



**Lösungsvorschlag zur  
10. Übung zur Vorlesung  
Public-Key-Infrastrukturen  
SS 2006**

**Aufgabe 1: Private Schlüssel**

- a) Warum ist der Schutz privater Schlüssel innerhalb eines Trust Centers besonders wichtig?
- b) Nennen Sie die Stationen im Lebenszyklus eines privaten Schlüssels!
- c) Wie stehen diese miteinander in Beziehung?
- d) Wo liegen die Gefahren der einzelnen Stationen?

**Lösungsvorschlag**

- a) Die Benutzung privater Schlüssel ist notwendige und hinreichende Bedingung zur:
  - Entschlüsselung chiffrierter Daten
  - Signatur von Dokumenten
  - Identifikation von Personen, Geräten oder Diensten

Einen privaten Schlüssel benutzen zu können reicht aus, um oben genannte Aktionen durchzuführen. Kommt ein privater Schlüssel in falsche Hände, kann der Angreifer diese Aktionen ausführen. Man kann dann nicht mehr zwischen dem Angreifer und dem eigentlichen Besitzer des privaten Schlüssels (bzgl. Signaturen, Identifikation und wer Dokumente lesen kann) unterscheiden. Das bedingt unter Umständen auch "legal" ausgefertigten Signaturen. Kommt der private Schlüssel der CA in falsche Hände, ist die gesamte PKI zerstört. Es kann dann nicht mehr einfach zwischen rechtmäßigen und gefälschten Zertifikaten unterschieden werden. Um das zu verhindern, ist der Schutz privater Schlüssel sehr wichtig.

b),c) Siehe Abb. 1

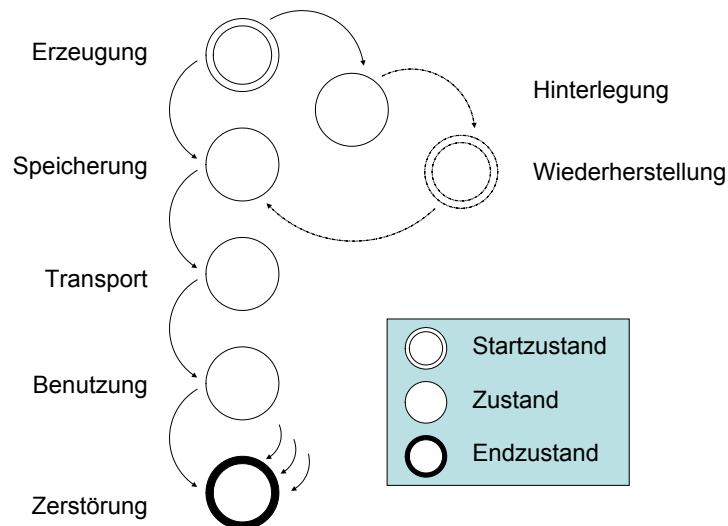


Abbildung 1: Lebenszyklus privater Schlüssel

d) **Erzeugung** Beim Generieren der Schlüssel muss darauf geachtet werden geeignete Parameter (Algorithmus, Schlüssellänge, ...) zu wählen. Es ist weiterhin wichtig einen sicheren Zufallszahlengenerator zu verwenden. Können Zufallszahlen voraus- oder zurückberechnet werden ist es möglich auch fremde Schlüssel zu berechnen. Es muss sichergestellt werden, dass die Schlüssel nicht ausgespäht (Abstrahlung, Memory Leak, ...) werden können.

**Speicherung** Die Speicherung der Schlüssel muss in jedem Fall persistent sein. Nach der Speicherung auf ein geeignetes Medium (PKCS#12, Chipkarte, ...) muss der Schlüssel aus dem Generator sicher entfernt werden. Der gespeicherte Schlüssel muss vor fremdem Zugriff geschützt werden (Passwort, PIN, ...).

**Transport** Es muss sichergestellt werden, dass das Token beim richtigen Empfänger ankommt. Die Zustellung muss garantiert erfolgen. Während des Transports muss der private Schlüssel durch eine geeignete Transportsicherung gegen unbefugten Zugriff geschützt sein. Eine Verletzung der Transportsicherung muss für den legitimen Empfänger erkennbar sein.

