SYMBOLON—A NOVEL CONCEPT FOR SECURE E-COMMERCE[‡‡]

Sebastian Fischmeister[*] Günther Hagleitner[*]

Wolfgang Pree[*] Gustav Pomberger[**]

Abstract

Electronic-banking applications (EBAs) are among the pioneers of electronic-commerce (e-commerce) applications. Like other e-commerce applications, they require sophisticated security mechanisms and intuitive usability so customers put trust in them and therefore use EBAs. Although EBAs have been existing for a long time and their concepts are well understood, current EBAs have severe security and usability restrictions. Also the authors claim that it is necessary to build secure and small e-commerce applications with intuitive usability in order to be able to create complex and still secure ones with good user acceptance.

The paper shows the usability and security problems of related technologies and introduces a new approach that is based on asymmetric encryption. The results of the evaluation show that it meets the intended criteria. Finally the work also includes examples that show how this approach can be used to build secure e-business and e-commerce applications while retaining intuitive usability.

Keywords: e-commerce, digital signatures, security, mobile computing, software architecture

[‡‡] This work is sponsored by the Austrian Raiffeisen Banking Group (RACON Software GmbH/GRZ GmbH Linz) through the Software Competence Center Hagenberg and mobilkom Austria AG.

[*] Software Research Lab, University of Constance, Campus PO D188, D-78457 Constance, Germany, e-mail: <firstname>.<lastname>@uni-konstanz.de

[**] Institut für Wirtschaftsinformatik (Software Engineering), Johannes Kepler University Linz, A-4040 Linz, Austria, e-mail: pomberger@swe.uni-linz.ac.at

1 INTRODUCTION

Electronic-banking applications (EBAs) and other money-related applications require a high degree of security. The most common approach is the use of personal-identification numbers (PINs) and transaction-authorization numbers (TANs). PINs and TANs are normally a combination of letters and digits not longer than ten characters. Once a user registered with the EBA, he receives a PIN and a number of TANs. He uses the PIN to authenticate himself, when he logs on to the EBA. After the user authenticated himself to the system, he uses TANs to authorize transactions (e.g., to transfer funds or buy stocks). Every TAN can be used only once by the user. Once the user used up all his TANs, an issuing organization sends a list of new TANs to the user.

A different approach is to provide security via digital signatures. A digital signature is a convenient and secure way to sign electronic documents. The advantages of such signatures include data integrity (a signed document cannot be modified without invalidating the signature), authentication of the message origin (the signer can be identified), and nonrepudiation (the signer cannot deny having singed the document). To ensure these security features, asymmetric cryptosystems are usually the basis for digital signatures. In an asymmetric cryptosystem a trusted third party called certification authority (CA) generates related public/private key pairs and binds them to people. The private key that the user applies to sign the documents has to be kept strictly secret. The public key that parties need to verify the digital signature is public and can be obtained from the CA. Since the security of the signature is a function of the length of the keys, private keys are typically too long be used like the PINs previously mentioned; they have to be stored electronically. The complexity of the key management implies long expiration times of the key pair. Smartcards can achieve this long-time storage of the private key in a secure way. In addition to the technical features, digital signatures must have a legal basis to be useful for e-commerce or e-business applications. The European Community, for instance, introduced the electronic-signature guideline [4] in 1999 and each member state enacted a corresponding law.

Smartcards are tiny computers that must be supplied with power and a clock. They provide a serial interface to the smartcard reader through which data and commands can be transferred. They have their own operating system that provides means for memory and file management, execution of applications, and protected access for data. Hardware mechanisms ensure that smartcards are highly tamperproof. Therefore smartcards provide key advantages towards security. For the resistance of cryptosystems often depends on the length of a key or the quality of a password, smartcards are the perfect place to store these relative lengthy cryptological data items. Besides being a tamperproof storage media, smartcards offer to perform cryptographic computations themselves, so the secret key never has to leave the smartcard. Problems with smartcards include that they introduce additional hardware, that they are often specialized for one application, and smartcards with sufficient processing power (e.g., with a coprocessor) and EEPROM are expensive. Also encryption of bulk data is unfeasible due to low bandwidth (e.g., 9600 bps), little RAM (e.g., 1 kbyte), and small processing power (e.g., 1 MHz). However, with digital signatures only the message needs to be encrypted. Furthermore the key pairs are typically not generated on the card, so digital signatures are apt for the use with smartcards. Smartcards are standardized by the Electronic Telecommunications Standardization Institute (ETSI) in [3] and further security features of smartcards are summarized by Nichols in [6].

