



PKI support in Windows 2000 and Windows Server 2003

Secorvo White Paper

Version 2.01e
20.01.2004

Holger Mack

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet <http://www.secorvo.de>

Table of contents

1 Foreword to version 2	6
2 Abstract	7
3 Introduction	9
4 PKI Support in Windows 2000/2003/XP	11
5 Architecture	13
6 Criteria for comparison	15
6.1 Trust model	15
6.1.1 Hierarchical model	15
6.1.2 Cross-certification	15
6.1.3 Other procedures	16
6.2 Support of standards	17
6.2.1 Certificates	17
6.2.2 Certificate revocation lists	19
6.2.3 Exchange formats	20
6.3 Directory support	20
6.4 Flexibility	20
6.5 Registration and renewal	21
6.5.1 Enterprise CA	21
6.5.2 Stand-Alone CA	22
6.6 Administration	22
6.7 Special security measures (CA)	25
7 Other features	26
7.1 Validity model	26
7.2 Integration with other products	26
7.3 Key management	27
8 Mixed Windows 2000 & 2003 environments	28
9 Additional products	29
10 Practical experience	30
10.1 Interoperability	30
10.2 Linking directory services	30
11 Strengths and weaknesses	32
11.1 Windows 2000	32
11.2 Windows 2003	33

12 Further developments.....	34
13 Bibliography	35

Acronyms

ADS	Active Directory Service
ADSI	Active Directory Service Interface
AIA	Authority Information Access
ANSI	American National Standard Institute
CA	Certification Authority
CDP	Certificate Distribution Point
COM	Common Object Model
CRL	Certificate Revocation List
CryptoAPI	Cryptographic Application Programming Interface
CSP	Cryptographic Service Provider
CTL	Certificate Trust Lists
DB	Database
DLL	Dynamic Link Libraries
DNS	Domain Name Service
EFS	Encrypting File System
HSM	Hardware Security Modulen
IE	Internet Explorer
IETF	Internet Engineering Task Force
IIS	Internet Information Server
IPSec	Internet Protocol Security
ISO	Internation Standardisation Organisation
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MMC	Management Console
NT	New Technology
OCSP	Online Certificate Status Protocol
PC/SC	Personal Computer/Smartcard
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	X.509-based Public Key Infrastructure
RFC	Request for Comment
SDK	Software Development Kit

SSL	Secure Socket Layer
TLS	Transport Layer Security
XML	Extensible Markup Language
XP	Experience

History

Version	Date	Change	Author
1.1	29.11.01	First published version	Holger Mack
2.0	10.04.03	Second edited version, expanded to include Windows Server 2003 PKI	Holger Mack
2.01	08.05.03	Proof-reading	Holger Mack
2.01e	20.01.04	English translation	

1 Foreword to version 2

Judging by the number of times the first version of this White Paper has been downloaded in the year since it was published, and the positive reaction to its contents, there is considerable interest in the Windows PKI. So much progress has been made in this area since the White Paper was last published that it now seems worthwhile to produce a new, revised version.

For a start, a year's experience with the Windows 2000 CA has made it possible to refine or expand upon some of the information in the first White Paper. Secondly, a new version is about to appear, in the shape of the PKI integrated in Windows Server 2003 (previously .NET Server), for which a number of improvements in the PKI functionality have been heralded. When this White Paper (i.e. the original German version) went to press, the final version of Windows Server 2003 (still under the name .NET) was not yet available. The information and tests refer to Release Candidate (RC) 1 of the Enterprise Server version. It has since been announced that there will be an RC2, but Microsoft has said that there will be no changes to the PKI functionality. It is unlikely that any significant changes will appear in the final version, but this cannot be guaranteed.

Although Windows 2000 has already been on the market for over two years and its successor is about to be released, many companies have only just updated their network server to Windows 2000, or are even still in the process of implementing it. This is due to the considerable changes required (e.g. Active Directory server) when converting from Windows NT to Windows 2000 and the substantial preparation involved. For many companies, Windows Server 2003 is not yet an issue, and Windows 2000 will continue to play a significant role on the server side for some time to come.

However, on the client side, many companies have missed out Windows 2000 and are installing Windows XP, which has already been on the market for some time. This White Paper is thus structured in such a way that it is of benefit to users of all current Windows versions (i.e. Windows 2000, XP, 2003). It is hoped that this will enable every reader to find the information relevant to his or her environment and combination of versions used. The White Paper aims to provide an insight into the implications of the differences between the various versions, so that, for example, users are better placed to decide whether it is worth waiting for the 2003 version or whether the planned functions can be carried out with the Windows 2000 CA. An extra chapter examines how hybrid forms, i.e. networks not based solely on Windows 2000 or Windows .NET, perform with regard to PKI functionality and whether an update is possible.

This approach is simplified by the fact that there have been no fundamental changes to the architecture of the Windows PKI, and so the structure of the document has remained largely unchanged.

2 Abstract

Microsoft has made public key infrastructure (PKI) functionality a core component of its security architecture since Windows 2000. While this is undoubtedly an important step, the focus of the PKI functionality is clearly on integrated support in a Microsoft environment. Microsoft also provides some neat solutions (e.g. for distributing trustworthy CA certificates) to issues that can often only be resolved with a great deal of difficulty in other environments.

Microsoft follows a similar path to that of Lotus Notes a few years ago, with the difference that Microsoft's PKI is more open and in greater conformity with standards than the solution offered by Lotus Notes.¹ This support of standards makes it possible to use the functionality outside a pure Windows environment or to integrate it with other environments and applications. However, it is essential to check closely that all the requirements are met to ensure this kind of support.

From a critical point of view, it has to be said that the PKI functionality available in Windows 2000 is not yet particularly advanced. The development of other CA products has demonstrated that it can take some time to produce an advanced PKI product. The main problems are the lack of flexibility and functionality, particularly when working outside a Windows 2000 environment.

New versions of the Microsoft operating system, i.e. Windows 2003 and Windows XP, are now available on the market and have enhanced PKI functionality. This demonstrates that PKI is an important element of Microsoft's future strategy. Considerable progress has been made in the area of PKI functionality in Windows Server 2003. For example, some important functions that were missing from Windows 2000 have been implemented here. However, the focus is still on issuing certificates for components (i.e. users, computers) in a Windows 2000 domain; the functionality for issuing certificates outside the Windows environment continues to be limited.

Furthermore, certain functions, such as the automatic loading of trustworthy certificates in the background, need to be examined more closely to ensure that there is no risk that they could enable a hacker to use the PKI functionality to prepare more extensive attacks. Since PKI is to play a significant role in the future Microsoft strategy (e.g. .NET architecture, Passport service), the security of the PKI functionality is an important issue.

In sum, it can be said that the PKI functionality in Windows 2000 offers all the basic functions of a PKI. Windows 2000, like the other PKI products on the market, has both strengths and weaknesses. It is therefore to be recommended that Microsoft be included in the list of possible products. If the basic conditions are right (e.g. the operational applications are primarily implemented in a Windows environment), Microsoft is a serious alternative to other specialised products. Other products generally have the advantage that they can be implemented more flexibly even in heterogeneous environments. Since heterogeneous environments dominate in practice, and PKI-based security functions are to be used not only in internal networks, but primarily with external partners and customers, a combination of a Windows PKI and other products may well be worthwhile.

The enhancements in Windows 2003 have not changed the fundamental implementation scenario of the Microsoft CA (the issue of certificates for internal components), but they have enabled Microsoft to make up considerable ground and to resolve certain problems (e.g. key

¹ From Version 5 Lotus integrates a X.509 conform PKI solution in Notes, the internal PKI however still only uses the proprietary certificates.

archiving). The fact that more applications use Microsoft's certificate management also means that its use is no longer restricted to pure Windows environments.

3 Introduction

With Windows 2000 Microsoft introduced a large number of new features by comparison with the previous version, Windows NT 4.0. Microsoft clearly made particular efforts in the area of security in order to shake off its bad reputation in this field: many of the security functions in Windows 2000 were revised, enhanced or provided with completely new functionality. This work has been continued with Windows XP and Windows Server 2003, the latest version of the Microsoft server operating system. However, the changes implemented in Windows XP and 2003 are nowhere near as far-reaching as those in the upgrade from NT4 to 2000. They represent small enhancements and improvements to the work begun in Windows 2000.

The integration of public key technology into the operating system is a particularly important aspect of the new security functionality in Windows 200x. Public key technology is used consistently as from Windows 2000 to improve existing security mechanisms (e.g. the implementation of certificate-based authentication), but also to support new security mechanisms directly in the Windows operating system (e.g. file encryption, IPSec).

The support of public key infrastructures (PKI) in Windows 200x/XP has received a great deal of attention, primarily because PKI is relevant to many different areas (such as secure e-mail) and many organisations are thus seeking ways in which to implement PKI solutions. The question of if and how Microsoft Windows fits into the PKI strategy of an organisation is raised ever more frequently in PKI projects.

