PKI in der Verwaltung

Allgemeine Richtlinien für den Einsatz von PKI in der Verwaltung

Dokumentinformation

Bezeichnung	Allgemeine Richtlinien für den Einsatz von PKI in der Verwaltung
Kurzbezeichnung	PKI
Version	0.9
Datum	10.04.2003
Dokumentenklasse	Konvention
Dokumentenstadium	Öffentlicher Entwurf
Kurzbeschreibung	Public Key Infrastructure (PKI) ist die Methode mit deren Hilfe nach dem derzeitigen Stand der Technik die Authentisierung, Identifizierung, Vertraulichkeit und Nichtabstreitbarkeit von elektronischen Daten sichergestellt wird. Dieses Dokument gibt einen Überblick über Einrichtung und Betrieb von PKI Strukturen innerhalb von Behörden.
Autoren	Alexander Leiningen-Westerburg (alexander.leiningen@cio.gv.at) Reinhard Posch (reinhard.posch@cio.gv.at)
Arbeitsgruppe	IKT-Stabsstelle des Bundes, Operative Unit

Inhalt

1 Einleitung

Public Key Infrastructure (PKI) ist die Methode mit deren Hilfe nach dem derzeitigen Stand der Technik die Authentisierung, Identifizierung, Vertraulichkeit und Nichtabstreitbarkeit von elektronischen Daten unterstützt wird. Sie ist daher eine technische Grundlage des e-Government. Ohne sie ist eine vertrauliche, gesicherte und rechtlich verbindliche Kommunikation zwischen BürgerInnen und Behörden sowie von Behörden untereinander nach standardisierten Prozeduren nicht möglich. PKI ist die Technologie die den sicheren Einsatz elektronischer Signaturen und Zertifikate ermöglicht. So stellt PKI unter anderem jene Informationen zur Verfügung, die aktuelle Informationen über den Gültigkeitszustand eines Zertifikats gewährleisten.

Ziel des vorliegenden Dokuments ist es, einen Überblick über Einrichtung und Betrieb von PKI Strukturen innerhalb von Behörden zu geben. Es soll Verantwortlichen, Planern und Umsetzungsbeauftragten der öffentlichen Verwaltung als Basisinformation zum Thema Implementierung und Betrieb einer PKI dienen. Gleichzeitig ist es die Grundlage für die damit verbundenen eigenständigen Dokumente:

- [ZERTIFIKATE FÜR WEBSERVICES]
- [SERVERZERTIFIKATE]
- [EMAILZERTIFIKATE]
- [VERSCHÜSSELUNGSZERTIFIKATE]
- [VERZEICHNISDIENSTE]

Diese Verteilung der Information spart dem Leser Zeit und ermöglicht es den Autoren im Bedarfsfall wesentlich raschere und zielgenauere Updates zu veröffentlichen. Welche Zertifikate anzuwenden sind, richtet sich nach den notwendigen [SICHERHEITSSTUFEN] der Kommunikation.

2 PKI in der Verwaltung

Der Aufbau und Betrieb von PKI Strukturen innerhalb der öffentlichen Verwaltung bedarf einer umfassenden Strategie. Die Grundprinzipien, die durch Signaturgesetz und –verordnung vorgegeben sind, müssen, sofern für den Einsatzzweck eines Zertifikates relevant, für den öffentlichen Bereich eingehalten werden. Um ein Zertifikat als einer Verwaltungsorganisation zugehörig zu kennzeichnen, ist es mit der Erweiterung „Verwaltungseigenschaft“ zu versehen, vgl dazu [X509ext]. Abhängig von der Verwendung werden verschiedene Arten von Zertifikaten unterschieden:

