THE PLACE AND ROLES OF THE CERTIFICATION AUTHORITY

Ing. Julius Lintner, RNDr. František Kaščák[1]

The development of electronic commerce on the Internet and the viability of any legal act carried out by electronic means is limited by the existence of adequate security guarantees ensuring that deals or legal acts can be implemented to their full extent.

The certification authority has an irreplaceable role in the information society, especially in the area of permanent provision of such security guarantees in the framework of constructing the Public Key Infrastructure (PKI). Security guarantees have to form the framework for application of the legally determined conditions for enforceability of the law for any participants in business or other legal acts carried out by electronic means. The aim of this paper is to point out tasks facing the certification authorities in the stage of building an information society.

Starting points for Public Key Infrastructure

Asymmetrical Ciphering

In so-called cryptography of a public key (or asymmetrical ciphering), the ciphering key is different from the deciphering key. There is an unambiguous link between the two keys in this case. This means that one specific ciphering key has only one specific deciphering key, and the value of the second key cannot easily be worked out from knowledge of the other. Protection of the ciphering (so-called public) key in a safe place is most important for security in asymmetrical ciphering. The deciphering (so-called public) key can appropriately be displayed in a publicly accessible place. The reasons for these statements are outlined in the following text.

One of the important possibilities for using the principles of asymmetrical ciphering is the possibility of preserving the principle of confidentiality in electronic communications, that is the possibility to send information (text, data), which can only be read by the person it is addressed to. This can be achieved by ciphering the original text with his public key. Such a ciphered text can be deciphered only using his private key, which should be under his exclusive control.

Any change, deliberate or accidental, in using these keys may have the result that the authorized recipient of the information or owner of the appropriate private key cannot read the ciphered data. In the case of bad intentions, important data may be deciphered only by the person who changed the key (the so-called attacker) or the recipient of information will regard somebody different as its author.

So-called certification authorities (CA) are formed to deal with such negative situations as frauds and mistakes. They create an environment in which they should not occur. They can be compared to verifiers of identity (for example, notaries or registry offices, which issue certificates or documents confirming the connection between the identity of the user and his public key.

The Use of Asymmetrical Ciphering in Practice

The principles of asymmetrical ciphering are used in the idea of the electronic signature. A file, data or text in electronic form with an unambiguously determined "mark" (so-called hash, mathematical result of the so-called hash function) ciphered by the private key of the author can be compared to a document signed by the hand of the author. The hand written signature of the author is replaced by the mark (hash) ciphered by the private key of the author.

In the case of an electronic document signed by an electronic signature, it is possible to attempt to change it (modification, misuse). In this case, cryptographic methods and related applications make it possible, not only to unambiguously identify who produced the text or who did not produce it, but also whether the text was modified by an unauthorized person from the time it was written or signed by the author until it was delivered to the recipient. These claims derive from the mathematically provable fact that if we decipher an electronic signature (that is hash of

[1] Ing. Julius Lintner (1958) is project manager of the society Ditec a.s. in which he works on preparing a commercial public certification authority and other projects for the PKI.

RNDr. František Kaščák (1961) is a member of the board of the company AmoNet a.s., which operates the payment portal Monex, constructed for the use of electronic signatures.

Both authors participated in work of the expert group of the Slovak information society, which proposed the Act on electronic signature, submitted to parliament in April 2001 as a private member's bill and approved by the plenary session of parliament on 15th March 2002.

the original text ciphered by the private key of the author) with the help of the public key of the author, the result of this operation will agree with the "hash" of the delivered text only if the text is exactly the same at the beginning and end of its journey, and if the private ciphering key and public deciphering key belong to each other.

It is clear that such a procedure is not sufficient to determine precisely what was changed in the text, if data were modified on the route from the author to the recipient, but this is not the purpose of introducing the electronic signature.

Claims about the security of the electronic signature, based on the principles of asymmetrical ciphering algorithms, and the potential possibility of its wide application depend on the fulfilment of the two following pre-conditions. There must be sufficient certainty that the published (public) key really belongs to the person who created the information or data or is the author of the electronically signed information (who signed the data using his private key). There must also be certainty of secure storage of the private key and its protection against unauthorized use, that is against its misuse by unauthorized use by a person other than its owner.

The Certification Authorities and their Place in the PKI

The Main Functions of Certification Authorities

The certification authority and its functioning can be very simply described as an institution, which provides the certificates used for identification of the owner of the public ciphering key. The certificate is an electronic document signed by the private key of the CA. It contains the public key and personal data of the holder of the certificate. By its signature on the certificate, the CA confirms that the owner of the public key contained in the certificate is really the person mentioned in the specifications of the certificate. Thus the certificate helps to prevent misuse or faking of the key with the intention of pretending to be somebody different.

