RAT DER EUROPÄISCHEN UNION

Brüssel, den 2. August 2013 (04.09)
(OR. en)

11660/13

CSCI 38
CSC 63

I/A-PUNKT-VERMERK

des	Sicherheitsausschusses des Rates
für den	AStV/Rat
Betr.:	Sicherheitskonzept für die Informationssicherung bei Public-Key-Infrastrukturen

1. Nach dem Beschluss des Rates über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen[1] billigt der Rat – soweit erforderlich – "auf Empfehlung des Sicherheitsausschusses Sicherheitskonzepte mit Maßnahmen zur Anwendung dieses Beschlusses" (siehe Artikel 6 Absatz 1).

2. Der Sicherheitsausschuss des Rates ist übereingekommen, ein Konzept zu empfehlen, mit dem für Public-Key-Infrastrukturen Standards festgelegt werden, nach denen EU-Verschlusssachen (EU-VS) in den Informations- und Kommunikationssystemen (CIS) hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie gegebenenfalls Authentizität und Nichtabstreitbarkeit zu schützen sind.

3. Vorbehaltlich der Bestätigung durch den AStV wird der Rat ersucht, das beigefügte Sicherheitskonzept zu billigen.

[1] Beschluss 2011/292/EU des Rates (ABl. L 141 vom 27.5.2011, S. 17).

absichtliche Leerseite

Sicherheitskonzept für die Informationssicherung bei Public-Key-Infrastrukturen

IASP 2-4

INHALT

I. ZWECK UND ANWENDUNGSBEREICH

1. Dieses Konzept, das vom Rat gemäß Artikel 6 Absatz 1 der Sicherheitsvorschriften des Rates (im Folgenden "SVR") gebilligt wurde, legt Standards für den Schutz von EU-Verschlusssachen (EU-VS) fest. Es soll dazu beitragen, dass die Sicherheitsvorschriften in einheitlicher Weise angewandt werden.

2. Mit diesem Konzept für Public-Key-Infrastrukturen (PKI) soll festgelegt werden, wie PKI zu nutzen sind, damit EU-VS geschützt sind, und zwar in folgender Hinsicht:

   (a) Organisation der PKI insgesamt;

   (b) Einschränkungen für die Nutzung von PKI entsprechend dem Geheimhaltungsgrad und anderen Parametern;

   (c) Verhältnis zu anderen Konzepten und Dokumenten der EU.

3. Der Rat und das Generalsekretariat des Rates wenden dieses Sicherheitskonzept für den Schutz von EU-VS in ihren Räumlichkeiten und in ihren Informations- und Kommunikationssystemen (CIS) an.

4. Die Mitgliedstaaten sorgen nach Maßgabe ihrer innerstaatlichen Rechts- und Verwaltungsvorschriften für die Einhaltung der in diesem Sicherheitskonzept für den Schutz von EU-VS festgelegten Standards, wenn EU-VS in nationalen Strukturen – einschließlich nationaler CIS – bearbeitet werden.

5. Die im Rahmen des Titels V Kapitel 2 EUV errichteten Agenturen und Einrichtungen der EU sowie Europol und Eurojust sollten dieses Sicherheitskonzept als Bezugsrahmen für die Anwendung der Sicherheitsvorschriften in ihren eigenen Strukturen verwenden.

6. Der Begriff "PKI" bezeichnet in diesem Dokument allein hierarchische Infrastrukturen, die Public-Key-Zertifikate[2] zum Schutz von EU-VS verwalten.

[2] Sonstige Zertifikate, z.B. Attributzertifikate sind nicht Gegenstand dieses Dokuments.

7. Dieses Konzept gilt nicht für PKI, die in Produkten gemäß Artikel 10 Absatz 6 der SVR[1] verwendet werden, welche einer Zweitevaluierung[3] unterzogen werden müssen.

8. Die PKI-Produkte müssen zudem mit dem Informationssicherungskonzept für die Verschlüsselung[4] vereinbar sein.

II. EINLEITUNG

9. Für die elektronische Kommunikation in einem Teilnehmernetz (das "offen"[5] sein kann) werden möglicherweise Mittel benötigt, um die Authentizität der Nachrichten zu beweisen und die Nichtabstreitbarkeit der Vorgänge zu gewährleisten.

