ARTICLE:

INTEGRATING QUALIFIED ELECTRONIC SIGNATURES WITH PASSWORD LEGACY SYSTEMS

WRITTEN BY:
HEIKO ROßNAGEL
AND **JAN ZIBUSCHKA**

Despite a common legal framework for electronic signatures within the European Union, qualified electronic signatures have not been a market success, although several governments are issuing or plan to issue signature capable identity cards to all their citizens. However, the high market penetration of smart cards does not necessarily lead to an increased number of signature transactions. To tap the potential for electronic signatures, there is a need for applications that are used on a frequent basis. In this paper, a method is proposed to achieve single sign on by using qualified electronic signatures. This solution can be used for all e-commerce sites, regardless of whether they accept or use electronic signatures.

Introduction

The EC Directive on electronic signatures sets out a framework of requirements for electronic signatures.[1] The Directive distinguishes between "electronic signatures" and "advanced electronic signatures". An advanced electronic signature is defined in article 2(2) as an electronic signature that meets the following requirements:

"(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;"

Certification service providers (CSP) can issue certificates for advanced signatures that will be qualified if they meet the requirements of Annex I of the directive. Those advanced signatures with qualified certificates will be referred to in this article as qualified signatures.

The market share of EC-directive conforming signature cards is disappointingly low, failing to meet expectations, perhaps with the exception of electronic identity cards issued by governments.[2] It can be argued that the lack of customers prevent companies from investing in signature products, which in turn implies there is almost no commercial reason for using qualified electronic signatures, and consequently potential customers do not seek to obtain signature products.[3] However, qualified electronic signatures offer the potential to transfer e-government processes from paper to electronic medium, and possibly to save tax payers' money.[4] But these potential savings can only be realized if a large proportion of the population has, and more importantly, uses qualified electronic signatures. Several governments are presently issuing[5] or plan to issue[6] identity cards with electronic signatures to all their citizens. The goal of these initiatives is to increase the penetration rate of smart cards with electronic signatures within the population.

However, the presence and availability of an innovation does not necessarily lead to a high adoption rate within the population.[7] One example is the German "Geldkarte". This smart card enables the user to make

[1] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).*
[2] *J. Dumortier, S. Kelm, H. Nilsson, G. Skouma and P. Van Eecke, "The Legal and Market Aspects of Electronic Signatures," (Leuven, 2003), for electronic ID (eID) schemes, see http://ec.europa.eu/idabc/en/document/4484/5584.*
[3] *H. Roßnagel, "Mobile Signatures and Certification on Demand," in S. K. Katsikas, S. Gritzalis and J. Lopez (Eds.) Public Key Infrastructures, (Springer, Berlin Heidelberg, 2004), pp 274-286.*
[4] *KPMG; Bundesministerium für Wirtschaft und Technologie, Einsatzmöglichkeiten der Elektronischen Signatur in öffentlicher Verwaltung und Wirtschaft, (Berlin, 2001).*
[5] *D. De Cock, "Total number of eID cards currently distributed to Belgian citizens," http://homes.esat.kuleuven.be/~decockd/wiki/bin/view.cgi/Main/BelgianEidCardGraphsTOC#Total_number_of_eID, J. Hvarre, "Electronic signatures in Denmark: free for all citizens", e-Signature Law Journal, Volume 1 Issue 1, 2004, pp 12-17.*
[6] *H. Reichl, A. Roßnagel and G. Müller, "Digitaler Personalausweis, Eine Machbarkeitsstudie," Deutscher Universitäts-Verlag,Wiesbaden, 2005.*
[7] *E. M. Rogers, Diffusion of Innovations, (Free Press, New York, 2003).*

small electronic payments, and is included on most German EuroCheque cards. Despite over 60 million cards already distributed in Germany, only 38 million transactions were made in 2004 (0.63 transactions per user per year).[8] Therefore, a high penetration rate of signature cards will not automatically lead to the adoption of qualified electronic signatures, especially if costs and benefits are not fairly distributed, and prices remain as high as they are.[9] In addition, the network for qualified electronic signatures does not increase with the distribution of signature cards but with the adoption of the signature functionality. So by simply distributing signature cards the critical mass will not automatically be obtained.[10]

