characteristic he either needs a device with an integrated biometric reader or an external device which could be a feature set of the external eIDAS token reader. Since a user might also use eGovernment services with his eIDAS token it is even more likely that he already possesses the appropriate hardware.

2.2 eIDAS token issuing and biometric enrolment

Within the proposed system a user is required to possess an eIDAS token which can either be a separate token or, in the common case, an integrated functionality of a national ID card or driver's license. As usual, the citizen applies for the national ID card (with eIDAS functionality), e.g. by presenting a breeder document, at a local government department and performs a supervised trusted biometric enrolment.

At the time of biometric enrolment a citizen presents a biometric characteristic, e.g. a fingerprint or iris, based on which biometric data is extracted. Biometrics create a strong link between the subject and the eIDAS token. It is important to note state-of-the-art biometric capturing devices, e.g. fingerprint readers, include liveness detection technologies which prevent from presentation attacks [32]. Biometric data M serves as input for a biometric template protection scheme [31] which permanently protects the privacy of the data subject in accordance with the ISO/IEC IS 24745 [21] on biometric information protection. Based on this standardized architecture a *pseudonymous identifier encoder* (PIE) generates a pseudonymous identifier PI and auxiliary data AD out of M in the enrolment process, $[PI, AD] = PIE(M)$. PI represents a protected identity of an individual and AD is user-specific data, which assists in reproducing PI in an authentication process. In the proposed system AD is stored via a visual 2D barcode, see Figure 1a, PI is stored in the internal memory of the eIDAS token chip and is therefore only available to the chip itself, and the unprotected biometric data M is deleted after the enrolment. The incorporation of biometric data is suggested to be implemented throughout the ongoing harmonisation of eID cards.

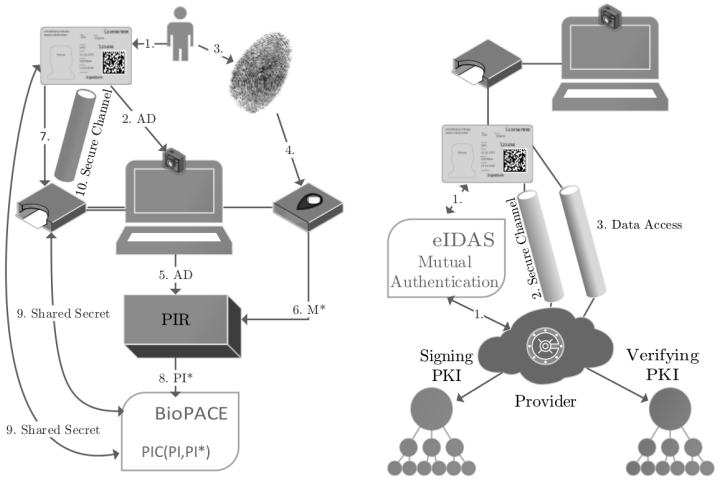
2.3 eIDAS provider activation

The eIDAS provider, e.g. a bank, requires access to the so-called *Signing* Public Key Infrastructure (PKI) [17] in order to check the originality of the eIDAS token presented by the user and to verify the authenticity and integrity of the personal data read from the eIDAS token (see: section 6).

Additionally, the eIDAS provider registers its service at the appropriate government department which handles the so-called *Verifying* PKI [7,27] in order to receive a service provider certificate. This certificate can be verified by the eIDAS token and also contains the eIDAS provider's access rights, i.e. the eIDAS token will only allow access to data groups granted by the service provider certificate, as shown in Figure 1b.

2.4 Entity authentication: Token – Reader

At authentication the user presents his biometric characteristic and the eIDAS token, which comprises AD in form of a visual 2D barcode, to the user's device. The *pseudonymous identifier recorder* (PIR) takes a queried biometric datum M^* and AD as inputs and calculates a pseudonymous identifier PI^*, $[PI^*] = PIR(M^*, AD)$. This PI^* is transferred from the reader to the eIDAS



(a) Entity auth.: Token – Reader (b) Entity auth.: Token – Provider

Figure 2: Wrap-up of authentication of token and (a) reader, and (b) provider.

token as part of the BioPACE [8] protocol which also performs the comparison of protected templates. Within a conventional template protection scheme the *pseudonymous identifier comparator* (PIC) compares PI^* with the stored PI, $v = PIC(PI, PI^*)$. Depending on comparators, the comparison result v is either a hard decision (yes/no) or a similarity score v which is then compared against a threshold t, in order to obtain a binary decision. Based on this static shared secret PI the eIDAS token and the eIDAS reader agree on an ephemeral shared secret authenticated with PI during the BioPACE protocol and establish a secure channel which provides authenticity, integrity and confidentiality for all data which is sent afterwards (see: section 6), as shown in Figure 2a.

