Das Policy-Rahmenwerk einer PKI

Secorvo White Paper

Certificate Policy, Certification Practice Statement, PKI Disclosure Statement

Version 1.2
Stand 16. Mai 2017

Petra Barzin, Stefan Gora

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Inhaltsübersicht

Abkürzungen

ABA	American Bar Association
CA	Certification Authority
CP	Certificate Policy, Zertifizierungsrichtlinie
CPS	Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb
DSG	Digital Signature Guidelines
EFS	Encrypted File System
eIDAS	Electronic identification and trust services for electronic transactions (EU-Verordnung)
NIST	National Institute of Standards and Technology
HSM	Hardware Security Module
IPRA	Internet Policy Registration Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCA	Policy Certification Authority
PDS	PKI Disclosure Statement
PEM	Privacy Enhanced Mail
PKI	Public Key Infrastructure
RFC	Request For Comments
URL	Uniform Resource Locator

Historie

Version	Datum	Änderung	Autor
1.0	06.06.07	Veröffentlichte Erstfassung	Petra Barzin, Stefan Kelm
1.1	27.03.08	Redaktionelle Änderungen und Erweiterungen, insbesondere in Anhang B	Petra Barzin, Stefan Kelm
1.2	16.05.17	Aktualisierung und Überarbeitung	Petra Barzin, Stefan Gora

1 Zusammenfassung

Dieses Dokument richtet sich in erster Linie an Autoren von Policy Dokumenten für eine PKI. Es ist auch für PKI Anwender hilfreich zum Verständnis des Policy-Rahmenwerks einer PKI, da es die Grundlage zur Vertrauensbildung von PKI-basierten Anwendungen darstellt.

Das Policy-Rahmenwerk einer PKI umfasst eine Certificate Policy (CP), ein Certification Practice Statement (CPS) und ein PKI Disclosure Statement (PDS). Dieses Whitepaper gibt einen Einblick in diese drei Dokumente. Dabei wird auch ein kurzer Rückblick auf die Historie von Policies gegeben. Der Schwerpunkt dieses Whitepapers liegt in der Darstellung von Inhalt und Zweck der einzelnen Policy Ausprägungen sowie einer Hilfestellung bei der Wahl der Strukturierung der Policy Dokumente.

Die Basis für die Erstellung einer Certificate Policy und eines Certification Practice Statement ist der bereits 2003 veröffentlichte Internet-Standard RFC 3647. Dieser Standard hat sich international etabliert, daher werden die zugrunde liegende Idee und die Vorgaben aus diesem RFC detailliert erläutert. Außerdem wird beschrieben, wie ein Zertifikatsprüfer (Relying Party) in der Praxis die Certificate Policies auswerten kann und ob und inwieweit verschiedene Certificate Policies überhaupt miteinander verglichen werden können. Für technisch interessierte Leser wird in einem separaten Kapitel ein Einblick in die technische Umsetzung von Certificate Policies in X.509v3 Zertifikaten gegeben.

Spezielle Fragestellungen aus dem Umfeld der sog. „qualifizierten Signaturen“ (gemäß deutschem Signaturgesetz – SigG – oder der europäischen Verordnung eIDAS) werden in diesem Dokument nicht diskutiert. Grundsätzlich gelten jedoch die in diesem Dokument getroffenen Darstellungen auch in diesem Umfeld.

2 Einführung

Wie viel Vertrauen kann ein Anwender in eine PKI und in die Glaubwürdigkeit eines Zertifikats haben? Diese Fragestellungen versuchte man schon 1993 – in den ersten Anfängen von PKI - zu lösen. Damals glaubte man, auf Basis von X.509 (v1) eine weltweite PKI unter einer einzigen globalen Root (Wurzelinstanz) – der sog. IPRA - erschaffen zu können.[1] RFC 1421 – 1424 definierten das “Privacy Enhancement for Electronic Mail”, wobei sich Teil 2 (RFC 1422, [PEM]) eingehend mit der Architektur und Infrastruktur für ein zertifikatsbasiertes Schlüsselmanagement beschäftigt: „Mechanisms must be provided to enable each user to be aware of the policies governing any certificate which the user may encounter.”

Unterhalb der globalen IPRA Root sollten die sogenannten Policy Certification Authorities (PCAs) betrieben werden, welche die Sicherheitsrichtlinien innerhalb ihres Teilbaumes in der Hierarchie vorgaben. Je nachdem, wo eine CA in der weltweiten IPRA-Infrastruktur angesiedelt war, konnte man das Vertrauen in die ausgestellten Zertifikate anhand der Policy der übergeordneten PCA ableiten. Dieser Ansatz erwies sich jedoch als ungeeignet und nicht praktikabel, da sich die Unternehmen und Organisationen weltweit nicht unter einer globalen IPRA Root vereinigen wollten. Auch blieb in diesem Zusammenhang unbeantwortet, welche Organisation für die IPRA verantwortlich sein sollte. Vielmehr entstanden vereinzelte Insellösungen, da in den Unternehmen eigene unabhängige PKIs

[1] Die Idee einer weltweiten PKI war zu jener Zeit eng verknüpft mit dem erhofften Aufbau internationaler Verzeichnisdienste. Eine Reihe von damaligen (teils heute noch gültigen) Standards definierten sowohl das Verzeichnis selbst (in X.500) als auch entsprechende Zertifikate (in X.509), die zur Authentisierung gegenüber den Verzeichnissen verwendet werden sollten.

aufgebaut wurden. Dabei blieb unklar, nach welchen Richtlinien diese Zertifikate ausgestellt wurden. Auch der Begriff „Certificate Policy“ wurde erst später eindeutig definiert (s. u.).

Die Frage nach der zugrunde liegenden Certificate Policy und der Haftung einer CA für ihre ausgestellten Zertifikate wurde 1994 zum ersten Mal von Michael S. Baum in seiner Publikation „Federal Certification Authority Liability and Policy“ [NIST] aufgeworfen.

In den Jahren 1995 und 1996 folgten als Vorreiter im Bereich der Policies die Zertifizierungsrichtlinie der UNINETT PCA aus dem Jahr 1995 und die DFN-PCA Policy von 1996. Keine anderen Policies wurden so oft kopiert und angepasst wie diese beiden. Die Policy der UNINETT PCA wurde als *informational RFC* (RFC 1875) veröffentlicht.