There are two main reasons for this. First, Microsoft provides certain functionality “free of charge” as part of the operating system which would have to be bought separately and at great cost from other specialised manufacturers of PKI software. Second, on account of its worldwide distribution and leading market position, Microsoft Windows always plays a significant role when IT projects are to be implemented. Understandably, when implementing an IT project, most companies endeavour to ensure that it is compatible with the technology supported by Microsoft, either because Windows 2000/XP (or maybe even already 2003) is already used throughout the company or a migration is planned, or because they wish to avoid technical problems when working with companies that use Microsoft.

Against this background, it is important to establish what the Windows PKI functionality really has to offer, and to what extent the PKI functionality should be included in the planning of PKI or IT projects. The (announced) release of Server 2003 and the PKI function enhancements it contains raise a further set of questions. Is it worth starting with the Windows 2000 CA at this stage, or would it be better to wait for the new version of the CA? Does the 2003 CA affect planning, and should new aspects be taken into consideration? The technical details of a PKI product and the effects of its technology on a PKI strategy are not always immediately apparent or explained in the documentation. Particularly in the PKI field it has been demonstrated that just because a function is described in the documentation of two different manufacturers (e.g. support of standards), it does not necessarily follow that the two products can work together in practice. The differences are often only very small, but they can have a considerable effect on the implementation. The relevant conditions must also always be taken into account (e.g. technical environment, special security requirements, etc.).

This White Paper primarily describes and analyses the functionality of Microsoft's Certificate Service, the Certification Authority (CA) component of Windows 200x. It examines how Microsoft's Certificate Service can assist in the construction of a PKI and which secondary issues are to be considered. It aims to provide the reader with a better understanding of Microsoft's Certificate Service so that he or she can judge its suitability. The analysis of the individual points will explicitly examine the differences in PKI between Windows 2000 and

Windows 2003. If there is no explicit reference to a version, the comments are applicable to both solutions.

However, Microsoft's PKI support does not just cover the CA functionality of the Certificate Service, but also includes client functionality, such as the certificate management that is integrated into the operating system. On account of the close interlinking across the Windows operating system, these aspects cannot always be completely separated, and the client functionality is thus also mentioned in some places. One crucial point to remember is that the 2003 CA has lost none of the features of the Windows 2000 PKI; in other words, all the functions in the Windows 2000 PKI can also be performed using the Windows 2003 PKI.

4 PKI Support in Windows 2000/2003/XP

The PKI support in the relevant Windows versions (2000/XP/2003) extends to many areas of the operating system. The most important components are illustrated in diagram 1. The Certificate Service plays a central role, taking on the function of a certification authority (CA), i.e. issuing and revoking certificates.

As in any Windows 200x domain, the integrated Active Directory Service (ADS) plays an important role in the Windows PKI. Depending on the mode of the CA (see below), the Active Directory is used for publishing certificates and certificate revocation lists, registering participants and centrally controlling the PKI functionality on the clients in a Windows domain.

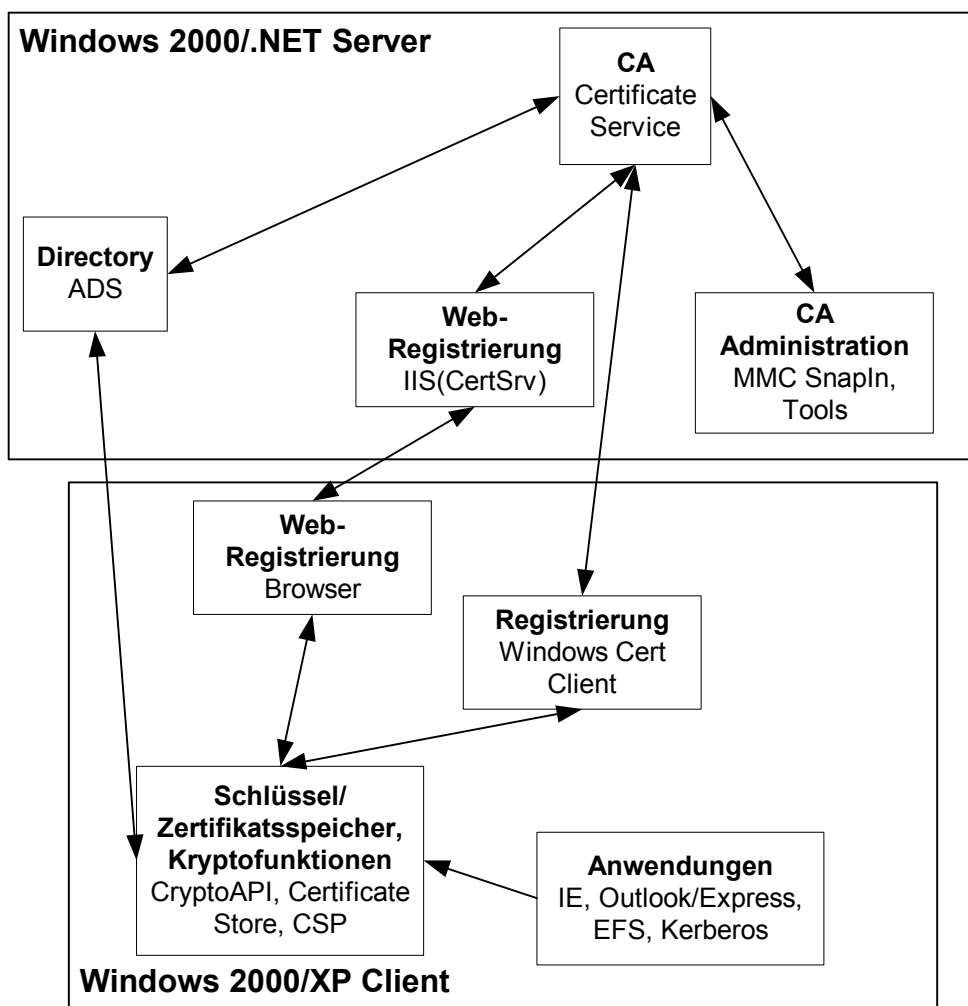


Diagram 1: Windows 2000 PKI components

Functions for managing certificates, certificate revocation lists and keys as well as for checking certificates and certificate chains are integrated into the operating system for the certificate user. Using the appropriate interfaces (e.g. CryptoAPI) these functions can be integrated into applications by developers. This functionality makes it possible to provide users with PKI functionality in a uniform manner. Parts of the user's certificate management can be managed and predefined from a central point in a Windows 200x domain. Some Microsoft applications, such as Outlook and Internet Explorer, already use this functionality,

and manufacturers of third products are increasingly making use of it. Cryptographic service providers (CSPs) – subroutine libraries that enable the operating system to access cryptographic operations via a defined interface – can also be used to enhance the standard functionality provided in Windows 200x, e.g. for supporting cryptographic hardware.

The sections below focus primarily on the CA component of Windows 2000/2003, the Certificate Service. This component is in competition with other products on the market, from companies such as Entrust or Baltimore who specialise in CA components.

5 Architecture

The Certificate Service is made up of a large number of modules which perform different certificate management tasks. Diagram 2 illustrates the architecture of the Certificate Service with related components.

The server engine is the central component of this architecture. It is responsible for issuing certificates and certificate revocation lists. Only limited functionality is integrated into the server engine itself (that is, the actual certificate generation). A significant proportion of the PKI functionality is implemented in the different modules used by the server engine:

- *Policy module*: Functions such as the validation and authorisation of a certificate request and the naming and contents of a certificate (use and verification of attributes) are implemented here.
- *Exit module*: Functions for publishing certificate revocation lists and certificates, e.g. in a directory service, are implemented here.
- *Extension Handler*: Certificate extensions for use in certificates are defined here.
- *Intermediaries*: These accept certificate requests from applications and pass them on to the server engine.

