Biometrics and IT Security

About the practical deployment of the new Technology

Dr. Norbert Pohlmann

New technologies such as Biometrics, are, on the one hand, very attractive and can help to further increase security. On the other hand, these technologies have always received a lot of criticism.

In the following article, the requirements and the realization of a selected project with integrated biometric solutions will be presented and the current criticism of biometrics will be addressed. Furthermore, general deployment areas of biometric security solutions for mechanisms like authentication, file encryption and digital signature, which are independent of the concrete project, will be presented.

[FOTO]

Dr. Norbert Pohlmann

Board member of Utimaco Safeware AG and Chairman of the board of TeleTrusT e.V.

E-Mail: norbert.pohlmann@utimaco.de

Introduction

In the past, most business processes were dealt with personally, or - by mail - paper-based. Nowadays, such transactions can be carried out in a much more efficient way through a common global IT infrastructure. The electronic data can be integrated into work processes directly and without a media break. This trend of re-engineering business processes in all areas accompanies internationalization and globalization. Highly optimized procedures represent an enormous saving potential and are therefore very attractive for the market.

For organizations and companies, it is very important to discover which new dangers the implementation of electronic business processes brings. Only when the risks are known the dangers can be properly assessed. With the help of appropriate security measures, the global information society is able to reduce its vulnerability. To be generally accepted, the security mechanisms used have to be simple and comfortable. Biometrics provides an enormous user comfort, but is faced as well with a multitude of objections. Generally, the following holds good: If security concepts and their implementation adhere strictly to the requirements and circumstances of the respective organization, the profit of electronic business processes provided with a simultaneous minimization of risks.

Practical Implementation of Biometrics in Administration

In November 2001 the provision of a secure IT environment for the "judicial organizations" of the Netherlands was realized by the Dutch Ministry of Justice under the project name ROBIN.

Administration processes which, up to now, have been handled in the traditional way, will be carried out electronically in the in future. At the same time, a security level equivalent to the previous will be achieved. To guarantee the binding character and the confidence of all electronic processes with highest security, mechanisms like identification, authentication, encryption and decryption or the digital signature will clearly be assigned to the individual user through biometrics.

Requirements of the ROBIN Project

In the first step, 12,500 workstations were secured.

Regarding the binding character and confidence, the following requirements were realized:

- Manipulation security of all important information which is transmitted over the Justice net or is stored on the systems of the Justice authorities.
- Only authorized persons or groups are allowed to read certain information (reports, files, ...).
- Clear identification of the author of a document as well as of the senders and receivers of messages.
- Certain competences are not to be delegated (e.g. the posting of documents, judicial decisions concerning monitoring measures etc.).
- Successful hacker attacks have to be prevented.

Realization

To achieve a security level appropriate to the intended purpose, a combination of several mechanisms is required:

- Strong authentication by biometric procedures
- File encryption
- E-mail security by encryption and digital signature
- Public Key Infrastructure (PKI)
- Unequivocal linking of the digital Identity (of the certificate) to the 'natural' person by means of person-related SmartCards with fingerprint comparison (biometric identity control). (1),(4) Persons where the fingerprint procedure does not work (less than 3 %) can activate the SmartCard by a PIN. This will be documented accordingly and be assessed depending on the situation - should problems occur.

The personal SmartCard serves as a central security token. It stores the certificate of the user, his passwords for all net resources as well as his private keys. It is used for authentication on PCs, servers and host systems, for file and e-mail encryption and for digital signatures.

The security infrastructure is based on a PKI through which the registration of the user, the key generation, the issuing of certificates and SmartCards and also the provision of directory services and revocation lists are organized.(3)

For this Registration Authorities (RAs) where the initial personalization of the employees is carried out, were set up in the personnel departments. The advantage of this is that the personalization achieves a higher quality and so the error rate can be clearly reduced.

Biometrics criticized

During the last months, it was discussed in the press and other media, how registration systems which use fingerprints can be partly "outwitted". Through these attacks, it is attempted to get unauthorized access to a computer system with a forged fingerprint.

Basically, there are two possibilities:

1. The authorized user provides his finger for the production of a copy.

2. Through forensic procedures, a fingerprint is e.g. taken from a used glass without the consent of an authorized user and, in several steps, a duplicate of the fingerprint is created.

Both procedures were solely successful because access to the computer system had been protected by the biometric procedure only. Not least because of this, in the ROBIN project biometric registration procedures are used only in combination with unforgeable SmartCards. Thus, the scenarios described above are ineffective, since only the combination of fingerprint and SmartCard enables access to a computer system.

Without a SmartCard, one can not do anything with a forged fingerprint as it is only used to directly unlock the SmartCard. With each registration, the SmartCard compares the fingerprint to a reference print stored on the card.