10. Solche Mittel können durch eine vertrauenswürdige dritte Instanz (Trusted Third Party) bereitgestellt werden, die als Notariat fungiert und Informationen für andere beglaubigt. Dies lässt sich technisch durch eine asymmetrische Verschlüsselung in Verbindung mit einer geeigneten Infrastruktur und Organisation erreichen, einer sogenannten PKI.

11. Von der PKI erzeugte Erklärungen, die die Authentizität der Informationen belegen, werden in Form eines Zertifikats aufgezeichnet. Bei dem Zertifikat, das ein Standardformat haben sollte, handelt es sich um ein elektronisches Dokument, das für eine bestimmte Zeit gültig ist. Zertifikate werden von Teilnehmern angefordert und für bestimmte Subjekte (Personen oder Systeme) ausgestellt. Ein Zertifikat, das die Authentizität eines öffentlichen Schlüssels belegt, heißt Public-Key-Zertifikat. Public-Key-Zertifikate können von jedermann benutzt werden, um die Authentizität von Informationen des Zertifikatssubjekts, beispielsweise andere Zertifikate, Sperrlisten, E-Mails usw. zu überprüfen.

12. An den PKI sind folgende Akteure beteiligt:

(i) Kunden

(a) Teilnehmer: Einheiten, die ein Zertifikat förmlich beantragen und die Informationen, deren Authentizität zu überprüfen ist, übermitteln.

---

[3] Beispielsweise geschlossene oder externe PKI, die in COMSEC-Systemen verwendet werden.
[4] IASP 2[RESTREINT UE/EU RESTRICTED] IA Security Policy on Cryptography, Dokument 10745/11.
[5] Ein offenes Netz können die Teilnehmer benutzen und verlassen, ohne jedes Mal einen neuen Schlüssel zu generieren.

(b) Subjekte: Einheiten, denen Zertifikate ausgestellt werden und die sie nutzen. Dabei kann es sich um Personen oder um IT-Systeme handeln.

(c) vertrauende Beteiligte: Einheiten, die die Authentizität der Informationen prüfen und hierfür das Zertifikat validieren.

(ii) Diensteanbieter

(d) Zertifizierungsstelle(n): eine Einheit, die den Teilnehmern förmlich Zertifikate ausstellt und eine bestimmte Haftung übernimmt.

(e) Registrierungsstelle(n): eine Einheit, die von der Zertifizierungsstelle mit der Registrierung der Teilnehmer beauftragt wird. Sie hat die Angaben der Teilnehmer zu überprüfen.

(f) Prüfstelle(n): ein unabhängiges Gremium, das sicherstellt, dass die vom Diensteanbieter ausgeführten Prozesse hinreichend transparent sind.

III. EINSCHRÄNKUNGEN FÜR DIE NUTZUNG VON PKI

13. Der Entscheidung, eine PKI zu nutzen, sollte ein Risikomanagementprozess vorausgehen. Gegebenenfalls kann eine alternative Lösung (z.B. ein Schlüsselverteilzentrum/Key Distribution Centre) gewählt werden.

14. Die PKI muss Gewähr für eine ausreichende Qualität der folgenden Vorgänge bieten:

(a) Registrierung – der Prozess der Beantragung des Zertifikats, einschließlich der Überprüfung der Angaben des Antragstellers (Teilnehmers).

(b) Erstellung eines Zertifikats – der Prozess der materiellen Herstellung eines elektronischen Dokuments, der Generierung des Schlüsselpaares und der Verknüpfung des öffentlichen Schlüssels mit dem Subjekt des Zertifikats.

(c) Speicherung, Veröffentlichung und Übergabe – Freigabe des Zertifikats für alle zugelassenen Dienstenutzer und Übergabe des Zertifikats an den Teilnehmer, der es nutzen will.

(d) Aussetzung/Entzug – Sperrung eines Zertifikats auf Antrag eines oder mehrerer zugelassener Nutzer.

(e) Widerruf eines Zertifikats – dauerhafte Sperrung eines Zertifikats auf Antrag eines Nutzers oder weil es abgelaufen ist.

(f) Verlängerung – Erneuerung des Zertifikats nach Ablauf seiner Gültigkeit unter Verwendung derselben Informationen über das Subjekt und desselben öffentlichen Schlüssels.

(g) Änderung des Schlüssels – Erstellung eines neuen Zertifikats für ein bestimmtes Subjekt mit einem neuen Schlüsselpaar.