All these modules are linked to one another via defined interfaces, but are otherwise set up independently of one another in the form of Dynamic Link Libraries (DLL). As a result, they

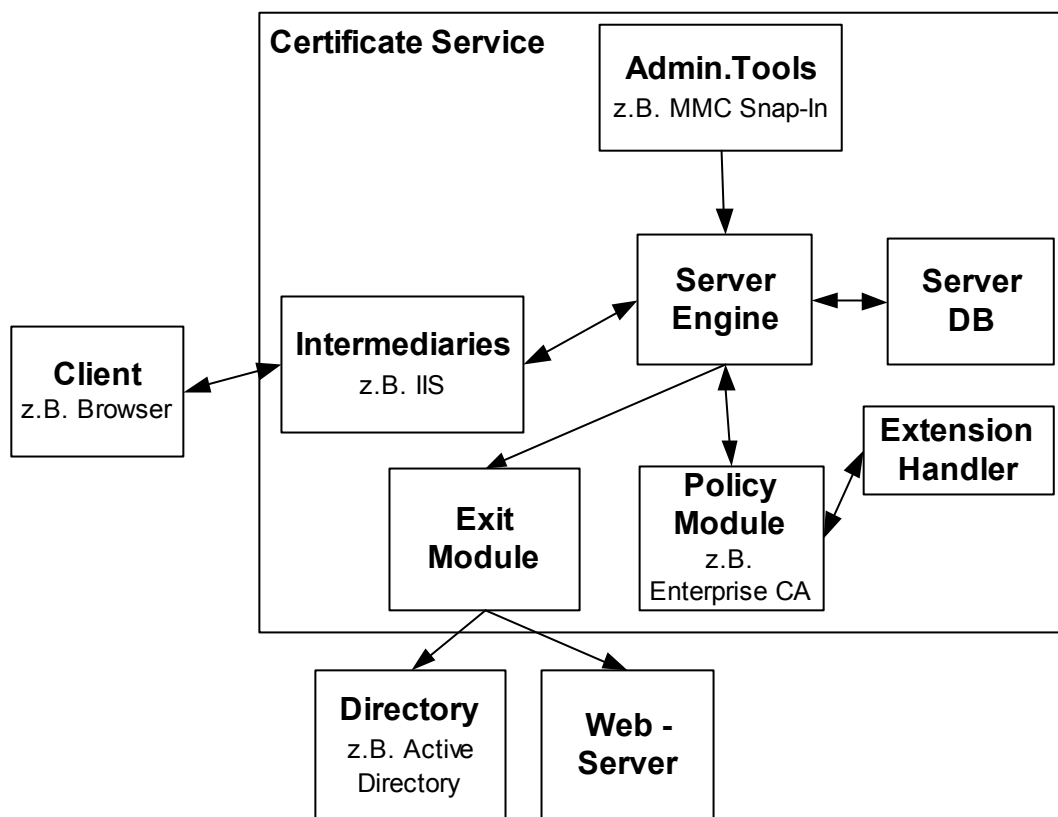


Diagram 2: Windows 2000 Certificate Service architecture

can be adjusted and exchanged. The modules communicate with the server engine mainly by means of common object model (COM) interfaces.

The modular set-up provides a high level of flexibility and offers the possibility of creating individual solutions, but in practice this involves a certain amount of work. The main reason for this is that individual modules can only be exchanged in their entirety, and the modules for implementing modifications have to be completely reprogrammed. The relevant functions are contained in the Microsoft Software Development Kit (SDK) [MSDN_01] and can be used in the programming languages C++ and Visual Basic. A number of modules are already contained in the standard version of Windows 200x. In certain cases, it is explicitly recommended that these are not exchanged (e.g. policy module for Enterprise CA).

The two policy modules Enterprise CA and Stand-Alone CA, which are contained in the standard Microsoft package, are of greatest significance for the PKI functionality. The decision as to which of these two policy modules is to be used is made at the point of installation. The main criterion in the decision is the purpose of the CA:

- The *Enterprise CA* is very highly integrated in the Windows 200x environment including Active Directory and requires a Windows 200x domain and Active Directory. The Enterprise CA is only to be used for the certification of users and computers within one domain.
- The *Stand-Alone CA*, by contrast, is largely independent of other components (such as Active Directory) and its operability is not dependent on a Windows 2000 domain. Certification is not dependent on domain accounts.

The sections below examine the different aspects of the two policy modules.

6 Criteria for comparison

In practice, the assessment of a PKI product is very strongly influenced by important conditions: the type of use, the applications to be supported, the technical environment and the required level of security are just some of the criteria that need to be considered in an assessment of this nature.

The observations in this chapter are not based on a specific scenario; rather, they attempt to be as general as possible. The functionality of the Windows 200x PKI should be judged within this framework on the basis of the most important criteria for a CA product. These criteria are:

- Trust models
- Support of standards
- Registration and key/certificate distribution
- Flexibility
- Administration
- Directory support (publication of certificates and certificate revocation lists)

The following sections describe these criteria in detail.

6.1 Trust model

6.1.1 Hierarchical model

In addition to the option of operating a Windows 200x CA independently, a hierarchical trust model (e.g. integration in or construction of a PKI hierarchy) is supported in both Windows 2000 and 2003. CA products from other manufacturers can be combined with Windows CAs as required. For example, a Windows CA can function under an external CA as a subordinate CA, but Windows can also issue certificates for subordinate CAs outside the Windows environment. The number of levels in the hierarchy is not limited. Certifications in a hierarchy are requested and processed via the standard formats PKCS#10 [PKCS_10] and PKCS#7 [PKCS_7], which are supported by virtually all manufacturers and providers.

6.1.2 Cross-certification

Cross-certification [HAM_01] as a second method is only officially supported from the 2003 CA and Windows XP.

A distinction must be made between cross-certification support by the CA and by the applications. If two CAs wish to cross-certify one another, this simply means that each CA issues a certificate to the other. In principle, these certificates are no different to those for subordinate CAs. Issuing a cross-certificate for another CA in the 2003 Certificate Service is thus no different to issuing a certificate for a subordinate CA, which is also in line with the standard. Seen in this light, cross-certificates can also be issued with Windows 2000.

The problem with cross-certification is that trust relationships through cross-certification can often become confused and difficult to control. It should also be possible to restrict cross-certification to certain applications or areas. For example, two companies wish to issue

cross-certificates so that mutual trust for e-mail communication can be established, but certificates for user authentication should not be accepted in the other company's network.

From the 2003 version, the Microsoft CA supports "qualified subordination", which makes it possible to control and limit acceptance and the trust granted to another PKI. It makes it possible to limit the trust in issued certificates to specific areas (e.g. applications), thus preventing a situation in which cross-certification leads to an unlimited trust relationship.

The restrictions are included in the certificate when it is issued, in the form of extensions. The restrictions can apply to different parameters, such as the name space, the policies used to issue the certificates, or the applications for which the certificates may be used. With one exception, all possible restrictions are part of the X.509 standard. The restrictions related to the application type are Microsoft-specific extensions of the certificate. In Windows 2003, therefore, support for cross-certification primarily refers to the supported of the qualified subordination functionality.

In practice, the actual issuing of cross-certificates is often the least problematic aspect of implementing cross-certification. The important question is whether the applications (e.g. the e-mail program) can deal with cross-certificates. The problems they are most likely to encounter relate to the compilation of certificate chains and the subsequent validity check. These functions are now in place in Windows XP clients, but other products frequently encounter problems. Even the Microsoft XP client implementation requires certain certificate content and the availability of information (i.e. certificates and certificate revocation lists) in the relevant directories (e.g. ADS). The provision of certificates and revocation information beyond company boundaries is often a critical issue in cross-certification.

The difficulty for an application to correctly evaluate certificates also applies to qualified subordination. The restrictions can only have the desired effect if all applications can interpret them correctly. This is not always a given with products that are not based on Windows XP or 2003 implementations, and so tests must be run to ensure overall security.

6.1.3 Other procedures

In addition to hierarchical models and cross-certification, Windows provides other options for establishing trust with other CAs, at least within an appropriate Windows domain structure. These options are supported by both Windows 2000 and 2003. Certificate trust lists (CTLs) are one of the tools used.

A CTL is a signed list of trusted CA certificates. It works on a similar principle as a certificate revocation list, with the difference that a CTL contains trusted certificates from CAs instead of revoked certificates. In a Windows environment, this list is signed by a trustworthy person (such as a PKI administrator) from within the organisation. The list can be distributed to the clients in a domain and deleted using the Active Directories and the Windows group policy mechanism.

In this way, CAs can be centrally declared or defined as trusted within a domain. Programs using the Windows 200x/XP client functionality will automatically recognise certificates from CAs in a CTL as trustworthy.

The proprietary format of CTLs also offers two possibilities for limiting the trust in the CA certificates contained in the list:

- Like CRLs and certificates, CTLs have a limited lifetime, i.e. a validity period can be defined.

- The use of CA certificates can be limited. It is possible to specify the use (e.g. object signing) for which the CAs in the CTL are trusted. The certificates will thus be recognised in the client as trustworthy for these uses only.

The CTL mechanism is a proprietary solution from Microsoft and does not correspond to any standards. For this reason, CTLs are currently only supported by Microsoft. Although they can be exported and distributed as a file, they can only be evaluated and used in a Windows environment.

A problem is represented by the fact that there is currently no provision for revoking CTLs in Windows 200x. When a certificate is no longer to be seen as trusted, the CTL must be deleted using Windows 200x mechanisms and a new CTL issued and distributed. If CTLs are distributed beyond a centrally administrated Windows 200x environment, the absence of a revoking option is a critical problem.