**Benutzung** Die Benutzung des privaten Schlüssels muss für Befugte sehr leicht sein. Unbefugten hingegen soll es unmöglich sein den Schlüssel zu benutzen. Es ist sehr wichtig, dass der private Schlüssel auch während der Benutzung geschützt bleibt (z.B. er verlässt die Chipkarte niemals).

**Zerstörung** Wird ein privater Schlüssel zerstört, so muss er unwiederbringlich gelöscht sein. Die Zerstörung soll leicht für Befugte und unmöglich für Unbefugte sein.

**Hinterlegung** Die Hinterlegung eines privaten Schlüssels muss persistent sein. Es ist darauf zu achten, dass nur bestimmte Schlüssel hinterlegt werden dürfen (z.B. ist die Hinterlegung eines Signaturschlüssels äußerst fragwürdig). Hinterlegte Schlüssel müssen durch geeignete Maßnahmen vor unbefugtem Zugriff geschützt werden.

**Wiederherstellung** Die Wiederherstellung eines Schlüssels muss korrekt erfolgen, d.h. es muss in jedem Fall exakt der ursprüngliche Schlüssel wiederhergestellt werden. Die Wiederherstellung muss leicht für Befugte und unmöglich für Unbefugte sein.

## Aufgabe 2: Aufgaben der KA

- a) Woraus definieren sich die Aufgaben der KA (abstrakt)?
- b) Nennen sie die Aufgaben der KA (konkret)!

## Lösungsvorschlag

- a) Die KA erledigt alle Aufgaben, für die nur sie die Befugnis hat (fremde, private Schlüssel).  
Sonst hat sie keinerlei Aufgaben.
- b) **Issuing** Unterschreiben von Zertifikaten  
**Revocation** Unterschreiben von Revokationslisten  
**Key Generation** Erzeugung aller Schlüsselpaare die der Eigentümer nicht selbst erzeugt  
**Personalization** Aufbringen erzeugter Schlüssel auf Tokens Erzeugen von Transport-PIN und PIN-Brief  
**Archiving/Backup/Recovery** Aufbewahrung von Schlüsseln, Wiederherstellung von Schlüsseln (falls notwendig und nicht vom Eigentümer vorgenommen)

## Aufgabe 3: Sicherheit durch KA

- a) Warum ermöglicht die KA eine einfache Durchsetzung von Sicherheit für private Schlüssel?
- b) Welche Sicherheitsanforderungen werden an die KA gestellt?
- c) Welche sonstigen Anforderungen werden an die KA gestellt?
- d) Welchen Grad an Schutz für private Schlüssel ermöglicht der Einsatz einer KA?

## Lösungsvorschlag

- a) Um private Schlüssel innerhalb eines Trust Centers zu schützen, genügt es die KA zu schützen.  
Die KA ist relativ leicht zu schützen, da sie
  - a) ein einzelnes, zentrales Schutzobjekt ist
  - b) in einer bekannten und zudem gestaltbaren Umgebung (Trust Center) residiert
  - c) durch bekannte technische und organisatorische Schutzmaßnahmen geschützt werden kann.
- b) **Zugangsschutz** Operatoren der KA müssen eine starke Authentifizierung durchlaufen. Möglicherweise haben verschiedene Operatoren verschiedenen Zugriffsrechte.

**sichere Kommunikation** Die Kommunikation mit den anderen Trust Center-Modulen muss in jedem Fall authentisch evtl. sogar geheim sein.

**kryptographische Flexibilität** Die KA muss in der Lage sein beliebige kryptographische Algorithmen von unterschiedlichen Providern zu benutzen. Die Algorithmen bzw. Provider müssen spontan ausgetauscht werden können. Außerdem müssen Rückfallmechanismen existieren, die ein Schaden im Falle der Kompromittierung eines Schlüssels oder eines Algorithmus abwenden.

**Protokollierung** Es muss jederzeit feststellbar sein, wer was wann gemacht hat.

- c) **Skalierbarkeit** Die Aufgaben der KA erfordern einen hohen Berechnungsaufwand. Zudem unterliegt die KA großen Lastschwankungen. Im "Normalbetrieb" erfolgen lediglich Routineoperationen wie die Erneuerung der CRLs. Zudem wird von Zeit zu Zeit ein Zertifikat gesperrt und / oder neu ausgestellt. Wird jedoch die PKI zum ersten mal ausgerollt (d.h. alle Teilnehmer bekommen Schlüssel und Zertifikate) oder werden regelmäßig alle Zertifikate erneuert, ist die Last um ein vielfaches höher. Skalierbarkeit meint hier, das die KA an die unterschiedlichen Lastniveaus angepasst werden kann. Zum Beispiel kann im Falle des Rollouts zusätzliche Hardware verwendet werden. Ist das Rollout fertig, kann diese als Reserve-System (Hot-/Cold-Standby) umfunktioniert werden.