An application domain of smartcards is the subscriber identity module (SIM) as specified for GSM by the ETSI in GSM 11.11 [3] and GSM 11.14 [2]. The SIM is used together with a mobile equipment (ME) in the **g**lobal **s**ystem for **m**obile communication (GSM). The system uses these cards to store subscriber-specific data, so that the customer can conveniently change the ME without loosing access to his personal data (e.g., telephone book and short messages). The SIM is also part of the GSM security mechanisms; it stores security-related data that can only be accessed by entering special PINs (typically four digits). Smartcards and readers typically follow a client/server pattern: the reader initiates the sessions and sends commands the smartcard, which executes them. However the GSM standard also specifies the SIM Application Toolkit (STK) that makes the SIM proactive. Thus, developers can create applications for the mobile subscriber that the mobile phone executes. Such applications are triggered by events (e.g., the user selecting a menu item). The STK standard comprises commands for the communication to the network and basic control over the ME. The STK-enabled SIM can, for instance, request local information (i.e., the cell identification) or ask the ME to send a short message to a given number. The problem with STK programs is, however, that they normally are preinstalled on the SIM by the network operator. Since remote management of the SIM is costly and complex, these installed programs are never changed unless the SIM cards are replaced.

2 RELATED WORK

Home-banking and Internet-banking applications concentrate on providing a user control over her financial status (e.g., her bank account, her bonds, and her stocks). As stated in the introduction these money-related applications require special security mechanisms.

A modern approach towards authorization, especially tailored to mobile devices such as mobile phones, bases on vouchers and coupons. First Hop [1] realizes this approach with its Escio-Tokens technique. The user can buy a voucher that is sent to her mobile device. This voucher (a digital code) can be used in different ways by the issuing company. E.g., it acts as a train ticket (the conductor verifies the voucher and then invalidates it) or it acts as an authorization code for a fund transfer (the bank verifies that this voucher entitles a person to withdraw money and then it invalidates this voucher), or it can be used as an entrance ticket (the voucher is valid for a week and the doorman verifies it on a daily basis). So basically the voucher can be either be an one-time authorization code or limited by an expiration date.

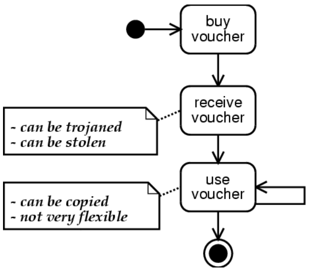
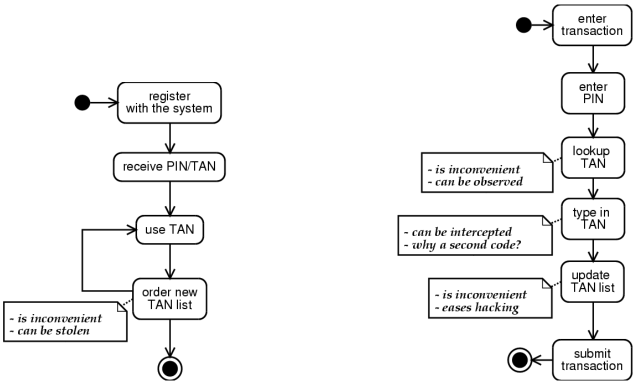


Figure 1. **Activity diagram for voucher-base solutions.**

This voucher-based approach has several drawbacks (see Figure 1). First, this approach does not provide security on a scalable basis. In the example stated before, the conductor verifies the voucher of the traveler. This is done by entering the voucher code in the conductor's device. So the code length of the voucher has to be reasonably limited, because long codes would introduce severe usability problems (e.g., the conductor mistypes the voucher code). However, short codes limit the flexibility of the voucher, as only limited information can be encoded in the voucher itself. Second, a voucher can be copied. In case of the entrance ticket, only one ticket could be bought and then passed on to another mobile phones via the short message service (SMS). Third, a voucher can be intercepted. Then the interceptor could for instance withdraw money before the original recipient withdraws it.