Therefore, it is defined in the security policy, that, if a user leaves the workstation, he has to take the SmartCard with him. Moreover, by removing the SmartCard, the workstation is automatically locked and an attack with a forged fingerprint is no longer possible.(2)

The use of biometric procedures in combination with a biometrics-enabled SmartCard has further advantages: since the reference print of the finger is stored on the SmartCard, no central and vulnerable reference databases are needed. The central storage of person-related data is also criticized by data protection representatives in this country. The solution used in the ROBIN project effectively meets this criticism.

Furthermore, additional sensitive information like passwords for Single Sign On, cryptographic keys and signature keys can be stored securely on the SmartCard. Another advantage of biometrics is the reduction of helpdesk costs, as no forgotten passwords have to be reset. Thus, the combination of Biometrics and SmartCards is a comfortable and secure solution for a broad application area in the field of IT security. (5)

In the following, the PKI-/SmartCard-based services authentication, e-mail security and data encryption will be presented.

Secure Access to the Workstation

The user wants to access his workstation (PC with Windows). The security software asks the user to insert his SmartCard and to activate it with the help of his fingerprint. After successful activation of the SmartCard, an "Advanced Security Log-On" is carried out. Afterwards, the user is able to carry out the actions he is allowed to on the PC.

Secure Access to the Server System

If the user wants e.g. to carry out further services which are subject to authentication on a remote NT server, a cryptographic authentication between the security software on the server and the SmartCard is carried out first.

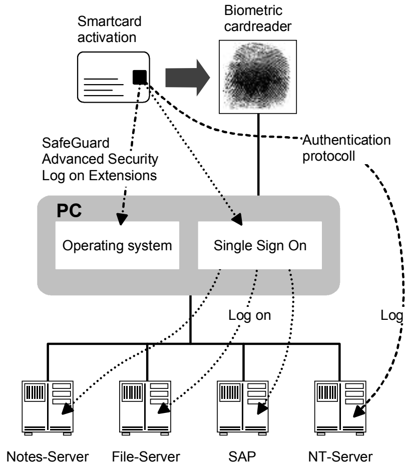


Abb. 1: User registration in the network

SingleSignOn System

If the user wants to work with another application (e.g. Lotus Notes or SAP), the SingleSignOn-System (SSO) of the security software on the PC organizes the log-on for the user. The SSO recognizes the request to enter a password, takes this password from the SmartCard and carries out the log-on for the user. If the application requires a password change, it is realized by the SSO according to the password rules. The new password is again stored on the SmartCard. By this procedure, maximum user comfort is achieved.

Activating the Electronic Signature

To digitally sign an e-mail, the user inserts his SmartCard and authenticates himself by fingerprint. If he is already logged in by SmartCard and fingerprint, he can use the same SmartCard for the digital signature and encryption of e-mails. The required keys are stored on the card as well.

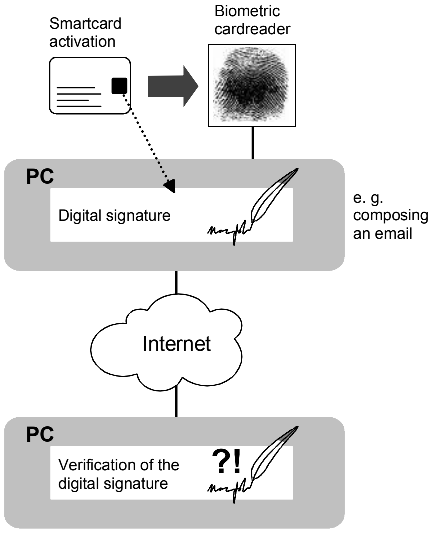


Abb. 2: Activation of the Digital Signature

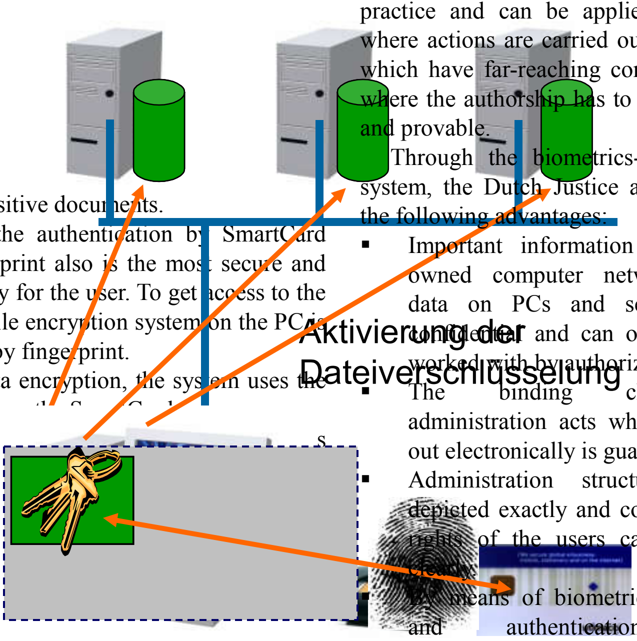
Activation of Data Encryption for User Groups

Within the organization's network, data encryption makes sure that authorized members exchange without worked user grou certain u key to sensitive documents.