Potential savings can only be accomplished if qualified electronic signatures are widely used. Furthermore, frequent usage of the system will help the users remember the Personal Identification Number (PIN) that is usually used to authenticate the user.[11] Limiting the length of a PIN will make it easier to remember the number. Therefore, in order to create an incentive for users to adopt applications with qualified electronic signatures, the application needs to generate a relative advantage[12] or increase perceived usefulness.[13] E-government applications will not be sufficient to create this kind of incentive, because they do not occur frequently enough. For example, according to Fox,[14] the average citizen in Germany is only required to deal with the public administration 2.1 times a year.

Authentication issues

Strong password dilemma

One of the biggest problems users are confronted with when interacting with current authentication systems, is choosing a strong password.[15] In the web environment, users need to have a number of passwords for a range of different uses. Examples are web based mail, e-commerce sites and discussion forums. Passwords are also widely used for authentication in e-mail, operating system login, remote shells, databases and instant messaging. This leads to a large number of passwords that a user has to generate, memorize, and remember. However, remembering a number of randomly selected, independent passwords is a strain, especially if a password is used only occasionally. Therefore, users tend to either choose weak passwords, or choose related passwords for several or even all accounts.[16] Also, users tend to write down their passwords, especially in the case of randomly generated passwords.[17]

Humans are able to remember short passwords and passwords that they can easily associate with something. It has been shown that users tend to choose weak passwords if the system allows it.[18] User defined passwords are often based on words from natural language; typical examples include family members or hobbies. However, such practices undermine the security of the authentication system. This can be exploited in dictionary attacks; an attacker just has to check a list of commonly used passwords. Sometimes, users have to change their passwords periodically, and may not reuse old passwords. The problems is that humans do not have a capacity for retaining arbitrary passwords, especially if they are required to remember a number of them. Forgotten passwords are a major problem, and resetting them are a cost to the organization. One study estimated that help desk staff have to reset user passwords manually in 82 per cent of cases.[19] This procedure will often take more than five minutes. As forgotten passwords are among the most common problems encountered by IT departments, this may result in high help desk costs. Additionally, the distraction and the time spent on resetting the password will reduce the productivity of users.

Current solutions

While it might be difficult to manage a large number of strong passwords, remembering only one strong password may possible, even for an occasional user. The term single sign on (SSO) describes a system that allows a user to authenticate themselves to a number of services using one master password. A significant

[8] *V. Koppe, "Die Geldkarte der deutschen Kreditwirtschaft: Aktuelle Situation und Ausblick," http://www.geldkarte.de/_www/en/pub/geldkarte/press/facts_and_figures/payment_transactions.php.*

[9] *S. Lippmann and H. Roßnagel, "Geschäftsmodelle für signaturgesetzkonforme Trust Center," in O. K. Ferstl, E. J. Sinz, S. Eckert and T. Isselhorst (Eds.), Wirtschaftsinformatik 2005, Physica-Verlag, Heidelberg, 2005, pp 1167-1187.*

[10] *L. Fritsch and H. Roßnagel, "Die Krise des Signaturmarktes," in H. Ferderrath (Eds.) Sicherheit 2005, Köllen Druck+Verlag GmbH, Bonn, 2005, pp 315-327.*

[11] *A. Adams, M. A. Sasse and P. Lunt, P "Making Passwords Secure and Usable," Proceedings of HCI on People and Computers XII, 1997, pp 1-19.*

[12] *E. M. Rogers, Diffusion of Innovations, (Free Press, New York, 2003).*

[13] *F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology" MIS Quaterly, (13 :3), September 1989, pp 319-340.*

[14] *D. Fox, "E-Government," Datenschutz und Datensicherheit (DuD), (27 :2), February 2003, p 103.*

[15] *R. E. Smith, "Picking PINs and Passwords," in Authentication: From Passwords to Public Keys, (Addison Wesley, Boston, 2002), pp 1-550.*

[16] *A. Adams, M. A. Sasse and P. Lunt, "Making Passwords Secure and Usable," Proceedings of HCI on People and Computers XII, 1997, pp 1-19.*