2.5 Entity authentication: Token – Provider

After the secure channel between eIDAS token and eIDAS token reader has been established, the eIDAS provider and the eIDAS token mutually authenticate with the help of the eIDAS protocols, the *Signing* PKI and the *Verifying* PKI. In case this step is performed successfully, it can be assured that (1) the eIDAS token communicates with a trusted eIDAS provider and knows its access rights, (2) the eIDAS provider knows that it communicates with a genuine eIDAS token, and (3) during this process both parties establish a secure channel.

Subsequently, the eIDAS provider can now access the eIDAS token's data over this secure channel to authenticate the user. Since now both parties are completely authenticated the user can perform an online banking transaction. This transaction is two-factor authenticated since the user proofed possession of the eIDAS token by holding it up to the camera and placing it on the reader,

and by presenting his biometric characteristic to the reader. Due to the separation of possession (eIDAS token) and being (biometric characteristic) the eIDAS provider can be certain that the user performed the transaction himself. The entire process is illustrated in Figure 2b.

3 Incorporation of Biometrics

The term biometrics is defined as *"automated recognition of individuals based on their behavioural and biological characteristics"* (ISO/IEC JTC1 SC37). Physiological as well as behavioural biometric characteristics are acquired applying adequate sensors and distinctive features are extracted to form a biometric template in an enrolment process. At the time of verification or identification the system processes another biometric input which is compared against the stored template, yielding acceptance or rejection [26]. From a privacy perspective most concerns against the common use of biometrics arise from the storage and misuse of biometric data. Biometric template protection schemes [31] which are categorized as biometric cryptosystems [34] and cancellable biometrics [28] address these concerns and improve public confidence and acceptance of biometrics.

Both technologies are capable of generating AD and PI out of a given biometric input M. In case, PIs are applied within further applications, e.g. data encryption, it is required that generated PIs exhibit sufficient entropy. The entropy of biometric input data M directly relates to the entropy of the corresponding PI. Since biometric features cannot be expected to be mutually independent, different techniques of how to measure entropy provided by biometric characteristics have been suggested.

3.1 Template protection

Biometric cryptosystems are designed to securely bind a digital key to a biometric characteristic or generate a digital key from a biometric characteristic [9] offering solutions to biometric-dependent key-release and template protection [10,25]. Replacing password-based key-release, biometric cryptosystems bring about substantial security benefits. It is significantly more difficult to forge, copy, share, and distribute biometrics compared to passwords [26]. Further, most biometric characteristics provide an equal level of security across a user-group. Due to biometric variance, see Figure 3, conventional biometric systems perform "fuzzy comparisons" by applying decision thresholds which are set up based on score distributions between genuine and non-genuine subjects. In contrast, biometric cryptosystems are designed to output stable keys which are required to match a hundred percent at authentication. Biometric templates are replaced through biometric-dependent public information (AD) which is used in order to release a key (PI).

Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transforms (AD) which provide a comparison of protected templates (PIs) in the transformed domain [28]. The inversion of such transformed biometric templates must not be feasible for potential imposters. In contrast to templates protected by standard encryption algorithms, transformed

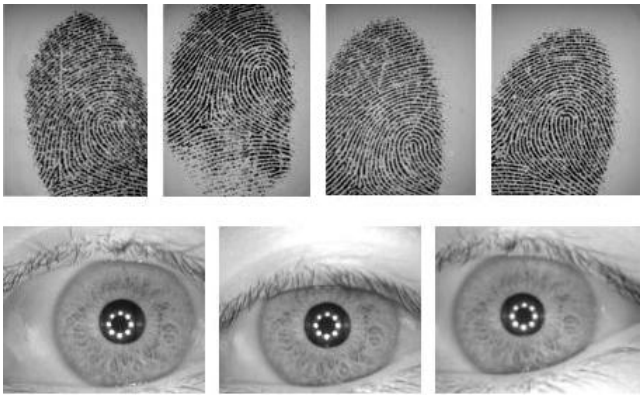


Figure 3: Biometric variance (images taken from FVC'04, CASIAv3 database).

templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of cancelable biometrics. Obviously, cancelable biometrics are closely related to biometric cryptosystems. In accordance with the ISO/IEC IS 24745, both technologies aim at meeting the two major requirements of irreversibility and unlinkability preventing from identity fraud and privacy violation:

- *Irreversibility*: knowledge of the protected template cannot be used to determine any information about the original biometric sample, while it should be easy to generate the protected template.
- *Unlinkability*: different versions of protected biometric templates can be generated based on the same biometric data, while protected templates should not allow cross-matching.

In past year numerous approaches to biometric template protection have been designed with respect to different biometric characteristics and application scenarios, see [25, 31]. In addition, various approaches to multi-biometric template protection schemes, i.e. systems which incorporate biometric data extracted from different biometric characteristics, have been proposed [30]. Nonetheless, the vast majority of template protection schemes report a reasonable decrease in recognition accuracy, yielding a trade-off between security and biometric performance.

