Biometric Transaction Authentication Protocol

Daniel Hartung, Christoph Busch
Norwegian Information Security Laboratory (NISlab)
Gjøvik University College
Gjøvik, Norway
{*daniel.hartung, christoph.busch*}*@hig.no*

***Abstract*—The threat of phishing or malicious software (malware)-based attacks is significant and growing, at the same time online banking gets more and more popular. Financial loss may be one of the consequences if credentials get stolen. In many protocols, the transaction information is not secured properly. The proposed *Biometric Transaction Authentication Protocol (BTAP)* is based on the one hand on the Helper Data Scheme for biometric template protection and on the other hand on a trusted biometric transaction device. BTAP provides data- and person authentic transactions since the relevant information in financial online transactions is fused with a secure biometric template from a verified natural person in a way that it is proven to the executing party, that the transaction, as it is received, was in fact initiated and confirmed by an identified natural person.**

***Keywords*-Electronic Payment Scheme; Online Banking; Biometrics; Non-Repudiation**

I. Introduction

An identity fraud can be defined as the exploit of an identity theft or more precisely a theft of an identity attribute with the intent to harm the affected person. The goal of an attacker is in most cases financial gain. The risk of being a victim of such an event has increased dramatically over the last years. The Identity Theft Resource Center (IDTRC) recorded recently a yearly increase of 46%. In the first three weeks of 2010 the IDTRC [1] registered 1,255,092 data records that were exposed whithin the reported breaches in the U.S. (where numbers were made available), not considering exposed encrypted data records. The list covers incidents of credit card misuse, bank account theft and banking defraud. Manipulated card readers, phishing attacks as well as sophisticated social engineering attacks were tracked. One of the reasons of increasing incidents is seen in the more and more widespread usage of online banking. According to the Federal Association of German Banks, the number of online bank accounts in Germany has increased from 15 Million in 2000 to 39 Million in 2008. The amount of online transactions is expected to increase even more within Europe with the implementation of the Single Euro Payments Area (SEPA) transaction initiative. A study of the Federal Association for Information Technology, Telecommunications and New Media (BITKOM) states that seven percent of all internet users above 14 years already experienced finicial loss through viruses, in online auctions or in online banking [2]. The vulnerability of knowledge-based finiancial transaction system became again obvious as hundred of thousand credit cards of German bank customers had to be re-issued after a data theft in a Spanish credit card processor in November 2009. Furthermore a year 2009 report from the German Federal Office for Information Security (BSI) claims that the threat from phishing attacks is still small but incidents related to online banking fraud will increase through the improved and technically mature mechanisms of malware [3]. Viruses and Trojan horses are representatives of malware. This kind of software is spread over various channels on private computers and is able to gather information like financial transactions. Without being noticed, this information can be sent to remote machines. The user will experience dramatical loss, if credentials like bank account numbers, passwords and valid transaction numbers will be used by the operator of the remote machine. The responsible software is often not detectable, since elaborate technologies like self-encryption and mutation make it impossible to match the malware against patterns used by anti-virus programs. On the other hand rootkits are used to infiltrate the whole operation system itself – this malware can hardly be detected with todays methods [4].

In consequence, a reliable transaction protocol is needed that securely links 1) Receiver-Account-Number, 2) Ordered Amount, 3) Sender-Account-Number, 4) Initiator and optionally various additional information like transaction number and time stamp in a reliable manner.

The paper is organized as follows: after introducing to the state of the art in biometric template protection and authentication in online transactions, the proposed protocol will be described in detail covering design objectives, sketching the use scenario, describing the components and their interaction. Furthermore the enrolment and the verification / authentication process are shown followed by a brief discussion of security considerations. The paper concludes after further research directions are identified.

II. State of the Art

The state of the art of the two main building blocks of the proposed protocol – biometric template protection and online authentication approaches – are described in this section.

A. Biometric Template Protection

Biometric systems determine whether the observed biometric characteristic of a subject and the previously recorded representation in the reference data match. In contrary to knowledge or token-based authentication methods a biometric characteristic is bound to a natural person and such the likelihood that a security policy is violated by unauthorized delegation of the authentication factor can be minimized. However the limited number of biometric characteristics for a natural person and privacy regulations do require protection of the biometric data. It is not sufficient to simply encrypt biometric templates with classic cryptographic functions since they can not be compared in the encrypted domain. Furthermore requirements on template protection systems are: **Revocability** – pseudonymous identifiers can be revoked, multiple identifiers can be constructed from the same biometric trait. **Unlinkability** – pseudonymous identifiers cannot be tracked back to the data subject and multiple pseudonymous identifiers of the same data subject cannot be linked against each other. **Removal of additional information** like medical information.