In a Windows 200x/XP environment, CA certificates can also be distributed to user PCs by means of group policies via the certificate stores of trusted CAs that are integrated into the Microsoft operating system. Certificates issued by these CAs are then automatically trusted. The problem with this function is that a Windows client comes with a preconfigured list of such certificates installed by Microsoft which the user then “automatically” trusts. There is no build-in mechanism to centrally uninstall these certificates from a user’s PC in a Windows 2000 environment; it is only possible to centrally install and then uninstall new certificates. In 2003 trust in all such automatically installed certificates can be deactivated centrally. However, this is only possible with a Windows XP client.

This function is particularly useful in a company environment for controlling which certificates are to be trusted within the company network.

The automatically trusted CA certificate function is further enhanced in 2003 and XP by means of an additional function which automatically downloads new CA certificates (automatic root update). This function loads CA certificates that have recently been categorised by Microsoft as trusted into the trusted certificate store. This is performed in the background without the user’s involvement. This function is activated in the standard configuration, but it can be deactivated. Careful consideration should be given to whether or not to use this function.

6.2 Support of standards

Just as Windows is generally opening up to established IETF, ISO and ANSI standards in many areas (e.g. DNS), the PKI functionality in Windows 200x is now also based to a large extent on international standards. The most important of these are:

- X.509v3/v2 [X509_97] and PKIX RFC 2459/3280 [RFC2459] for certificate and certificate revocation list formats
- PKCS for signature formats [PKCS_1] and exchange formats [PKCS_7], [PKCS_10], [PKCS_12]
- LDAPv3 [RFC2251]
- PC/SC for smart card integration [PC/SC_97]

6.2.1 Certificates

Microsoft’s certificate formats are adapted to X.509v3 and the certificate and certificate revocation list profiles defined in PKIX (RFC3280). In principle, the architecture of the

Certificate Service permits flexible certificate content. However, there are significant differences in terms of implementation between the CAs in Windows 2000 and 2003.

- The options for adjusting the content of certificates are extremely limited with the policy modules contained in the standard Windows 2000 installation. The content and layout of the certificates are predefined using certificate templates and can only be adapted to a very limited extent.² Windows 2000 contains a range of application-specific certificate templates covering most of the standard applications. These templates are managed in the Active Directory. In Windows 2000 the templates cannot be adapted or redefined.
- In the 2003 CA, the certificate content is still defined using the templates mentioned above but, by contrast with Windows 2000, there are several options for adapting them. Factors such as the minimum key length, the validity and certain certificate extensions can be individually defined. The certificate content is not completely flexible; certain parts cannot be adapted, or can only be adapted to a limited extent.

The templates can also be used to configure a range of other parameters that affect the way in which the certificate type is processed. The details will be examined at the relevant points in this document.

In all but a few details, the certificate contents (which are the same in both versions) defined in the standard certificate templates correspond to the formats defined in important standards. However, these details can play an important role in practice. A distinction should be made between the following two scenarios:

- The Microsoft Certificate Service is used to issue certificates for non-Windows products.
- A CA product from another manufacturer is to be used to issue certificates for Windows 2000/XP applications.

The cases described below have different effects depending on which of these scenarios is relevant.

In addition to the certificate extensions defined in the standards, Microsoft has defined its own "Private Extensions", which are primarily necessary for original Microsoft applications (e.g. Encrypting File System (EFS)) or used for internal processing.

The standard X.509 explicitly permits the definition of own extensions of this type, but there may be problems in practice if applications cannot interpret these extensions or if products from third parties do not support the functionality related to an extension. However, many PKI manufacturers have now built support for Microsoft extensions into their current products, so that these products can also be used to issue certificates with the extensions defined by Microsoft, for example for certain Windows 200x/XP applications (such as EFS). Since none of these extensions are flagged as "critical", other client products should, according to the standard, at worst ignore them. In practice, however, there are sometimes problems such as program crashes. In the case of doubt, therefore, the usability of certificates with Microsoft-specific extensions in non-Microsoft products should be tested.

Furthermore, in its predefined certificates Microsoft does not always follow the standard recommendations with regard to the flagging of certificate extensions as "critical". When extensions are used in predefined certificate templates, they are never flagged as "critical". This is also the case for extensions such as key usage, which the standards recommend be

² The certificate templates do not just contain specifications regarding the content of the certificates, but also information that is necessary for their issuance (checks, etc.).

flagged as “critical”.³ However, the certificate templates in Windows 2003 allow the key usage extensions, for example, to be set to “critical”.

However, it should be noted that, in principle, the Certificate Service already supports the issuance of critical extensions; however, this functionality is not used in the predefined certificate formats.

A third problem that the certificate formats used by Microsoft can cause lies in the fact that Microsoft applications have strict requirements with regard to the availability and precise appearance of certain certificate extensions (e.g. Certificate Distribution Points (CDPs)). This is of particular significance in the case of certificate validity checks. If those extensions are not available to the specified extent, the client functionality may be restricted (when finding and importing certificate revocation lists, for example).

In the 2003 version, certificate content can be adapted in such a way that some of these problems can be resolved. However, each individual case must be examined to see whether the adjustment options meet the requirements of the relevant environment. It is important to check (preferably through tests) that changing the certificate content does not restrict the functionality of the Windows applications.

Overall, within the framework of different (incomplete) tests, other manufacturers' products were generally able to import certificates issued by Windows 200x, and it was also possible to use certificates issued by CA products from other manufacturers in Windows 200x. However, caution is recommended in the case of a guarantee being given that the certificate details will not cause any functional or security-related restrictions. This may be the case particularly if existing infrastructures are to work together with Windows 200x. The well-known case of a fake Verisign certificate for Microsoft [MAC1_00] clearly demonstrated the extent of the problems that can occur in this context.

6.2.2 Certificate revocation lists

The standard Windows 2000 installation supports Certificate Revocation Lists (CRLv2) as a mechanism for revoking certificates. Certificate revocation lists are used in accordance with the X.509 standard [X509_97], which is the standard generally applied at present. The certificate revocation lists are always complete, i.e. the CA creates a certificate revocation list containing all the revoked certificates in a CA which have not yet expired. More extensive mechanisms, which are provided for in the standard and now supported by many CA products, such as the differentiation between CRLs and ARLs (Authority Revocation Lists), delta CRLs or the protocol OCSP [FOX_99], are not supported in Windows 2000, either on the CA side or on the client side.

The Windows 2003 CA also supports delta CRLs. Delta CRLs can help to minimise the size of the required download because they do not generate a complete CRL containing all entries each time, but rather a supplement containing all the certificates revoked since the last list was published. This means that not only is a complete CRL created at regular intervals (e.g. once a week), a delta CRL is also created more frequently (e.g. once a day), containing only those certificates revoked since the last complete CRL was generated. In the 2003 CA the validity period of each CRL can be set independently of the other. It is also possible to manually create a new CRL or delta CRL outside the normal update period. The validity settings are dependent on the relevant security requirements. When installing a PKI

³ This is unfortunately a common approach taken by various PKI providers in order to avoid interoperability problems by accepting possible security issues.

solution, however, it should be borne in mind that not all products support these delta CRLs, and that problems can arise as a result of this.

It is important to note that Windows 200x/XP clients can only find certificate revocation lists in directories if the CDP extension is contained in the certificate with the relevant information in the correct format. If this extension is not contained (which is primarily the case with older certificates), Windows 200x/XP can only run checks against locally imported certificate revocation lists.⁴

6.2.3 Exchange formats

In addition to the standards for certificates and certificate revocation lists described above, Windows 200x supports a number of standards from the PKCS series for the exchange of certificate requests, keys and certificates. The supported standards are:

- PKCS#10 for certificate requests [PKCS_10]
- PKCS#7 for exchanging certificates and certificate chains [PKCS_7]
- PKCS#12 for exchanging private keys [PKCS_12]

These standards are supported by virtually all other PKI products.

6.3 Directory support

The Certificate Service only provides direct directory support if the Enterprise Policy and related exit module are used. If this is the case, certificates and certificate revocation lists are automatically published in the Active Directory (via ADSI). Automatic publication in other directories via LDAP is not supported. Direct integration with a directory is not possible in the stand-alone mode.

Active Directory supports LDAPv3 in such a way that applications can access Active Directory and the certificates and certificate revocation lists via LDAPv3. Applications from other manufacturers can also access certificates and certificate revocation lists, but only if the clients support the Certificate Distribution Point (CDP) and Authority Information Access (AIA) extensions for finding certificate revocation lists or CA certificates in the Active Directory. Because the structure of the Active Directory differs in practice from the name structure in the certificates and certificate revocation lists, it can be difficult for applications that do not support these extensions to find the correct information.