Damals gab es jedoch weder „Vorlagen“ wie RFC 3647 noch die Unterscheidung zwischen Certificate Policy und Certification Practice Statement, sondern die Anforderungen und die Umsetzung der Anforderungen wurden in einem einzigen Dokument beschrieben. Diese Zertifizierungsrichtlinien waren – auch für den Durchschnittsanwender - noch leicht verständlich und überschaubar.[2] Heutige CP und CPS Dokumente umfassen bis zu 100 Seiten, die oftmals – obwohl aus dem technischen Umfeld stammend – von Juristen formuliert und und somit nicht gerade intuitiv verstanden werden können.

3 Certificate Policies und Certification Practice Statement

Die Unterscheidung zwischen einer Certificate Policy und einem Certification Practice Statement wurde 1996 durch die Definition des „Certification Practice Statement“ und 1997 durch die Definition und Verankerung der „Certificate Policy“ in einem X.509 Zertifikat getroffen.

Die American Bar Association definierte 1996 ein **Certification Practice Statement** in ihren „Digital signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce” [ABA-DSG] als *„A statement of the practices which a certification authority employs in issuing certificates“*.

Die ITU-T definierte dann 1997 eine **Certificate Policy** in ihrer „Recommendation X.509: Information Technology - Open Systems Interconnection: The Directory: Authentication Framework“ [X.509] als *„A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements“*.

Eine Certificate Policy (Zertifizierungsrichtlinie) beschreibt also die Anforderungen an die Ausstellung und Verwendung von Zertifikaten, wohingegen ein Certification Practice Statement (Regelungen für den Zertifizierungsbetrieb) darlegt, wie diese Anforderungen von der CA umgesetzt werden.

> Eine Certificate Policy erklärt *„Was?“*
>
> Ein Certification Practice Statement erklärt *„Wie?“*

Im Jahre 1998 veröffentlichten S. Chokhani und W. Ford schließlich den ersten PKIX Draft über ein *Certificate Policy and Certification Practices Framework*, welcher in darauffolgenden Jahr als Internet-Standard RFC 2527 veröffentlicht wurde. Dieser bietet einen

[2] Dies lag – am Beispiel der DFN-PCA – unter anderem daran, dass die Endanwender in den Prozess der Policy-Erstellung mit einbezogen wurden.

Gliederungsrahmen zur Erstellung von Certificate Policies und Certification Practice Statements. Nachfolger dieses RFCs ist der heute aktuelle RFC 3647, der im wesentlichen um zwei weitere Kapitel zu den vertrauensbildenden Thema Haftung und Audit der CA ergänzt wurde. Sowohl in der Certificate Policy als auch in dem Certification Practice Statement werden die technischen, physischen und operativen Sicherheitsmaßnahmen der CA detailliert beschrieben.

4 PKI Disclosure Statement

Die Beschreibung der technischen, physikalischen und operativen Sicherheitsmassnahmen interessieren den Anwender oft nicht im Detail. Für den Anwender ist es vor allem wichtig zu wissen, welchen Verpflichtungen die Anwender nachkommen müssen und wie die Haftung im Schadensfall geregelt ist. Zu diesem Zweck ist ein **PKI Disclosure Statement** (PDS) geeignet.

Ein PKI Disclosure Statement ergänzt CP sowie CPS und beschreibt auf maximal 1-3 Seiten die Validierungsprozedur zur Überprüfung der Identität eines Antragstellers, den Anwendungsbereich der Zertifikate, die Verpflichtungen des Zertifikatsinhabers und Zertifikatsprüfers und wie die Haftung im Schadensfall geregelt ist.

Die American Bar Association (ABA) hat das Modell und die Struktur eines PKI Disclosure Statements als Anhang zu ihrem PKI Assessment Guidelines (PAG) [ABA-PAG] aufgenommen.

Im Umfeld der qualifizierten Signaturen hat das European Telecommunications Standards Institute (ETSI) Security Technical Committee ein PDS als Anhang zu den beiden folgenden Standards ergänzt:

- “Policy Requirements for Certification Authorities Issuing Public Key Certificates” [POL-REQ] und
- „Policy Requirements for Certification Authorities Issuing Qualified Certificates“ [POL-REQ-QUAL]

Die Inhalte eines PKI Disclosure Statements werden kurz und knapp auf wenigen Seiten beschrieben und umfassen:

1. Kontaktdaten derZertifizierungsstellen
   Kontaktinformationen der CA, wie diese erreichbar ist (postalische Adresse, E-Mail Adresse, Telefon-, Faxnummer).
2. Zertifikatstyp, Validierungsprozeduren und Verwendung
   Welche Art von Zertifikaten werden ausgestellt (Benutzerzertifikate, Serverzertifikate, Maschinenzertifikate für Clientgeräte)? Wofür werden die Zertifikate eingesetzt (Signatur und/oder Verschlüsselung von E-Mails, eine der handschriftlichen Unterschrift gleichgesetzte elektronische Signatur, VPN, SSL, etc.)? Wie sieht die Validierungsprozedur der CA zur Überprüfung der Identität eines Antragstellers aus?
3. Begrenzung der Nutzung und der Verlässlichkeit von Zertifikaten (Reliance limits)
   Wofür dürfen die Zertifikate der CA verwendet werden, d.h. bei welchen Anwendungen kann ein Zertifikatsprüfer diesen Zertifikaten vertrauen und sich auf die Haftung der CA verlassen?
4. Auflagen für Zertifikatsinhaber („Subscriber“)
   Welchen Verpflichtungen muss ein Zertifikatsinhaber nachkommen?