**Robustheit** Dies meint die Fähigkeit, trotz aufgetretener Fehler (in der Software selbst oder in der Umgebung) korrekt weiterzuarbeiten. Wenn zum Beispiel die Datenbankverbindung vorübergehend (wegen eines Backupvorgangs) nicht zur Verfügung steht, muss die KA trotzdem weiterarbeiten. In diesem Fall bedeutet das, alle von der Datenbank abhängigen Operationen einzustellen und zu warten.

Diese Eigenschaft ist besonders wichtig, da die KA üblicherweise in stark geschützten Umgebungen läuft und selbst das Starten und Stoppen der Anwendung überwacht werden muss. D.h. wenn die KA aufgrund kleiner Fehler ihren Betrieb einstellt, erfordert das einen großen Aufwand, sie wieder zu starten.

**Transaktionalität** Die Operationen auf den Daten müssen vollständig, konsistent, isoliert und persistent sein. Beispiel: Die KA erzeugt ein Schlüsselpaar, personalisiert eine Chipkarte, erstellt ein Zertifikat für den öffentlichen Schlüssel und läßt dieses durch die CMA veröffentlichen. Tritt ein Fehler auf, z.B. wenn das Zertifikat nicht die CMA erreicht, muss der gesamte Vorgang unter Umständen vollständig zurückgerollt werden. D.h. der Schlüssel und die Chipkarte werden zerstört und das Zertifikat gesperrt. Wird umgekehrt das Zertifikat veröffentlicht, so müssen auch alle anderen Operationen vollständig und gültig durchgeführt worden sein. Andere Vorgänge müssen von dem Ausgang dieses Vorgangs unberührt bleiben.

- d) Die KA bietet den maximalen, in der Praxis möglichen, Schutz privater Schlüssel. Sie schützt alle Issuer-Private-Keys und alle fremden privaten Schlüssel innerhalb des Trust Centers.

Außerdem unterstützt sie den Schutz eigener, privater Schlüssel durch die jeweiligen Eigentümer. D.h. sie gibt zum Beispiel vor, wie die Schlüssel zu erzeugen sind, oder erzwingt, dass die Schlüssel auf einer Chipkarte gespeichert werden.

## Aufgabe 4: Trust Center-Abläufe

Im Trust Center der Rechnerbetriebsgruppe findet die Registrierung von Mitarbeitern und Professoren dezentral statt. Die Erstbeantragung eines Zertifikat geht in etwa so von statten: In jedem Fachgebiet ist ein Mitarbeiter verantwortlich und berechtigt für die Beantragung von Zertifikaten für seine Kollegen. Die pro Antrag erfassten Daten werden in einer Datenbank zentral abgelegt, von dort zum Zertifizieren verbracht und die entstanden Produkte an die im Zertifikat enthaltene Emailadresse des Mitarbeiters (dies ist eine X.509-Extension) zugestellt. Der Distinguished Name wird hierbei aus den Antragsdaten wie folgt gebildet:

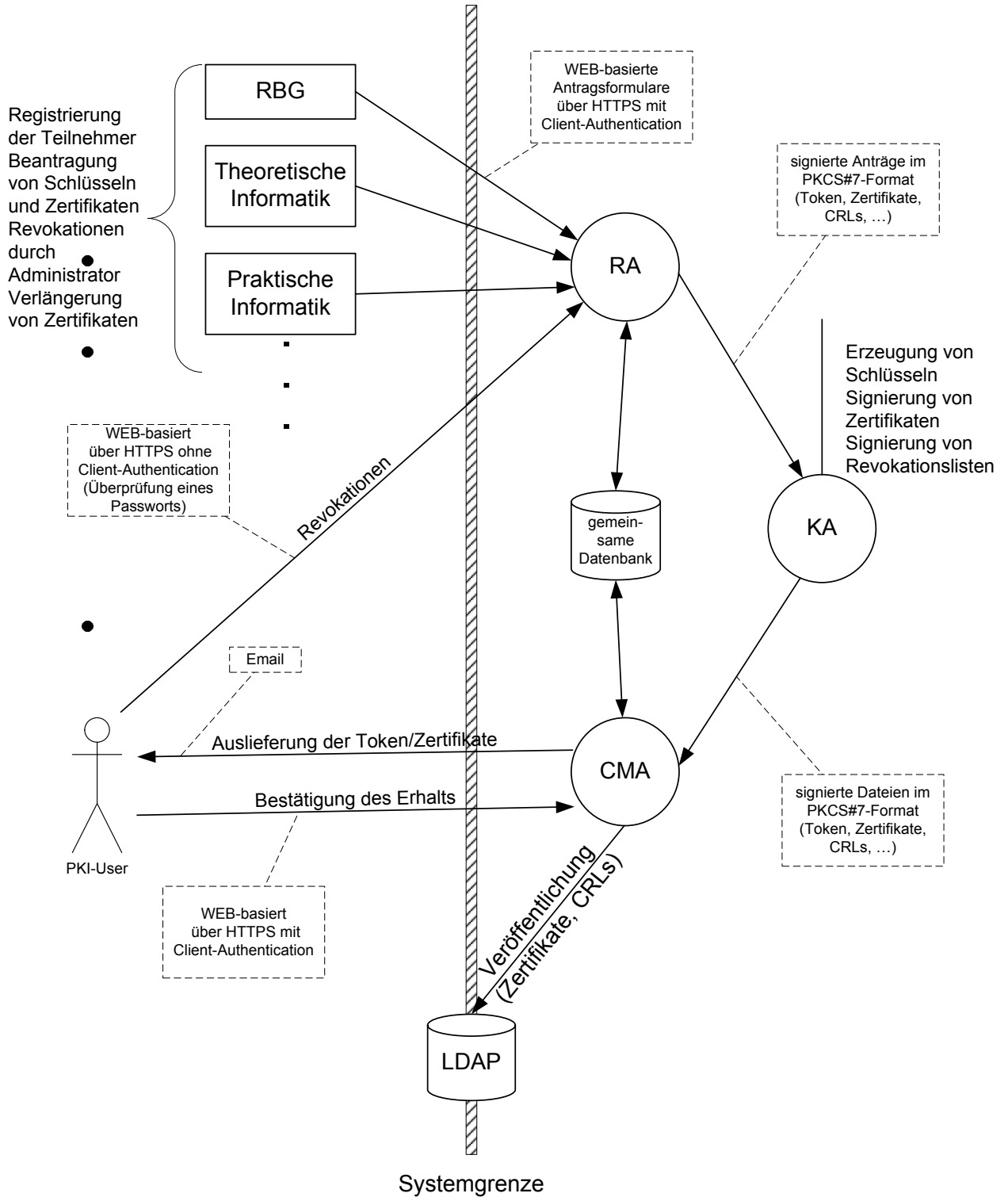
CN	<i>Titel, Vorname und Nachname</i>
OU	<i>Kürzel des Fachgebiets</i>
OU	FB Informatik
O	TU Darmstadt
C	DE

Die Schlüsselpaare werden ebenfalls zentral erzeugt und als PKCS#12-Datei mit der Mail verschickt. Die Vertraulichkeit des privaten Schlüssels wird hierbei durch ein Passwort gesichert, welches der Mitarbeiter, der das Zertifikat erhalten soll, bei der Antragstellung angibt.

- a) Welche Trust Center-Aufgaben werden wann und wo wahrgenommen? Skizzieren Sie den Ablauf!
- b) Welcher Typ Registration Authority (bezogen auf Dezentralisierung) trifft hier zu? Welche Vorteile ergeben sich?
- c) Die RA erzeugt die Subject Distinguished Names. Ist es in diesem Szenario schwierig, die Eindeutigkeit zu gewährleisten?
- d) Angenommen, es würden LRAs (Local Registration Authorities) eingesetzt. Ist es dann immer noch einfach, eindeutige Namen zu erzeugen? Ist dies immer so?
- e) Wie würde sich der Ablauf ändern, wenn die Mitarbeiter ihre Schlüsselpaare erzeugen?

# Lösungsvorschlag

a) Trust Center-Ablauf RBG:



b) Verteilte Registrierung bei zentraler Datenhaltung.

