International Working Group
on Data Protection
in Telecommunications

Working Paper on

Data protection aspects of digital certificates and public-key infrastructures

adopted at the 30th meeting of the Working Group on 28 August 2001 in Berlin

Parties that communicate with each other-whether by electronic means or otherwise-may have all sorts of requirements for the security and reliability of their exchange of information. Important issues include identification, authentication, authorization, confidentiality, integrity and non-repudiation.

Cryptography is an almost inevitable technique for guaranteeing these characteristics in an open electronic environment. A technique that is rapidly gaining in popularity is *public-key cryptography*. This technique uses two different keys, one of which is used for encrypting messages and the other for decrypting them. One of these two keys, the private key, the owner must keep a secret, the other one he makes public. Public-key cryptography can be employed in two ways. When the encryption key is made public, everyone can use this key to create an encrypted message that only the owner of the corresponding private key can decrypt. When on the other hand the decryption key is made public, it can serve to authenticate the source of an encrypted message: only the owner of the corresponding private key could have encrypted the message. This last application is known as a *digital signature*.

The use of public-key cryptography requires that the key be linked in a reliable way to the identity or other attributes of the key holder. The infrastructure required to facilitate this is known as a *public-key infrastructure* (PKI). A *trusted third party* (TTP) guarantees this link in a PKI[1]. The TTP does so by using a digital signature itself. A *digital certificate* is any digitally signed document. Digital certificates are most commonly issued and digitally signed by a TTP, and then link a public key to attributes of the key holder.

At least three major data protection issues are connected with the use of public PKI's:

A. naming and identity, pseudonimity, anonymity;
B. dissemination of PKI information;
C. lawful access.

A Naming and identity, pseudonimity, anonymity

It is usually desirable that the identity of a digital signer is known. This does not mean, however, that this identity must also be stated on the certificate. It is often sufficient that it can be traced if necessary, for instance in the case of fraud. Since the user of a pseudonymous certificate has the appar-

[1] European directive 99/93/EC has introduced the term "certification service provider" for TTP's that offer all or some of the services necessary to provide this guarantee.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

ent intention to keep his identity hidden, it must be very clear exactly which circumstances are sufficient grounds for nonetheless providing these data to others.

Models for 'PET[2] certificates', which protect privacy by using pseudonyms, among other things, deserve more attention than they have received so far. This would help public-key cryptography to realise its potential role as an important privacy-enhancing technology.

Traditional identity data such as name, address, and city of residence are an insufficient basis for reliably linking personal data. Such linking benefits the quality of the data, but may also entail great privacy threats. For this reason the introduction of nationally or even globally unique identifiers to that end is undesirable. Sectoral or chain-based identifiers may provide an alternative solution. Public keys or, even more dangerous, biometric templates, must be prevented from becoming alternative unique identifiers.

B Dissemination of PKI information

Within a PKI it is necessary to disseminate different kinds of information. The most important ones are certificate information and revocation information.

The most popular way of disseminating certificates is through a repository. This should only be done with the permission of the certificate owner, who must also have a real alternative. The permission must be given voluntarily and needs to be based on correct, clear and complete information. When certificates are publicly accessible on a large scale, this opens up all sorts of possibilities for building up detailed profiles. For this reason private dissemination, where the certificate holder himself is responsible for delivering the certificate to a verifying party, deserves serious attention as an alternative.

Revocation information that is disseminated must not contain more data than is necessary, for instance a serial number rather than the entire revoked certificate.

PKI information is disseminated for a certain purpose. Further processing of the information must be compatible with this purpose. This also holds for dissemination by means of a repository; the repository should be designed accordingly.

C Lawful access

Different parties may claim access to data available at TTP's. The desired information may be the identity of the owner of a pseudonymous certificate, keys for decrypting encrypted messages or files, or the messages or files themselves. Law enforcement and intelligence agencies tend to have several specific legal powers in this area. Others usually have lawful access on the basis of a more general right to certain information. The Working Group advocates an approach which balances the investigation needs of governments and their citizens' right to privacy.

The customer's trust is a *conditio sine qua non* for TTP's. It is therefore fashionable in TTP circles to pay lip service to the principles of privacy protection. Unfortunately this rarely goes beyond general remarks along the lines of 'TTP's of course adhere to privacy laws'. Guaranteeing adequate safeguards for personal privacy however requires this aspect to be taken into account from the earliest stages of the designing phase of technologies and infrastructures. If this is done, TTP services in general and digital certificates in particular can provide an important contribution to privacy protection for electronic communication and transactions.

[2] PET = privacy-enhancing technology.

The Working Group therefore makes the following recommendations.

1. Pseudonymous (or even anonymous) certificates are preferable to identity certificates in all cases where identification of the certificate holder is not required in view of the specific purpose for which the certificate is being used. TTP's should contribute actively to the development of technologies and infrastructures allowing for the widest possible use of such certificates, whether within the framework of the X.509 standard or not. In situations where the use of identity certificates cannot be avoided, anonymous or pseudonymous use should be made of such certificates whenever possible.

2. The use of nationally or even globally unique identifiers should be avoided in view of its serious privacy risks. There are alternative possibilities for sectoral or chain-based numbers. Information exchanges based on these should be surrounded with sufficient safeguards. PKI's should be designed in such a way - e.g. by allowing for multiple, short-lived and/or role-based certificates -that certificate numbers, public keys or biometrical templates will not turn into alternative unique identifiers.

3. Public certificate directories should be designed as much as possible in such a way as to allow only those queries that are necessary in view of the purpose of the directory. Individuals should have the choice not to be included in such directories, i.e. private dissemination of certificates must be available to the certificate holder as a real alternative.

4. TTP's may only divulge the identity that goes with a pseudonym in the case of a legal obligation based on a pressing social need or with the express permission of the certificate holder.

5. Powers of investigation services and intelligence services with respect to obtaining lawful access should be in balance with the protection of fundamental rights and freedoms and in particular personal data.