So that a certificate can be trusted, the CA must prove that it deserves trust. This means that, among other things, it must perform its activity openly, publish and especially observe its certification policy or rules for issuing certificates (the so-called Certification Practice Statement), its operational rules and so on. Certificates produced by a trustworthy CA cannot easily be falsified. They must be obtained by secure procedures, and must be designed so that they cannot be misused. Issued certificates must be resistant to possible attack. The procedures for their use must provide a sufficient degree of trustworthiness and a simple method of verifying the authenticity of these certificates.

The CA should be a trustworthy third party, which "connects" the public key with the identity of the user (his identity is verified according to its internal procedures). The CA uses its own pair of keys (private and public) to confirm the identity of its clients. The certificate containing the public key of the client is signed with the private key of the CA.

Certification Policy

Apart from signing of the public keys of applicants for issuing of certificates or publication of data about issued certificates, the CA can also perform further supplementary activity, connected with the use of certificates. All these activities, together with the rules directing them, form the certification policy of the given CA. In accordance with its certification policy, a CA may issue certificates of various levels according to the degree of trustworthiness, for example:

- A certificate without verification of the identity of the applicant, but not providing any guarantee of the identity of the user. It may serve for testing the appropriateness of use of the certificate for a specific application and so on. The fact that the certificate has a limited range of application and trustworthiness must be mentioned on the certificate and must be clearly recognizable to the recipient. These certificates are usually not paid. They are also available from various commercial CA.
- A certificate with verified identity of the applicant - usually for payment. A personal visit to the office of the CA or its contractual partner is necessary when obtaining it. After the client has filled in the appropriate forms and the data has been verified, he will receive a valid certificate. As in the case of other personal documents, the validity of the certificate has a time limit. Before it expires, the CA can be asked for a renewal. This does not require the personal participation of the applicant. It is enough to fill in the appropriate electronically signed form.

In both cases, a way must exist to add to the application the public key of the applicant for a certificate. There must also be a way to verify that the client has a private key corresponding to the public key, which is added to the application for a certificate. This verification must be done so that the private key of the client cannot be revealed in any situation.

The Structure of Certification Authorities

Certification authorities can have various structures, and in connection with this various levels of trustworthiness. Trustworthiness can be mutually confirmed, so that certificates issued by one CA can be verified by another CA. This method is appropriate mainly for communication on the Internet, which is not restricted by the frontiers of states and the existence of locally appropriate CAs.

Since we can assume that the technological demands of establishing a trustworthy certification authority will be very high, we expect that only a small number of CAs, at most two or three, will be established in Slovakia. This clearly applies in the case of a so-called open system or of a so-called public certification authority. Apart from them, there will be an uncertain number of certification authorities in so-called closed systems, which will provide their services to a limited range of users, either clients of one company, or within a limited LAN or WAN or otherwise for the defined internal needs of the owner. These specific certification authorities can also provide specific services, which will go beyond the services and obligations defined in legislation. They can go beyond the framework of the demands of the law or they tighten up some security demands of their certificates or some of the legally defined obligations for the public CA. They do not have to be fully secured in the area of their activity.

The Place of Registration Authorities in the PKI

In the event of the existence of a smaller number of public certification authorities, the accessibility of their services will be important for the clients. For the lower level of certificates, which do not require the personal presence of the client for verification of identity or if verification of identity is not done, accessibility of the service is guaranteed by access through the Internet.

The situation in the area of higher classes of certificate will be different. Since the personal presence of the applicant is necessary to verify his identity, the CA will delegate some of its functions to other bodies (registration authorities - RA), which have offices closer to the client. This will especially concern functions connected with the collection of primary data from clients and with verification of their identity according to the rules valid in a given CA, or deriving from legislative norms. The registration authorities must provide the same level of security as the CA itself, especially from the point of view of the protection of the data of clients, as well as from the point of view of guaranteeing protection of the ciphering keys (of clients and the CA) and certificates.

Certificates and their Use

After successful verification of the necessary information, the CA will give the client a certificate. This certificate can be provided in various formats for various programmes working according to different norms, or they can be placed on different media.

The client can use the certificate as evidence that he personally created the electronic signature used to sign a document (file, e-mail). The usual way of using a personal certificate (issued to a person not to technical equipment) results from its varied purpose. One of the usual methods is that the client wants to electronically sign a document (commercial document, order) with the private key corresponding to the public key for which the certificate has been issued. Then he will send it, perhaps by e-mail to a commercial partner. After signing the document, he can add his certificate to it. The recipient of the document can use the public key from the certificate, or he can verify the validity of the certificate with the certification authority, which issued it.

Verification of the Validity of Certificates

The validity of a certificate can be verified in two ways. The first method assumes that the recipient of a document will send a request to verify the validity of the certificate to the appropriate CA. The reply of the CA will show whether the certificate is valid and in order, or whether it is not for any reason (the certificate could have expired, be invalid, not existing, awaiting processing and so on). The use of this method is appropriate if the reply of the CA is prompt and precisely defined in time. Implementation of this procedure is technically more demanding and it is expected to be a paid service.