6.4 Flexibility

On account of the various modules, the architecture of the Certificate Service offers a relatively high degree of flexibility in principle. As described in chapter 5, however, this flexibility can only be exploited in many areas if a considerable amount of programming is carried out, particularly in the case of the Windows 2000 CA. The possibilities for configuration are limited with the standard policy modules for the Enterprise and Stand-Alone CAs. The options for configuring the PKI functionality in the 2000 CA are limited to a small number of parameters (e.g. CDPs), which can be adjusted accordingly. The attributes are pre-set also for the creation of the distinguished name of CAs and users.

⁴ However, checks against locally imported certificate revocation lists are not supported in all cases or by all applications (see [MAC1_00]).

However, this is one of the greatest differences represented by the 2003 CA. The possibility of adapting certificate templates greatly improves the flexibility of the solution. The certificate template settings affect both the technology (e.g. certificate content) and the processes (e.g. manual approval of requests) in the PKI. These issues are examined at various points in this document.

Chapter 9 examines the possibilities for enhancing functionality through third products.

On the client side, flexibility is provided by exchangeable CSPs, which mainly enable the adjustment of the cryptographic functions and key storage. Alternatively, revocation providers can be used to enhance the check routines contained in Windows. This would enable e.g. a Windows 2000/XP client to check certificates also using OCSP.

6.5 Registration and renewal

The procedures for registering users and computers differ greatly depending on which policy module is used. The two modules are therefore discussed separately below.

6.5.1 Enterprise CA

In an Enterprise CA, a user or computer is registered when an account is created in the Windows 200x domain. If a user is registered here, he or she can use, for example, the Certification Manager in the Management Console (MMC) or the CA's registration website (assisted by the Internet Information Server (IIS)) to request a certificate. A preconfigured website is provided by Microsoft for this purpose. The user is authenticated by means of his or her Windows domain account using the information stored in the Active Directory, and the certificate is then issued automatically.

2003 offers the additional option of specifying that manual approval of a certificate request must be performed by an administrator, even in the Enterprise CA. This can be specified either individually for each certificate type as a parameter of the certificate template or for a whole CA. There is no limit to the number of certificates with which a user can be issued in this way, but the types of certificate that a user can request can be limited and controlled via the access rights to the certificate templates in the Active Directory. Access to the certificate website can also be controlled using the standard IIS mechanisms (password, SSL/TLS, etc.).

In addition to these methods initiated by the user, there are two further possible ways of issuing certificates. The first of these is known as "autoenrolment" and can be used to issue certificates automatically, without manual involvement. It is used in conjunction with the Encrypting File System (EFS); the first time a user tries to encrypt a file, the corresponding key is generated and signed by the Enterprise CA. This happens automatically and is not seen by the user.

Autoenrolment can be controlled centrally via the Active Directory and Group Policies, i.e. central specifications can be made to determine who or what will be issued with a certificate upon next registering. Windows 2000 provides this function only for computer certificates. From Windows 2003 this option can also be used to issue user certificates. The autoenrolment mechanism also includes automatic renewal of the certificates. This cannot be configured in Windows 2000; from Windows 2003 the certificate renewal parameters can be configured using the certificate templates.

Another special case is the issue of certificates for the smart card login supported in Windows 200x. In the standard system, these certificates cannot be requested directly by the

user. The request must be made by a special administrator (such as a PKI officer), that is, an administrator with a special certificate, who then passes on the smart card to the user. In the standard system, the transaction is carried out via an appropriate website. This requires a relatively high level of manual involvement and is therefore not really viable when large numbers of users are involved. Some manufacturers are currently developing enhancements to improve the situation (see also chapter 9).

Looking at the Enterprise CA from a PKI perspective, the registration points are the points at which accounts are set up for users or computers. The security is thus heavily dependent on the process of setting up accounts in a domain. It may therefore be necessary to check whether this process satisfies the security requirements set for the certificates (or the related applications). Additional organisational measures could ensure enhanced security when using the 2003 CA via the option of explicit manual approval of a certificate request.

6.5.2 Stand-Alone CA

With the Stand-Alone CA there is no integration in a domain, and so certificates can only be requested via the IIS website. In the standard set-up the certificate requests are then passed onto the CA, where an operator explicitly approves (or refuses) the request. It is also possible to configure the system to automatically issue all incoming requests, but this does not involve any authentication. However, apart from the very limited details contained in the certificate request, the administrator does not have any additional information with which to check the request.

As with the Enterprise CA, access to the websites – and authentication and authorisation of access to the websites – can be protected using the standard IIS protocols and mechanisms (e.g. SSL, TLS).

The Stand-Alone CA functionality in Windows 2003 does not differ greatly from that in Windows 2000. The Stand-Alone version does contain certain changes, such as delta CRLs and the concept of roles, but the Stand-Alone CA does not work with certificate templates and therefore does not permit changes to be made to the settings in the templates.

6.6 Administration

Along with the pure PKI functionality, the administration of a PKI plays an important role in practice. It is crucial to the work required to operate the PKI, and therefore to both the cost and the security of the PKI. As long as no additional special data or processes are necessary, the administrative investment required for the Enterprise CA can be kept relatively low as a result of its integration with the operating system and the use of existing information from the Active Directory.

Microsoft offers a range of tools for managing the PKI. The most important graphical tool is a snap-in for the MMC, which can be used to carry out the most fundamental CA functions, such as revoking certificates (see diagram 3).

The visual set-up is like that of the file manager and is therefore relatively clear and simple. It is fairly easy to operate, involving the procedures to be expected in a Microsoft environment. However, the layout can soon become disorganised if there are a large number of certificates, but filter options can be used to prevent this from happening.

In addition to issuing and revoking certificates, this tool can also be used to perform a number of additional administrative functions, such as starting and stopping the Certificate Service, renewing a CA certificate⁵, and saving and resetting the CA database.

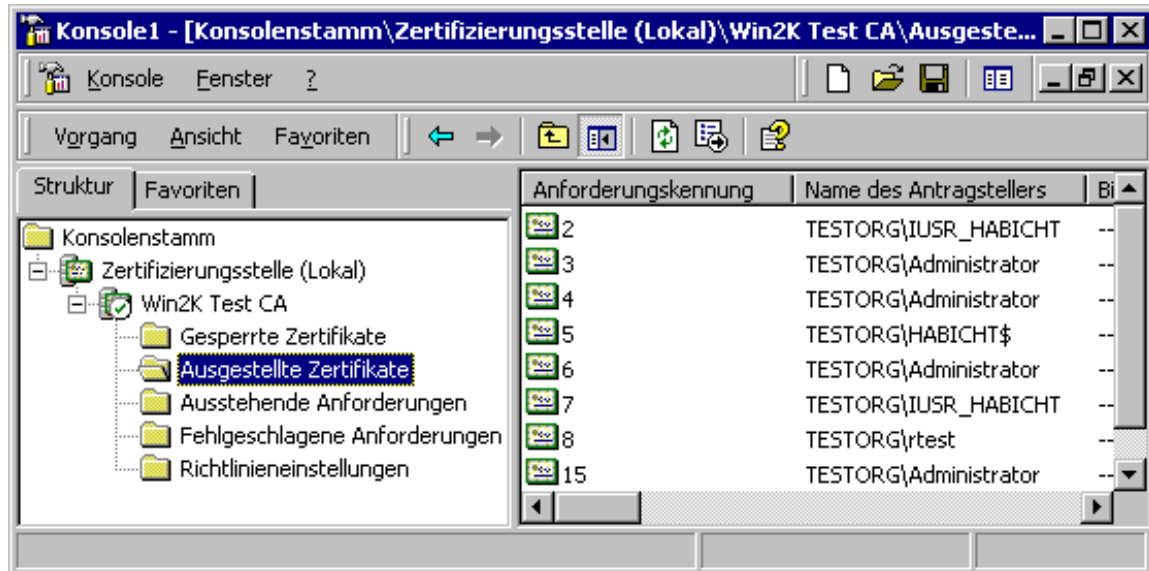


Diagram 3: MMC snap-in administration certification authority (Windows 2000)

In addition to this graphical interface, there are a number of very useful command line tools that can be used for administration. The two most important are *certutil.exe* and *dsstore.exe*.

- In principle, Certutil provides the most important functions of the graphical interface as well as some significant additional functions on the command line level.
- DSStore provides functions that are important for the interaction of the Active Directory and Enterprise CA. It is particularly helpful in solving PKI and Active Directory problems. Unlike Certutil, which is supplied with Windows 2000 Server, DSStore is only available as part of the Server Resource Kit.

Since the Enterprise CA is highly integrated into the Active Directory, certain LDAP and Active Directory tools can be very useful for problem-solving. Some of these are provided with Windows 200x and others are contained in the Resource Kit.

To control access to the CA functionality, Microsoft uses the rights management model used in Windows 200x. The Certificate Service and certain important components (such as the certificate templates) are – as everything in a Windows 200x environment – objects for which special access rights can be assigned. Access rights to the CA can be restricted using special permissions for the CA object.