3.2 Entropy of biometric data

As previously mentioned, biometric features must not be expected to be mutually independent, e.g. fingerprints underlie distinct structures. Focusing on data storage, binary biometric templates represent a favourable representation, enabling compact storage and rapid comparison. So far, numerous approaches have been proposed to extract binary feature vectors from diverse biometric characteristics, i.e. without loss of generality we will restrict to analyse entropy of biometric data according to a binary representation of biometric features.

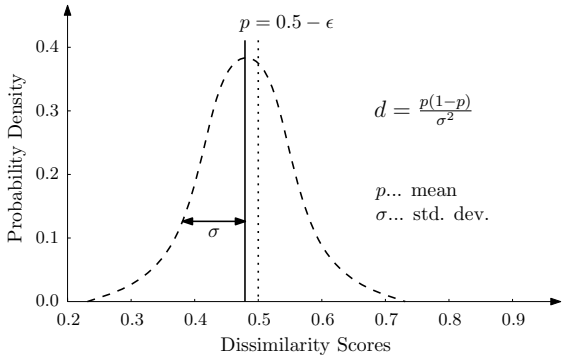


Figure 4: Binomial distribution of scores between different pairs of vectors.

Biometric characteristic	Feature extractor	Entropy (in bits)	Ref.
Fingerprint	Minutia-based	84	[29]
Iris	2D Log-Gabor wavelets	249	[13]
Face	Fusion of FLD and PCA	56	[1]

FLD ... Fisher linear discriminant PCA ... Principal component analysis

Table 1: Entropy reported in literature for different biometric characteristics.

A common way to estimate the average entropy ($\simeq$ amount of mutually independent bits) of biometric feature vectors is to measure the provided "degrees-of-freedom" which are defined by $d = p(1-p)/\sigma^2$, where p is the mean Hamming distance (HD) and σ^2 the corresponding variance between comparisons of different pairs of binary feature vectors, shown in Figure 4. In case all bits of each binary feature vector of length z would be mutually independent, comparisons of pairs of different feature vectors would yield a binomial distribution, $\mathcal{B}(z,k) = \binom{z}{k} p^k (1-p)^{z-k} = \binom{z}{k} 0.5^z$ and the expectation of the HD would be $1/z \cdot \mathbb{E}(X \oplus Y) = zp \cdot 1/z = p = 0.5$, where X and Y are two independent random variables in $\{0,1\}$. In reality p decreases to $0.5 - \epsilon$ while HDs remain binomially distributed with a reduction in z in particular, $\mathcal{B}(d, 0.5)$ [35]. Reported entropy in literature of relevant biometric characteristics are summarised in Table 1. Estimated entropy can be directly transferred to AD and PIs which are applied in further application. However, techniques which are employed to overcome biometric variance, e.g. severe quantisation, may reduce the entropy of resulting protected templates [1].

In addition the amount of degrees-of-freedom can be directly derived from the false match rate (FMR) provided by a biometric (template protection) system. According to the ISO/IEC IS 19795-1 [24] the FMR defines the proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template. At a targeted false non-match rate ($FNMR$), the proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample, provided entropy (in bits) is estimated as $\log_2(FMR^{-1})$, which directly relates to entropy estimations which are frequently applied to passwords or PINs.

4 (Bio)PACE

The Password Authenticated Connection Establishment (PACE) protocol was first introduced in the German electronic ID card and standardised by the German Federal Office for Information Security (BSI). It has become an international standard in form of the PACE-based Supplemental Access Control (SAC) [18] which will be added to ePassports by the end of 2014 as a supplementing access control protocol and will replace the current ePassport access control protocol Basic Access Control (BAC) by 2018 [20]. The BioPACE protocol utilises PACE as its basic building block, but instead of using a knowledge-based shared secret like PACE, it uses a biometric-based secret instead.

The idea of BioPACE was first introduced in [14] and later extended in [8] in the form of BioPACE version 2. Since version 2 fixes a tracking issue and adds some useful security properties relevant for the eIDAS context, in this work we will from now on refer to BioPACE version 2 as BioPACE.

In the eIDAS system the PACE protocol is used to mutually authenticate the eIDAS token and the eIDAS token reader, and to establish a secure channel between the two entities which provides authenticity, integrity and confidentiality of the transferred data by means of the *Secure Messaging* sub-protocol.

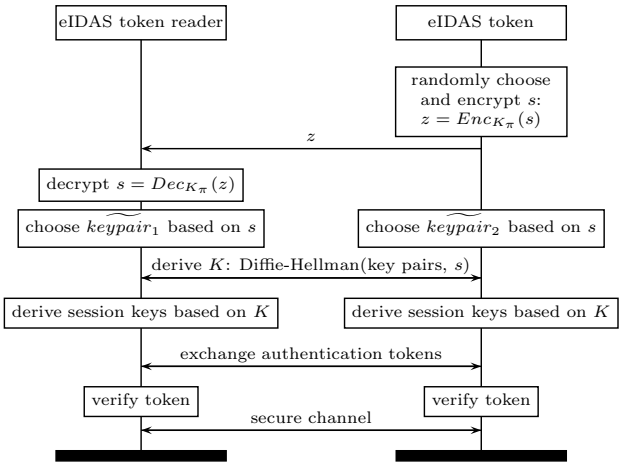


Figure 5: Basic operation mode of the PACE protocol.