The second method starts from the idea of so-called negation. This means that if we can exclude that the given certificate is negative (at the moment of need, its use was not revoked, it is not invalid or non-existent, awaiting processing and so on) and there is no other state, in which it could be found, then it must be valid. Use of this method is represented in the existence of a so-called Certificate Revocation List (CRL). It includes certificates, which are unusable for any reason for proving the trustworthiness of the given public key of the client to whom it was issued. These lists are issued periodically and contain data about the precise time of their issue.

Revocation of the Validity of a Certificate

Every client has the right to demand the early revocation of his certificate, if he gets the impression that his private key was misused and that it can no longer be trustworthily used. There may be reasons entitling the CA to end the validity of one of its certificates early. The CA has worked out its rules, according to which it deals with applications to revoke certificates. Every change of state of the certificate must be correctly interpreted and the appropriate action implemented on this basis.

Guaranteeing the security of information by both methods of verification of the validity of a certificate is another of the critical functions of the correct functioning of any certification authority, which wants to be trustworthy. In both methods, time was an important part of the data, which the CA must give to the client, whether from the point of view of creating (signing, sending and so on) an electronic document, or for the purpose of verifying various facts connected with such a document. In the case of signing an electronic document, it can be essential to know whether the certificate of the signing person was valid at a certain time (for example at the time of signing the document or at the time of verifying the validity of the signature), that is whether the signature is valid. Therefore, the so-called time stamp service is one of the services provided by a CA.

The Main Roles of the Certification Authorities in an Information Society

The aim of the preceding brief summary of terms was also to show that the construction of a functional and especially a secure public key infrastructure (PKI) is highly dependent on the degree and level of security, which the certification authority can guarantee, and on the characteristics and extent of the functions the CA is able to provide for its clients. The degree of fulfilment of these aspects also contributes to the potential possibilities for development of secure electronic communication in the given region and the possibilities to widen the applications on the basis of these principles.

Further potential possibilities for the development of secure communication depend on the legal environment connected with this area in the given region or country. It is a matter of specific legislative norms determining the basic framework for development in the given area and prescribing what is possible or what is not permitted in a particular area, with regard for the solution of this problem in other countries and the recommendations of international organizations.

The Strategic Importance of Certification Authorities

One of the most important positive features of this area of information technology is an effort to substantially raise the level of security in the existing kinds of electronic communication and the creation of conditions for the development of such secure communication in other areas. Achievement of the necessary level of security for any communication can also contribute to the spread of new applications into different areas of the life of society and their consistent use to raise and improve the quality of life of the inhabitants. The principles of cryptography based on asymmetrical ciphering are considered sufficiently secure at present, for a PKI system based on their use to be considered stable.

Positive expressions about the possibility of secure electronic communication with the public administration and the state in general are beginning to appear in the statements of competent figures close to the problem of electronic signatures. This possibility should guarantee not only a simplification of contact between the citizen and the state in most of its forms, but also improvement of the links between the citizen and the state (for example in tax administration, referenda, elections and so on.) The possibilities of new comprehensive applications based on secure communications between citizens in the health service or between the elements of it (hospitals, pharmacies, insurance companies, medical suppliers and others), are interesting. The advantages of secure electronic communication in business, especially in its electronic form, are clear. The most rapid return on investment is expected here.

Protection of the Private Key – the Basis for Security of the System

As we already said, protection against misuse of the private key of each user is considered most important in the PKI system. The need for protection is essentially the same, in the case of the private key of any participant in the PKI, whether a private person, server or the certification authority itself. There is a substantial difference in the potential damage, which can result from misuse of the private key of individual participants. Misuse of the private key of a private person can do harm connected with the activity of this person, and can be very serious, depending on his activity. In the case of misuse of the private key of a server belonging to a particular company or organization, the harm may be many times greater, since various other participants may use this server. Misuse of the private key of the CA can have catastrophic results for the whole PKI. In an extreme case it can affect the level of the state and its economic or political institutions. The extent of the catastrophe depends on the degree of development of the information society, the applications used and the penetration of certificates from the given CA in society.

The Roles of Certification Authorities in the PKI

The main role of the CA is to become a trustworthy third party, which can permanently secure protection of confidential information against any misuse, by means of its technical equipment, operational rules and internal security attributes. It must be able to provide services compatible with other existing certification authorities throughout the world, especially because of the present internationalisation of business and electronic communication.

Users of the service of a certification authority must have permanent security that the reliability of the data and services of the CA and its products is not threatened, and that they are fully under the control of the CA. The security and reliability of the CA is not only a question of the level of its hardware and software, but especially of its internal operational rules and procedures during the issuing of certificates and the administration of products and in it internal personnel reliability.

The construction of a CA is not a static process, which ends with the completion of its hardware and software and putting into routine operation. At present, the process of building up a good name is only beginning. However, it is a continual process with the certification authority and the data of its certificates and clients on one side, and an unknown number of attackers of various types, levels, degrees of knowledge, possibilities and interests on the other.