Digitized Handwritten Signatures replacing PIN/TAN

PIN/TAN AS AUTHENTICATION PROCEDURE FOR ONLINE BANKING HAS CERTAIN LOOPHOLES. THUS, WE HAVE DESIGNED AND IMPLEMENTED A SYSTEM THAT USES THE DIGITIZED HANDWRITTEN SIGNATURE AS AUTHENTICATION METHOD TO OVERCOME THOSE PROBLEMS.

NICOLAS REPP
OLIVER HECKMANN
RAINER BERBNER
RALF STEINMETZ

Introduction

Nowadays, online banking is widespread in Germany. According to the Deutscher Sparkassen- und Giroverband (2004) there were about 35 million online banking accounts in Germany in late 2004. But approximately only 1/3 of the online banking accounts are frequently used by their owners as reported by Hardock and Wübker (2002).

Key reasons not to use existing online banking accounts are often security concerns of the respective account owners. Those concerns are strengthened by the incidents with regard to security reported by the press over the last year. Spoofing, phishing, and Trojan horses are possible attack patterns used by fraudsters with regard to online banking.

This article gives an overview about the approaches for authentication and authorization used in current online banking systems. Furthermore it investigates a user friendly alternative to existing approaches based on digitized handwritten signatures.

The use of digitized handwritten signatures in a prototype including its unique biometric characteristics as authentication tool for login to online banking applications and proof of intent for an online transaction is shown thereafter.

The prototype is a result of the cooperation between E-Finance Lab Cluster 2, the Multimedia Communications Lab of Technische Universität Darmstadt and Softpro, a leading manufacturer of software for biometric signature handling.

The remainder of this article is organized as follows: in the next section we give an overview about different authentication and authorization approaches that can be used in online banking scenarios. Furthermore security issues of the approaches used today are discussed. The prototype, which is using digitized handwritten signatures for online banking, is described in the following section. The article closes with an outlook on future research issues and practical applications.

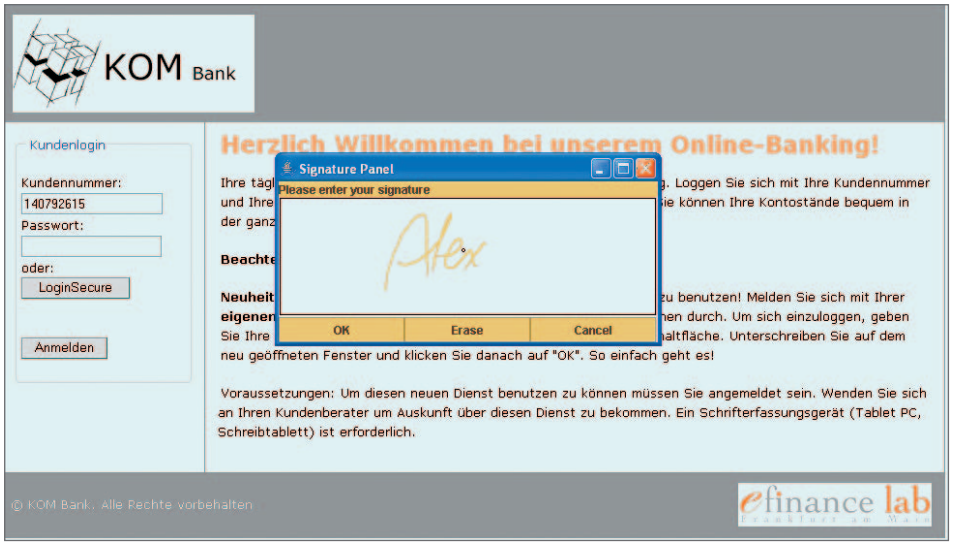

Figure 1: Login to Online Banking using a Handwritten Signature.

Authentication and Authorization for Online Banking

In this section, we describe the most important approaches used to implement authentication and authorization in current online banking. Our focus is hereby on approaches used by banks and other financial institutions in Germany.

PIN/TAN

The most commonly used system for authentication of a user and authorization of transactions is the so-called PIN/TAN approach. Personal Identification Numbers (PIN) and Transaction Numbers (TAN) enable online banking without the use of dedicated hardware. A client needs his user ID (e.g. account number) in combination with his secret PIN to login to the online banking system of his bank. To authorize a transaction the client further needs to enter an arbitrary TAN from his TAN sheet which only can be used for a single transaction and gets invalid thereafter. The PIN/TAN approach has certain loopholes. Its security relies on the client's ability to remember his PIN code and to securely store his TAN sheet. PINs and TANs are subject to phishing attacks and forgotten access codes are causing additional helpdesk efforts.