Here, the authentication by SmartCard and fingerprint also is the most secure and easiest way for the user. To get access to the data, the file encryption system on the PC is activated by fingerprint.

For data encryption, the system uses the key stored

For th s goes on th on their unreadabl required the file computer there.



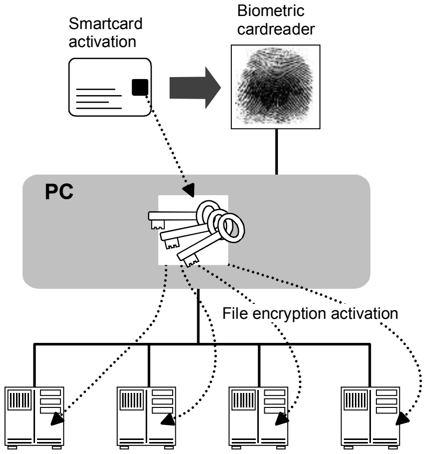


Abb. 3: Activation of the File-Encryption

Summary of the ROBIN Project

The ROBIN project makes clear that user comfort and convenience, in connection with security functions, are important factors of success for the use of security mechanisms. Biometrics-enabled security applications and SmartCards as well as a PKI-based security infrastructure are the basis of this concept. The solution presented is well-tried in practice and can be applied to all areas where actions are carried out electronically which have far-reaching consequences and where the authorship has to be unequivocal and provable.

Through the biometrics-based security system, the Dutch Justice authorities have the following advantages:

- Important information on authority-owned computer network (e-mails, data on PCs and servers) remain confidential and can only be read or worked with by authorized persons.
- The binding character of administration acts which are carried out electronically is guaranteed.
- Administration structures can be depicted exactly and competences and rights of the users can be assigned clearly.
- By means of biometric identification and authentication, security mechanisms like data encryption, e-mail security and digital signature are available to all users.
- The SmartCard with digital signature is serves as an "identity card for the electronic world" for the users. They do not have to remember passwords – their fingerprint is sufficient.
- The person-related biometric data is stored securely on the SmartCard; there is no central storage. Thus, data protection is guaranteed.
- The security mechanisms can be integrated smoothly into existing systems and are simple and comfortable to use. Accordingly, user acceptance is high.
- Training and administration costs are comparatively low; there will be no more queries to the helpdesk because of forgotten passwords. By that, operation costs (TCO) remain low.

As a "drawback" of the biometrics-supported security system, one has to put up with the fact that person-related processes cannot be delegated to other employees any longer.

Conclusion

Many organizations and companies want a higher security for the new business processes. The initiation of actions with weighty consequences has to be unequivocal and provable, so that critical business processes can be carried out, too. A secure and controllable information technology has to be realized.

User comfort and convenience, in connection with effective security functions, are essential factors of success for the application of security mechanisms.

Through biometric methods, not only convenience and comfort can be increased, but, at the same time, a much higher level of security can be achieved. The drawbacks and risks of passwords do not have to be put up with any longer; with the help of SingleSignOn procedures, they simply can be avoided. The use of Biometrics instead of a password or PIN simplifies the process for the user even more and further increases the level of security of the e-Business implementation.

The combination of both identification and authentication procedures is so convenient because it offers a high level of security appropriate for business processes and, at the same time, guarantees highest user comfort, great cost savings and security of investment.

Literature

(1) N. Pohlmann: ”Aktivierung von SmartCards durch Biometrie", KES - Kommunikations- und EDV-Sicherheit, SecMedia Verlag, 3/2001

(2) N. Pohlmann: "Trusted IT-Infrastructures: Not only a Technical Approch", DuD Datenschutz und Datensicherheit - Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 09/2001

(3) N. Pohlmann: „Nutzen und Chancen von Public-Key-Infrastrukturen", in "Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung", Hrsg.: Patrick Horster, IT Verlag, 2002

(4) „Biometrische Verfahren”, IT-Report 2002, Report Verlag, 2/2002

(5) N. Pohlmann: „Weil der Fingerabdruck einmalig ist“, Die Sparkassenzeitung – Nachrichten für die Sparkassen – Finanzgruppe, Deutscher Sparkassenverlag, 24.05.02