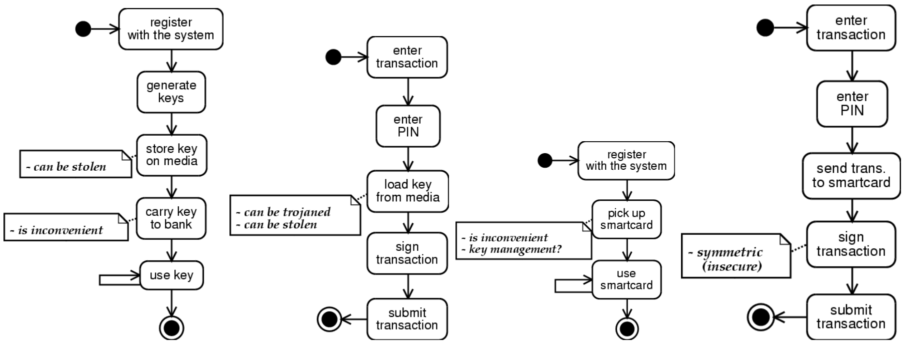


(a) **Registration for PIN/TAN-based solutions.**

(b) **Submitting a transaction using PIN/TAN.**

Figure 2. **Activity diagrams for PIN/TAN solutions.**

The most common approach, to solve the security issues of EBAs such as home banking or Internet banking is to use PINs for authentication and TANs for authorization. Figure 2 sums up the registration process (see Figure 2(a)) and the regular use (see Figure 2(b)) of the PIN/TAN mechanism. These figures point out the security risks and usability flaws of this mechanism. First, TANs are one-time passwords and are unlikely to be memorized by the user. So he will have to keep a written list with him, that can be lost, stolen, or copied unnoticed. Second, the user must enter the TAN via the keyboard. A Trojan-horse program could snoop for keyboard events and so obtain the next valid TAN. Then the Trojan horse would modify the entered TAN—thus, invalidating it—and therefore win time to transmit the data to the originator of the Trojan horse. Third, a TAN does not have an expiration date per se, so theoretically a TAN is valid for an unlimited time. This amplifies the previous security problem. Besides these security risks, the PIN/TAN approach provides only limited usability. Concerning learnability, the concept of TANs and one-time passwords is rather different to usual authorization mechanisms (e.g., permanent passwords). Furthermore TANs are one-time authorization codes, thus the user typically marks used codes. Although this behaviour positively influences error avoidance, it further weakens the security concept, because it enables strangers to determine the next valid TAN. Finally, since it is hard to memorize TANs, the user has to keep the list of TANs with him. This is inconvenient and inefficient, for the user needs to copy a TAN from the list to authorize a transaction.



(a) **Registration for HBCI/RDH.**

(b) **Submitting a transaction using HBCI/RDH.**

(c) **Registration for HBCI/DDH.**

(d) **Submitting a transaction using HBCI/DDH.**

Figure 3. **Activity diagrams for HBCI solutions.**

A newer approach to security with Internet banking is the home-banking computer interface (HBCI) described by Stein in [8]. The aim was to create an open, transport mechanism independent, flexible, and secure standard to enable software to handle bank transactions. There are two main variations (see Figure 3): the RSA-DES Hybrid (RDH) and the DES-DES Hybrid (DDH). The RDH bases on asymmetric encryption.

The registration process is depicted in Figure 3(a). The user and the bank exchange their public keys via a storage medium (e.g., a floppy disk). The user retains her private key and the public key of the bank on her hard-disk. The DDH relies on symmetric encryption. The registration process merely consists of a user obtaining a smartcard that contains the cipher keys (see 3(c)). Both, the RDH and the DDH approach, have drawbacks. Although the RDH process (see Figure 3(b)) makes use of asymmetric encryption, the secret key is stored on the local hard-disk. This poses a threat to security as it is possible to steal the secret key. The DDH approach (see Figure 3(d)) solves this issue, because the cipher key is stored on a smartcard. The smartcard also executes the encrypting and deciphering processes, so the key never leaves the smartcard. However, this approach relies on 2-key-Triple DES. So the system is very inflexible as it cannot be used with other banks or other applications. The financial institutes or service provider would have to share the user's secret key with each other or a trusted CA.

The discussed drawbacks of the related work form the basis of the motivation to find a novel solution and especially to get rid of the PIN/TAN mechanism. So the Symbolon approach tries to cope with the security and usability flaws that are intrinsic to voucher-based, PIN/TAN, and RDH-based mechanisms. Besides this, Symbolon tries to introduce flexibility that is not given with the DDH mechanism.

