Polish Cards 2012 almanac
Polish Card Industry Almanac: Regional Information, Global Perspective

This article will appear in Polish Cards 2012 Almanac, published by Medien Service, organizer of Central European Electronic Card conference, and will have its premiere on 30.11-01.12. 2011, during this event. More information can be found at www.cardsalmanach.eu and www.conkarta.pl

Lightweight electronic signature certificate

PKI 2.0

The enacted over a decade ago directive on electronic signature [1]specified a paradigm binding in electronic signature technology that a certificate should identify the signer (regardless whether it is a natural or legal person). It implies that if signature is verified with certificate, it unambiguously indicates signer. In this article I would like to discuss whether this paradigm, restricted with technology of Public Key Infrastructure (PKI) should remain unchanged in new wording of the directive and Polish legislation.

Public Key Infrastructure is implemented basing on X.509 certificates, which above all contain the public key associated with signer's private key. In addition, identification data of signer and of certificate issuer as well as certificate validity date have to be included in certificate content. Very often certificates contain additional information, including signer's organization, scope of authorization or maximum transaction value. The purpose of including these pieces of information in certificate is to meet the requirements of signature verification scheme, in which certificate contents constitutes the basis on which its validity can be ascertained.

The above signature mechanism had the advantage of allowing the signatory to create a signature at any time, which verification was based on a static certificate included in the signature itself. Thanks to their contents such certificates provide the verifier with all pieces of information that can be helpful for full verification of validity and value of electronic signature.

Inclusion of many features in a certificate has this basic disadvantage that a change in any of them results in the necessity to invalidate the certificate and to issue a new one. For example: if an employee has a certificate that authorizes him or her to perform some legal activity, change in the scope of this activity means a change in certificate contents - i.e. a new one has to be issued. Because of this disadvantage of certificate based signature already several years ago attribute certificate technology was created, which aims at confirmation of short-term features. However, attribute certificates as mechanisms to support electronic signature were not successful on the market, mainly because they complicated using this mechanism even more.

The requirement that certificate should identify the signer makes it impossible to use electronic signature in a way that we use it daily – as a simple confirmation mechanism, which in itself does not contain any identification attributes . In the light of the above, electronic signature eliminated the possibility to use simplified security mechanisms in electronic transactions, which in many contacts ensured our privacy, e.g. by not disclosing our personal data, e.g. name,surname or the PESEL number, to the other party.

In many electronic transactions that we perform in Internet, disclosing personal data does not seem necessary, because there are more important features: having sufficient means in the account, address or age. Storing this kind of information in certificate is not always possible due to the fact that they change and that signer may not always want to use this information and disclose it in all transactions. Therefore, for example in Poland some public administration employees refuse to use qualified certificate as it discloses their age, coded in PESEL number.

Certificate in PKI is a basis for electronic signature verification; the Directive distinguished qualified certificate from all certificates, stressing that electronic signatures verified with such certificate will have special legal recognition in European Union countries. This approach enforces the requirement that on the certificate issue level it is already known what the electronic signature will be used for and what will be its limitations. It has become a basis for all certification services but also it hampers the development of electronic signature technology and its wider application. The main problem lies in the fact that public key certification in PKI needs to be connected with registration and identification of signer, his explicit commitment to the application of security policy as well as with ensuring proper level of security and guarantees related to this signature.

The signature needs to be more flexible, allowing signature cooperants the possibility to learn, to use various techniques depending on the required security level and to base signature reliance on risk analysis. Electronic signature based on classic certificate does not allow all this, because it requires that application rules and conditions are specified at the beginning of registration. Classic card based qualified signature has only two PIN protections and invalidation - hence it is impossible to add later security features to the signature based on one time passwords or additional elements for transaction authorization.

Being aware of problems of this kind many companies changed the course of action and based electronic signature services on services that create authorization mechanisms for the user and generate electronic signature on their behalf. The most recognized companies in the market DocuSign and EchoSign function this way and enable users easy registration in Internet and creation of electronic signature on this basis and after credit card is confirmed they offer an increase in electronic signature reliance. Even some European Union countries agreed that qualified signatures can be based on services of this kind, which gives rise to controversy related to signer's sole control over the means for electronic signing. On the other hand, it needs to be considered who really has more control over electronic sign: the one who has a cryptographic card with keys or the one who has access to the register of created electronic signature.

In Poland restrictions related to electronic signatures verified with a certificate resulted in a very limited use of them by natural persons to settle their matters. In response to these problems, e.g. mechanism for submitting tax declarations was made available which used data possessed by the signer as signature. Another solution is the possibility to confirm the right to sign a document through specialized service. An example of this mechanism is ePUAP platform, launched for public in July 2011.