Die Registrierung erfolgt dezentral durch lokale Administratoren (so gesehen sind diese bereits ein Teil des Trust Centers resp. der RA). Die Qualität der Identifikation ist sehr gut, da

die Administratoren alle Teilnehmer in ihrem Fachgebiet kennen. Die Registrierung ist weniger zeitaufwendig, da nicht alle zu einer zentralen Stelle kommen müssen. Sie kann quasi am Arbeitsplatz durchgeführt werden.

Die Daten werden zentral gehalten, damit nicht in jedem Fachgebiet Möglichkeiten zur sicheren Datenhaltung vorgesehen und administriert werden müssen. Es benötigt keinen Aufwand, die verteilten Daten zu synchronisieren, bzw. für die Produktion einzusehen (es gibt nur eine CA). Es kann Administratoren geben, die das gesamte System steuern dürfen.

- c) Dies ist einfach, da die Datenhaltung zentral erfolgt. Es kann also jederzeit festgestellt werden, welche Namen schon vergeben sind und welche nicht.
- d) Im konkreten Fall ist das kein Problem, da die lokalen Registrierstellen für getrennte Namensräume (bzgl. DN) registrieren. Es kann hier also auch dann nicht zur Mehrfachvergabe von DNS kommen, wenn die Daten dezentral verwaltet werden.

Dies muss aber nicht so sein. Sind die Namensräume bzgl. DN nicht disjunkt, müssen andere organisatorische Maßnahmen getroffen werden wie z.B. verteilte Transaktionen.

- e) *kurze Antwort:*

Nicht viel: Anstelle der PIN würde der Mitarbeiter seinen öffentlichen Schlüssel übergeben und ggf. nachweisen, dass er den zugehörigen privaten Schlüssel besitzt und benutzen kann (Proof of Possession, PoP). Der Registrierer muss den Benutzer im Moment der Übergabe des öffentlichen Schlüssels identifizieren.

*lange Antwort:*

Anstelle der PIN wird der öffentliche Schlüssel übergeben (wie schon oben gesagt). Entscheidend ist hier die Feststellung der Authentizität des öffentlichen Schlüssels. Die Frage ist also: Wer kann den zugehörigen privaten Schlüssel benutzen. Dazu sind nun zwei Schritte notwendig:

- a) Die RA identifiziert den Teilnehmer in dem Moment, indem er ihr den öffentlichen Schlüssel übergibt und stellt ab da sicher, dass niemand (in ihren Daten) diese Zuordnung öffentlicher Schlüssel zu Person manipulieren kann.
- b) die RA stellt sicher, dass der Benutzer den privaten Schlüssel benutzen kann (PoP). Ist der übergebene öffentliche Schlüssel zum Signieren geeignet, kann ich das z.B. dadurch machen, dass der Antragsteller (in dem Fall der Mitarbeiter) den öffentlichen Schlüssel mit dem privaten signiert. Ggf. kann man noch andere Daten mit signieren. Dieses Vorgehen ist z.B. im PKCS#10 Standard festgehalten. Ist der Schlüssel nur für Verschlüsselung geeignet, kann man den Proof of Possession *indirekt* führen, indem man beim Versand das Zertifikat mit dem (darin enthaltenen) öffentlichen Schlüssel verschlüsselt. Der Empfänger muss nun das erhaltene Zertifikat entschlüsseln, wozu er den privaten braucht. Das Zertifikat kann nur dann veröffentlicht werden, wenn der Proof of Possession erfolgreich ist.

Aus diesen Überlegungen folgt: Wenn der Schlüssel (wie bei 4.a)) im Trust Center erzeugt wird, muss man die Feststellung der Identität dann machen, wenn der Teilnehmer den erzeugten privaten Schlüssel aushändigt bekommt und nicht bei der Registrierung. Das Trust Center muss ja nicht sicherstellen, dass der richtige den Antrag gestellt hat, sondern dass der richtige den privaten Schlüssel besitzt! Dies kann man aber (wie bei RBG geschehen) umgehen, indem

- a) man bei der Registrierung auch identifiziert und
- b) Teilnehmer und RA bei der Registrierung ein Geheimnis teilen (z.B. einen Schlüssel, eine PIN, ...). Damit kann das Trust Center hinterher sicherstellen, dass der richtige Empfänger den privaten Schlüssel bekommt.