4.1 Password Authenticated Connection Establishment

PACE is patent-free, provides strong session keys even in the presence of low-entropy passwords, and is resistant against off-line brute-force attacks [5]. The shared password is denoted by π and can either be received from the Machine Readable Zone (MRZ), a PIN, or the Card Access Number (CAN), which is printed on the eIDAS token and consists of a six digit number. Since eIDAS tokens can be contactless or contact-based both variants have different requirements in the eIDAS standard. The contactless version must support a CAN and

a PIN, and the contact-based version requires only the PIN, the CAN is optional. For our eIDAS system only the PACE variant which derives π from a six digit numeric PIN is relevant. PACE is based on symmetric and asymmetric cryptography, depicted in Figure 5, details are summarised in Appendix A.1.

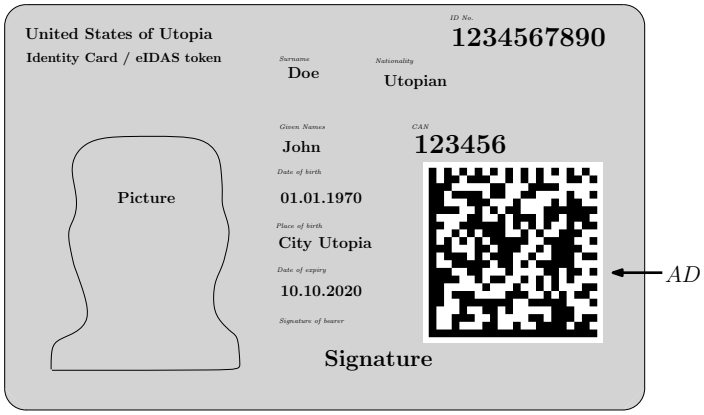


Figure 6: The eIDAS token with AD printed as data matrix code.

4.2 BioPACE

BioPACE is a pre-processing step to the PACE protocol which replaces the commonly used knowledge-based shared secret by a biometric-based secret. In [14] the idea to make use of biometric template protection based on the ISO/IEC 24745 standard for biometric information protection is introduced (see Section 3). BioPACE does not favour a biometric characteristic, i.e. BioPACE may be implemented using the facial image, fingerprints, iris, etc. The BioPACE protocol consists of two phases: (1) initialisation phase and (2) regular use phase.

For every eIDAS token the initialisation phase has to be conducted before the manufacturer can personalise the eIDAS token. During the application of an eIDAS token a user is enrolled and feature extraction is applied to the captured biometric sample, resulting in a biometric reference consisting of a pseudonymous identifier PI and auxiliary data AD.

After the biometric enrolment AD is printed on the eIDAS token in form of a 2D barcode (e.g., a QR code [23] or a Data Matrix code [22]), which is shown as part of Figure 6. PI is not publicly available, instead it is stored in the internal memory of the eIDAS token chip and is therefore only available to the chip itself, but not to the eIDAS token reader.

After initialisation BioPACE is ready for the regular use phase which consists of a new feature extraction from a biometric sample and an optical scan of previously enrolled AD. An eIDAS token reader requires optical access to the eIDAS token in order to scan the 2D barcode and receive AD to calculate PI^*, which equals PI if and only if the same person provided the biometric sample and therefore a biometric match occurs, this phase is depicted in Figure 7.

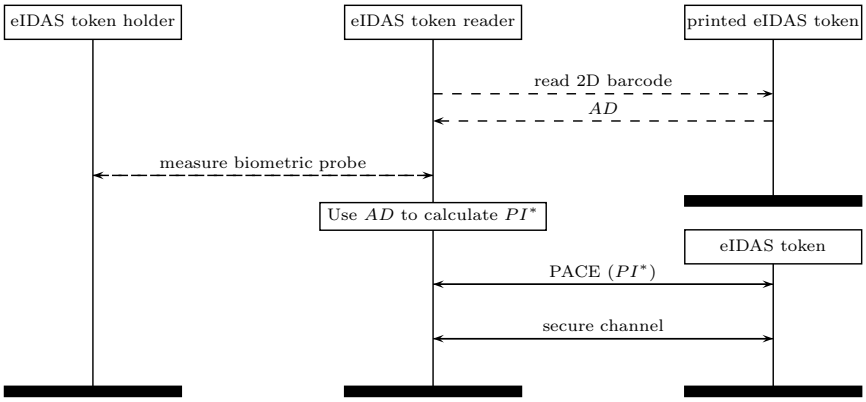


Figure 7: Basic operation mode of the BioPACE protocol.