2.1 Zertifikate für Webservices

In Zukunft werden viele Organisationen der Verwaltung Signaturdienste verwenden, um Daten im Namen der Organisation automationsgestützt elektronisch zu signieren. Ausschließlicher Verwendungszweck dieses Zertifikats ist das automationsgestützte Signieren von beliebigen Daten durch einen Signaturdienst zum Zwecke der Datenintegrität sowie der Authentisierung des Ursprungs. Beispiele für einen Signaturdienst könnten die Unterzeichnung von Datenauszügen eines Registers oder die Unterzeichnung von ausgehenden Bescheiden einer Organisation der Verwaltung sein. Das Signaturdienstzertifikat dient daher einerseits zur Absicherung der Integrität von Daten und andererseits zur Identifikation ihres Ursprungs. Für die

zu diesen Zwecken einsetzbaren Zertifikate werden im Dokument [ZERTIFIKATE FÜR WEBSERVICES] sowohl Richtlinien für die Inhalte als auch für bestimmte Abläufe in ihrem Lebenszyklus wie Anforderung oder Widerruf definiert.

2.2 Serverzertifikate

Serverzertifikate sind Zertifikate, die die digitale Authentifizierung eines Servers ermöglichen, indem sie Informationen über einen Webserver (Domain Name) und die für den Webinhalt des Servers verantwortliche Organisation enthalten. Ein solches Zertifikat ermöglicht einerseits Benutzern eine Authentifizierung des Servers durchzuführen und wird andererseits zum Aufbau einer sicheren Verbindung mit einem identifizierten Server benötigt. Das Dokument [SERVERZERTIFIKATE] beschreibt nicht nur den Aufbau solcher Zertifikate sondern auch grundsätzliche technische und organisatorische Aspekte und Anforderungen.

2.3 E-Mailzertifikate

Zur Erhöhung der Vertrauenswürdigkeit von ausgehenden e-Mails der Verwaltung sind diese in Hinkunft möglichst flächendeckend zu signieren. Dafür werden Zertifikate benötigt, deren ausschließlicher Verwendungszweck das Signieren von elektronischer Post zum Zwecke der Datenintegrität sowie der Authentisierung des Ursprungs ist. Diese Einschränkung des Verwendungszwecks muss mit geeigneten technischen und organisatorischen Mitteln festgehalten werden. Das Papier [EMAILZERTIFIKATE] definiert Regeln hinsichtlich Zertifikatsinhalte und Prozessabläufe im Lebenszyklus.

2.4 Authentisierungszertifikate

Werden Zertifikate benötigt, die nur dem Authentisierungszweck dienen sollen, können dafür eigene Authentisierungszertifikate ausgestellt werden. Prinzipiell sind diese wie e-Mailzertifikate zu behandeln (siehe [EMAILZERTIFIKATE]). Authentisierungszertifikate werden beispielsweise für Benutzer von SSL Servern verwendet.

2.5 Verschlüsselungszertifikat

Dies ist ein Zertifikat, dessen Zweck es ist, die Vertraulichkeit von elektronischen Dokumenten und elektronischer Post sicherzustellen. Diese Einschränkung des Verwendungszweckes wird mit geeigneten technischen und organisatorischen Mitteln erreicht. Gemäß den internationalen Richtlinien (z.B. OECD) ist vom Verwenden eines Zertifikats sowohl zur Verschlüsselung als auch zur digitalen Signatur abzusehen. Das Dokument [VERSCHLÜSSELUNGSZERTIFIKATE] legt Richtlinien für Zertifikatsinhalte fest und definiert Anforderung und Widerruf von Verschlüsselungszertifikaten.

2.6 Qualifiziertes Zertifikat

Die Verwendung eines *qualifizierten Zertifikats* ist eine der in [SigG] festgeschriebenen Voraussetzungen für das Vorliegen einer *sicheren elektronischen Signatur*. Eine solche Signatur erfüllt nach [SigG] das rechtliche Erfordernis der eigenhändigen Unterschrift, insbesondere der Schriftform nach §886 ABGB.