[17] *R. E. Smith, "Picking PINs and Passwords" in Authentication: From Passwords to Public Keys, Addison Wesley, Boston, 2002, pp 1-550.*

[18] *B. J. Brown and K. Callis "Computer Password Choice and Personality Traits Among College Students," Working Paper, Southeast Missouri State University, Cape Girardeau, Missouri, 2004, http://cstl-cla.semo.edu/callis/xResearch/PasswordsBettyBrown/PasswordsRevs5.30.04.doc.*

[19] *RSA Security "RSA Security Survey Reveals Multiple Passwords Creating Security Risks and End User Frustration," http://www.rsasecurity.com/press_release.asp?doc_id=6095.*

advantage is that it limits the number of passwords that need to be used. The master password will also generally be used quite frequently, which helps to recall the password. However, such a password must not be easy to guess. It should also be closely guarded, as it will enable an attacker to obtain access to all services of the user.

There are quite different approaches to implement single sign on. Several systems that provide secure and usable user authentication are described below.

Encrypted password lists

One of the most trivial and widely employed solutions for the password management challenge is to save user passwords to a file. There are several applications that offer the possibility to save users' service passwords in a file that is stored on the user's hard drive. One open source example is Schneier's Password Safe application.[20] The feature is also included in most modern browsers. Examples are Opera (The Wand), Internet Explorer (AutoComplete) or Firefox (Password Manager). The password list is encrypted using a key that is derived from a master password. This method offers a reasonable level of security. However, it has several drawbacks. If the stored data is lost, users are unlikely to recall the stored passwords, as the master password is the only authentication information they have to remember regularly. Therefore, the user is unable to recover any of his service passwords without help from the service provider. In addition, the password file has to be present on any machine from which services are to be obtained. As it is sensitive, albeit encrypted, information, this can be quite cumbersome.

Tokens

An alternative to password based authentication is the use of tokens. In contrast to passwords, where the authentication process is based on something the user knows, token authentication utilizes something the user has. One example of such a token is a smart card. It usually stores keys for a public key infrastructure (PKI) or other cryptographic application, and is able to perform the relevant algorithms. Because of the physical nature of tokens, it is harder for an attacker to acquire it without the user noticing the theft. An attacker might steal a token, clone it, and then return it to the user. This would require considerable technical skills and an additional interaction with the victim, though.

However, a user might lose his token. This will lock the user out of the system, and can probably only be fixed with help from an administrator, and will incur the costs of buying a new token. Additionally, a token might be acquired by an attacker, which would grant them access to the protected services. Tokens are therefore often combined with additional forms of authentication to minimize the security risk of loss.

Smart cards may be used as a secure place to store encrypted password lists. In combination with a secure password generator, this allows for secure, two factor authentication. There are a number of products and similar implementations that store encrypted passwords and other authentication information on a smart card or similar token. The user authenticates to the card using a PIN, unlocking the data. While a token based authentication works well in closed user groups, it is not suitable for authenticating at various e-commerce websites from different vendors. No e-commerce vendor would be willing to issue expensive hardware tokens to its customers or, even more unlikely, potential customers.

Centralized SSO systems

In addition to client side or token based password storage mechanisms, a number of SSO solutions use authentication servers run by a trusted third party to authenticate a user to service sites. In such a system, the user authenticates to a trusted server, which in turn identifies the user to the service requested, using a mix of personal information that the user has stored on the server, and the authentication token that is recognized by the services. Also, most SSO Systems in use require that specific protocols be used at the server side. This leads to increased implementation costs, and also carries the risk of vendor lock-in, as implementing another protocol on top of an existing service may prove quite a challenge.

Furthermore, centralized systems require strong trust towards the SSO service provider, as potentially valuable data, for example credit card information, might be stored on the server side. Additionally, the SSO service might claim to be the user without the user's authorization. As most organizations do not enjoy this level of trust, a single sign on solution that does not require a third party seems preferable. Also, even if an organization seems trustworthy initially, this trust may well be undermined by security breaches or weaknesses, or even by a simple shift in users' perception of the company.