After this pre-processing step PI^* is used as input for the PACE protocol. PI^* is implicitly compared to PI by the completion of the PACE protocol, because if PI^* and PI do not match the PACE protocol will fail. With respect to provided entropy biometric-based PIs exhibit sufficient entropy, cf. Table 1, compared to a PACE-based six digit numeric PIN which provides $\log_2(10^6) \simeq 20$ bits entropy.

5 eIDAS

eIDAS heavily relies on protocols and infrastructure introduced for electronic machine readable travel documents (eMRTD) [4]. Currently, eIDAS token functionality exists solely as feature of national identity cards which represent eMRTDs. Nevertheless, an eIDAS token does not necessarily have to be an eMRTD, but could also be a standalone token or part of a driving license.

5.1 eIDAS security goals

Between two entities (e.g. a user and a bank with an eID enabled service) eIDAS provides mutual authentication and key agreement to establish a secure channel. On the one hand the user can be certain that he is communicating with his bank and the bank can be assured to communicate with a user in possession of a valid eIDAS token. On the other hand, during the eIDAS procedure, user and bank agree on an ephemeral common secret to create a secure channel between the two parties which provides authenticity, integrity and confidentiality for further communication (see: section 6).

5.2 eIDAS infrastructure

The infrastructure of eIDAS consists of two PKIs which are both common in the eMRTD domain [7, 17, 27], i.e. the *Signing* PKI and the *Verifying* PKI.

Every eID service provider requires an authorisation certificate which regulates his access control rights for the information stored on the eIDAS token and serves as means of authentication towards the eIDAS token. The authorisation certificate belongs to the *Verifying* PKI and must be part of a certificate chain which has the eIDAS token's issuing country's Country Verifying Certificate Authority for eID (CVCA-eID) root certificate as trust anchor. This is crucial because the CVCA-eID certificate is stored on the eIDAS token and used during *Terminal Authentication* (TA) by the token in order to authenticate the service provider and validate its access rights.

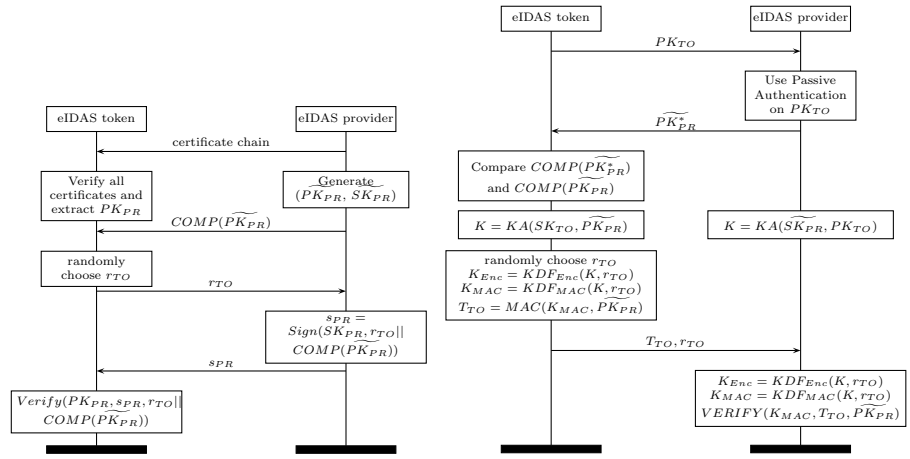
The *Signing* PKI fulfils the opposite role for the eID service provider. On the one hand it can check the originality of the eIDAS token, i.e. it communicates with a genuine uncloned eIDAS token. On the other hand the eID service provider needs the *Signing* PKI to check the authenticity and integrity of the personnel data send by the eIDAS token. Therefore, every country which issues eIDAS tokens needs a Country Signing Certificate Authority (CSCA) which constitutes the root anchor of the *Signing* PKI and signs a certificate of the domestic eIDAS token manufacturer. During the eIDAS token personalisation process the manufacturer digitally signs a hash list of all data groups stored on the eIDAS token. The CSCA certificate and the certificate of the eIDAS token manufacturer enable the eID service provider to verify the digital signature stored on the eIDAS token to ascertain the origin and the genuineness of the data.

5.3 eIDAS operation mode

The regular operation mode of eIDAS starts with a mutual authentication and key agreement between the eIDAS token chip and the local eIDAS token reader of the user. Therefore, the entities either perform the PACE or, as in the proposed system, the BioPACE protocol which is described in Section 4. Focusing on PACE the user ensures his willing to use the eIDAS service and the token reader to transfer his private data by placing the eIDAS token on the reader and entering a PIN. For BioPACE the user provides his declaration of consent by scanning the eIDAS token's 2D barcode with the device's camera, placing the eIDAS token on the reader and disclose his biometric characteristic to the eIDAS reader. Subsequently, PACE/ BioPACE establishes a secure channel between the eIDAS token chip and the user's eIDAS token reader.

eIDAS provider authentication: the next step in eIDAS process is the authentication of the eID service provider towards the eIDAS token and its holder with the TA protocol. After TA, the eIDAS token holder can be assured about the authenticity of the eID service provider he is communicating with as well as about the communication partner's access rights. Additionally, he receives an authentic ephemeral public key from the eIDAS provider. TA is depicted in Figure 8a, detailed steps are summarized in Appendix A.2.