5. Auflagen der Zertifikatsprüfer („Relying Parties“) zur Zertifikatsstatusüberprüfung
   Welchen Verpflichtungen muss ein Zertifikatsprüfer bei der Statusüberprüfung eines Zertifikats dieser CA nachkommen?
6. Ausschluss- und Haftungsbegrenzungsklauseln
   Wie sehen die Garantie- und Haftungsbeschränkungen aus?
7. Anwendbare Vereinbarungen, Certification Practice Statement, Certificate Policy
   Wonach richtet sich die Ausstellung der Zertifikate bei dieser CA? Was ist die Grundlage für die Nutzung von Zertifikaten dieser CA?
8. Datenschutzerklärung
   Welche Datenschutz-Richtlinien gibt es bei dieser CA?
9. Rückvergütung
   Gibt es Rückerstattungs-Richtlinien bei dieser CA?
10. Anwendbares Recht und Streitbeilegungsklauseln
    Welches Recht und welcher Sitz gelten als Gerichtsstand im Streitfall?
11. CA und Zertifikatsverzeichnis Lizenzen, Prüf- und Gütesiegel der CA
    Welche Lizenzen, Prüf- und Gütesiegel hat die CA vorzuweisen, um das Vertrauen eines Zertifikatsprüfers zu stärken?

Ein Auszug aus den PAG ist im Anhang A zu finden.

5 RFC 3647

RFC 3647 bietet einen umfassenden und vollständigen Gliederungsrahmen für eine Certificate Policy und ein Certification Practice Statement. Zu jedem Gliederungspunkt ist im RFC stichwortartig dargestellt, welche Inhalte in diesem Abschnitt beschrieben werden sollen. Wenn ein Gliederungspunkt bei der Erstellung einer Certificate Policy oder eines Certification Practice Statement nicht relevant ist, soll der CP/CPS Editor dieses Kapitel nicht löschen, sondern durch einen Vermerk „no stipulation“ oder „keine Anforderung/Festlegung“ kennzeichnen. So wird eine bessere Vergleichbarkeit von Certificate Policy bzw. Certification Practice Statement Dokumenten sichergestellt.

Der Gliederungsrahmen in RFC 3647 sieht folgende Inhalte in einer Certificate Policy oder einem Certification Practice Statement vor:

1. Einleitung
   Die Einleitung beschreibt die Identifikation, den Inhalt und den Zweck des Dokuments, gibt einen Überblick über die Architektur der Zertifizierungsinfrastruktur und beschreibt die Teilnehmer der Zertifizierungsinfrastruktur. Es werden die geeigneten und untersagten Zertifikatsnutzungen festgelegt. Weiterhin sollen folgende Fragen in der Einleitung adressiert werden: Wer ist für die Verwaltung der Richtlinie zuständig? Wie ist das Änderungsmanagement der Richtlinie definiert? Nach welchem Verfahren werden fremde Regelungen für den Zertifizierungsbetrieb (CPS) anerkannt? Wer prüft die Eignung fremder Richtlinien?
2. Veröffentlichungen und Verzeichnisdienst
   Welche Daten (CA Zertifikate, Benutzerzertifikate, Sperrlisten) werden veröffentlicht? In welchem Verzeichnisdienst werden sie bereitgestellt? Wie häufig findet eine Aktualisierung dieser Daten statt? Wer hat lesenden und schreibenden Zugriff auf den Verzeichnisdienst?
3. Identifizierung und Authentifizierung
   Wie sieht das Namenskonzept der CA aus, d. h. nach welchen Regelungen vergibt die

CA die Namen für Antragsteller? Welche Richtlinien und Prozesse gibt es bei der Identifizierung und Authentifizierung bei Neuanträgen, bei Zertifikatserneuerungen und bei Rückruf eines Zertifikats?

4. Ablauforganisation
   Beschreibung der Richtlinien und Prozesse für den gesamten Lebenszyklus eines Zertifikats: Zertifikatsantrag, Bearbeitung eines Zertifikatsantrags durch die CA, Ausstellung eines Zertifikats von der CA, Akzeptanz des Zertifikats durch den Antragsteller, Verwendung des Schlüsselpaares und des Zertifikats, Schlüssel- und Zertifikatserneuerung, Änderung des Zertifikatsinhalts, Widerruf eines Zertifikats, Dienst zur Statusabfrage von Zertifikaten, Beendigung des Vertragsverhältnisses zwischen CA und Zertifikatsinhaber, Schlüsselhinterlegung und –wiederherstellung.
5. Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen
   Wie sehen die infrastrukturellen Sicherheitsmaßnahmen aus, um einen sicheren IT-Betrieb zu gewährleisten? Welche organisatorischen Sicherheitsmassnahmen wurden getroffen, um einen geeigneten Schutz für die CA zu bieten? Welche personellen Sicherheitsmaßnahmen gelten für die Mitarbeiter der CA? Welche Operationen der CA werden protokolliert und wer überprüft wie häufig diese Log-Dateien? Wie sieht das Datensicherungskonzept der CA aus? Welche Daten und Dokumente werden wie lange archiviert? Wie sind die Archive geschützt? Wie sieht der Prozess beim Schlüsselwechsel der CA aus? Wie wird bei Sicherheitsvorfällen und Kompromittierung der CA vorgegangen? Wie wird der laufende Betrieb wieder hergestellt? Was passiert, wenn die CA ihren Dienst einstellt?
6. Technische Schutzmaßnahmen
   Wie wird das Schlüsselmaterial erzeugt? Welche Schlüssellängen werden unterstützt? Wird eine Smartcard oder ein HSM zum Schutz des privaten Schlüssels der CA verwendet? Wie gelangen der private und der öffentliche Schlüssel bei zentraler Schlüsselgenerierung sicher zum Endanwender? Gibt es eine Sicherungskopie des privaten CA-Schlüssels? Wie wurde diese erzeugt und wie wird die Sicherungskopie sicher verwahrt? Wie wird der CA-Schlüssel aktiviert? Wie sind die Aktivierungsdaten geschützt? Durch welche Sicherheitsmassnahmen ist der CA-Rechner geschützt?
7. Profile für Zertifikate, Sperrlisten und Online-Statusabfragen
   Festlegung des Zertifikatsprofils, Sperrlistenprofils und des Profils für OCSP Responder-Zertifikate.
8. Konformitätsprüfung
   Wie sieht die Überprüfung auf Einhaltung der entsprechenden CP/CPS-Richtlinien aus?
9. Andere geschäftliche und rechtliche Angelegenheiten
   Werden Gebühren für die Dienstleistungen der CA erhoben? Wie wird mit vertraulichen Informationen und personenbezogenen Daten umgegangen? Welche Auflagen gelten für CA, RA, Zertifikatsinhaber und Zertifikatsprüfer? Wie sehen Gewährleistung und Haftungsbeschränkungen der CA aus? Welches Recht gilt und wo ist der Gerichtsstand im Streitfall?