15. Eine PKI kann nur Zertifikate für die folgenden Sicherheitsdienste verwalten:

(a) Identifizierung und Authentifizierung der kommunizierenden Parteien;

(b) Überprüfung der Quelle (Authentizität) und Integrität bestimmter EU-VS;

(c) Nichtabstreitbarkeit der Vorgänge – Gewährleistung, dass Nutzer ihre Vorgänge (gegenüber anderen kommunizierenden Parteien oder forensischen Diensten) nicht bestreiten können und dass sie beweisen können, dass Transaktionen stattgefunden haben;

(d) Austausch der Sitzungsschlüssel für die Verschlüsselung von EU-VS;

(e) Vertraulichkeit – nur bis zu einer bestimmten Geheimhaltungsstufe;

(f) eine Zeitstempelfunktion, die belegt, dass bestimmte Daten vor einem bestimmten Zeitpunkt vorgelegen haben.

16. Das Sicherheitsniveau und die Einschränkungen (in Bezug auf die zugelassenen Dienste und Geheimhaltungsstufen usw.) für die Nutzung des Public-Key-Zertifikats müssen in einem Zertifizierungskonzept erläutert werden. In den Zertifikaten, die eine Zertifizierungsstelle für Endnutzer ausstellt, muss angegeben werden, welche Zertifizierungskonzepte für sie maßgeblich sind[6].

17. Die Anzahl der Zertifizierungskonzepte muss strikt begrenzt werden, damit es nicht für jede PKI eine anderes Zertifizierungskonzept gibt.

18. Sofern sie mit dem Informationssicherheitskonzept für die Verschlüsselung zu vereinbaren sind, sollten die PKI (und damit die Zertifizierungskonzepte) vorzugsweise die Auflagen der Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[7] und die diesbezüglichen Normen[8] für qualifizierte Signaturen einhalten.

IV. ORGANISATION DER PKI

19. Die PKI sollten in einer einzigen Organisation zusammengefasst sein. Unabhängige CIS-spezifische PKI sollten nur genutzt werden, wenn die Ergebnisse des Risikomanagementprozesses dies rechtfertigen.

20. Die PKI sollten mindestens die beiden folgenden Organisationsebenen umfassen (siehe Figure 1):

    (a) Ebene 1: PKI-Verwaltungsstelle, Prüfstelle und Akkreditierungsstelle, Zertifizierungsstelle (Policy Certification Authority) und oberste Zertifizierungsstelle (Root CA);

---

[6] Mit Hilfe von Objektbezeichnern und/oder Verweisen, die zum jeweiligen Zertifizierungskonzept und/oder der Zertifizierungsregelung (siehe Nummer 34) führen.

[7] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Abl. L 13 vom 19.1.2000, S. 12-20.

[8] Entscheidung 2003/511/EG der Kommission vom 14. Juli 2003 über die Veröffentlichung von Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen.

(b) Ebene 2: nachrangige Zertifizierungsstellen, fakultative Registrierungsstellen, Dienste für Endnutzer (z.B. Helpdesk), fakultative Zertifizierungsstellen. Ebene 2 kann entfallen, wenn nur eine nachgeordnete Zertifizierungsstelle benötigt wird.