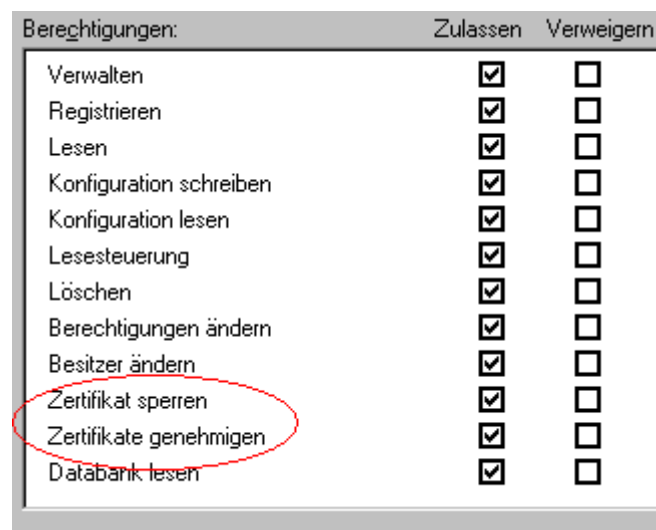
The simple rights in Windows 2000 have been grouped together and further developed into a role concept in Windows 2003. The central aim of the role concept is to group individual permissions together in typical roles within the PKI administration. The Windows 2003 CA includes direct PKI roles for a CA Administrator and a CA Manager. These roles are complemented by the standard Backup-Operator and Auditor roles, which are defined using standard Windows access rights.

⁵ It is possible to renew the certificate and to generate a new key.

A feature of this role concept is that there is technical support for a separation of the roles of CA Administrator and CA Manager. This means that, if required, it is possible to ensure that no one person (or account) is given both permissions (CA Manager and CA Administrator). This makes it possible to separate roles, as well as to separate a standard Administrator from the CA administration. However, great care must be taken when assigning rights if this is to be possible (for example, local administrators are also CA administrators by default). By contrast with Windows 2000, in Windows 2003 the PKI functionality varies between the different server versions (Enterprise, Datacenter, etc.). The role separation option is a component of the Enterprise server and Datacenter. The other server versions (Standard, Web) support the roles, but not role separation.

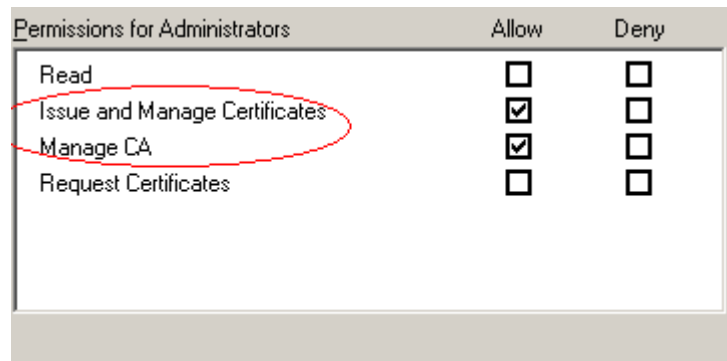
There is also the option of adjusting the rights for the CA or the user by restricting access to the certificate templates. This method provides the option of configuring which types of certificate can be issued by which CA, and who can request which certificate types. An even more refined adjustment can be made by assigning rights to the various enrolment controls which are necessary for requesting certificates.

A 4-eye principle can be achieved at some points through a combination of different restrictions (e.g. request by the Enrolment Agent, manual approval by the CA Manager). The large number of different options however, means that the management of permissions can easily become confusing.

A screenshot of the 'Berechtigungen' (Permissions) dialog box for the Certificate Service in Windows 2000. The dialog has two columns: 'Zulassen' (Allow) and 'Verweigern' (Deny). The 'Zulassen' column has checkboxes checked for all listed permissions, while the 'Verweigern' column has all checkboxes unchecked. The permissions listed are: Verwalten, Registrieren, Lesen, Konfiguration schreiben, Konfiguration lesen, Lesesteuerung, Löschen, Berechtigungen ändern, Besitzer ändern, Zertifikat sperren, Zertifikate genehmigen, and Datenbank lesen. The 'Zertifikat sperren' and 'Zertifikate genehmigen' rows are circled in red.

Berechtigungen:	Zulassen	Verweigern
Verwalten	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Registrieren	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Konfiguration schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Konfiguration lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesesteuerung	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Löschen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Berechtigungen ändern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Besitzer ändern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Zertifikat sperren	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Zertifikate genehmigen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Datenbank lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Diagram 4: Managing rights in the Certificate Service (Windows 2000)

A screenshot of the Windows 2003 Certificate Service permissions configuration window. The window title is "Permissions for Administrators". It has two columns: "Allow" and "Deny". The permissions listed are: "Read", "Issue and Manage Certificates", "Manage CA", and "Request Certificates". The "Issue and Manage Certificates" and "Manage CA" rows have their "Allow" checkboxes checked. A red oval highlights the "Issue and Manage Certificates" and "Manage CA" rows.

Permissions for Administrators	Allow	Deny
Read	<input type="checkbox"/>	<input type="checkbox"/>
Issue and Manage Certificates	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Manage CA	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Request Certificates	<input type="checkbox"/>	<input type="checkbox"/>

Diagram 5: Managing rights in the Certificate Service (Windows 2003)

6.7 Special security measures (CA)

Depending on your specific security requirements, relevant measures must be taken to safeguard the CA server and the PKI components (e.g. certificate templates). Such measures can range from hardening the operating system platform (e.g. switching-off unnecessary services, restrictive assignment of access rights, patch management) to physical security measures (e.g. lockable cupboards, separation from the network). In addition, special configurations are necessary to safeguard the CA services and the other PKI-relevant components, because the standard access rights granted here are often too generous. In complex Windows 2000 domain structures, this configuration is of particular significance.

If particular requirements need to be met (such as the 4-eye principle), this can only be done through organisational measures (e.g. split passwords) or additional functions of third-party products (e.g. Hardware Security Modules). The role concept and role separation provided in the Windows 2003 version do not allow for the dual control principle in the CA administration either.

The close integration of the operating system and the CA makes it virtually impossible to prevent administrators from also having far-reaching rights for the CA functionality. A clear-cut separation of roles cannot therefore be reproduced in a Windows 2000 PKI. Improved separation of the administration of the operating system and the PKI administration can be achieved using the role concept in the Windows 2003 PKI (see above).

7 Other features

This chapter describes some further characteristics of the Windows 2000 PKI that were not mentioned under any of the above topics.

7.1 Validity model

The Certificate Service issues nested validity periods for the certificates [BER_01]. This means that a CA only issues certificates which have a validity period that falls completely within the validity period of the CA certificate [MS_CS_00]. In practice this means that a CA whose certificate is only valid for a further six months, for example, can only issue certificates with a maximum validity period of six months. This fact must be taken into account when planning an update of the CA certificates. In older client versions Microsoft applications (such as Internet Explorer) checked for these nested validity periods and rejected certificates in the case of violation. However, more recent versions no longer appear to run this check, so Microsoft applications no longer require this validity model to be observed.

7.2 Integration with other products

Other PKI-component manufacturers have reacted quickly and integrated support for the Windows PKI into their products. The form of this integration ranges from the simple option of implementing other products to run on the Windows 200x operating system to a far-reaching integration into the functions of the operating system. Particularly the large manufacturers of CA products endeavour to have their products work with Windows 200x in such a way that the customer sees the enhancement provided by these products vis-à-vis Windows 200x.

The support and integration differ from product to product. In principle, there are a number of different strategies and starting points for integration. The most important of these are:

- *Active Directory support:* Products can write certificates and certificate revocation lists directly to the Active Directory.
- *Certificate extension support:* The option of issuing certificates with the special Microsoft extensions and the certificate extensions in the form that Microsoft expects.
- *Certificate management:* Provision of a user certificate management via the CryptoAPI/CSP interface.
- *Integration into the PKI hierarchy/cross-certification:* The option of integrating other products and Windows 2000 CAs within one hierarchical structure.

If, therefore, a manufacturer claims to support the Windows PKI, it is advisable to examine the form of that support in detail.

One frequently asked question is whether the Microsoft Certificate Service can be replaced completely by another product. For many Microsoft applications (such as Outlook) this is, in principle, possible, i.e. certificates from other CAs can also be used (e.g. via PKCS#12-Import). However, this does not allow the same degree of integration as the use of the Enterprise CA. The existence of an Enterprise CA is necessary for some applications, such as autoenrolment. Such functions therefore cannot be supported if an external CA product alone is used.

7.3 Key management

Key pairs for users and computers are usually generated decentrally, that is, with the user. In Microsoft clients, the type and quality of key generation and storage therefore depends on the cryptographic service provider (CSP) used. In the case of integrated CSPs, the standard Microsoft system allows keys to be generated and stored (only) in software. However, there are a number of manufacturers that provide the option of integrating CSPs with special characteristics, such as for generating and storing keys on smart cards or special hardware security modules (HSMs).