After successful TA the eIDAS provider's name is extracted from its authorisation certificate and presented to the user either on the eIDAS token reader



(a) eIDAS provider authentication (Terminal Authentication)

(b) eIDAS token authentication (Chip Authentication)

Figure 8: Basic operation mode of the eIDAS mutual authentication.

or on the user's client device. The user has to manually accept that he wants to share his personal data according to the eIDAS provider's access rights by pressing a specified button on the eIDAS token reader or by accepting a dialog on the client device.

eIDAS token authentication: the closing protocol prior to the actual personal data transfer is called *Chip Authentication* (CA), which ensures originality of the eIDAS token and establishes session keys between the eIDAS token and the service provider.

In order to proof its originality an eIDAS token possesses a static Diffie-Hellmann key pair of which the corresponding private key is safely stored in the inaccessible internal memory of the eIDAS token. The public key has been signed by the eIDAS token manufacturer during personalisation, i.e. the public key can be verified with the help of the *Signing* PKI via Passive Authentication. CA is depicted in Figure 8b, detailed steps are summarised in Appendix A.3.

eIDAS data access and user authentication: both parties restart *Secure Messaging* with the derived session keys. The eIDAS provider can now be assured that it is communicating with a genuine eIDAS token, but it cannot yet uniquely identify the user, because the eIDAS token's static Diffie-Hellman key is not unambiguous among eIDAS tokens. The ambiguity of the static Diffie-Hellman keys exists to prevent tracking based on the CA keys. To uniquely identify the eIDAS token holder the eIDAS provider is required to read the actual data from the chip over the established secure channel.

6 System Security Properties

Table 2 presents an overview of security properties provided by applied technologies and protocols. The majority of listed security property contributions have already been outlined in the corresponding technology sections. Biometric technologies create a strong bond between the eIDAS token holder and the token, thus preventing identity theft and mitigating eBanking fraud. Since BioPACE relies on a biometric-based secret, in contrary to PACE's knowledge-based secret it cannot be forgotten, lost, stolen, shared or duplicated by the user which enhances usability and reduces user frustration. The eIDAS standard unambiguously proves the authenticity of the service provider to the user. This process does not only protect eBanking customers from fraud, but, by presenting them with the access rights granted to the service provider, also protects their privacy.

Properties	Biometrics	PACE	BioPACE	eIDAS	Proposed
$\text{Authenticity}_{token \leftrightarrow reader}$		✓	✓		✓
$\text{Authenticity}_{token \leftrightarrow provider}$				✓	✓
Access rights control				✓	✓
Data integrity		✓	✓	✓	✓
Confidentiality		✓	✓	✓	✓
Privacy preserving	✓		✓	✓	✓
Identification	✓		✓	✓	✓
Fraud detection	✓			✓	✓
Identity theft protection	✓				✓
Usability enhancing	✓		✓		✓
Phishing protection	✓			✓	✓
High entropy key seed	✓		✓	✓	✓
Standardised	✓	✓	(✓)	✓	(✓)

Table 2: Summarized security properties of applied technologies and protocols.

All security protocols which comprise the upcoming eIDAS standard are openly standardised and have been proven secure in the civil aviation domain [4]. These protocols have been standardised for the EU, since no international standardised protocol fulfilled the high security and privacy requirements which were demanded by the EU to protect sensitive user data, i.e. eIDAS builds upon carefully crafted security protocols. BioPACE has not been standardised but builds upon standardised components, i.e. biometric template protection and the PACE protocol.

6.1 Trusted hardware and trusted enrolment

eIDAS tokens can be standalone tokens, but much more likely they will be part of a sovereign document such as a national ID card. Therefore they will be manufactured and personalised under highest government security regulations

and certified using information technology evaluations. Therefore, eIDAS tokens can be considered trusted hardware which nearly any citizen will own in the near future.

The biometric enrolment is conducted in a supervised, trusted environment by trained operatives. In comparison to other systems, e.g. [16], the user has to present a valid breeder document before he is allowed to enrol for the new document. That is, there exists a strong, trusted link between the eIDAS token and the eIDAS token holder.

6.2 Security assumptions

The PACE protocol has been formally proven in [3]. A detailed security discussion of Chip Authentication and Terminal Authentication can be found in [12]. Technologies of biometric template protection are standardised in the ISO/IEC IS 24745 [21] and have been reported to provide biometric-based secret which exhibit sufficient entropy to be applied in the proposed system architecture.