A recent overview of existing biometric template protection systems is given in Breebaart [5]. The described harmonized reference architecture is integrated in the international standard ISO/IEC CD 24745 *Biometric Template Protection* and its nomenclature is used throughout this paper. The Fuzzy Commitment Scheme [6] is one of the systems for template protection, it introduced shielding functions to secure biometric data. An essential building block of our proposed protocol is the Helper Data Scheme (HDS) [7] that uses the principle of fuzzy commitments to privacy protect biometric features and satisfy the above-mentioned requirements.

B. Authentication in Online Transactions

Up to now, many different systems are being used for online transactions that are, depending on the threat assessment, not adequately secure [8].

PIN/TAN – Since 1990 international banks were using two dynamic factor authentication based on personal identification number (PIN) and transaction number (TAN), which are pre-shared secrets between the customer and the bank. A list of a certain number of TANs is in the possession of the customer. To authenticate a transaction, the next valid TAN in the list is used and it gets invalid automatically. A new list can be sent via post. Due to the increasing threat posed through phishing attacks, the PIN/TAN approach is nowadays rarely in use.

PIN/iTAN In response to phishing attacks a new attempt of online transaction authentication, the iTAN, is used since 2006. It is based on the PIN/TAN approach, but in contrast it uses indexed TANs. For a certain transaction a TAN with a specific index is requested from the customer, therefore iTAN. Still, phishing is not prevented. If malware is on the customers computer, a man-in-the-middle attack is possible and the transaction can be manipulated (rerouting to a new beneficiary).

Mobile TAN (mTAN) This concept introduces a second channel towards the banking customer, through which relevant transaction data is sent. The channel is realized as a *Short Message Service* (SMS) towards the customers mobile phone. In this way the receiver is able to check the integrity of the transaction through visual comparison and is furthermore able to confirm the transaction with a one time password (mTAN) that was also sent within the SMS. The mTAN has a limited validity and needs to be typed into the online banking software. Compared to the TAN and iTAN method mTAN is considered to be more secure. Man-in-the-middle attacks that intend to re-route the transaction fail. The mTAN-method requires a trusted platform (mobile phone) that can not be manipulated at the same time as the client computer of the customer. The method met with criticism because SMS messages can be traced [9]. During the next years the line between mobiles and web clients is blurring more and more, with the consequence of loosing this independent communication channel.

TAN Generators – Mobile tokens are used as TAN generators that produce sequentially new TANs. Some tokens like the RSA-token work on a timer basis. The different approaches are described below. **sm@rt-TAN** – a TAN can be generated if the banking card with chip and EMV TAN generator is inserted into the token. This approach is vulnerable to phishing and transaction monitoring through malware. **eTAN generator** – TANs are generated with the time and receiver bank account number as parameters. As the receiver number has to be typed into the token the approach is less convenient for customers but it is phishing proof. **chipTAN manual** – the banking cards needs to be inserted in order to generate a TAN. The transaction data (receiver account number, ordered amount) that needs to be secured has to be typed manually into the token. The device computes a transaction specific TAN. The approach results in a high level of security but also in inconvenience for the customer. **chipTAN comfort** – extension of the before mentioned approach. The transaction data is read through optical sensors into the generator. Furthermore the token is able to display the transaction data. With the activation of the generator the customer confirms the transaction. An assumption is that man-in-the-middle attacks are not possible because a generated TAN is only valid for one transaction. One comfort features make this assumption invalid: collective transfers are possible. In this case the receiver account number is not displayed by the device any more, which allow attacks that – assuming carelessness of a customer – can also effect single transactions. This online protocol and the interface to the used *Hand Held Device* (HHD) are standardized through the German Central Credit Committee (ZKA) as *HHD 1.3.2 with optical interface*.

photo TAN – *photoTAN* equates to the HHD 1.3.2 standard with optical interface, even though the transaction data is displayed as a two dimensional bar code from the banking server and captured with the mobile phone of the bank customer.

Digital Signature / HBCI – Digital signatures can also be used for online banking authentication. Its application was standardized with the *Home Banking Computer Interface* (HBCI) that was developed since 1996 from several German banking groups and standardized through the ZKA. This interface supports chip card based online transaction protocols. The protocol was further developed by the ZKA under *Financial Transaction Services* (FinTS) [10]. HBCI / FinTS render TAN lists unnecessary with a security assessed chip card and reader in the possession of the customer. HBCI establishes a secure tunnel from the client computer to the banking server and uses a public key infrastructure to digitally sign the transaction data with the private keys of the customer (signing key pair). This key pair is stored securely inside the chip card. The transaction data with the signature is then send to the banking server. As with all signature based approaches, also the HBCI suffers from the modification of the transaction data before the signature is done. The deployment of secure signature units can minimize this risk. A manipulation could never the less been performed by malware on the client computer before the signature is done by the chip card. The assumption that the client computers are malware free is not firm, in fact it is very improbably. Online banking based on digital signatures therefore requires a secure visualization concept for the transaction data that should be signed, as implemented in the *Secoder*.