3 CONCEPTS AND ARCHITECTURE OF SYMBOLON

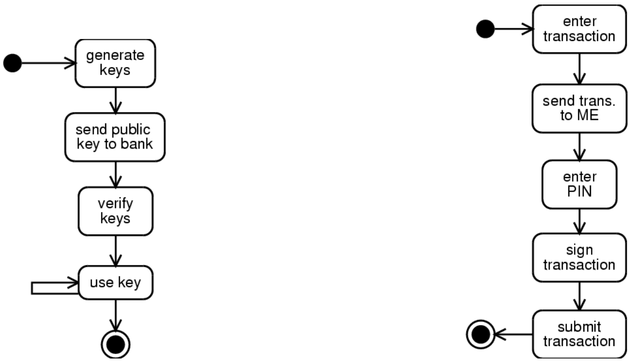
In the following sections the scenario of a user transferring funds from his account to another serves as a representative example to introduce Symbolon—an approach using digital signatures and mobile equipments to provide security in EBAs. Symbolon is currently applied in a pilot project at Raiffeisen to enhance the security of its EBA and to prepare it for a convenient mobile commerce application.

3.1 Scenarios

Registration. Before the user can use the Symbolon approach, he has to register (see Figure 4(a)). The precondition for the registration is that the user has already installed the EBA software on his computer and his SIM card has the appropriate encryption algorithm. The registration succeeds when the financial institute knows the user's public key and the private key resides on the user's SIM card. The flow of events is triggered by the user.

1. **Generate the key pair:** The user initiates the generation of the cryptographic key pair on the ME. The private key never leaves the device and is stored on the SIM card.
2. **Send keys to the financial institute:** The public key that the ME generated is electronically sent to the financial institute by the EBA by the user.
3. **Verify key:** The user has to verify the correctness of the public key (e.g., by

reading out the fingerprint of the key to the clerk).



(a) **Registration for the Symbolon-based solutions.**

(b) **Submitting a transaction using Symbolon.**

Figure 4. **Activity diagrams for Symbolon-based solutions.**

Transfer of funds. After the user registered himself, he can make use of Symbolon (see Figure 4(b)). The precondition for the transfer-money scenario is that the user has successfully registered, his mobile phone is connected to the system, and his SIM card can compute the encryption of the message digest using the digital signature algorithm. The success end condition is reached when the financial institute has received the signed request for a transfer of funds and thus executes the transaction. The primary actor is the user, secondary actors are the financial institute and the CA. The scenario is triggered by the user who submits the form that specifies the transaction. The flow of events is as follows:

1. **Transmit transaction form:** After having filled out all the relevant information for a transfer of funds, the user asks the system to process the data.
2. **Create transaction:** The system extracts the entered data, puts it in a standardized form, and calculates the message digest using a hash algorithm.
3. **Transfer transaction:** The system opens a connection to the ME either via a serial cable, SMS, or the infrared (IR) port and sends the calculated message digest.
4. **Enter security PIN:** The user is prompted to enter his security PIN, which he enters on the ME.
5. **Perform the encryption:** The SIM card encrypts the received message digest and sends it (with the help of the ME) back to the calling application.
6. **Forward transaction:** The system sends the signed transaction to and receives acknowledgment from the financial institute.

7. **Execute transaction:** The financial institute verifies the signature and executes transaction.

It is important to note that the user must enter the security PIN on a per-encryption basis. This prevents Trojan-horse programs from performing statistical analyses of the encryption and eventually reconstructing the private key.

3.2 Architecture of Symbolon

Figure 5 shows the components, their interaction and interfaces as well as their topology for the Symbolon approach. The functionality is spread on three nodes: the *ME,* the *user's computer,* and the server of the *financial institute.* The *ME* and the *user's computer* need to have means of communication to realize their tasks. The *Signature Client Back End* has to read from and write to the *SMS Inbox* of the *ME* that serves as a shared data repository. The link between the *ME* and the *user's computer* can have one of the following three forms:

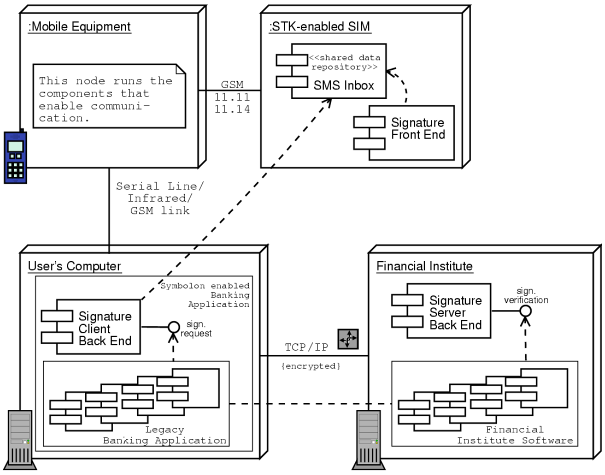

:Mobile Equipment
This node runs the components that enable communi- cation.
GSM
11.11
11.14
:STK-enabled SIM
<<shared data repository>>
SMS Inbox
Signature Front End
Serial Line/ Infrared/ GSM link
User's Computer
Symbolon enabled Banking Application
Signature Client Back End
sign. request
Legacy Banking Application
TCP/IP
{encrypted}
Financial Institute
Signature Server Back End
sign. verification
Financial Institute Software

Figure 5. **The overall architecture.** The *Signature* component runs on the STK, which collaborates with the user's computer to prepare transactions. These transaction are sent to the *financial institute* that verifies the transaction and executes it.

Hardware cable connection: The communication between the *ME* and the *user's computer* is handled via a hardware cable. So these two devices communicate either via the serial line or the parallel line port.

Wireless connection: To communicate via a wireless connection both nodes, the *ME* and the *user's computer,* need additional hardware (e.g., an infrared port or Bluetooth). The *user's computer* sends the data to the *ME* and the *ME* returns the signed data to the *user's computer* using this hardware.

Operator based connection: The communication bases on GSM. This network provides means to transmit SMS from one ME to another. So the *ME* and the *user's computer* communicate via SMS messages.

The *user's computer* and the server of the *financial institute* communicate with each other via TCP/IP. This communication, however, must be encrypted since digital signature mechanisms do not cover privacy issues.

The *user's computer* runs the *EBA*, which among other tasks, provides the main interface to the user and coordinates the communication within the system. The transactions entered by the user are transformed into standard documents. Then the message digest of this document will be calculated using a hash algorithm. Afterwards the output of this algorithm is sent to the *Signature Front End.* After the user acknowledged the pending transaction on the mobile phone by entering his security PIN, the *Signature Front End* reads in the data from the *SMS Inbox* and encrypts it. Then the *Signature Front End* returns the result to the *Banking Application* that forwards the signed transaction to the *financial institute.* Finally the *Financial Institute Software* verifies the signature and processes the user's transaction.

4 EVALUATION AND COMPARISON TO RELATED WORK

The approach described in the previous paragraphs, combines several different technologies. The results of the following evaluation of Symbolon show that it meets the intended requirements. The evaluation of the system covers security, usability, and flexibility.

4.1 Security

The security evaluation excludes the components running on the *ME* and also the connection between the *ME* and the *STK-enabled SIM*. The components running on the *ME* are not modified by Symbolon. The connection between the *ME* and the *STK-enabled SIM* is tamperproof since the SIM card is integrated into the *ME*.

Connections. Section 3.2 names different technologies the user can choose from to connect the *ME* and his *computer.* The operator-based transmission method provides the least security of these three connection types. The main problem is that this mechanism relies on the network operator in terms of security and availability. This introduces many potential security risks that the user cannot assess. And even if the user trusts the network operator, Golic describes in [5] ways to successfully attack the GSM cryptographic algorithms.

The wireless connection scores second in the security ranking. Its main security flaw is the natural scattering of the used medium (e.g., infrared light). Although the communication range is limited, the scattering eases eavesdropping. But in contrast to the previous transmission method—to send the data via GSM—the user has control of the surrounding environment. So she can eventually spot possible eavesdropping devices.

The most secure connection type is the hardware cable. It provides the most effective protection mechanisms against attacks (e.g., eavesdropping). It is nearly impossible to eavesdrop the serial line at the time data is transferred from one device to another without taping the cable or one of the devices. Furthermore, all hardware components are visible to the user. So attacks in general are hard to drive, because of the user paying attention to these devices. Utilizing this transportation mechanism, Symbolon provides increased security compared to the voucher-based approach that transports the vouchers via the GSM link.