Der Gliederungsrahmen aus RFC 3647 ist in englischer Sprache gehalten. Es gibt keine anerkannte deutsche Übersetzung dieses Gliederungsrahmens, welche die bessere Vergleichbarkeit deutscher Certificate Policies gewährleisten würde. Im Anhang B ist daher eine von Secorvo erstellte deutsche Übersetzung der Gliederung enthalten, die als Vorlage für deutsche Zertifizierungsrichtlinien herangezogen werden kann.

Praxisbeispiele für Certificate Policies, Certification Practice Statements und PKI Disclosure Statements sind in Anhang C aufgeführt.

6 Strukturierung von Policy Dokumente

Typischerweise werden Certificate Policies nach Anwendungsklassen oder Benutzergruppen unterschieden, z. B. kann es eine Certificate Policy für Benutzerzertifikate und eine für Maschinenzertifikate geben. Passend zu jeder Certificate Policy kann es ein eigenständiges Certification Practice Statement geben oder die Umsetzung aller Anforderungen ist in einem einzigen Certification Practice Statement enthalten, wenn nur eine CA betrieben wird. Umgekehrt kann es auch eine übergreifendes Certificate Policy geben, die alle Anforderungen enthält, die dann durch verschiedene Certification Practice Statements von untergeordneten CAs umgesetzt werden. Als dritte Alternative können die Inhalte aus Certificate Policy und Certification Practice Statement auch in einem Dokument verschmolzen werden, wobei in diesem Fall die Certificate Policy nicht veröffentlicht werden kann, ohne die Details aus dem Betrieb der CA ebenfalls zu veröffentlichen. Welche Alternative in der Praxis gewählt wird, hängt dabei vom zugrunde liegenden Geschäftsmodell ab. RFC 3647 gibt keine Hilfestellung, ob ein bestimmter Sachverhalt oder eine bestimmte Formulierung in die CP bzw. das CPS aufgenommen werden soll.

Bei der Wahl der geeigneten Dokumentenstruktur muss berücksichtigt und geklärt werden, ob und ggf. welche Dokumente publiziert werden sollen oder dürfen. Bei einer geschlossenen PKI müssen keine Policy Dokumente von einer CA veröffentlicht werden, da alle Teilnehmer die zugrunde liegenden Zertifizierungs- und Betriebsrichtlinien der PKI kennen und kein Austausch mit Teilnehmern fremder PKIs stattfindet. Andererseits enthalten die Dokumente üblicherweise keine vertraulichen Informationen. Sobald aber signierte und/oder verschlüsselte Daten zwischen fremden PKIs ausgetauscht werden, sollte es die Möglichkeit geben, das Sicherheitsniveau der anderen fremden PKI einschätzen zu können, d. h. es sollten Policy Dokumente öffentlich bereitgestellt werden.

Das PKI Disclosure Statement ersetzt gemäß seiner Definition nicht die Certificate Policy und das Certification Practice Statement, sondern dient nur zur verkürzten und vereinfachten Darstellung der wesentlichen Inhalte. In der Praxis erweist sich jedoch oft die Veröffentlichung eines PKI Disclosure Statement als ausreichende Darstellung der Richtlinien für externe Kommunikationspartner.

Hilfestellung bei der Wahl geeigneter Policy Dokumente sollen folgende Fragestellungen geben:

- An wen richten sich die Dokumente?
- Welche Dokumente sind zur Veröffentlichung bestimmt?

Je nach Interesse der externen Kommunikationspartner am Sicherheitsniveau der PKI kann es ausreichend sein, ein PKI Disclosure Statement zu veröffentlichen. Bei weitergehenden Fragen muss eine Certificate Policy bereitgestellt werden, welche die Anforderungen an die Ausstellung und Verwendung von Zertifikaten detailliert beschreibt.

Wenn ein PKI Disclosure Statement zur Veröffentlichung ausreichend ist, kann die Certificate Policy und das Certification Practice Statement in einem einzigen internen Dokument beschrieben werden. Soll die Certificate Policy auch veröffentlicht werden, so müssen Certificate Policy und Certification Practice Statement in separaten Dokumenten beschrieben werden, um die internen Regelungen für den Zertifizierungsbetrieb (CPS) nicht zu veröffentlichen.

Die Erstellung einer Certificate Policy und eines Certification Practice Statement ist ein anspruchsvoller, zeit- und kostenintensiver Prozess, der häufig unterschätzt wird. Hierbei ist eine Vielzahl an Personen beteiligt:

- Informations-/IT-Sicherheitsbeauftragter (CISO, CSO, etc.) oder PKI-Verantwortlicher

- Rechtsabteilung / Betrieblicher Datenschutzbeauftragter / Betriebsrat
- IT-Betrieb
- Bei Bedarf externe Unterstützung durch Datenschutzberater, Versicherungsberater, PKI-Experten

Insbesondere im Unternehmensumfeld werden diese Dokumente von Juristen und Technikern gleichermaßen geschrieben, da die Haftung für Zertifikatsinhalte einen wesentlichen inhaltlichen Aspekt darstellt. Es gilt daher zunächst einmal, eine einheitliche Terminologie sowie gemeinsame Zielvorstellungen über die zu erstellenden Dokumente festzulegen. Ferner müssen diese Dokumente auch langfristig gültig sein, damit nicht regelmäßig neue Policy-Dokumente geschrieben werden müssen und somit bspw. die Glaubwürdigkeit der PKI sinken könnte. Es gilt daher, die Dokumente sowohl technisch als auch juristisch „stabil“ zu halten.

In der Praxis werden Certificate Policy, Certification Practice Statement und PKI Disclosure Statement nicht ausreichen. Es werden weitere Vereinbarungen in Form von Verträgen zwischen einem Zertifikatsinhaber (Subscriber) und der CA bzw. zwischen einem Zertifikatsprüfer (Relying Party) und der CA erforderlich sein. Diese Vereinbarungen werden Subscriber Agreement bzw. Relying Party Agreement genannt. Mit der Zustimmung zu einem Subscriber Agreement bzw. Relying Party Agreement erklärt sich der Benutzer mit seinen dort genannten Rechten und Pflichten einverstanden.