Online-Banking with USB-Token – A token-based approach is followed by KOBIL with the *mIDentity*-USB-token, where the URL of the banking server is cast in hardware to avoid rerouting to an attacker URL. In addition secure communication channels can be established. One drawback: authentication against the stick is based on on knowledge (PIN) typed into a (probably) insecure client program. Another provider for USB-token-based transaction security is Novosec: here not the communication itself is secured but the approach is based on digital signatures of the transaction data. Weigold et al. presented the *Zurich Trusted Information Channel (ZTIC)*, which is especially designed for insecure environments like malware-infected client computers [9]. The token establishes a secure connection to the banking server and displays the received transaction information, which can be accepted or denied on this dedicated piece of hardware.

III. Biometric Transaction Authentication Protocol

This section describes the proposed *Biometric Transaction Authentication Protocol* in detail. The abstract pipeline of the Helper Data Scheme (HDS) as a building block and the BTAP are sketched in Figure 3. The acronyms are described in Table II.

A. Design Objectives

We designed a new protocol, which addresses the two main requirements for online banking transactions. **Reliable Person Authentication**: the enrolled banking customer and only this natural person has initiated and confirmed the transaction. Repudiation of de facto executed transactions should be impossible. **Reliable Data Authentication**: The enrolled banking customer has checked the transaction within a trustworthy environment and confirmed the data with the supported biometric modality. The authentication data is send via a second autonomous and secure channel to a banking server.

B. Assumptions

The scenario in which the BTAP might be used can be described as follows: on a potentially insecure and malware infected client computer an Online Banking Software (BSW) is running, which communicates with a secure Online Banking Server (OBS). The BSW transmits the transaction data to the OBS and to a secure dedicated token, the Biometric Transaction Device (BTD). On the BTD the transaction is confirmed through the customer, a seal is created over the transaction data (the Transaction Order Seal (TOS)), which fuses the transaction data with the biometric data of the customer. The threat scenario for the BTAP is illustrated in Figure 1.

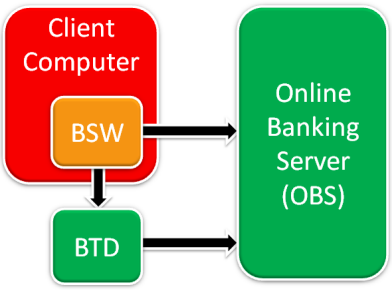


Figure 1. Sketch of threat scenario for the BTAP components. Green: trustworthy, tamper-proof (OBS, BTD); red/orange: probably insecure, malware infected (BSW)

The following list identifies components that are interacting for secure online transactions (Figures 4 / 5) and outlines their individual properties:

- **Secure Online Banking Server (OBS)**: has access to customer data; establishes communication with the Online Banking Software (BSW); conducts capital transactions; is able to identify a Biometric Trusted Device (BTD) as communication partner and preferably establishes a secure connection.

- **Online Banking Software (BSW) on insecure client computer**: executed on client computer that is threatened by Trojan horses, root kits, etc.; implemented as client software or browser based application; communicates with OBS and transfers transaction data as Transaction Order Records (TOR); TOR consist of: Transaction Identifier (TID), Sender Account Number (SAN), Receiver Account Number (RAN) and Ordered Amount (ORA); connected to the client computer is a trusted Biometric Transaction Device (BTD)
- **Secure Biometric Transaction Device (BTD)**: trusted piece of hardware, ideally with assessed security (e.g., common criteria), minimal and provable secure functionality; cannot be manipulated by malware; captures a biometric modality through Biometric Capture Device (BCD) as a fake resistant sensor, which is qualified for unsupervised operation in home and office environments; is able to connect to an Online Banking Server (OBS); is able to receive a TOR and visualize it on the trusted display (elements of a TOR are TID, SAN, RAN and ORA).

C. Enrolment Protocol

The enrolment process for the Biometric Transaction Authentication Protocol (BTAP) is sketched in Figure 4. The enrolment process of the Helper Data System (HDS) is modified for BTAP – the necessary steps are the following (executed operations are highlighted in *italic*, numbers in brackets indicate the time of execution and refer also to Figure 4):

1) Enrolment on the Online Banking Server (OBS):

- Generate shared Secret SBV, send it to customer(secure mail)/BTD(secure connection) (1)
- Create user record with: Account Number (AN) and Pseudo Identifier PI $= h(\mathrm{SBV})$, which is derived from preshared secret SBV (2)

2) Enrolment steps inside the Biometric Transaction Device (BTD):