Beside the data connection between the *ME* and the *user's computer,* there is another one between the *user's computer* and the *financial institute.* The EBA initializes the communication to the financial-institute software located at the *financial institute.* The security of this connection need not be evaluated, because applying Symbolon does not require modification of components that are involved in this communication.

Components. The smartcard in the mobile phone stores the private key of the user. So the security of the *ME* is critical for the overall system. Reflection mechanisms can guarantee the software integrity for such systems [7]. In contrast to HBCI/RDH, in the Symbolon approach the private key never leaves the device that creates the signature. The *STK-enabled SIM* signs the data itself. This boosts the security of the system, because even if the connection between the *ME* and the *user's computer* is eavesdropped, no secret data can be tapped (excluding privacy issues). This is a security advantage compared to the HBCI/RDH approach that stores the key at the local hard disk and compared to the PIN/TAN mechanism that stores the keys on a printed sheet of paper.

The *user's computer* and the *financial institute* do not need special security precautions (except for privacy reasons). The data is already signed by the *ME.* The *user's computer* so only forwards the signed data to the *financial institute.* The *financial institute* then verifies the signed data and processes it.

4.2 Usability

Quality attributes that are part of usability are learnability, error avoidance, satisfaction, and efficiency. One of the driving ideas of Symbolon was to improve the usability compared to other related work. Symbolon can utilize different connection types. The following usability study assumes that the hardware cable is use to link the *ME* and the *user's computer.*

Symbolon positively influences all four quality attributes significantly. The main reason is that the user does not require TANs anymore to authorize a transaction. The *ME* signs the transaction. The digital signature authorizes the bank to execute the transaction. Compared to the PIN/TAN approach Symbolon improves (1) learnability, because now the user does not have to learn the TAN concept and needs no TAN list, (2) error avoidance, because the user only needs to memorize one PIN, (3) satisfaction and efficiency, because the user does not have to enter two passwords (i.e., a PIN and a TAN) and therefore he also does not need to look up a TAN. Compared to the HBCI/DDH approach Symbolon provides better efficiency, because the user need not go to her financial institute to pick up the smart card. Instead she can verify the finger print via the telephone.

However, Symbolon also introduces constraints on the environment that reduce the usability. So the *user's computer* and the *ME* require compatible connection types: for wireless connection both require an infrared port, for cable connection both need a serial or parallel port, and for GSM link the *user's computer* needs an extra short message service center. Also the *ME* must support digital signatures, so eventually the user must get a new SIM card. Finally as mobile phones are battery powered, the system does not work if it runs out of battery power. However, better battery-life times will render this issue superfluous.

4.3 Flexibility

Besides providing sophisticated security mechanisms and intuitive usability, the intent of Symbolon was to create a flexible mechanism that can be reused. The mechanism should be at least as flexible as HBCI/RDH. The focus of the flexibility evaluation concentrates on reuse and integrability.

The Symbolon approach can be introduced into a wide variety of e-systems. This is a principal difference between the HBCI/DDH approach and Symbolon. In the HBCI/DDH approach the symmetric encryption prevents using the same smartcard for several different applications. Although the secret key of the user could be shared among different vendors, spreading the key introduces additional security risks. The Symbolon approach combines the two best elements of the HBCI/RDH and the HBCI-/DDH approach: it uses asymmetric encryption and the private key never leaves a tamperproof media. So the user can use the same key pair for several different applications (see Section 5 for examples).

Concerning integrability, Symbolon provides a lean interface that is used by the calling application. The Symbolon component *(Signature-Client Back End)* that applications need to integrate is encapsulated and therefore eases integration. If an EBA or an e-commerce application wants to integrate Symbolon it uses the SignRequest interface (see Figure 5) and includes the *Signature-Client Back End* with its distribution.

5 VISIONS

The idea—mobile equipment replacing smartcard readers combined with asymmetric encryption—is not restricted to electronic banking. The main advantages of this approach are acceptance and proliferation of mobile phones (thus implying low hardware cost) and high security based on asymmetric cryptography combined with smartcards. A wide variety of products that rely on secure authentication and authorization can be realized using Symbolon.