In der Praxis gibt es nur Subscriber Agreements, aber kaum Relying Party Agreements, da ein Zertifikatsprüfer in der Regel keine Vertragsbeziehung zu der CA hat, die das zu prüfende Zertifikat ausgestellt hat. Eine Ausnahme stellte die Identrus PKI der Banken dar, deren Vertrauensmodell („Four Corner Model“) darauf basierte, dass die PKI-Teilnehmer eine etablierte Geschäftsbeziehung zu ihren Banken haben, die als CAs in der Identrus PKI auftraten. Ein Teilnehmer kontaktierte sowohl in der Rolle als Subscribing Party als auch in der Rolle als Relying Party stets nur seine eigene Bank. Somit schloss er beide, das Subscriber Agreement und das Relying Party Agreement mit seiner eigenen Bank.

7 Bewertung und Vergleichbarkeit von Policies

Bevor ein Benutzer ein fremdes Zertifikat akzeptiert und ihm vertraut, muss er eine Gültigkeitsprüfung durchgeführt haben. Diese Gültigkeitsprüfung umfasst den Namen des Zertifikatsinhabers, die mathematische Korrektheit der Signaturen aller Zertifikate in der Zertifikatskette, den Sperrstatus dieser Zertifikate, die Akzeptanz eines fremden Root Zertifikats und die Certificate Policy, nach der das Zertifikat ausgestellt wurde. Nur wenn alle Prüfungen ein positives Ergebnis liefern, kann der Benutzer diesem Zertifikat vertrauen.

Die meisten dieser Prüfungen lassen sich automatisieren. Lediglich die Akzeptanz fremder Root Zertifikate und damit verbunden die Prüfung der Certificate Policy müssen manuell durchgeführt werden. Dieses „Prüfen“ ist jedoch alles andere als trivial: Einerseits ist der bloße Umfang der meisten Policies schon sehr groß, andererseits existieren keine etablierten Prozesse für die Überprüfung. Helfen können an dieser Stelle die bereits erwähnten PKI Assessment Guidelines (PAG, [ABA-PAG]). Dieses sehr detaillierte Dokument der US-Amerikanischen Anwaltskammer gibt Hilfestellungen bzgl. der Evaluierung von Public Key-Infrastrukturen und kann auch zur Überprüfung von (eigenen sowie „fremden“) Policies dienen.

Dies ist jedoch einem Benutzer nicht zuzumuten. Daher sind in Standardanwendungen, die Zertifikate nutzen, immer eine große Anzahl an Root Zertifikaten bereits enthalten und als vertrauenswürdig vorkonfiguriert, denen der Benutzer so automatisch und unbesehen

vertraut. In Abbildung 1 ist beispielhaft die Zertifikatsansicht der CA Zertifikate in den Browsern Mozilla Firefox und Internet Explorer dargestellt.

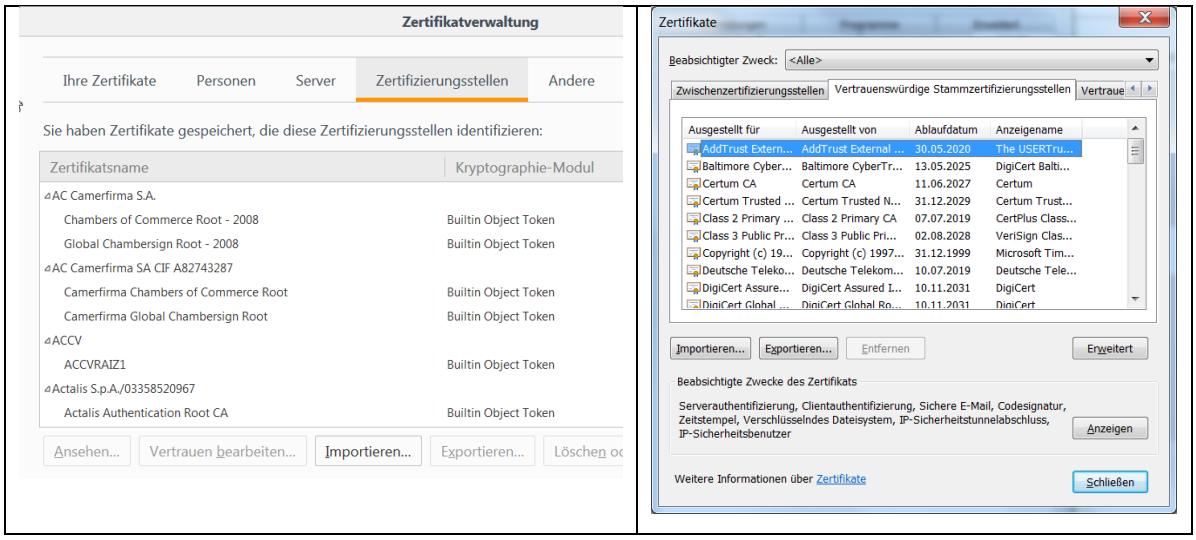

Abbildung 1: Vorkonfigurierte Root Zertifikate in Mozilla Firefox und Internet Explorer

Es ist empfehlenswert, die Prüfung von Policies zentral in einem Unternehmen von kompetenten Fachpersonal durchführen zu lassen und das Ergebnis dann allen Benutzern zur Verfügung zu stellen, so dass nicht jeder Benutzer einzeln diese Policy-Überprüfung durchführen muss. Eine solche Möglichkeit bietet theoretisch die Cross-Zertifizierung. Bei einer Cross-Zertifizierung prüft ein Verantwortlicher die Certificate Policy der fremden PKI und stellt bei Akzeptanz ein Cross-Zertifikat aus. So können die Anwender seiner PKI den Zertifikaten der anerkannten, cross-zertifizierten PKI automatisch vertrauen, da der Zertifizierungspfad wieder bei dem eigenen Root Zertifikat endet.