Dafür müssen qualifizierte Zertifikate besonderen, in [SigG] und [SigV] festgeschriebenen Voraussetzungen genügen. Insbesondere gilt dies hinsichtlich der organisatorischen Voraus-

setzungen und Abläufe beim Zertifizierungsdiensteanbieter oder der einzusetzenden Produkte für die Schlüsselgenerierung, die Schlüsselverwahrung, sowie die Signaturerstellung.

Die Zertifikatsinhalte werden in §5 SigG geregelt. Aufgrund der detaillierten und umfangreichen Regelungen des [SigG] und der [SigV] ist es nicht notwendig qualifizierte Zertifikate in einem eigenen Subdokument darzustellen.

2.6.1 Einsatzbereich

In [SigG] wird der einfachen elektronischen Signatur ihre rechtliche Wirksamkeit nicht allein deshalb abgesprochen, weil sie nicht auf einem qualifizierten Zertifikat beruht. Der Vorteil der sicheren Signatur (und damit als Voraussetzung der Einsatz eines qualifizierten Zertifikats) liegt darin, dass die sichere elektronische Signatur von Haus aus der eigenhändigen Unterschrift gleichgestellt ist, während die „gewöhnliche“ elektronische Unterschrift der freien Beweiswürdigung des Gerichts unterliegt.

Der Einsatz von qualifizierten Zertifikaten empfiehlt sich daher insbesondere für elektronische Abläufe, die konventionelle Abläufe modellieren sollen, in denen die eigenhändige Unterschrift vorausgesetzt wird.

2.7 Verzeichnisdienste

Für die Überprüfung der Authentizität von Signaturen und für eine vertrauliche Kommunikation mit Hilfe von PKI muss der öffentliche Schlüssel des Kommunikationspartners bekannt sein. Dies kann durch Speicherung und Publikation der Zertifikate in einem oder mehreren Verzeichnisdiensten erreicht werden. Das vereinfacht die praktische Verwendung von PKI innerhalb großer Benutzergruppen erheblich. Jedes Zertifikat hat eine Gültigkeitsdauer. Wird es vorzeitig wegen Verlust, Kompromittierung oder anderen Gründen widerrufen, so ist dies in einem speziellen Verzeichnis, einer sogenannten CRL (Certificate Revocation List) zu veröffentlichen. Aufgrund der eingeschränkten Software Unterstützung wird OCSP (Online Certificate Status Protocol) im Verwaltungsbereich derzeit nicht angewandt. CRLs müssen allgemein zugänglich sein. Bei Einsatz von Verschlüsselungszertifikaten ist sinnvollerweise ein Verzeichnis vorzusehen, dass das Auffinden von Zertifikaten einer bestimmten Person ermöglicht, es sei denn es besteht im Einzelfall berechtigtes Interesse an Datenschutz.

Das Dokument [VERZEICHNISDIENSTE] beschreibt zu verwendende Protokolle, Zugriffe auf Verzeichnisdienste und Standards.

2.8 Zertifizierungsdiensteanbieter (ZDA)

Die Qualität einer PKI beruht nicht zuletzt auf der Qualität bei der Ausstellung ihrer Zertifikate. Dem Zertifizierungsdiensteanbieter (ZDA) kommt daher eine wichtige Rolle zu. Um eine qualitativ hochwertige PKI aufzubauen, müssen Zertifizierungsdiensteanbieter strenge Auflagen erfüllen. Grundsätzlich kommen all jene Zertifizierungsdiensteanbieter in Frage, die verwaltungskonforme Zertifikate ausstellen.[1]

[1] Eine entsprechende Auflistung ist auf www.cio.gv.at zu finden

3 Sensibilisierung

Das beste Sicherheitskonzept ist wertlos, wenn die Benutzer nicht verantwortlich mit den in ihre Obhut gegebenen Werkzeugen, im konkreten Fall mit Zertifikaten und den damit verbundenen Schlüsseln umgehen. Neben den eigentlichen BenutzerInnen (die persönliche Zertifikate erhalten) müssen im Zuge der Schulung auch jene Personen miteinbezogen werden, die für Application- und Webserver bzw. für andere betroffene Systeme (VPN Administratoren, etc.) zuständig sind. Ziel soll es sein, den BenutzerInnen verständliche und verfügbare Informationen so bereitzustellen, dass Sie Zertifikate sicher und verantwortungsvoll einsetzen können.