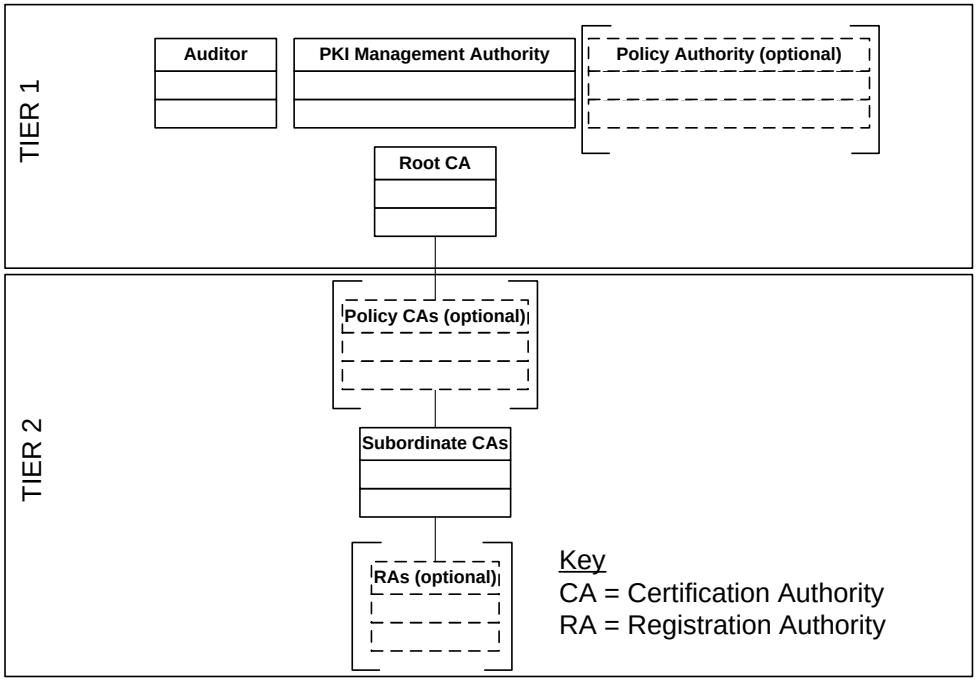

Schaubild 1 PKI-Hierarchie und -Stellen

21. Die Verantwortung für den Aufbau und die Verwaltung einer PKI muss einer PKI-Verwaltungsstelle übertragen werden, die auch die Aufgaben eines Verwalters sensibler CIS (SCISM) oder einer für den Betrieb zuständigen Informationssicherungsstelle übernehmen kann.

22. Die PKI muss von einer Prüfstelle, die von Betriebsfunktionen wie dem SCIM und der Informationssicherungsstelle unabhängig sein sollte, regelmäßig überprüft werden. Ausmaß und Häufigkeit der Überprüfung sind im Einzelnen in den jeweiligen Zertifizierungskonzepten und Zertifizierungsregelungen festzulegen.

23. Wenn ihre Größe dies rechtfertigt, sollte die Organisation eine zentrale Zertifizierungsstelle einrichten, die für folgende Aufgaben zuständig ist:

(a) Formulierung von Zertifizierungskonzepten;

(b) Beratung anderer Parteien beim Verfassen eigener Zertifizierungskonzepte;

(c) Bewertung von Zertifizierungsregelungen;

(d) Bewertung externer Zertifizierungskonzepte und Zertifizierungsregelungen bei Entscheidungen über Überkreuz-Zertifizierungen;

(e) Führung eines Zentralregisters über bestehende CAs und ihre Vereinbarkeit mit bestehenden Zertifizierungskonzepten;

(f) Beratung betreffend die Nutzung einer bestimmten CA.

24. Vorzugsweise sollte es nur eine oder nur sehr wenige zentrale CAs, sog. Root CAs, geben, die Zertifikate für die nachgeordneten CAs signieren.

25. Für bestimme Zertifikate für Endnutzer und somit für besondere Zertifizierungskonzepte wie beispielsweise Server-Authentifizierung für R-UE/EU-R CIS sollten CAs der zweiten Ebene (nachgeordnete CA in Figure 1) eingerichtet werden.

26. Die PKI können zwischengeschaltete CAs (Policy Certification Authorities[9]) benennen. Diese Stellen dürfen dann jeweils nur ein Zertifizierungskonzept unterstützen und können nur Zertifikate für Teilnehmer nachrangiger CAs (ausstellende CAs) ausstellen.

27. Die den Policy Certification Authorities nachgeordneten CAs können zusätzliche Auflagen für die Verwendung der von ihnen ausgestellten Zertifikate vorgeben (und beispielsweise bestimmte Verwendungen wie die Server-Authentifizierung oder Signatur ausschließen).

[9] Mit RFC 1422 eingeführtes Konzept, dass seither durch flexiblere Zertifizierungskonzepte ersetzt wurde.

28. Die Registrierung und Überprüfung der Angaben der Teilnehmer kann an eine Registrierungsstelle delegiert werden.

29. Die Schlüsselgenerierung ist eine strategische Entscheidung, die der die PKI verwaltenden Organisation obliegt. Die Bedingungen und Zuständigkeiten für die Generierung und Speicherung von Schlüsseln müssen im jeweiligen Zertifizierungskonzept festgelegt werden.

V. FÜR PKI MASSGEBLICHE DOKUMENTE

30. PKI müssen im Einklang mit den einschlägigen Sicherheitskonzepten und Sicherheitsleitlinien der EU, insbesondere dem Informationssicherungskonzept für die Verschlüsselung, akkreditiert werden.