The Windows 2000 CA does not support the automatic and configurable archiving or recovery of user keys (known as “key recovery” or “key backup”).

The automatic renewal of certificates is not currently integrated in Windows 2000 either. The user must request a new certificate when the old one expires. The exception to this rule is autoenrolment for EFS and computer certificates, where new certificates are automatically issued. There is a mechanism for renewing CA certificates.

The Windows 2003 CA has enhanced functionality in both these areas.

Participant key archiving is supported by an optional key archival function. The relevant templates are configured for each certificate to determine which keys are to be archived. Only keys to be used for encryption will be archived. Signature key archiving is not supported.

When a key is archived, it is passed on to the CA after it has been generated, where it is stored securely (i.e. encrypted). The keys are individually encrypted using a symmetrical key. This key is then encrypted using the public key of one or more recovery agents. The recovery agents are independent of the CA roles and can be freely configured for a CA. When a key needs to be retrieved, a CA Manager must first export the encrypted key pair from the database. One of the recovery agents must then decode the file, assign it a password and send it to the appropriate user as a PKCS#12 file. This process can only be performed using command line tools.

The 2003 CA also differs from earlier versions in the area of automatic certificate renewal. Important parameters for certificate renewal can be configured via the certificate template. Together with the enhanced autoenrolment function (see above), this allows the automatic and transparent renewal of certificates.

8 Mixed Windows 2000 & 2003 environments

As mentioned above, many organisations have only just finished converting to Windows 2000, or are even still in the process of installing it. It will thus be some time before Windows Server 2003 is completely up and running. With regard to the PKI and the much greater range of functions offered by the Windows Server 2003 CA by comparison with the Windows 2000 CA, the question arises as to whether the enhanced PKI functionality of the Windows 2003 CA cannot also be used in a Windows 2000 environment.

Generally speaking, a Windows 2003 Certificate Service can only run on a Windows 2003 server, and so the environment must be updated. The schema of the Active Directory must be updated so that new features such as the adjustable certificate templates can be supported. This also applies to the other connected domain controllers and ADS authorities. Microsoft provides tools with which to perform such an update. However, this only applies to the Enterprise CA; a Windows 2003 Stand-Alone CA can be operated in a Windows 2000 environment without this update.

The versions also vary with regard to the client, with the result that the full PKI functionality can only be used with the right combination of Windows XP client and Windows 2003 server. If Windows 2000 clients are still in use, functions such as autoenrolment for users, key archiving and adjustable certificate templates cannot be used.

9 Additional products

As mentioned above, there are interfaces and starting points in the Windows 200x CA via which the standard functions of the Windows 200x PKI can be enhanced or replaced.

The standard cryptography functions integrated into the operating system – which can be accessed via the Microsoft CryptoAPI and which are used by all Microsoft applications and the Certificate Service – can be enhanced or replaced by means of a so called provider. The most frequently used method is via a Cryptographic Service Provider (CSP), which makes it possible, for example, to integrate hardware modules such as smart cards or HSMs. It is not important for the applications whether the cryptofunctions are implemented in the hardware or the software. Almost all manufacturers of smart cards, USB tokens and HSMs provide a CSP implementation for their products so that they can be used by applications. However, caution is advised here, since not all CSP manufacturers implement the full range of functions (e.g. key generation).

The second type of provider is the revocation provider. These can be used to add further routines and techniques to those contained in the standard Windows system to check the revocation status of certificates. In this way, Windows can be enhanced, for example, with functions such as OCSP for revocation checks. Some manufacturers also provide solutions in this area, primarily for OCSP.

On the client application side, an increasing number of manufacturers support the certificate store integrated into Windows, that is, the applications access the keys (and the cryptofunctions, if applicable) via the Microsoft interface CryptoAPI. This is sometimes offered as an alternative to the manufacturer's own key storage and sometimes as the only solution. These applications can then also benefit from the integrated solution of the Windows PKI and use the certificates issued by the Windows CA. It is often difficult to integrate products that do not use this interface into a Windows 200x CA, and manual involvement may be necessary (e.g. manual export and import from PKCS#12 files).

A number of products with which the PKI core functionality of the Microsoft CA can be enhanced have recently appeared on the market, or are still being developed. These solutions are built around the Microsoft CA and mainly add PKI management functions, such as more flexible and enhanced registration options, certificate management and even smart card management systems. The type of integration may vary: some products operate as a proxy in front of the Windows CA, while others use the Microsoft PKI architecture and replace the Policy Module. It remains to be seen how useful these products will be.

10 Practical experience

When the first version of this White Paper was drawn up, relatively little was known about how the Windows 2000 CA operated outside a test environment. However, because the Windows 2000 PKI has since played a significant role in a number of practical projects, it has been possible to gain relevant experience. Some of the lessons learned are summarised in this chapter.

10.1 Interoperability

One of the critical factors in PKI projects is often the interoperability between the products of different manufacturers. Microsoft in particular had, and continues to have, a reputation for creating enhancements for standards that impair interoperability with other products. It is thus interesting to see how Microsoft fares in this area.

An important project in Germany in this area is the ISIS-MTT specification [ISIS-MTT_02], which is the result of co-operation between TeleTrust⁶ and the association of CA providers⁷. The aim of this project is to resolve the interoperability problems in current PKI implementations. The first application to be targeted is secure e-mail, but work is also being done to include TLS/SSL. ISIS-MTT is not a new standard, it is based on the main PKI standards (X.509, PKIX, LDAP, PKCS#11, S/MIME) and tries to resolve interoperability problems with the existing standards by means of “tailoring”, that is, enhancements, detailed specifications and clarification of open issues. The aim is to ensure the interoperability of products that conform to the ISIS-MTT specification.

A generally available test bed was developed⁸ with which to test the level of conformity to ISIS-MTT in a number of different PKI products. A test using the ISIS-MTT test bed reveals that, with one exception, the CA certificates issued by the Microsoft CA⁹ conform to ISIS-MTT: the key usage extension is not flagged as being critical. However, this setting could not be changed for an own CA certificate. The settings can be configured for certificates issued by the CA (sub-CAs, users, etc.). However, as mentioned above, the certificate details cannot be configured, which means that it was not possible in every case to issue a certificate that conformed completely to ISIS-MTT.

The project Federal Bridge CA¹⁰ has been running for a few years in the United States. It uses the cross-certification mechanism to create trust relationships between the PKIs of the various US authorities. Interoperability is a major factor in this project, and products must pass an interoperability test before they can be included. The Microsoft CA passed the test.

10.2 Linking directory services

Another problem that often occurs in PKI projects is the link to directory services. The problems are intensified if there is need for secure communication outside the company. It

⁶ <http://www.teletrust.de>

⁷ <http://www.t7-isis.de>

⁸ The test bed can be found under <http://www.teletrust.de>.

⁹ A CA certificate from a Windows 2003 CA with the standard Microsoft settings was tested.

¹⁰ <http://csrc.nist.gov/pki/fbca/>

can be difficult to distribute certificate revocation lists, as well as certificates. Problems arise because directory services are not generally available outside the company network, various organisations experience problems with certain naming conventions and directory structures, and different products have different requirements for finding revocation information.

Microsoft uses CDPs and AIA extensions, which means that the location of revocation information and/or CA certificates is encoded in the certificate. The Microsoft CA issues certificates in this way and the Microsoft client also expects this type of CDP. There is no other way for a client to get the revocation lists. This means that if a certificate to be checked does not contain an appropriate CDP or the location in the CDP cannot be accessed (for example, because the directory cannot be accessed through firewalls), the client cannot run any tests. In the same way, products that do not support CDPs frequently have difficulty finding certificate revocation lists in the Active Directory because the name of the CA and the location of the certificate revocation list in the directory do not match up.

This problem was supposed to be resolved through a central directory in PKI1-Verwaltung¹¹. Since Windows 2000 was also being used in this case, its requirements had to be taken into account. See [BSI_02] for information on the problems that occurred and the work involved in combining the directory services.

¹¹ PKI1-Verwaltung is an Infrastructure for the German administration.

11 Strengths and weaknesses

The division of this chapter into two sections reflects the need to evaluate the two versions of the Microsoft PKI separately. However, the evaluation of the 2003 CA cannot be read in isolation – it is heavily based on the evaluation of the Windows 2000 CA and describes the main differences between the two versions.

11.1 Windows 2000

The strengths of the Windows 2000 PKI clearly lie in the high level of integration in the Windows 2000 environment. This integration allows a large degree of transparency or automation in many places, with the result that tasks that are often complicated in connection with PKIs, such as registration, distribution of certificates, etc., can be performed relatively easily. The administrative effort of using an Enterprise CA is thus reduced to a minimum. On account of the integration of applications, the Enterprise CA is also suitable for improving security within a Windows 2000 domain.