Folgende Punkte sollten Teil einer Belehrung sein:

- BenutzerInnen müssen die für ihre Arbeit notwendigen Grundlagen für Zertifikate vermittelt werden. Dazu zählen u. a. die Inhalte von Zertifikaten selbst, der Zweck sowie deren Nutzung und Besonderheiten.
- Zertifikate stellen keine Ermächtigung dar, etwas zu tun. Vielmehr wird - je nach Zertifikatstyp - die Authentizität und Sicherheit beim digitalen Signieren bzw. Vertraulichkeit beim Übertragen garantiert.
- der unmittelbare Nutzen bzw. die unmittelbare Notwendigkeit eines Zertifikats müssen BenutzerInnen verständlich mitgeteilt werden.
- Private Schlüssel müssen entsprechend geschützt werden. Sollte der Schutz mit einem Passwort oder anderem (geheimen) Wissen erfolgen, so hat eine Weitergabe bzw. private Speicherung des Passwortes zu unterbleiben.
    - Richtlinien für die Auswahl von Passwörtern sind auszugeben, in denen eine Mindestlänge des Passwortes, die Verwendung von Sonderzeichen, der regelmäßige Wechsel des Passwortes und weitere sicherheitsrelevanten Maßnahmen geregelt werden.
- Verbot der Speicherung privater Schlüssel auf Laufwerken bzw. anderen Datenträgern die Dritten zugänglich sind.
    - Eine private Datensicherung des Zertifikats inklusive dem privaten Schlüssel (z.B. im PKCS12 Format) auf einem sicher zu verwahrenden externen Datenträger ist zu empfehlen.
- Widerrufsgründe für das Zertifikat
    - Weder das Zertifikat noch eine Sicherung ist verfügbar (zB aufgrund von Löschung)
    - Das Passwort ist nicht mehr bekannt
    - Es besteht der begründete Verdacht auf Kompromittierung des Schlüssels
    - Versetzungen oder Beendigung eines Dienstverhältnisses (gilt für e-Mail- , Verschlüsselungs- und qualifizierte Zertifikate)
- Vorgehensweise bei Verlängerung des Gültigkeitszeitraumes.
- Zwang zur Zertifikatserneuerung bei Änderung von Zertifikatsinhalten (e-Mailadresse, Namensänderung etc.)
- Da manche e-Mailclients die erhaltenen verschlüsselten e-Mails nicht dechiffriert speichern, dürfen die BenutzerInnen auch nach Ablauf der Gültigkeit eines Zertifikats

- bzw. des zugehörigen privaten Schlüssels – dieses nicht löschen, da es zur Dechiffrierung der verschlüsselten e-Mails dient.

- Der Verlust des Verschlüsselungsschlüssels führt zu unwiderruflichem Datenverlust aller verschlüsselten Dokumente. Dies ist den Benutzern entsprechend zu kommunizieren. Prinzipiell ist bei Zertifikaten, die der Verschlüsselung dienen, eine entsprechende Backup-Strategie vorzusehen,
- Generell kann die unsachgemäße Verwendung von Zertifikaten schwerwiegende rechtliche Folgen haben.

Auf Seiten der Verwaltung und der mit der PKI betrauten Verantwortlichen müssen Regeln geschaffen werden, wer technisch und organisatorisch für Beschaffung und Widerruf von Zertifikaten verantwortlich ist. Ebenso sind für die von der Behörde durchgeführte Datensicherung Maßnahmen zu setzen, die im gemeinsamen Interesse der Dienststelle und des Mitarbeiters erfolgen.