7 Conclusion and Future Work

In this work the eIDAS standard, which has been harmonized and regulated on 14th October 2013 by the ITRE, is (1) adapted towards trusted eBanking and eBusiness, and (2) extended with respect to privacy compliant biometric authenticated transactions. The proposed system fully relies on standardised and provable secure protocols, infrastructure, and technologies, which is vital for any kind of banking transaction application. Based on a detailed description and investigation of constituting system components we identify a significant improvement of user convenience, trust, and confidence towards eBanking and eBusiness. Compared to other systems involved costs are considered negligible for both parties since users can rely on hardware which, for the most part, already available. Furthermore, service providers can employ an already established infrastructure and, more importantly, delegate expensive hardware support to government departments. Based on presented investigations we identify eIDAS as an appropriate key driver in future eBanking services. In order to underline the potential of the proposed infrastructure future work will be focused on providing a formal proof of the BioPACE protocol.

Acknowledgment

This work was supported by the European Commission through the FIDELITY EU-FP7 project (Grant No. SEC-2011-284862) and CASED.

References

1. Adler, A., Youmaran, R., Loyka, S.: Towards a measure of biometric information. In: Canadian Conference on Electrical and Computer Engineering, (CCECE'06). pp. 210–213 (2006)

2. Ahlswede, S., Gaab, J.: eIDS in Europe – Not (yet) yielding profits for the cross-border financial services sector (9 2010), Deutsche Bank Research
3. Bender, J., Fischlin, M., Kügler, D.: Security analysis of the pace key-agreement protocol. In: Information Security, LNCS, vol. 5735, pp. 33–48. Springer Berlin Heidelberg (2009)
4. BSI: Technical Guideline TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents - Part 1 – eMRTDs with BAC/PACEv2 and EACv1, 2.10 edn. (3 2012)
5. BSI: Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS), 2.20 beta edn. (9 2013)
6. BSI: Technical Guideline TR-03110-4 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 4 – Application and Profiles, 2.20 beta edn. (9 2013)
7. BSI: Technical Guideline TR-03139 Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Member States, 2.1 edn. (5 2013)
8. Buchmann, N., Peeters, R., Baier, H., Pashalidis, A.: Security considerations on extending PACE to a biometric-based connection establishment. In: Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the. pp. 1–13 (2013)
9. Cavoukian, A., Stoianov, A.: Biometric encryption. In: Encyclopedia of Biometrics. Springer Verlag (2009)
10. Cavoukian, A., Stoianov, A.: Biometric encryption: The new breed of untraceable biometrics. In: Biometrics: fundamentals, theory, and systems. Wiley (2009)
11. Committee on Industry, Research and Energy: EU e-signature plan to make electronic deals safer and easier. `http://www.europarl.europa.eu/pdfs/news/expert/infopress/20131014IPR22239/20131014IPR22239_en.pdf` (10 2013)
12. Dagdelen, O., Fischlin, M.: Security analysis of the extended access control protocol for machine readable travel documents. In: Information Security, LNCS, vol. 6531, pp. 54–68. Springer Berlin Heidelberg (2011)
13. Daugman, J.: Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. Proc. of the IEEE 94(11), 1927–1935 (2006)
14. Deufel, B., Mueller, C., Duffy, G., Kevenaar, T.: BioPACE – Biometric passwords for next generation authentication protocols for machine-readable travel documents. Datenschutz und Datensicherheit - DuD 37(6), 363 – 366 (2013)
15. European Payments Council (EPC): SEPA - Key Figures. `http://www.europeanpaymentscouncil.eu/` (10 2013)
16. Hartung, D., Busch, C.: Biometric transaction authentication protocol: Formal model verification and "four-eyes" principle extension. In: Financial Cryptography and Data Security, LNCS, vol. 7126, pp. 88–103. Springer Berlin Heidelberg (2012)
17. ICAO: Doc 9303 Part 1 Machine Readable Passports Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability. International Civil Aviation Organization (ICAO), sixth edition edn. (2006)
18. ICAO: Supplemental Access Control for Machine Readable Travel Documents. International Civil Aviation Organization (ICAO), 1.01 edn. (11 2010)
19. ICAO: Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) – Twenty-First Meeting – Montreal. International Civil Aviation Organization (ICAO) (11 2012)
20. ICAO: SUPPLEMENT to Doc 9303. International Civil Aviation Organization (ICAO), 13 edn. (10 2013)