However, the high level of integration also has disadvantages. The links to the operating system functionality may mean that changes, updates and the incorporation of new functions are more difficult because the interaction with other operating system functions must be taken into account.

Very high security criteria can only be met if considerable efforts are made.

The Stand-Alone CA is really only suitable for issuing a small number of certificates (e.g. for SSL servers or as a root CA) or for experimenting with a PKI within the framework of limited pilot tests. When certificates are issued for a large number of participants, the inadequate management options and lack of certain functions (such as directory integration) are of great consequence.

One of the greatest shortcomings is the generally limited functionality and the lack of flexibility of the current implementation. The Windows 2000 CA demonstrates weaknesses particularly when required to operate outside a Windows 2000 environment. In this regard, it clearly lags behind other products on the market. The fact that more manufacturers now use the Microsoft certificate store means that the Microsoft CA can also be more widely used, since such applications can benefit from the CA's integration into Windows and the CA is not restricted to pure Microsoft applications.

Provided that Microsoft's default settings are suitable for a "standard" IT environment, the lack of flexibility is unlikely to pose a problem. In the case of a more varied solution in heterogeneous environments, however, problems certainly can occur.

One of the main arguments in favour of the Certificate Service is the price. The Certificate Service comes free with every Windows 2000 server version. By contrast, CA products from other manufacturers create high additional costs or have licensed models which are dependent on the number of certificates issued. There is undeniably a significant difference in price. Depending on the type of PKI and its use, however, the cost of purchase tends to represent a very small proportion of the overall cost of setting up and operating a PKI. It is therefore important to consider to what extent the required concept can be fulfilled using a Windows 2000 PKI, and how much more work the latter will require by comparison with other products. In many cases, the better manageability of other products can certainly offset the higher purchase costs.

11.2 Windows 2003

Since the Windows 2003 Certificate Service builds on the Windows 2000 CA, some of the key points mentioned in the analysis of the Windows 2000 PKI also apply here. The fundamental advantages (such as simple registration) and disadvantages (such as very strong links to the operating system functions) remain the same.

In the 2003 server, Microsoft has extended and enhanced a significant number of important PKI functions that were missing from the Windows 2000 PKI. The main improvements are functions such as key archival, cross-certification control through qualified subordination, enhanced autoenrolment, the role concept and the possibility to adapt certificate templates. These improvements have primarily increased flexibility and in certain areas (e.g. user autoenrolment) made possible further simplifications. Consequently, Microsoft has caught up with other manufacturers in certain areas. It is now significantly easier to adapt the Windows PKI to the needs of an organisation.

The theoretically appropriate scenario for using the Windows 2003 CA has not changed significantly from the Windows 2000 CA. The main strength and orientation clearly continues to lie in issuing certificates for components (users, computers, etc.) in a Windows domain. The changes to the Stand-Alone CA in Windows 2003 do not significantly change the evaluation made of the Windows 2000 solution, i.e. the Windows 2003 Stand-Alone CA is also only of limited use for issuing certificates outside a Windows domain. The main results of the changes in the Windows 2003 Enterprise CA are as follows:

- The greater flexibility of the certificate content makes it easier to work with applications outside the Windows 2000 domain. The same applies to working with other PKIs and CAs. However, certain restrictions remain, and tests must still be run to establish whether these restrictions are acceptable for the individual case.
- Functions such as the automatic issuance of certificates and automatic renewal simplify a number of processes. Furthermore, processes can be better steered and adapted to requirements via template adjustments.
- The role separation and configuration options provide increased security.

Whereas relatively little planning is necessary for the Windows 2000 CA with its limited configuration options, more planning and tests should be allowed for before the 2003 CA is used. Certain improvements, such as the adjustment of templates, are only of use if they are taken into account in the planning stage. Such adjustments go beyond the tried and tested realm of Microsoft.

It is therefore essential that, as with all manufacturers and PKI installations, any changes made are sufficiently tested to ensure that problems do not arise in the internal installation as a result of opening up outwards.

Caution is advised with regard to the extent to which the flexibility can be used in practice, particularly as the scope for configuration is limited by the specifications and requirements for certificates made by the applications.

12 Further developments

An examination of the development from the Windows 2000 PKI to the Windows 2003 PKI reveals that it is more evolutionary than revolutionary. It would appear that many of the options now available already actually existed in the 2000 version, but were not made accessible in that version owing to a lack of time and stability (e.g. adapting certificate templates). The current version does not seem to contain any "hidden" features of this nature, so further leaps in development should not be expected. The Windows 2000 Enterprise CA covers virtually all the functions to be expected in an integrated solution of this kind. Functions that do not yet exist, such as smart card management, are more likely to be provided by third products than added to the core product by Microsoft.

There is still certainly room for improvement in the Stand-Alone CA, which remains very limited. However, no great changes are expected here, since in Microsoft's strategy the Stand-Alone CA mainly plays the role of a root CA or an "emergency solution" for a small number of certificates. Microsoft does not appear to be making any attempt to compete with independent PKI manufacturers in the area of certificate issuance in heterogeneous environments. The Stand-Alone CA could, however, be developed in this direction by means of enhancements currently being developed by certain manufacturers. However, because these products only use the core functionality of the Certificate Service, many of them do not differ greatly from other third products.

It is therefore likely that the next versions of the Windows CA will contain small improvements and enhancements rather than significant developments in functionality. However, PKI functionality forms an important and permanent part (on both the client and the server side) of the security functions of future Microsoft applications and platforms.

The digital signing of program parts plays a role in the .NET platform, and the roadmap proposed by Microsoft and IBM [IBMMS_02] for secure XML web services is based in many respects on PKI functionality, for example, in the areas of XML signatures and the resulting secure SOAP messages. PKI is also significant in the areas of Digital Rights Management (DRM) and Trusted Computing Platform, although it is not yet clear to what extent.

It thus appears that Microsoft has made a strategic decision to integrate PKI in its products, and that PKI will continue to play a significant role in the foreseeable future.

13 Bibliography

- [BER_01] Bertsch, Andreas, *Digitale Signaturen*, Springer, 2001
- [BSI_02] Hammer, Neundorf, Rosenhauer, *Zertifizierungsinfrastruktur für die PKI-1-Verwaltung, Verzeichnisdienstkonzept, V1.2*, Bundesamt für Sicherheit in der Informationstechnik
- [FOX_99] Fox, Dirk: *Zum Problem der Gültigkeitsprüfung von Schlüsselzertifikaten*. Tagungsband 6. Deutscher IT-Sicherheitskongreß des BSI 1999, SecuMedia Verlag, Ingelheim 1999, S. 215-230.
- [HAM_01] Hammer, Volker, *Cross-Zertifikate verbinden*, DuD 2/2001, Verlag Vieweg
- [IBMMS_02] *Security in a Web Service World: A Proposed Architecture and Roadmap, Version 1.0*, IBM, Microsoft, April 7, 2002
- [ISIS-MTT_02] *ISIS-MTT Specification v1.02*, 19. Juli 2002
- [MAC1_00] Mack, Holger: *Sperren von Zertifikaten in der Praxis – eine Fallanalyse*, DuD 8/2001, Verlag Vieweg,
- [MSDN_01] MSDN Library, *Platform Software Development Kit*, 2001, Microsoft Corporation
www.msdn.microsoft.com
- [MS_CS_00] *Windows 2000 Certificate Service*, Microsoft Corporation, 2000
- [MS_TN_01] Microsoft TechNet, *Microsoft Root Certificate Program*, Microsoft Corporation, 2001
- [NSA_00] S.Christman, *Guide to the Secure Configuration and Administration of Microsoft 2000 Certificate Services*, National Security Agency, 2000
- [PC/SC_97] *Interoperability Specification for ICCs and Personal Computer Systems, Part 1. Introduction and Architecture Overview*, PC/SC Workgroup, 1997
- [PKCS_1] *PKCS #1: RSA Encryption Standard*, v1.5, 1993, RSA Laboratories
- [PKCS_7] *PKCS #7 - Cryptographic Message Syntax Standard*, v1.5, 1993, RSA Laboratories
- [PKCS_10] *PKCS #10 v1.0: Certification Request Syntax Standard*, 1993, RSA Laboratories
- [PKCS_12] *PKCS #12 v1.0: Personal Information Exchange Syntax*, 1999, RSA Laboratories
- [RFC2251] M.Wahl u.a., *Lightweight Directory Access Protocol (v3) (RFC2251)*, 1997, IETF
- [RFC2459] R. Housley u.a., *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, IETF, January 1999
- [WEB_01] AICPA/CICA, *WebTrust Program for Certification Authorities*, Version 1.0, WebTrust
- [X509_97] ITU-T Recommendation X.509 „Information Technology-Open Systems Interconnection-The Directory: Authentication Framework“, June 1997