Allerdings wird heutzutage die Cross-Zertifizierung von den meisten Produkten in der Praxis nicht unterstützt. Es bleibt daher nur die Möglichkeit, von zentraler Stelle aus die Root Zertifikate mit geprüften gültigen Certificate Policies sicher und möglichst transparent an die Anwender zu verteilen; so bietet z. B. Microsoft einen automatischen Verteil-Mechanismus von vertrauenswürdigen CA Zertifikaten über das Active Directory.

Wie aber kann man Certificate Policies miteinander vergleichen, um festzustellen, ob eine fremde Certificate Policy mit der eigenen Certificate Policy vergleichbar ist? Welche Abweichungen sind tolerabel und wann ist eine fremde Certificate Policy zu verschieden von der eigenen, um sie akzeptieren zu können?

Angenommen, bei der einen PKI ist der Root CA Schlüssel in einem HSM gespeichert und der CA Rechner mit dem HSM befindet sich in einem Rechenzentrum; bei einer anderen PKI sind die Schlüssel in Software gespeichert, aber dafür befindet sich der CA Rechner in einem Hochsicherheitsbereich mit Vereinzelungsschleuse, zu der nur wenige ausgewählte Personen Zugang haben. Ist das Sicherheitsniveau dieser beiden PKIs miteinander vergleichbar? Als weiteres Beispiel sei angenommen, dass die Sperrhotline der einen PKI 24x7 Stunden erreichbar ist und sofort bei einem Sperrantrag eine neue Sperrliste ausgestellt wird, wohingegen die Sperrhotline der anderen PKI nur werktags von 8:00 bis 17:00 Uhr verfügbar ist, um einen Sperrantrag entgegenzunehmen und eine neue Sperrliste auszustellen. Auch hier stellt sich wieder die Frage, ob die Certificate Policy akzeptiert werden kann.

Diese beiden Beispiele zeigen nur zwei der zahlreichen Kriterien, in denen sich PKIs unterscheiden können. Es gibt aber noch viele mehr, die letztendlich zusammen das

Sicherheitsniveau einer PKI ergeben. Daher ist der Vergleich von Certificate Policies eine sehr anspruchsvolle Aufgabe.

Hilfreich wäre eine automatisierbare Auswertung von Certificate Policies, wenn diese entsprechend parametrisiert und z. B. in XML geschrieben wären. Das gibt es aber in der Praxis (noch) nicht. Tatsächlich ist es wegen der oben beschriebenen Komplexität sehr schwierig – wenn nicht unmöglich – die Auswertung von Certificate Policies zu automatisieren.

So bleibt es bzgl. der Prüfung und Akzeptanz von Certificate Policies weiter bei dem Spagat zwischen Benutzerfreundlichkeit durch vorkonfigurierte Root Zertifikate auf der einen Seite sowie hohem Sicherheitsbewusstsein mit manueller Prüfung von Certificate Policies auf der anderen Seite.

8 Technische Umsetzung

Wie wird der Bezug zwischen einem Zertifikat und der Certificate Policy, nach der es ausgestellt wurde, hergestellt und wie kann eine CA die Verarbeitung von Certificate Policies in untergeordneten Zertifikaten steuern? Hierfür definiert die Version 3 des X.509 Standards verschiedene Erweiterungen („certificate extensions“) für das Zertifikatsformat und ermöglicht außerdem die Definition beliebiger weiterer privater Zertifikatserweiterungen.

8.1 Certificate Policies

Eine der X.509v3 Zertifikatserweiterungen (*certificatePolicies*) dient dazu, in einem Zertifikat die Zertifizierungsrichtlinie zu benennen, nach der das Zertifikat ausgestellt wurde. Die Benennung erfolgt über sogenannte OIDs (Object Identifier), welche ein Objekt – in diesem Fall eine Zertifizierungsrichtlinie - eindeutig identifizieren. Diese OID wird auch in der Zertifizierungsrichtlinie selbst festgeschrieben. Zusätzlich zu diesem OID können in der Zertifikatserweiterung *certificatePolicies* optional noch weitere Kennzeichner angegeben werden, z. B. eine URL der Zertifizierungsrichtlinie oder der Regelungen für den Zertifizierungsbetrieb (CPS) oder um zusätzliche Informationen als Freitext für die Zertifikatsprüfer zur Verfügung zu stellen.

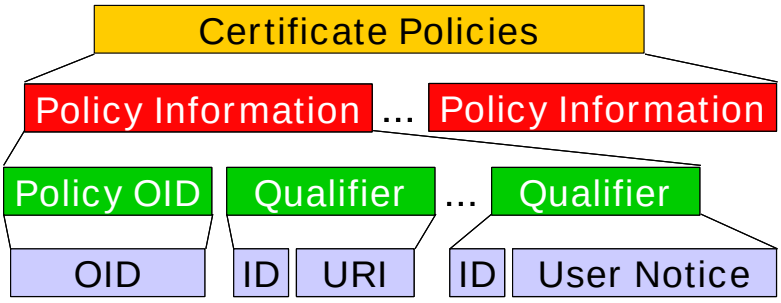

Abbildung 2: „X.509v3 Zertifikatserweiterung Certificate Policies“

Eine Anwendung, die diese Zertifikatserweiterung unterstützt, müsste die Konfiguration von OIDs ermöglichen, die bei einer Zertifikatsprüfung automatisch als vertrauenswürdige Zertifizierungsrichtlinie akzeptiert werden. Heutige Standardanwendungen unterstützen diese Zertifikatserweiterung allerdings noch nicht in dieser Form, sondern zeigen lediglich den Inhalt der Erweiterung an. Dennoch ist es unbedingt empfehlenswert, den OID seiner Zertifizierungsrichtlinie in die ausgestellten Zertifikate einzutragen, um den Zertifikatsprüfern die Möglichkeit zu geben, zumindest manuell die Richtlinie zu prüfen, nach welcher das Zertifikat ausgestellt wurde.

8.2 Policy Mappings

Eine weitere Zertifikatserweiterung (*PolicyMappings*) für CA Zertifikate erlaubt die Zuordnung von fremden Zertifizierungsrichtlinien zu der eigenen Richtlinie. Die CA kann so den Zertifikatsprüfern in ihrem Zertifikat anzeigen, welche Zertifizierungsrichtlinien als gleichwertig gelten. Diese Zertifikatserweiterung hat jedoch keine praktische Relevanz, da sie von heutigen Public Key Infrastrukturen nicht verwendet und auch von Standardanwendungen nicht unterstützt wird.