4 Rechtlicher Rahmen

Der rechtliche Rahmen für die Erstellung und Verwendung elektronischer Signaturen, sowie die in diesem Zusammenhang zu erbringenden Signatur- und Zertifizierungsdienste sind im [SigG] und [SigV] geregelt.

AVG §14 Abs 8 legt fest, dass Niederschriften, die mittels automationsunterstützter Datenverarbeitung erstellt worden sind, nicht der Unterschrift des Leiters der Amtshandlung und der beigezogenen Personen bedürfen, wenn sichergestellt ist, dass auf andere Weise festgestellt werden kann, dass der Leiter der Amtshandlung den Inhalt der Niederschrift bestätigt hat. Um die Unverfälschtheit der Daten zu garantieren, ist jedoch die elektronische Signatur zu empfehlen.

5 Sonstiges

Prinzipiell ist davon abzusehen, Berechtigungen und Rollen in Zertifikaten abzubilden. Jede Änderung von Berechtigungen und Rollen, die vor allem in einer dynamischen Arbeitswelt häufig vorkommen, würde die Neuausstellung eines Zertifikates nach sich ziehen. Ein erhöhter und letztlich sinnloser Verwaltungsaufwand wäre die Folge.

Das Zertifikat soll daher lediglich Angaben zur Identität beinhalten. Rollen und Berechtigungen sind davon getrennt zu halten. Sie können beispielsweise nur behauptet, und vom Empfänger mit geeigneten Maßnahmen überprüft (z.B. Registerabfrage) werden. In besonderen Fällen ist es auch denkbar zertifizierte Rollen beizulegen, wobei eine Bestätigung über die Rolle, z.B. ein Attributszertifikat oder eine selbstdefinierte Struktur beigefügt wird.

6 Referenzen

EMAILZERTIFIKATE

Karlinger, Gregor und Posch, Reinhard: Richtlinien für e-Mailzertifikate der Domäne gv.at. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 1.0.1, 13. Januar 2003.

ETSI QC

European Telecommunications Standards Institute: ETSI TS 101862: Qualified Certificate Profile, v1.2.1. Technical Specification, June 2001. Abgerufen aus dem World Wide Web am 20. November 2002 unter http://pda.etsi.org/pda/home.asp?wki_id=13385.

NETSCAPEEXTENSIONS

Netscape Certificate Extensions. URL: http://wp.netscape.com/eng/security/comm4-cert-exts.html (Abgerufen aus dem World Wide Web am 20. November 2002)

SigG

BGBl I Nr. 190/1999 idF BGBl I Nr. 152/2001.

SigV

BGBl II Nr. 30/2000.

Serverzertifikate

Martin, Bernd und Posch, Reinhard: Richtlinien für Serverzertifikate. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 1.0.4, 11.April 2003.

Sicherheitstufen

Besenmatter, Wolfgang: Sicherheitstufen im Bereich e-Government. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, noch nicht erschienen

Zertifikate für Webservices

Karlinger, Gregor und Posch, Reinhard: Richtlinien für Zertifikate für Webservices in der Verwaltung. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 1.0.3, 14. Februar 2003.

Verschlüsselungszertifikate

Karlinger, Gregor und Posch, Reinhard: Richtlinien für Verschlüsselungszertifikate in der Verwaltung. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, noch nicht erschienen.

Verzeichnisdienste

Schamberger, Rudolf: Richtlinien für PKI Verzeichnisdienste der Domäne gv.at. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 0.9.0, 11. April 2003

X509ext

253 Hollosi, Arno: X509 Zertifikatserweiterungen für die Verwaltung. Konvention zum e-
254 Government Bund Länder Gemeinden, erarbeitet von der IKT-Stabsstelle des Bundes,
255 Operative Unit/Technik. Öffentlicher Entwurf, Version 1.0.2, 18. Februar 2003.

256