[20] *Schneier, B. "Password Safe," http://www.schneier.com/passsafe.html.*

Therefore, from a user perspective, the usefulness of these systems is quite limited. On the other hand, such systems are very dependent upon acceptance among the various service providers, as they are normally not able to communicate with authentication mechanisms that use another protocol. Also, it seems unlikely that all service providers would uniformly trust the central authentication authority.

Identity Federations

However, there certainly are partners that an organization would trust for the purpose of authenticating users. These partners would not be the same from organization to organization, but one could expect clusters of companies that are held together by mutual trust. Some examples of such protocols and standards are the Liberty Alliances set of protocols[21] and the Security Assertion Markup Language (SAML).[22] However, such identity federation protocols still require modifications on the service side. Additionally, there are several federation standards in the market, so the actual benefits of investments in a specific technology are often unclear.

PKI

Public key infrastructures provide secure communication using asymmetric cryptography. In addition to simple token based systems that offer only authentication, they enable users to create digital signatures. Using digital signatures enable users to authenticate themselves and sign transactions, ensuring the integrity of their messages. Furthermore, certificates that are issued by a third party are used as proof of authenticity as well as assurance of certain attributes of the users. Like password files, the private keys are usually stored on the user's hard disk or a smart card, and encrypted using a password.

However, the establishment and operation of a PKI requires large investments.[23] E-commerce vendors might be willing to accept PKI as an additional method for authentication. However, they will not be willing to build and maintain a PKI of their own. It is not surprising that PKIs have not achieved a large market penetration. Furthermore, like SSO systems, PKI is usually not able to authenticate the user to competing authentication protocols. The system's usefulness is also dependent of the acceptance on the server side.

However, if a global PKI is already in place, such as, for example in Belgium,[24] using such an existing infrastructure for e-commerce authentication is a logical step. The problem then is to encourage the e-commerce vendor to accept this kind of authentication. Since this will require investment by the e-commerce vendor, it is unlikely to happen unless the group of potential customers, demanding this form of authentication, is large enough to justify the investment. While waiting for e-commerce vendors to accept digital signatures might be viable in the long run, a different approach that is not dependent on the vendors' cooperation might be more promising.

Integrating qualified electronic signatures and password legacy systems

Naturally, a single sign on solution that is usable 'out of the box' with already deployed signature cards is highly desirable from the perspective of the user. Such a solution offers additional security for the central authentication secret. It provides two-factor authentication, using a token and a PIN. To enable the system to be deployed easily in association with an existing signature card infrastructure, it is preferable to only use algorithms that are used during the signature processes and are present on all smart cards that can produce digital signatures. This eliminates the possibility of storing the service passwords on the smart card, since freely accessible memory may not be present on all cards, and if present, it may already have been allocated for other uses.[25] One possibility is to use the signature card to encrypt password lists for external storage. This will have the same drawbacks as encrypted password lists, which have already been discussed above.

Generation of passwords using Smartcard functions

Apart from storing passwords in an encrypted form, it is also possible to generate them on the fly, using strong cryptography. However, such methods have to guarantee several security properties. The generated passwords should be pseudorandom and independent. To summarize the key property in a more concise way: the generated service passwords must not be capable

[21] *W. Duserick, P. Madsen, S. Silk, L. B. M. Mathan, N. Karhuluoma, S. Adachi, E. Norlin, L. Elliott, K. Murphy, T. Candia, P. Cole and S. Deadman, "Whitepaper on Liberty Protocol and Identity Theft," Whitepaper, Liberty Alliance, 2004 www.projectliberty.org/resources/whitepapers/Liberty_Identity_Theft_Whitepaper.pdf.*

[22] *OASIS Consortium "Security Assertion Markup Language (SAML) V2.0," http://www.oasis-open.org/specs/index.php#samlv2.0.*

[23] *J. Lopez, R. Opplinger and G. Pernul, "Why Have Public Key Infrastructures Failed So Far?" Internet Research, (15:5), October 2005, pp 544 – 556.*

[24] *Belgium's eId Portal http://eid.belgium.be/en/navigation/12000/index.html.*

[25] *H. Reichl, A. Roßnagel and G. Müller, Digitaler Personalausweis: Eine Machbarkeitsstudie, (Deutscher Universitäts-Verlag,Wiesbaden, 2005).*

of being forged, even giving service passwords for another service. This implies that no information about the central secret is leaked.