- Data subject (i.e., bank customer) presents the biometric characteristic (3)
- Capture multiple biometric (enrolment) samples (4)
- Extract real number reference feature vectors RRV (5)
- Binarize biometetric features into quantized form QBV (6)
- Derive Auxiliary Data 1 (AD1) from biometric samples in the Reliable Bit Selector (RBS) block (7)
- Keep Robust Binarized Feature Vector RBV extracted from enrolment samples and AD1 (7)
- Insert shared Secret Bit Vector (SBV), e.g., sent via secure mail and typed in (8)
- Calculate Codebook Vector (CBV): CBV $=$ *ENC*(SBV) (9) (e.g., using an error correction code like BCH)
- Calculate Auxiliary Data 2 (AD2) from CBV and RBV: AD2 $=$ CBV *XOR* RBV (10)
- Store non-sensitive data AD1 and AD2 into BTD or on personal chip card (11)

D. Transaction Authentication Protocol

To confirm an online transaction initiated by a bank customer, the Biometric Transaction Authentication Protocol (BTAP) extends the authentication with a biometric verification system. This protocol therefore follows a new approach, where a Transaction Order Seal (TOS) is computed locally and is sent instead of a TAN (sketched in Figure 5). The exchanged messages are sketched in Figure 2.

1) Operations executed by the insecure Online Banking Software (BSW):

- Creates through interaction with banking customer a Transaction Order Record (TOR), that contains: Transaction Identifier (TID), Sender Account Number (SAN), Receiver Account Number (RAN) and Ordered Amount (ORA)
  $\mathrm{TOR} = (\mathrm{TID}, \mathrm{SAN}, \mathrm{RAN}, \mathrm{ORA})$ (1)
- Transmits TOR to Online Banking Server (OBS) (2)
- Transmits TOR to Biometric Transaction Device (BTD), which is connected to client computer (3)

2) Operations executed within the Biometric Transaction Device (BTD):

- Displays relevant information from TOR (at least RAN, ORA) on trusted display (4)
- Initiator and banking customer presents unforgeable biometric characteristic to the Biometric Capture Device (BCD) (5) for the transaction confirmation, that is further on processed as the probe sample image (6)
- Extract features from probe (7)
- Binarize features (8)
- Load Auxiliary Data AD1 from BTD memory or smart card (9)
- Compute binarized probe vector XBV from probe sample and AD1 (9)
- Compute codebook vector CBV' from stored Auxiliary Data 2 (AD2) and XBV: $\mathrm{CBV}' = \mathrm{AD2}$ *XOR* XBV (10)
- Decode CBV' into SBV': $\mathrm{SBV}' = \mathit{DEC}(\mathrm{CBV}')$ (11)
- Compute Pseudo Identifier (PI') from SBV': $\mathrm{PI}' = h(\mathrm{SBV}')$ (12)
- Compute Transaction Order Seal (TOS') from Transaction Order Record and reconstructed PI': $\mathrm{TOS}' = \mathit{MAC}(h(\mathrm{TOR}), \mathrm{PI}')$ (13)
- Transmit Transaction Order Seal (TOS') to Online Banking Server (13)

3) Operations executed on the Online Banking Server (OBS):

- Received the Transaction Order Record (TOR) from the Online Banking Software (BSW) (2)
- Received also the Transaction Order Seal (TOS') from the Biometric Transaction Device (BTD) (13)

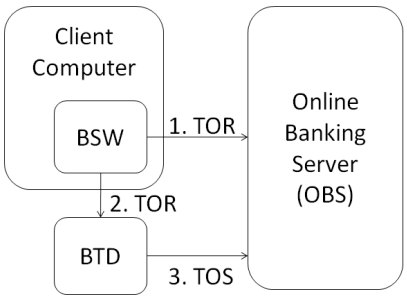


Figure 2. Arrows indicate messages exchanged between the different entities. Transaction Order Record TOR $=$ (TID, SAN, RAN, ORA), Transaction Order Seal TOS $= MAC(h(\text{TOR}), \text{PI})$

- Hash the received TOR (14)
- Load stored Pseudo Identifier (PI) in the database for the customer (PI $= h(\text{SBV})$) (15)
- Reconstructs TOS: TOS $= MAC(h(\text{TOR}), \text{PI})$ (15)
- Compares TOS with the received TOS' from the BTD: TOS $==$ TOS$'$ (16)

The transaction is person and data authentic if, and only if, TOS and TOS' are identical. In this case the transaction, encoded into the Transaction Order Record (TOR), is considered authentic and confirmed and thus the order will be conducted by the OBS. The various steps of the protocol that are executed in the BTD and on the OBS to confirm a transaction and to validate the authenticity of the data and the initiator are sketched in Figure 5. The BTAP Protocol operates on a minimal number of message that are transferred between the components as illustrated in Fig. 2.