If the above mentioned mechanisms pose a limitation or they have insufficient legal recognition it is worth to describe here a mechanism, which would be flexible and allow dynamic adjustment of the signature to current needs of user and market, in which this user functions, at the same time giving the user sole control over the means for creation of an electronic signature. Sole control of signer means application of such

[1] Directive of the European Parliament and of the Council 1999/93/EC as of 13 December 1999 on a Community framework for electronic signatures.

technical means which prevent generation of electronic signature without the conscious action on part of the user.

PKI 2.0

This mechanism consists of application of technologies described in the idea of PKI 2.0, which ensure such division of means for electronic signature creation between signer and service provider that signature can be created only when signer used the means which are only under his control but cannot be used without mechanisms that are controlled by service provider, called Signature Authority. There are several algorithms and technologies which execute PKI 2.0 concept. There are for example algorithm with mediator, discrete logarithm signature with split key, technologies based on a remote cryptographic card management and one based on limited public key certificate and attribute certificates.

PKI 2.0 electronic signature is created by two independent parties which results in the fact that signer controls the signature not only by having private key but also through services made available by service provider - in the same way in which banks offer access to bank accounts via Internet. It creates the basic advantage of the fact that data included in signature content can be confirmed by Signature Authority at the moment of signing, controlled with additional technical means (e.g. mobile phone) and verified by a central registration of signatures. PKI 2.0 certificate can be limited only to confirming that signature was created in an environment controlled by Signature Authority and using means (private key) in possession of signer (without revealing the identity features of the signatory) . On the other hand, all pieces of information which identify the user, information about their authorizations and restrictions will be verified during signing process by Signature Authority, in particular in form of valid only at the time of signing, short-term attribute certificates attached to the signature.

PKI 2.0 life cycle and use can be the following:

1. User registers in Signature Authority a service and defines basic mechanisms for management of his/her signatures. Registration may be confirmed by submitting one's e-mail address or mobile phone number.

2. User generates keys in his or her environment (TPM on computer or mobile phone, cryptographic card, file). Signature Authority issues and provides the user with certificate containing public key but does not include signer identification data.

3. User can use this form of electronic signature for various activities. Signatures can confirm information which was confirmed during registration process, e.g. e-mail address or mobile phone number. This confirmation is carried out only on signer's request.

4. If it is necessary to use advanced electronic signature for some legal actions , beginning of using such signature requires confirmation of signer's identification data. Signature Authority can make it basing on bank account statement or credit card payment. Signature marked as advanced during signing contains identification information about signer within the scope specified by him or her. Signer still can use simpler signatures which do not identify him or her.

5. If some legal activity requires financial guarantee, Signature Authority can act as trusted third party, which confirms financial means blocked on credit card.

6. If some activity requires a signature with trust attribute of public administration, there can be executed a suitable mechanism for that.

7. Signer, whose organization is registered in Signature Authority, can have his or her authorizations given dynamically by this organization.

8. Signer, who is obliged to use qualified signature confirms his or her identity and accepts the certification policy as before (e.g. by currier), but always uses the same means as for electronic signing, defining only additional authorization parameters for qualified signature, e.g. based on one time password authentication.

The example described above allows flexible use of electronic signature depending on one's needs and basing on Signature Authority service. It also allows the user to familiarize with tools and use mechanisms which are optimal to the needs. Only the use of qualified signature may require contact with the registration point but all other kinds of signature can be available to the signer without the necessity to leave home.

The requirement for this approach is to minimize the amount of information contained in the certificate and to remove identification data. All additional confirmations are transferred to attribute area (which may take the form of attribute certificates) in the moment when Signature Authority generates the electronic signature. Application of these mechanisms regardless of used algorithm allows to offer many added services and to create a wider scope of signature application.

In the light of nearing amendment of the Directive it is necessary to take strategic action related to the question whether mechanisms of certificate based electronic signature created clearly for the needs of public administration is sufficient for the needs of business development and application of various authentication mechanisms in Internet. The change in approach from providing certification services to providing services related to electronic signature requires a wider consideration of the question whether signature verification based on certificate which identifies the signer is the only correct solution.

Michał Tabor

Graduate of the University of Warsaw - Faculty of Mathematics, Informatics and Mechanics, Institute of Informatics. *Holder of CISSP certificate. Expert on electronic signature, electronic administration and security of IT systems. In 2002-2006 manager of Signet TP Internet Certification Centre, with responsibility for preparation of this entity for providing qualified certification services and WebTrsut certification. Author of specialist publications in the area of electronic documents and electronic signature. Architect of authentication mechanisms for users of public administration systems in ePUAP, author of technical solution of tax declaration authentication which are submitted without the necessity of adding a secure electronic signature, originator of the idea of electronic signature mechanisms confirmed with trusted profile. Author of PKI 2.0 concept - service model for electronic signature.*

http://pki2.eu