The abstracted idea is shown in Figure 6. The signature-creation device (SCD) is separated from the data-creation device (DCD). These two nodes communicate with each other. The DCD creates the data to be signed, the SCD signs the data and returns it to the DCD. Finally, the DCD transmits the data to the data-processing device that processes incoming signed data.

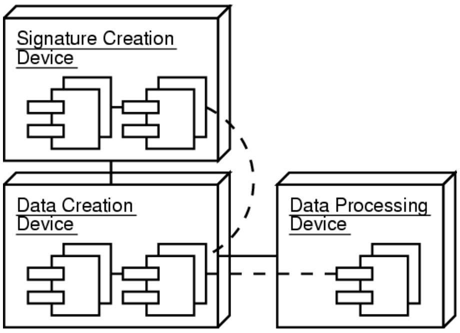


Figure 6. **The deployment of the abstract components.** The components show the basic idea to separate the concern of authentication/authorization from typical client server applications.

5.1 Products

This abstract idea can be used to build secure e-commerce, e-business, and e-government applications. All it needs would be a browser plugin: The user can access an e-commerce application via the world-wide web. Her browser is extended with the Symbolon plugin that can create a digital signature for a purchase offer. So she puts all items in her basket and at the checkout point the browser opens the Symbolon plugin. There she can verify what she is going to sign, can create a digital signature at the mobile phone, and submit the signed offer to the e-commerce company.

Symbolon can also increase the security of e-business applications. Here the plugin is part of a whole business-to-business application and the manager signs contracts on his mobile phone. This is not limited to only stationary applications. So the manager could run his b2b application at the airport and transmit the new contract via e-mail.

Also e-government solution can make use of the Symbolon approach. Once the key pairs are distributed and users know how to handle digital signatures, it is possible for them to submit all relevant kind of forms via the Internet. Finally mobile commerce combines the SCD and the DCD. So it is possible to buy items using the wireless application protocol enabled through digital signatures.

6 CONCLUSION

E-commerce applications must be secure to be accepted by customers. The fundamental idea is that first a small and well understood system must be made secure before complex and still secure ones can be built.

The paper presents an approach that introduces security to an electronic-banking application. The approach combines the best parts of related approaches and thus forms a new one. It combines sophisticated and strong encryption technologies, a secure storage medium, secure connections and mobility in one approach: Symbolon. Symbolon uses digital signatures to sign data, smartcards to store the secret key of the user, hardware cable, infrared, or a GSM link as connection between the signature-creation device to the data-creation device and finally, the encryption takes place in a mobile phone. So the user can carry his personal-signature device with him.

The presented approach improves several key points that related approaches (i.e., TAN/PIN, the HBCI/DDH, the HBCI/RDH, and voucher-based ones) miss. These key points are that (1) the private key never leaves the tamperproof storage medium, (2) the encryption takes place in a tamperproof environment, (3) the system improves usability compared to related approaches, and due to asymmetric encryption (4) different applications provided by different vendors can use one key pair.

Future work should be to create a browser plugin for further probing in this research area. Also the authors will use Symbolon to build e-commerce applications that corroborate that the Symbolon concepts and architecture scale up.

REFERNCES

[1] First hop. WWW Site. `http://www.firsthop.com`.

[2] Digital Cellular Telecommunications System (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM–ME) interface. ETSI standard, April 2000. Version 8.2.0, GSM 11.14.

[3] Digital Cellular Telecommunications System (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM–ME) interface. ETSI standard, April 2000. Version 8.2.0, GSM 11.11.

[4] European Parliament and European Council. Directive 1999/93/EC Of The European Parliament and Council of 13 December 1999 on a Community framework for electronic signatures. *Official Journal of the European Community*, pages 13/13–13/20, January 2000.

[5] J. Golic. Cryptanalysis of Alleged A5 Stream Cipher. In W. Fumy, editor, *Advances in Cryptology – EUROCRYPT'97: International Conference on the Theory and Application of Cryptographic Techniques*, LNCS1233, pages 239–255. Springer-Verlag, Berlin, Germany, 1997.

[6] R. Nichols. *ICSA Guide To Cryptography*. McGraw-Hill, 1999.

[7] D. Spinellis. Reflection as a Mechanism for Software Integrity Verification. *ACM Trans. on Inf. and Sys. Sec.*, 3(1):52 to 62, February 2000.

[8] Stein. *HBCI: Homebanking-Computer-Interface*, 2.2 edition, June 2000.