E. Security Considerations

The proposed BTA-protocol is based on the Helper Data Scheme for Template Protection and on generic standard cryptographic primitives. The following primitives are used: Hash Function, Message Authentication Code, Error Correction Code and the XOR-operation used as a Vernam pad (where the key and the message are of the same length). The Biometric Transaction Device (BTD) is considered to be a tamper-proof trusted environment that cannot be modified nor eavesdropped. Assuming a secure enrolment process the following attacks aiming at gaining control over the transactions are identified according to the pipeline of BTAP and the exchanged messages (Figures 2 / 3(b)).

1) Attacks on the Helper Data Scheme (HDS): The Helper Data Scheme is not leaking information about the secret nor the biometric features if the biometric information can be modeled as independent and identically-distributed (i.i.d.) random variables [7]. Further research on the security of template protective systems can be found in Ignatenko *et al.* [11] and Zhou *et al.* [12]. The main requirements of the HDS are in fact requirements on the entropy of the underlying biometric system.

2) Modification of Transaction Data: The transaction data encoded in the Transaction Order Records (TOR) can easily be modified inside the potentially insecure client computer. There are two possibilities how to proceed an attack if the transaction data (e.g., the Receiver Account Number (RAN) and the Ordered Receiver Amount (ORA)) has been modified by malware.

The first approach is modifying the data that is sent to the Online Banking Server (OBS) and to the Biometric Transaction Device (BTD) in the same way. This attack focuses on the human factor, since the initiator of the transaction has to check and confirm the transaction data that is displayed on the trusted display of the BTD. If the transaction is confirmed the attacker succeeded.

The second approach attacks the protocol itself. The transaction data forwarded to the BTD is not changed but the data sent to the OBS is modified. In this scenario the initiator would confirm the intended transaction. The comparison on the server site would result in a negative authentication if the Transaction Order Seals (TOS and TOS') are not equal. The TOR sent to the BTD could be constructed by choice. Assuming that a transaction initiated and authenticated by the customer will always be positively authenticated by the system, the secret SBV has to be error free when inputted to the MAC block. What follows directly: h(TOR) has to be the same on both sides, in the BTD as well as in the OBS. A construction attack on TOR turns out to be an attack on the full hash space (assuming the MAC block is secure, completely random guesses for the TOS' have to be made that could fit the chosen TOR). By replacing the hash function the protocol would still be secure.

3) Replay Attacks: Since the Transaction Identifier (TID) is included within the transaction information, which is hashed afterwards, a replay attack cannot succeed. A modification of the TOR results in a different hash value h(TOR) and therefore the value of the Transaction Order Seal (TOS) results in a not foreseeable different value.

4) Attack on the Transaction Order Seal (TOS): If the independent and preferably secure channel between the BTD and the OBS is broken or an attacker gets hold of the communication between the parties (Man-in-the-Middle Attack), the Transaction Order Seal (TOS) can be attacked, since there is the possibility to extract information about the Pseudo Identifier (PI) from the TOS. The TOS is the result of a Message Authentication Code (MAC) that is applied with the hash value of TOR as message and the Pseudo Identifier (PI) as key. If the MAC is broken, PI could be extracted. In this scenario the security of the TOS depends on the MAC, which has to be exchanged if broken.

Another approach would be a brute force attack on the key (PI) when TOS and TOR are known to an attacker. To solve this issue the size of the key has to be sufficiently large to make this attack too expensive considering the computational effort.

Attack	Authentication Method TAN	iTAN	mTAN	Electr. Signature	Security Token	BTAP
Password Phishing	1	1	0	0	0	0
Visual Spoofing	1	1	0	1	0	0
Malware	1	1	1	1	0	0
Man-in-the-Middle	1	1	1	0	0	0
Denial of Service	1	1	1	1	1	1
Human Factor	1	1	1	1	1	1
Delegation / Repudiation	1	1	1	1	1	0

Table I
VULNERABILITY OF AUTHENTICATION METHODS (STRONGEST REPRESENTATIVE) IN ONLINE BANKING BASED ON THREATS AS CATEGORIZED IN [8].

Assuming the BTD to be powerful enough to perform asymmetric cryptography, TOS can be encrypted with the public key of the OBS to secure the link.

5) Limitations and Attacks on Biometric Subsystem: Limitations and potential attacks on the biometric subsystem need to be considered, as this is an essential component in the BTAP:

- Imposter Authentication – an attacker could try to authenticate a transaction, this would refer to an attack on the biometric system in combination with the Helper Data Scheme (HDS). If the reliable bit vector (XBV) consists of equally distributed bits (over the population and inside each feature vector) and the RNG block generates also equally distributed secrets, the chances of having the same two reliable bit vectors from two different data subjects depends on the length of the XRV. The next points resumes this issue.
- Limited biometric performance – it has to be clearly stated that the error correction capability should be chosen as small as possible to add as less as possible redundancy to the secret. This is in fact a challenge of the underlying biometric system, the feature extraction has to be accurate in order to render the need for error correction unnecessary.
- Aging and Changes in the biometric characteristic – the biometric modality should be chosen in a way that aging can be neglected and that changes in the characteristic can be handled by the feature extraction. In the worst case the biometric characteristic has to be re-enrolled.
- Attacks on the Biometric Capture Device – the sensor - as part of the BTD - is considered to be trusted, non-attackable and also qualified for unsupervised biometric verification.
- Hill Climbing – cannot be conducted since the output of the system is not a comparison score but a binary decision.