31. Weitere Einzelheiten zur Umsetzung dieses Konzepts und genauere Angaben zu den Einschränkungen werden in den IA-Sicherheitsleitlinien für PKI niedergelegt.

32. Das Format der Zertifikate muss die Norm X.509[10] erfüllen.

33. Einzelheiten zu den Einschränkungen für die Verwendung eines bestimmten Zertifikats müssen in den Zertifizierungskonzepten festgelegt werden. Hierauf muss gemäß dem Rahmen für PKI-Zertifizierungskonzepte und Zertifizierungsregelungen[11] im Zertifikat hingewiesen werden.

34. Einzelheiten zur Funktionsweise einer bestimmten Zertifizierungs- oder Registrierungsstelle müssen gemäß dem Rahmen für PKI-Zertifizierungskonzepte und Zertifizierungsregelungen in der Zertifizierungsregelung festgelegt werden. Aus der Zertifizierungsregelung muss hervorgehen, wie die Stelle die Anforderungen der Zertifizierungsstelle erfüllt.

[10] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[11] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

BEGRIFFSBESTIMMUNGEN

Akkreditierung	das Verfahren, das zu einer förmlichen Erklärung der Sicherheits-Akkreditierungsstelle (SAA) führt, wonach ein System für den Betrieb mit einem definierten Geheimhaltungsgrad, in einem bestimmten Sicherheitsmodus in seiner Betriebsumgebung und bei einem akzeptablen Risikoniveau unter der Voraussetzung zugelassen wird, dass ein anerkanntes Bündel von Sicherheitsmaßnahmen in den Bereichen Technik, physischer Schutz, Organisation und Verfahren durchgeführt wird.
Gewährleistung der Sicherheit	quantitative Gründe, die das Vertrauen darin rechtfertigen, dass eine Einheit ihre Sicherheitsziele erfüllt.
Gewährleistungsstufe	diskreter Gewährleistungswert. Bei Kryptokonzepten und kryptografischen Produkten gibt es nur zwei Stufen – zugelassen (was zum Ausdruck gebracht wird, indem ein Produkt in ein Produktverzeichnis aufgenommen wird) und nicht zugelassen (was zum Ausdruck gebracht wird, indem ein Produkt nicht in das Verzeichnis aufgenommen wird).
Authentifizierung	der Prozess der Feststellung, dass Personen, Organisationen oder Dinge diejenigen sind, für die sie sich ausgeben. Im Rahmen einer PKI kann Authentifizierung bedeuten, dass festgestellt wird, dass es sich bei der Person oder Organisation, die unter einem bestimmten Namen Zugang zu etwas beantragt oder erhalten will, tatsächlich um diese Person oder Organisation handelt.
Authentizität	die Garantie, dass die Informationen echt sind und aus Bona-fide-Quellen stammen.
Verfügbarkeit	der Umstand, dass die Informationen auf Anfrage einer befugten Stelle verfügbar und nutzbar sind.
Zertifikat	eine elektronische Bescheinigung, die von der Zertifizierungsstelle elektronisch signiert wurde.
Zertifizierungskonzept	eine namentlich bezeichnete Regelung, aus der hervorgeht, dass ein Zertifikat für eine bestimmte Gruppe und/oder Art von Anwendungen mit gemeinsamen Sicherheitsanforderungen gilt. Beispielsweise kann im Einzelfall in einem Zertifizierungskonzept angegeben werden, dass eine Art von Zertifikat für die Authentifizierung von Parteien, die am Geschäftsverkehr für den Handel mit Waren oder Dienstleistungen einer bestimmter Preiskategorie teilnehmen, anzuwenden ist.
Zertifizierungsregelung	eine Erklärung darüber, wie eine Zertifizierungsstelle bei der Ausstellung, bei der Verwaltung, beim Widerruf und bei der Verlängerung von Zertifikaten oder bei der Änderung von Schlüsseln verfährt.