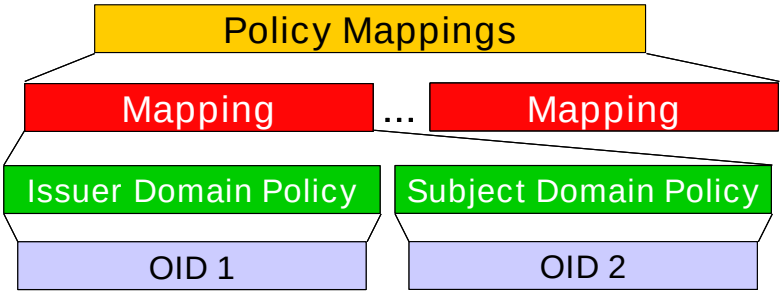

Abbildung 3: „X.509v3 Zertifikatserweiterung Policy Mappings“

8.3 Policy Constraints

Über eine weitere Zertifikatserweiterung (*PolicyConstraints*) kann eine CA für untergeordnete CAs die Verwendung von *certificatePolicies* (8.1) erzwingen oder die Verwendung von *PolicyMappings* (8.2) verbieten.

Wird durch eine CA die Verwendung von *certificatePolicies* erzwungen, können nur diejenigen Zertifikate erfolgreich verifiziert werden, bei denen eine vertrauenswürdige Zertifizierungsrichtlinie in der *certificatePolicies* Erweiterung aufgeführt ist. Die ausstellende CA kann dabei die Tiefe in der Hierarchie festlegen, ab der dieser Zwang zur Verwendung der *certificatePolicies* Erweiterung oder das Verbot der Verwendung von *PolicyMappings* gelten sollen. Gemäß RFC 3280 „Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile“ und ISIS-MTT Teil 1 „Certificates and CRL Profiles“ müssen konforme Anwendungen diese Zertifikatserweiterung *PolicyConstraints* unterstützen, d. h. sie verarbeiten können; praktisch spielt jedoch auch diese Erweiterung keine Rolle, da sie von heutigen Public Key Infrastrukturen nicht verwendet wird.

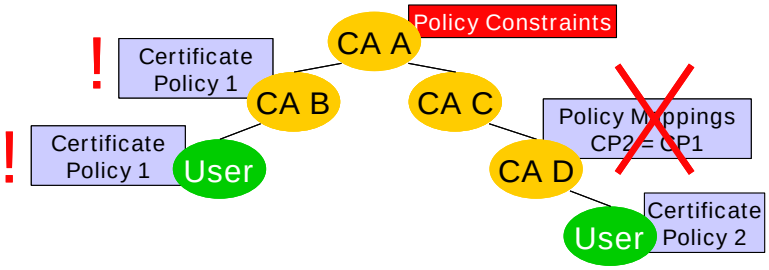

Abbildung 4: „X.509v3 Zertifikatserweiterung Policy Constraints“

8.4 Private Erweiterungen

Der X.509 Standard bietet die Möglichkeit, beliebige eigene Zertifikatserweiterungen zu definieren, wenn die im X.509v3 Standard definierten Erweiterungen nicht ausreichen. So hat beispielsweise Microsoft eine eigene private X.509v3 Zertifikatserweiterung definiert (*application policies)*, die anzeigt, ob ein Zertifikat für eine bestimmte Anwendung eingesetzt

werden darf. Als Beispiel für einen möglichen Wert in dieser Microsoft-proprietären Erweiterung könnte hier der OID für die Zertifikatsanwendung Smart Card Logon eingetragen werden (1.3.6.1.4.1.311.20.2.2). Dieser OID kann aber alternativ auch in der standardisierten Zertifikatserweiterung *ExtendedKeyUsage* im Zertifikat eingetragen werden.

9 Fazit

Zum Betrieb einer PKI gehören in jedem Fall eine Certificate Policy und ein Certification Practice Statement. Hierdurch wird den Anwendern oder anderen CAs die Möglichkeit gegeben, sich über den Betrieb der CA zu informieren.

Je nach Anwender muss die Certificate Policy oder ein PKI Disclosure Statement öffentlich verfügbar sein. Bei der Erstellung eines internen Certification Practice Statement kann auf im Unternehmen existierende Betriebskonzepte oder andere passenden Regelungen verwiesen werden.

Die Erstellung dieser Dokumente ist ein zeit- und ressourcenaufwändiger Prozess. Aktuelle Certificate Policy oder Certification Practice Statement Dokumente sollten konform zu RFC 3647 erstellt werden, um die Aufwände zu verringern und den Lesern eine bessere Vergleichbarkeit von Policies zu ermöglichen. Bei der Erstellung von PKI Disclosure Statements sollte die durch PAG bzw. ETSI vorgegebene Struktur und Inhalt eingehalten werden.

Literatur

[PEM] S. Kent: „RFC 1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management“, Februar 1993.
http://www.rfc-editor.org/rfc/rfc1422.txt

[NIST] M. S. Baum: *„Federal Certification Authority Liability and Policy“*, NIST-GCR-94-654, Juni 1994.
http://www.itl.nist.gov/lab/list91.htm

[X.509] International Telecommunication Union: „Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks, ISO/IEC 9594-8:2008, ITU-T Recommendation X.509, Ausgabe 2008.
http://www.iso.org

[ABA-DSG] American Bar Association: „Digital signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce“, 1996.
http://www.abanet.org/scitech/dch/PKIGuidelines.pdf

[ABA-PAG] American Bar Association: „ PKI Assessment Guidelines, Version 0.3”, 18.Juni 2001
http://www.abanet.org/scitech/ec/isc/pagv30.pdf

[POL-REQ] European Telecommunications Standards Institute (ETSI): „Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, (EN 319 411-1 – V1.1.1)”, Februar 2016
http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf

[POL-REQ-QUAL] European Telecommunications Standards Institute (ETSI): Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (EN 319 411-2 – V2.1.1), Februar 2016.
http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf

[RFC 1875] N. Berge: „RFC 1875: UNINETT PCA Policy Statements “, Dezember 1995.
http://www.rfc-editor.org/rfc/rfc1875.txt

[DFN-PCA] „DFN-Bericht Nr. 82: Zertifizierungsrichtlinien des Projekts ‚PCA im DFN‘“, April 1997. http://www.dfn.de/index.php?id=11816

[RFC 2527] S. Chokhani, W. Ford: „RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“, März 1999.
http://www.rfc-editor.org/rfc/rfc2527.txt

[RFC 3647] S. Chokhani, W. Ford, R. Sabett: „RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“, November 2003.
http://www.rfc-editor.org/rfc/rfc3647.txt

Anhang A – PKI Disclosure Statement (ABA PAG)

Nachfolgend ist ein Auszug aus den American Bar Association Information Security Committee's *PKI Assessment Guidelines* (Appendix 6) angegeben [ABA-PAG]:

The following table represents the PDS categories, listing a section for each defined statement type (category) and a corresponding descriptive statement that may include hyperlinks or computer references to the relevant CP or CPS sections.