6) Attacks on Privacy:

- If TOR can be read by an attacker, transactions can be tracked. This could happen through malware on the client computer or weak links between either the BSW and the OBS or between the BSW and the BTD.
- Cross-Matching attacks cannot succeed if different Pseudonymous Identifiers (PI) are used in different application scenarios. To achieve this, different secrets have to be created and merged with the biometric information.
- Biometric Additional Information cannot be extracted if the BTD is secure and the used Helper Data Scheme for privacy protection is not broken.

7) The Human Factor: As mentioned earlier the system can only operate in a secure manner, if the human factor is not exploited. A risk that could be foreseen is that to much information (e.g., long IBAN numbers) is displayed to the natural person. In such a case the likelihood that the subject approves that information without carefully comparing displayed information to the intended information is high (this happens widely, when users accept ”blindly” software license conditions). This risk of information overflow is in no way specific to the BTA-protocol.

A comparison of BTAP with standard approaches for transaction authentication is shown in Table I indicating that BTAP show robustness against more attacks than current alternative protocols.

As long as the building blocks of the Biometric Transaction Authentication Protocol are not broken, the protocol is secure against various attacks. The modular design provides the possibility to exchange most of the cryptographic primitives with limited effort in the case of an incident. The knowledge about the correct implementation of the system is a root of trust. Thus in order to increase trust of operators and users in the system, components and desirably the whole system should be subject to Common Criteria security analysis and its trustworthiness should be certified by an independent institution.

IV. FUTURE WORK

The proposed protocol for transaction authentication can be used also in a more general context, since the biometric information can be fused with any kind of information. The resulting biometric signature system can be used in various applications. A future extension will handle multiple person transaction authentication to reach a higher level of

security e.g., confirm transaction of large volumes in the cooperate and inter-banking sector or to satisfy regulations like the four-eyes principle. The BTAP can be hardened using multi-factor authentication adding also knowledge and/or possession factors.

From the biometrics perspective further research has to focus on unsupervised biometric capture devices that generate biometric samples with sufficient entropy to make the proposed protocol strong against brute force attacks on the secret.

An interesting aspect is also the concrete implementation using existing technologies and products available on the market to realize the BTAP.

From an economic point of view the question has to be solved if the return of investment is guaranteed with the usage of the BTAP and the BTD. Considering not only that BTAP would prevent online transaction frauds but also the fact that the quantity of incidents is increasing rapidly one could assume that the investment is amortized after a rather short time span depending on the costs of the device and changes in the infrastructure.

A more formal security analysis is needed in order to prove the properties of the protocol – it is in preparation.

V. Conclusions

The proposed Biometric Transaction Authentication Protocol solves a basic problem of nowadays online banking: how to realize a person and transaction data authentic protocol in a potentially insecure environment. Furthermore the requirement to use biometrics in online banking scenarios to reach a binding of the biometric trait with the intended transaction data, is fulfilled in BTAP. At the same time the biometric information is sealed in a privacy preserving way and cannot be extracted by any party. BTAP offers two important features of a security protocol: low complexity and strong modularization.

References

[1] Identity Theft Resource Center, "2009 ITRC Breach Report," http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml, Feb. 2010.

[2] Branchenverband BITKOM, "Fast 4 Millionen Opfer von Computer- und Internet-Kriminalität," http://www.bitkom.org/de/presse/56204_53100.aspx, Jul. 2008.

[3] Bundesamt für Sicherheit in der Informationstechnik, "Die Lage der IT-Sicherheit in Deutschland 2009," https://www.bsi.bund.de/cae/servlet/contentblob/476182/publicationFile/30725/Lagebericht2009_pdf.pdf, Jan. 2009.

[4] J. Rutkowska, "Introducing Stealth Malware Taxonomy," http://www.invisiblethings.org/papers/malware-taxonomy.pdf, Nov. 2006.

[5] J. Breebaart, C. Busch, J. Grave, and E. Kindt, "A reference architecture for biometric template protection based on pseudo identities," in *BIOSIG*, 2008, pp. 25–38.

[6] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.