The basic architecture of this approach can be summarized in four steps:

1. Define a scheme for deriving service identifiers for the different service providers the user might want to authenticate to. This can be implemented by concatenating several attributes of the service, such as a service name, URL, the user's login, and so on. Data for the service identifier may be provided by the user, or automatically loaded from the target application. Such functionality might be provided by a browser plug-in in the e-commerce case, or by a service integrated in the operating system to allow for support of a broader range of target applications.
2. Combine the identifier for the service with the user's master password using strong cryptography.
3. Transform the resulting value into a pseudorandom account password. This can be done using a simple Base64 encoding, although more complicated schemes may be used to ensure the compliance of passwords with service policies.[26]
4. Transfer the password to the appropriate service login form. This may be realized by an application that integrates with current browsers, such as a plug-in.[27] Other implementations that generate passwords for additional services, such as database access or remote login are also possible.

Several cryptographic primitives, such as hash functions and signatures, are suitable for step 2. The details of the different implementations will be described in the following sections.

Hash Functions

A possible implementation of such a password generation scheme using hash functions was patented by Abadi and others in 1997.[28] Recently there has been renewed interest for this method in the context of web single sign on and phishing protection, and several papers have been published describing different implementations.[29] Service identifier and master password are combined, for example concatenated, and then hashed, as shown in Figure 1.

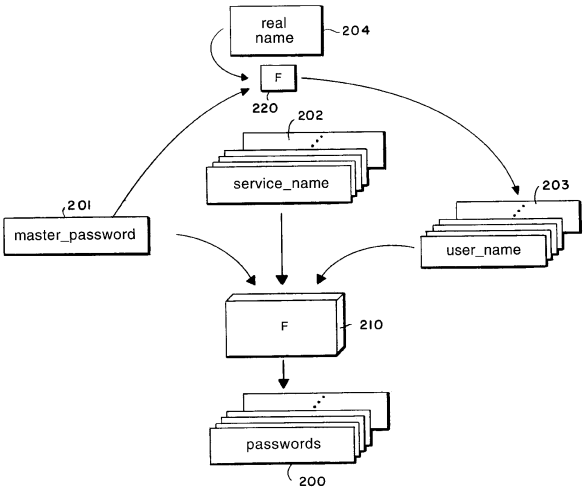


Figure 1. Diagram of the password creation process using hash functions [30]

The result is unique for each account, due to the collision resistance of hash functions. It should also be impossible to compute the master password from it, because of the one-way property of the hash function.

This scheme could be implemented using a smart card to do the hashing. However, this does not provide any additional security, as the hash function does not utilize any data stored on the smart card. Additionally, the user has to authenticate twice. He first has to provide his PIN to the smart card, and then provide the master password for the password generation scheme. Of course, this is quite cumbersome and contrary to the notion of single sign on. To make matters worse, hash functions do not provide clear security guarantees when some of the information about the inputs may already be known to the attacker or attaining part of the input is sufficient to mount an efficient attack. In the presented single sign on application, an attacker can probably determine at least part of the service identifier for any given service, and will benefit greatly if he can determine a part of the master password as well, which might be chosen in a way that knowing part of it makes guessing the whole password quite easy.

[26] *Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, John C Mitchell, "Stronger Password Authentication Using Browser Extensions," Proceedings of the 14th Usenix Security Symposium, 2005, http://www.usenix.org/events/sec05/tech/ross.html.*

[27] *J. A. Halderman, B. Waters and E. W. Felten, "A convenient method for securely managing passwords," WWW '05: Proceedings of the 14th international conference on World Wide Web, 2005, pp 471-479 http://www2005.org/cdrom/contents.htm.*

[28] *M. Abadi, K. Bharat and J. Marais, "System and method for generating unique passwords," 1997, US Patent #6141760*

http://www.cs.auc.dk/~luca/PA-WG/resume-wg-abadi.pdf.