21. ISO/IEC JTC 1 /SC 27 Security Techniques: ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection. International Organization for Standardization (2011)
22. ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques: Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification. ISO/IEC 16022:2006 (2006)
23. ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques: Information Technology – Automatic Identification and Data Capture Techniques – QR Code 2005 Bar Code Symbology Specification. ISO/IEC 18004:2006 (2006)
24. ISO/IEC TC JTC1 SC37 Biometrics: ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework. International Organization for Standardization and International Electrotechnical Committee (Mar 2006)
25. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Signal Process 2008, 1–17 (2008)
26. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. on Circuits and Systems for Video Technology 14, 4–20 (2004)
27. NORMA, C.T.: CSN 36 9791 ed. A – Information technology - Country Verifying Certification Authority Key Management Protocol for SPOC (12 2009)
28. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40, 614–634 (2001)
29. Ratha, N., Connell, J., Bolle, R.: An analysis of minutiae matching strength. In: Audio- and Video-Based Biometric Person Authentication, vol. 2091, pp. 223–228. Springer (2001)
30. Rathgeb, C., Busch, C.: Multibiometric template protection: Issues and challenges. In: New Trends and Developments in Biometrics. pp. 173–190. InTech (2012)
31. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security 2011(3) (2011)
32. Sousedik, C., Busch, C.: Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biometrics (January 2014)
33. Tractis – Negonation: World Map of eID deployments. `https://www.tractis.com/help/?p=3670` (12 2012)
34. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric cryptosystems: issues and challenges. Proc. of the IEEE 92(6), 948–960 (2004)
35. Viveros, R., Balasubramanian, K., Balakrishnan, N.: Binomial and negative binomial analogues under correlated bernoulli trials. The American Statistician 48(3), 243–247 (1984)

A Appendix – detailed protocol steps

A.1 Password authenticated connection establishment

1. The eIDAS token chip randomly chooses a nonce s and encrypts it with K_π which is derived from the shared password π. The eIDAS token sends the ciphertext $z = Enc_{K_\pi}(s)$ to the eIDAS token reader.
2. The reader recovers s with π and receives $s = Dec_{K_\pi}(z)$.
3. Chip and reader create ephemeral key pairs, and perform a Diffie-Hellman key agreement protocol and s. By performing Diffie-Hellman both entities agree on a new shared secret K.

4. Based on K both parties derive session keys.
5. Chip and reader exchange and verify authentication tokens based on a MAC.
6. *Secure Messaging* sub-protocol is started with the derived session keys to establish a secure channel, which provides authenticity, integrity and confidentiality.

A.2 eIDAS terminal authentication

1. The eIDAS provider sends a certificate chain to the eIDAS token starting with its authorisation certificate and ending with a certificate signed with the private key which corresponds to the CVCA-eID certificate stored on the eIDAS token.
2. The eIDAS token's chip verifies the signatures of all received certificates, checks their validity periods, and extracts the access rights and public key of the eIDAS provider PK_{PR} from its authorisation certificate.
3. The eIDAS provider generates an ephemeral Diffie-Hellman key pair $\widetilde{PK_{PR}}, \widetilde{SK_{PR}}$ and sends the compressed public key $COMP(\widetilde{PK_{PR}})$to the eIDAS token.
4. Based on PK_{PR} the eIDAS token checks if the eIDAS provider is in possession of the private key SK_{PR} with a simple challenge-response protocol. Therefore the eIDAS token chooses a random challenge r_{TO} and sends it to the eIDAS provider.
5. The eIDAS provider signs r_{TO} and the compressed ephemeral Diffie-Hellman key $COMP(\widetilde{PK_{PR}})$ with its private key SK_{PR} and sends the digital signature $s_{PR} = Sign(SK_{PR}, r_{TO}||COMP(\widetilde{PK_{PR}}))$ back to the eIDAS token.
6. The eIDAS token verifies the signature $Verify(PK_{PR}, s_{PR}, r_{TO}||$ $COMP(\widetilde{PK_{PR}}))$ with PK_{PR}.

A.3 eIDAS chip authentication

1. The eIDAS token sends its static Diffie-Hellman public key PK_{TO} to the eIDAS provider which checks the public key for authenticity via Passive Authentication.
2. The eIDAS service provider sends its ephemeral Diffie-Hellman pubic key $\widetilde{PK^*_{PR}}$ to the eIDAS token.
3. Based on the received public key the eIDAS token computes the compressed public key $COMP(\widetilde{PK^*_{PR}})$ and compares it to the compressed public key $COMP(\widetilde{PK_{PR}})$ received during TA.
4. Next the eIDAS token and the eIDAS provider both compute their shared secret K via the Diffie-Hellman key agreement employing the exchanged public keys $K = KA(SK_{TO}, \widetilde{PK_{PR}}) = KA(\widetilde{SK_{PR}}, PK_{TO})$.
5. The eIDAS token derives session keys $K_{Enc} = KDF_{Enc}(K, r_{TO})$ and $K_{MAC} = KDF_{MAC}(K, r_{TO})$ with K and a random chosen nonce r_{TO}. To prove possession of the private key SK_{TO} the eIDAS token derives an authentication token $T_{TO} = MAC(K_{MAC}, \widetilde{PK_{PR}})$ with the just derived MAC session key K_{MAC} over the eIDAS provider's ephemeral public key $\widetilde{PK_{PR}}$ and sends r_{TO} together with T_{TO} to to eIDAS provider.
6. After receiving the random nonce r_{TO} the eIDAS provider computes the session keys $K_{Enc} = KDF_{Enc}(K, r_{TO})$ and $K_{MAC} = KDF_{MAC}(K, r_{TO})$, and verifies the authentication token $VERIFY(K_{MAC}, T_{TO}, \widetilde{PK_{PR}})$.