[7] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *Biometric Authentication*, ser. Lecture Notes in Computer Science, vol. 3087. Springer Berlin / Heidelberg, 2004, pp. 158–170. [Online]. Available: http://www.springerlink.com/content/9d4287d5hq0311mt/

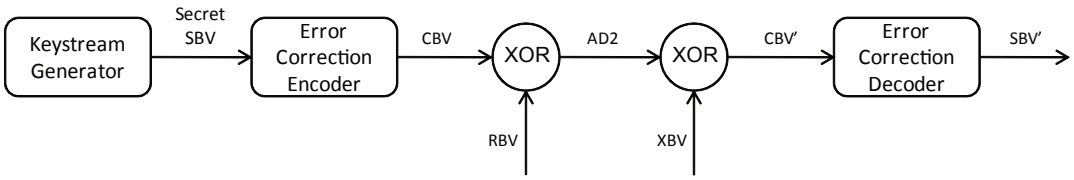
[8] A-SIT: Secure Information Technology Center Austria, Österreichische Nationalbank, "Risikoanalyse - E-Banking Angebote österreichischer Kreditinstitute," May 2008.

[9] T. Weigold, T. Kramp, R. Hermann, F. Höring, P. Buhler, and M. Baentsch, "The zurich trusted information channel — an efficient defence against man-in-the-middle and malicious software attacks," in *Trust '08: Proceedings of the 1st international conference on Trusted Computing and Trust in Information Technologies*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 75–91.

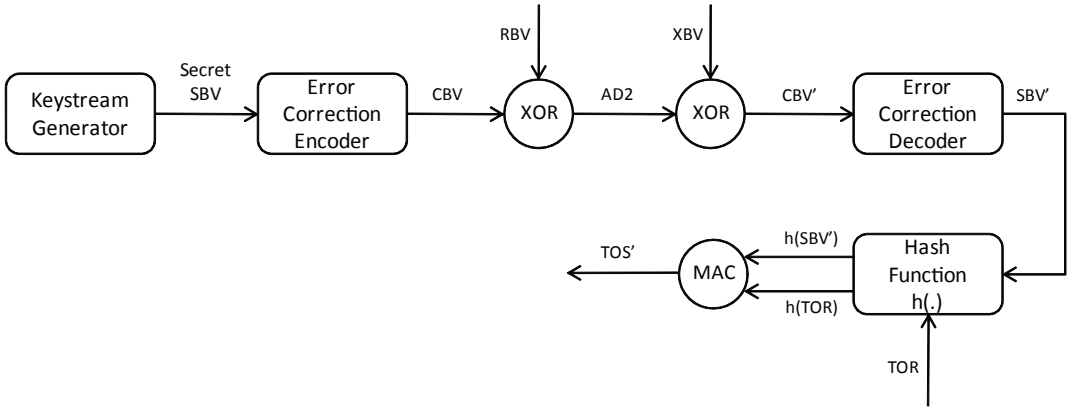
[10] Zentraler Kreditausschuss (ZKA), "Financial Transactions Services (FinTS)," http://www.hbci-zka.de/, Feb. 2010.

[11] W. F. Ignatenko, T., "Biometric systems: Privacy and secrecy aspects," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 4, pp. 956 –973, Dec. 2009.

[12] X. Zhou, S. D. Wolthusen, C. Busch, and A. Kuijper, "A security analysis of biometric template protection schemes," in *Image Analysis and Recognition*, ser. Lecture Notes in Computer Science, vol. 5627. Springer Berlin / Heidelberg, 2009, pp. 429–438. [Online]. Available: http://www.springerlink.com/content/687662382j240634/



(a) Building block HDS. Input: RBV/XBV (robust reference/probe bit vectors of the biometric subsystem for enrolment/verification), Output: SBV'



(b) BTAP. Input: RBV/XBV, TOR (Transaction Order Record); Output: TOS' (Transaction Order Seal).

Figure 3. Abstract pipelines of the Helper Data Scheme (HDS) and the Biometric Transaction Authentication Protocol (BTAP).

Name	Description
AD1	Auxiliary Data 1: Reliable Bit Indexes from RBS block
AD2	Auxiliary Data 2: AD2 = CBV *XOR* RBV
AN	Account Number
BCD	Biometric Capture Device
BSW	Online Banking Software
BTAP	Biometric Transaction Authentication Protocol
BTD	Biometric Transaction Device
CBV	Codebook Vector: CBV = $ENC(\text{SBV})$
ENC	Error Correction Encoding Block
DEC	Error Correction Decoding Block
HDS	Helper Data Scheme
OBS	Online Banking Server
ORA	Ordered Amount
PI	Pseudo Identifier: PI = $h(\text{SBV})$
QBV	Quantized Binary Vector
RAN	Receiver Account Number
RBV	Robust binarized feature vector from enrolment process (derived from QBV at positions AD1)
RBS	Reliable Bit Selector block (identifies stable positions in feature vectors)
SAN	Sender Account Number
SBV	Preshared Secret (Binary Vector)
TID	Transaction Identifier
TOR	Transaction Order Record: TOR = $(\text{TID}, \text{SAN}, \text{RAN}, \text{ORA})$
TOS	Transaction Order Seal: TOS = $MAC(h(\text{TOR}), \text{PI}) = MAC(h(\text{TID, SAN, RAN, ORA}), h(\text{SBV}))$
XBV	Robust binarized probe vector for the verification process: XBV = RBV'

Table II
ACRONYMS OF THE USED VARIABLES AND COMPONENTS IN BTAP.