[29] *See references at footnotes 36 and 37.*

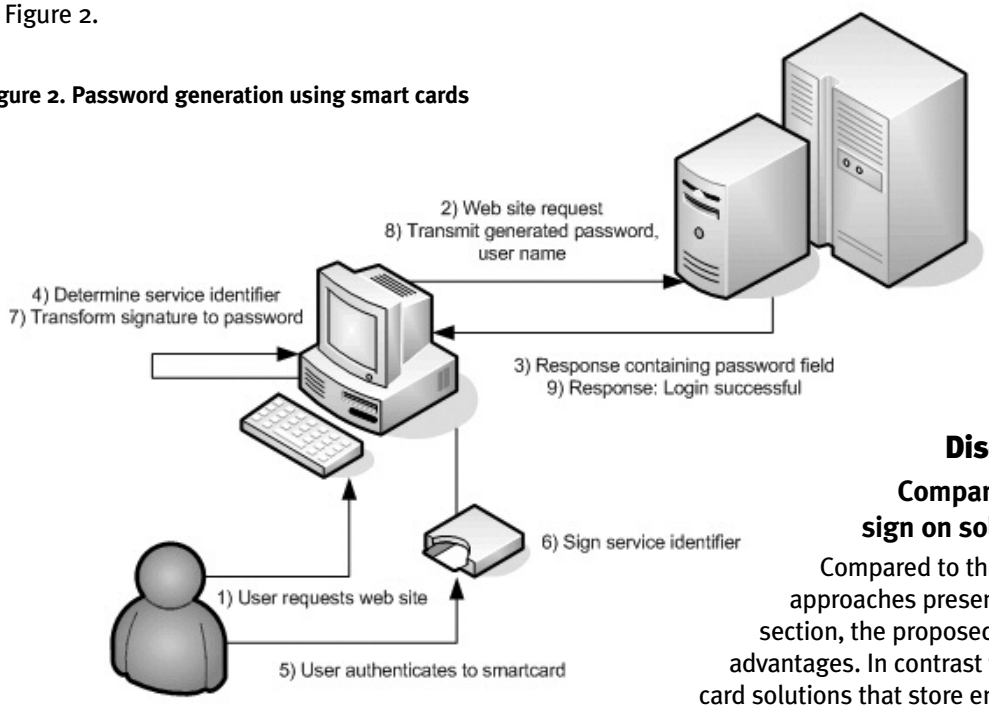
[30] *M. Abadi, K. Bharat and J. Marais, "System and method for generating unique passwords," 1997, US Patent #6141760.*

Digital signatures

Like hash functions, digital signatures can be used to generate strong service passwords for the user. Unlike hash functions, digital signatures cannot be forged, meaning that an attacker cannot produce the user's signature for any text if they do not have the secret key, even if the attacker has obtained the user's public key and several examples of signed messages. The aim is to translate this guarantee to passwords: an attacker should not be able to compute any of the user's passwords without knowing the secret key stored on the smartcard, even if the attacker knows the user's passwords for several other accounts. Towards this end, the general password generation procedure structure outlined above is commended, using digital signatures for the combination step.

To illustrate the process, the following section will give a description of an application of this technique to a web surfing scenario. The whole process is illustrated in Figure 2.

Figure 2. Password generation using smart cards



When the user needs to authenticate to an e-commerce site (1-3), the local system first derives the service identifier from the available context information (4) e.g., a browser plug-in reads out the URL of the target site and the contents of the login name field. The user authenticates to the smart card using the PIN, thus unlocking the private signature key (5). The service identifier for the relevant account is then signed by the signature card using the private key, producing a digital signature (6). The resulting value is encoded as a password (7) and transmitted to the service provider requiring authentication, along with the user's login name (8). The user is then permitted to gain access to the protected resources (9).

One advantage of this approach is that the central secret – the user's private key - is actually stored on the smart card and not directly dependent upon a password chosen by the user. Guessing the PIN will only allow access to this key if the attacker is also in possession of the token (or a cloned version of it). Furthermore, the passwords derived from the signature links the user's identity to using the service. The signature, encoded as a password, may be verified by the service provider using the user's public key. To accomplish this, the service provider first decodes the password to the original signature, and then follows the usual verification procedure.

Obviously, this is only possible if reversible encoding schemes are used. Of course, signatures in this scenario are not linked to individual transactions. This is due to the fact that the widely deployed password systems do not perform user authentication on a transaction level.