In order to overcome the problems resulting out of the PIN/TAN approach different enhancements were developed. The most popular is the indexed TAN (iTAN) approach. Instead of accepting an arbitrary TAN from the TAN sheet the online banking system asks for a dedicated TAN reducing the risk of

authorizing a transaction with only a few TANs stolen.

A hardware based TAN enhancement is the electronic TAN (eTAN). A hardware token creates a valid TAN on basis of a control number issued by the online banking system during a transaction. The token has to be paid by the client in most cases.

An enhancement of traditional PIN/TAN, which is used by some banks in Germany, is the mobile TAN (mTAN) approach. A client has to escrow his mobile number in the banking system. In case a transaction is started in the online banking system the systems sends a valid TAN as a short message (SMS) to the client. The TAN is only valid for the transaction started.

HBCI

As an alternative to PIN/TAN, the Home Banking Computer Interface (HBCI) can be used. HBCI is based on asymmetric encryption methods thus using public and private key encryption for transactions and authentication purposes. Usually the keys are stored on smartcards only accessible using a dedicated card reader. The private key can be unlocked only with a PIN.

HBCI is only protected against fraudsters using Trojan horses if the PIN to unlock the private key is entered directly on the card reader using a pin pad. But similar to the eTAN approach the dedicated hardware has to be bought by the client in most cases.

Both PIN/TAN and HBCI are integrated in the Financial Transaction Services Framework (FinTS) of the Zentraler Kreditausschuss (ZKA).

Digitized Handwritten Signatures

Often neglected is an obvious method for authentication and authorization. Every client knows the process of signing important documents in order to actively agree to its content. Furthermore almost every client is aware not to sign off a document without checking it before.

Using signature capturing devices as for example integrated in a Tablet PC or in form of specialized hardware (Figure 2 – http://www.signplus.com/de/press/gallery/), it is possible to use handwritten signatures in various electronic processes.

Other types of authentication and authorization based on biometrical features are not

Figure 2: Capturing of Handwritten Signatures using a Pen Pad.

widely accepted in the financial community for application in processes with client interaction. The application of those methods is hard to explain to clients and needs a massive effort to implement and roll out. On client side there often exist concerns with regard to the security of the biometrical features and to privacy.

The handwritten signature has an exceptional position under all biometrical methods because it uses one of the few biometrical features that can only be captured if the client agrees to. In contrast to the capturing of e.g. retina patterns or finger prints, which is completely passive and can be accomplished without explicit approval of a person, signing always is an active process.

The handwritten signature has further advantages. It is hardly possible to forget your own handwritten signature. Furthermore theft of a handwritten signature with all its biometrical features is a complex task because of the dedicated hardware needed for that process. For example it is not possible to use the data captured by a parcel service on a signature pad for online banking fraud because the pad is not able to capture enough features of the handwritten signature.

A handwritten signature consists of static and dynamic features as described by Schmidt (1999) and van Gemmert et. al. (1996). Part of those features is for example the image of the signature, the acceleration or the pressure measured during the signing process. After initially capturing the features they are saved as a reference.

A single handwritten signature consists of several strokes. The start- and endpoints of those strokes are static features of every signature with unique characteristics. They can be extracted from a single signature or by comparison of several signatures. Analyzing the dynamical features of a handwritten signature it can be assured that a signature given is not only identical to its reference by its image but was also really created by the person the reference belongs to.

Financial institutions can reach a higher acceptance by their clients as signing a document is a well known process and not as abstract as PIN/TAN or HBCI. Furthermore the usage of a handwritten signature will improve the usability for the client.

Prototypical Implementation

The prototype we have developed is currently used to evaluate the potentials of such a solution with possible users.

After accessing the web portal of our online bank the user gets access to a typical login screen implemented and used in several real world online banks.

The user now can enter his account number as user-ID. Furthermore he has to enter a PIN (using PIN/TAN approach) or to sign a specia-

lized form which opens after pressing a dedicated button („LoginSecure“), as depicted in Figure 1. In our prototype, the signature is captured using a Tablet PC but any other signature capturing device can be used instead (e.g. a pen pad connected to standard PC).