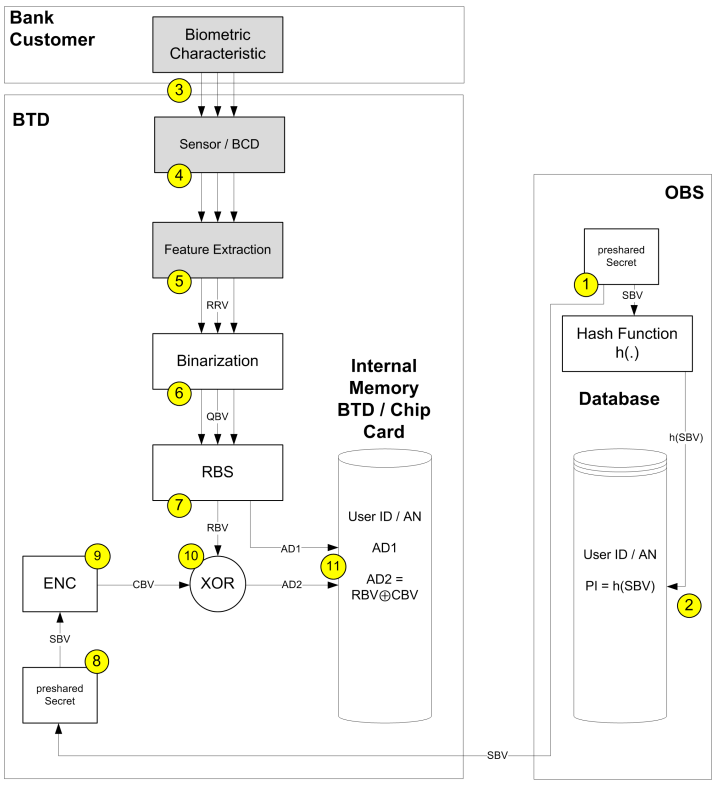


Figure 4. Process flow of the enrolment protocol

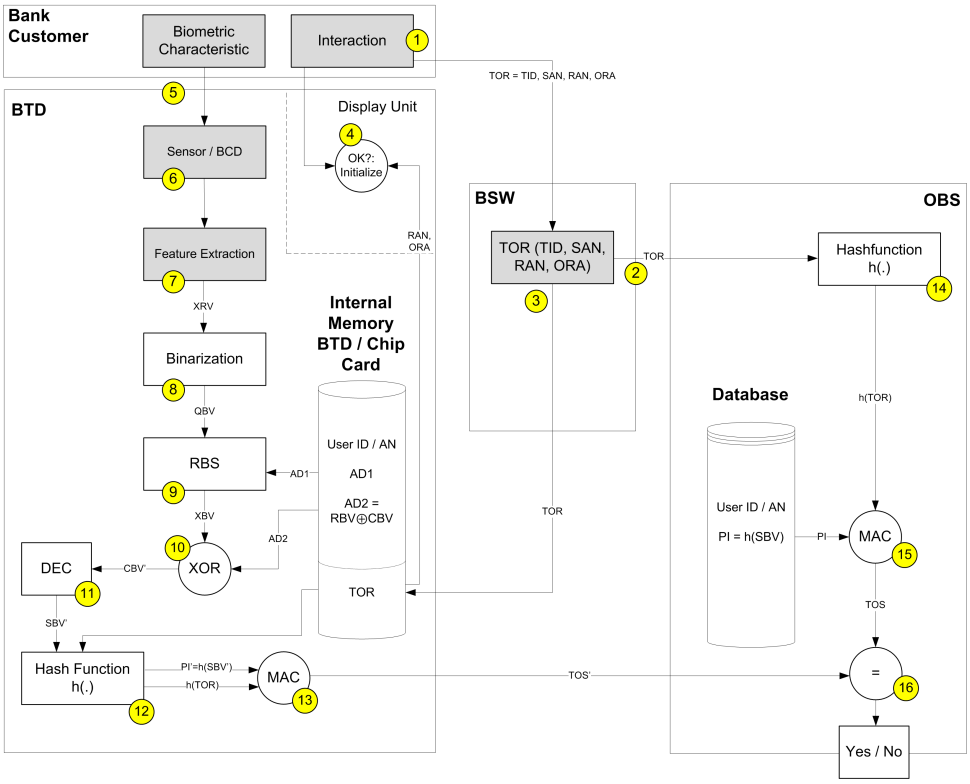


Figure 5. Process flow of the transaction verification protocol