Zertifikatsnutzer	Siehe unten unter "vertrauender Beteiligter".
Informations- und Kommunikationssystem (CIS)	ein System, das die Bearbeitung von Informationen in elektronischer Form ermöglicht. Zu einem Kommunikations- und Informationssystem gehören sämtliche für seinen Betrieb benötigten Voraussetzungen, einschließlich der Infrastruktur, der Organisation, des Personals und der Informationsressourcen. Siehe Artikel 10 Absatz 2 der SVR.
Vertraulichkeit	der Umstand, dass die Informationen nicht gegenüber unbefugten Personen, Stellen oder Verarbeitungsprozessen offengelegt werden.
Elektronische Signatur	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.
EU-Verschlusssachen (EU-VS)	alle mit einem EU-Geheimhaltungsgrad gekennzeichneten Informationen oder Materialien, deren unbefugte Weitergabe den Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße schaden könnte. Siehe Artikel 2 Absatz 1 der SVR.
Identifizierung	die Feststellung der Identität einer Person oder Organisation, d.h. der Nachweis, dass es sich bei einer Person oder Organisation um eine bestimmte Person oder Organisation handelt. Im Rahmen einer PKI bezeichnet der Begriff "Identifizierung" zweierlei: (1) die Feststellung, dass dem Namen einer Person oder Organisation eine reale Identität einer Person oder Organisation entspricht, und (2) die Feststellung, dass es sich bei der Person oder Organisation,die unter diesem Namen Zugang zu etwas beantragt oder erhalten will, tatsächlichum die genannte Person oder Organisation handelt. Bei der Person, die identifiziert werden möchte, kann es sich um einen Zertifikatsantragsteller, einen Bewerber um eine Vertrauensstelle bei einem PKI-Teilnehmer oder einePerson handeln, die Zugang zu einem Netz oder einer Software-Anwendung erhalten möchte, beispielsweise umeinen Sachbearbeiter einer CA, der Zugang zu den Systemen der CA erhalten möchte
Integrität	der Umstand, dass die Genauigkeit und die Vollständigkeit der Informationen und Werte gewährleistet sind.
Nichtabstreitbarkeit	die Fähigkeit, nachzuweisen, dass ein Vorgang oder ein Ereignis stattgefunden hat, so dass dieser Vorgang oder dieses Ereignis nicht nachträglich abgestritten werden kann.

Public-Key-Zertifikat (PKC)	elektronische Daten, die den öffentlichen Schlüssel einer Einheit (etwa einer Person, einer Organisation, eines Kontos, eines Geräts oder einer Website) an ein Bündel von Informationen binden, mit dem die Einheit identifiziert wird, die mit der Nutzung des entsprechenden privaten Schlüssels in Zusammenhang steht. In den meisten Fällen setzen sie Identitätszertifikate voraus.
Registrierungsstelle	eine Einheit, die für eine oder mehrere der folgenden Aufgaben verantwortlich ist: Identifizierung und Authentifizierung von Zertifikatsantragstellern, Genehmigung oder Ablehnung von Zertifikatsanträgen, Einleitung des Widerrufs oder der Aussetzung eines Zertifikats unter bestimmten Umständen, Bearbeitung von Teilnehmeranträgen auf Widerruf oder Aussetzung ihrer Zertifikate und Genehmigung oder Ablehnung von Teilnehmeranträgen auf Verlängerung ihrer Zertifikate oder Änderung der Schlüssel. Registrierungsstellen signieren jedoch keine Zertifikate und stellen keine Zertifikate aus (sie führen lediglich bestimmte Aufgaben im Namen einer Zertifizierungsstelle aus).
Vertrauender Beteiligter	eine Empfänger eines Zertifikats, der sich auf dieses Zertifikat und/oder die digitalen Signaturen, die dieses Zertifikat verwenden, verlässt. Die Begriffe "Zertifikatnutzer" und "vertrauender Beteiligter" sind austauschbar.
Risiko	die Möglichkeit, dass bei einer bestimmten Bedrohung die internen und externen Schwachstellen einer Organisation oder eines der von ihr verwendeten Systeme ausgenutzt und dadurch die Organisation und ihre materiellen und immateriellen Werte geschädigt werden. Gemessen wird das Risiko als die Kombination der Wahrscheinlichkeit des Eintretens von Bedrohungen und ihrer Auswirkungen.
Subjekt (Zertifikatssubjekt)	die Einheit, deren öffentlicher Schlüssel oder andere Attribute mit dem Zertifikat bescheinigt werden.
Teilnehmer (Zertifikatnehmer)	die Einheit, die sich einer Zertifizierungsstelle anschließt, um Zertifikate zu erhalten.