After the successful capturing of a handwritten signature and its comparison to the reference stored the user gets access to a page containing an overview of all possible transactions. Same goes for the successful authentication of the user by PIN. Our prototype currently supports the following transactions:

- Check of balance for account and credit card
- Create and submit bank transfers
- Change personal information.

All transactions with need for authentication can additionally use the digitized handwritten signature.

There are two different approaches for the creation of bank transfers that can be used in our prototype. The first method is identical to the approach used in all current online banking systems. A user can fill out a bank transfer form using the keyboard. The second method allows filling out a bank transfer form using handwriting recognition and a capturing device.
After filling out the bank transfer form the user is led to a page showing all data inserted in the form before. No matter which method the user chose to fill out the form he can decide to use TAN or digitized handwritten signatures for authentication thereafter. In case handwritten signatures are used a special form will be shown in which the user can enter his signature. The captured signature is analyzed thereafter and compared to the reference stored in the online banking system. If the comparison was successful the bank transfer will be authorized and submitted to the backend banking system.
Changing of personal information is done in the same fashion.

Practical Applications and Outlook

Digitized handwritten signatures can be used in almost every channel of a bank that needs authentication and authorization. For example, it is possible to apply signature capturing and digitized handwritten signature processing to front-office processes like the account opening process. Furthermore, the integration of different channels of a financial institution organized as a multi channel institution can be realized using digitized handwritten signatures. The integration would be implemented in form of a consistent system for authentication and authorization shared by different channels as depicted in Figure 3. A signature captured during the account opening process using a capturing device (e.g. Tablet PC of clerk) could be used for self service terminals, at the point of sale or in the online banking. Additionally the account opening form would not have to be scanned after the signing because it is already in digital form.

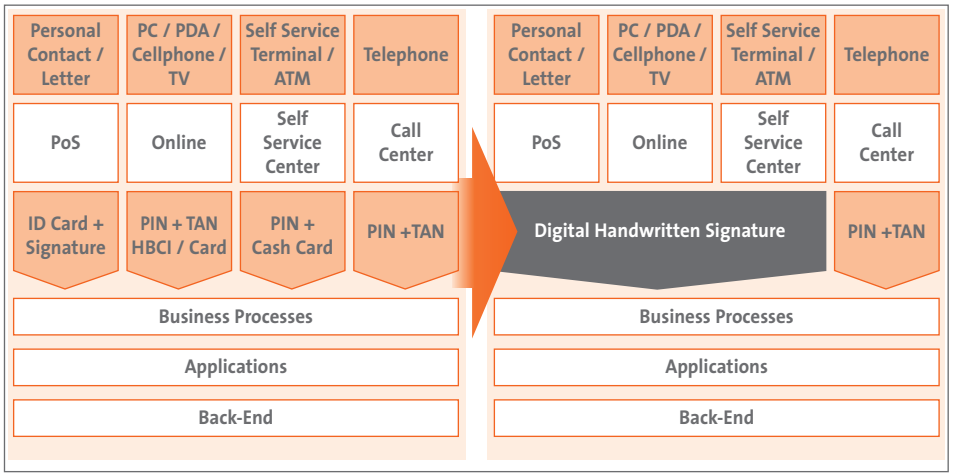

Figure 3: Multi Channel Integration using Digitized Handwritten Signatures

Results of such integration could be:

- Reduction of costs for administration of user authentication and transaction authorization
- Reduction of media discontinuities generating faster and error resilient processes
- Enhancing flexibility of processes
- Improved usability for clients
- Higher acceptance on client side
- Enhanced security on base of in-creased user awareness

In the future it is planned to evaluate the application of digitized handwritten signatures in various scenarios with our partners of the E-Finance Lab.

References

Deutscher Sparkassen- und Giroverband
“Sparkassen-Finanzgruppe führt fast jedes zweite Online-Konto in Deutschland”, press release, 7/2004.

Hardock, P. and Wübker, G.
“Online Banking: Weit verbreitet, doch kaum genutzt?”, Die Bank, 6/2002, pp 376.

Schmidt, C.
“Online Unterschriftenanalyse zur Benutzerverifikation”, PhD Thesis, RWTH Aachen, 1999.

van Gemmert, A., van Galen, G., and Hardy, H.
“Dynamical features of disguised handwriting”, Proceedings 5th European Conference for Police and Handwriting Experts, The Hague, Netherlands, 1996.