Discussion

Comparison to current single sign on solutions

Compared to the conventional approaches presented in the previous section, the proposed solution offers several advantages. In contrast to conventional smart card solutions that store encrypted passwords on the token, this proposal can be deployed on top of an already existing signature card infrastructure, thus limiting costs for the user and also the amount of authentication tokens the user has to manage. The card is portable but it is – in many cases, for example where signature cards are deployed as part of e-government initiatives - not obvious that it is used as a SSO token, so the security risks of portability are partially mitigated. Using the SSO system does not require trust towards any third parties, as opposed to systems based

on an authentication proxy or similar architecture. The authentication secret is only handled by the user and the service, with the central authentication secret remaining on the user side – more specifically, on the token - at all times.

Additionally, this system does not require a specific interface on the server side. This saves implementation costs for the service provider in comparison to a standardized SSO system or a PKI. The system may even work together with services that are completely unaware of its existence. It allows for the use of a simple password mechanism on the service side, which should keep implementation costs and reduce the barriers for new users at a minimum level. The system offers an alternative to hash functions for the purpose of generating passwords on the fly. In addition to the capabilities of hash function based systems, the implementation takes full advantage of the strengths of smart card based two-factor authentication. The portability and convenience of this solution can be further enhanced by using mobile qualified electronic signatures.[31]

Contribution to the adoption of qualified electronic signatures

It is proposed that an application can be made for qualified electronic signatures that enables citizens to authenticate themselves at all e-commerce websites, regardless of whether these websites accept or use electronic signatures. Therefore, the usage of qualified electronic signatures is no longer dependent on the cooperation and acceptance of e-commerce vendors. Since the proposed solution can be used with any web site that requires authentication, it has the potential to be used frequently. It uses infrastructure deployed by some European countries and offers several advantages compared to current single sign on solutions.

The user can employ the solution for password management, which is an everyday task. This in turn might ameliorate the acceptance of digital signatures, leading to a wider usage of signature cards and readers and to a more secure, multi-factor authentication infrastructure. However, it will probably not be the "killer application" for digital signatures. Users have to understand the benefit of generating strong passwords. This is further complicated by the tendency of users to believe that negative events are less likely to happen to them than to others, and that positive events are more likely to happen to them than others.[32] On the other hand, users are frustrated by the challenge of managing vast numbers of passwords and will probably also appreciate the additional protection of the central secret.

Conclusion

This article proposes a method that allows qualified electronic signatures to be used with password authentication systems without any modification at the service side. This might help to break the deadlock between missing applications and digital signatures. It is an application for an infrastructure that is already deployed, and that can be used frequently by the card owners. Therefore, the number of transactions based on digital signatures might increase, and citizens can become familiar with signature cards, which could speed up the diffusion of digital signatures, unlocking the potential to transfer e-government processes from paper to electronic medium.

Heiko Roßnagel is Research Associate at the Chair of Mobile Commerce and Multilateral Security, Johann Wolfgang Goethe - University of Frankfurt/Main, Germany. His research interests are in the area of information systems security, with a special interest in electronic signatures.

heiko.rossnagel@m-lehrstuhl.de

Jan Zibuschka is Research Associate at the Chair of Mobile Commerce and Multilateral Security, Johann Wolfgang Goethe - University of Frankfurt/Main, Germany. His research interests are in the area of information systems security, with special interest in the use of passwords in authentication systems.

jan.zibuschka@m-lehrstuhl.de
http://www.m-lehrstuhl.de

[31] *H. Roßnagel, "Mobile Signatures and Certification on Demand," in S. K. Katsikas, S. Gritzalis and J. Lopez (Eds.), Public Key Infrastructures, (Springer, Berlin Heidelberg, 2004), pp 274-286.*

[32] *H. Rhee, Y. U. Ryu,C. Kim, "I Am Fine But You Are Not: Optimistic Bias and Illusion of Control on Information Security," Proceedings of the Twenty-Sixth International Conference on Information Systems (ICIS 2005), 2005, pp. 381-394; http://aisel.isworld.org/article.asp?Subject_ID=391&Publication_ID=57.*