Statement Types	Statement Descriptions
CA contact information	Name, location and relevant contact information for the CA.
Certificate type, validation procedures and usage	Description [Note 3] of each class/type of certificate issued by the CA [Note 4] corresponding validation procedures [Note 5], and any restrictions on certificate usage [Note 6].
Reliance limits	Reliance limits, if any.
Obligations of subscribers	Description of, or reference to, the critical subscriber obligations [Note 7].
Certificate status checking obligations of relying parties	Extent to which relying parties are obligated to check certificate status, and references to further explanation [Note 8]
Limited warranty and disclaimer/Limitation of liability	Summary of the warranty [Note 9] disclaimers, limitations of liability and any applicable warranty or insurance programs.
Applicable agreements, Certification Practice Statement, Certificate Policy	Identification and references to applicable agreements, CPS, CP [Note 10].
Privacy policy	Description of and reference to the applicable privacy policy, if any.
Refund policy	Description of and reference to the applicable refund policy, if any.
Applicable law and dispute resolution	Statement of the choice of law and dispute resolution mechanism.
CA and repository licenses, trust marks, and audit	Summary of any governmental licenses, seal programs and a description of the

Statement Types	Statement Descriptions
	audit process [Note 11] and, if applicable, the audit firm.

[Note 3] Including the corresponding certificate policy object identifier that must also be included in the certificates.

[Note 4] Alternatively, there can be separate PDSs for each type or class of certificate.

[Note 5] May simply reference the X.509 certificate processing rules.

[Note 6] Including the requirements to qualify as a subscriber or relying party and any restrictions on the applications for which the certificates are approved to be used.

[Note 7] Including the requirement to protect the confidentiality of the subscriber's private key and report actual or suspected compromise or change of material circumstances.

[Note 8] Including the requirement to protect the integrity of the CA's public key, and, optionally, including instructions for retrieving certificates the CA issues.

[Note 9] Including whether the CA warrants the accuracy of the information contained in the certificate.

[Note 10] Particularly if the PDS is simply an extract from the CP.

[Note 11] Including a reference to the current specific audit report.

Anhang B – Deutscher Gliederungsrahmen nach RFC 3647

Übertragung ins Deutsche durch Secorvo Security Consulting GmbH.

1 Einleitung
1.1 Überblick
1.2 Name und Kennzeichnung des Dokuments
1.3 PKI-Teilnehmer
1.3.1 Zertifizierungsstellen
1.3.2 Registrierungsstellen
1.3.3 Zertifikatsnehmer
1.3.4 Zertifikatsnutzer
1.3.5 Andere Teilnehmer
1.4 Verwendung von Zertifikaten
1.4.1 Erlaubte Verwendungen von Zertifikaten
1.4.2 Verbotene Verwendungen von Zertifikaten
1.5 Pflege des Policy-Dokuments
1.5.1 Zuständigkeit für das Dokument
1.5.2 Ansprechpartner/Kontaktpersonen
1.5.3 Zuständiger für die Anerkennung einer CP in Hinblick auf diese Mindestanforderungen
1.5.4 Annahmeverfahren für Teilnehmer-CP
1.6 Definitionen und Abkürzungen
2 Veröffentlichungen und Verzeichnisdienst
2.1 Verzeichnisdienste
2.2 Veröffentlichung von Informationen zur Zertifikatserstellung
2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen
2.4 Zugriffskontrollen auf Verzeichnisse
3 Identifizierung und Authentifizierung
3.1 Namensregeln
3.1.1 Arten von Namen
3.1.2 Notwendigkeit aussagefähiger Namen
3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern
3.1.4 Regeln für die Interpretation verschiedener Namensformen
3.1.5 Eindeutigkeit von Namen
3.1.6 Verwendung von Markennamen
3.2 Erstmalige Überprüfung der Identität

Anhang C – Beispiele für Policies

Beispiele für Certificate Policies:

DFN-PKI:	https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CP.pdf
Symantec Trust Network:	https://www.symantec.com/content/en/us/about/media/repository/stn-cp.pdf
Deutsche Bundesbank:	http://www.bundesbank.de/Redaktion/DE/Downloads/Service/Services_Banken_Unternehmen/PKI/certification_policy_email_security_certificates_counterparties.pdf
Smart-Meter-PKI:	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/PKI_Certificate_Policy.html

Beispiele für Certification Practice Statements:

DFN-PKI:	https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CPS.pdf
Symantec Trust Network:	https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf

Deutsche Bundesbank:	http://www.bundesbank.de/Redaktion/DE/Downloads/Service/Services_Banken_Unternehmen/PKI/certification_practice_statement_counterparties_cps.pdf

Beispiele für PKI Disclosure Statements:

Deutsche Renten-versicherung:	http://www.deutsche-rentenversicherung.de/Bund/de/Inhalt/5_Services/05_fachinformationen/Trustcenter/TCDRV_PDS_DRV-QC-Root-CA_010000_20170421_DE.html
Stadtwerke Bochum	http://www.stadtwerke-bochum-netz.de/etc/medialib/nmr/kommunikationsdaten.Par.0006.File.tmp/PKI%20Disclosure%20Statement.pdf
Carl Zeiss AG	https://www.zeiss.it/content/dam/Corporate/about_cz/downloads/pdf/pki-disclosure-statement_email-ca.pdf