## Aufgabe 5: Certificate Management Authority (CMA)

- a) Welche Aufgaben hat die CMA?
- b) Welche Nachteile soll die CMA ausgleichen? (Motivation)
- c) Muss die CMA online sein? (Begründung!)
- d) Die CMA verarbeitet Produkte der Key Authority. Welche Sicherheitsziele müssen für den Transport der Daten von der KA zur CMA gelten?
- e) Die CMA kann Certificate Revocation Lists (CRLs) ausstellen. Wie heißen diese? Was ist der Unterschied zwischen dieser Art CRL und denjenigen, die von der KA ausgestellt werden?

## Lösungsvorschlag

- a) Die Aufgaben der CMA sind:
  - veröffentlichen der PKI Informationen  
Dazu werden Zertifikate und CRLs in Internetverzeichnissen wie LDAP Servern benötigt. Um die PKI Idee zu verwirklichen, ist dies nötig, da die Informationen öffentlich und für jedermann zugänglich verfügbar sein müssen.
  - Zertifikate revozieren  
Zertifikate werden von dem Endanwender oder Administrator revoziert. Sie sollten in der Lage sein, dieses über ein Webinterface zu erledigen, das ein Revokationspasswort oder andere autorisierte Informationen abfragt. Das kann in Echtzeit, ohne Verzögerung der echten Revozierung, bis zu dem Zeitpunkt der Herausgabe der neuen CRL passieren.
  - Versendung der Zertifikate und PSEs und den Endnutzer  
Der tatsächliche Nutzer sollte die Zertifikate und PSEs (PKCS#12) erhalten.
  - Zertifikatsstatus kennen und Anfragen dazu beantworten können (OCSP)  
Es ist wichtig zu wissen, ob ein Zertifikat revoziert ist oder nicht, da man Anfragen von Endnutzern über die Validität des Zertifikats korrekt beantworten muss.
  - Archivierung von Zertifikaten  
Es werden alle Zertifikate für ihre zukünftige Verwendung gespeichert.
  - Zertifikate erneuern  
Wenn ein Zertifikat abläuft, wird die CMA eine Zertifikatserneuerung bei der RA oder Zertifikatsinstanz anfragen. Dies kann transparent für den Nutzer geschehen.

- Fehlerinformationen

Falls ein Fehler gefunden wird, wird der Administrator mittels einer Email benachrichtigt, um diesen zu beheben. Zusätzlich könnte die CMA nach einem erneuert herausgegebenen Zertifikat fragen (falls etwas falsch gelaufen ist) oder sie könnte ein Zertifikat revozieren, falls ein ernsthafter Fehler gemacht wurde.

b) Die CMA versucht folgende Probleme zu lösen:

- Offline KA.

Wenn die KA nicht erreichbar ist, kann sie ihre Zertifikate nicht veröffentlichen und zu dem Endnutzer senden. Daher ist es nötig, dass es eine Komponente innerhalb des Trust Centers gibt, die diese Aufgaben übernimmt.

- mögliche dezentralisierte RAs

Dezentrale RAs können zu operationalen Problemen führen, wie z. B. die Administrierung der Zertifikate jeder einzelnen RA durch sich selber. Ebenfalls könnte dies in höheren Kosten münden, da die Lösung der Aufgaben die für ein Zertifikat anfallen (Veröffentlichen, Versenden, etc.) für jeden Registrierungsplatz umgesetzt werden müssen. Letztlich könnte dies ebenfalls Sicherheitsprobleme nach sich ziehen, da nicht jede Lösung die gleiche Sicherheit aufweisen wird. CMA lösen dieses Problem mit einer zentralen Zertifikatsverwaltung.

- Langsame Revokation

In einigen Umgebungen wird die Revokation sehr langsam sein (KA unter der Erde, in einer anderen Stadt, physikalische Kontrollen). Daher kann die Revokationsaufgabe an eine andere Komponente delegiert werden, die in der Lage ist, die CRL so schnell wie möglich zu signieren. Da die CMA online ist, könnte man an eine online Revokation denken, die genau in dem Moment ausgeführt wird, in dem sie gebraucht wird.

- virtuelles Hosting.

Viele Trust Center in einer physikalischen Umgebung zu hosten könnte zu extremen Problemen in der Handhabung führen. Eine KA Instanz könnte Zertifikate für mehr als einen Herausgeber erzeugen. Aber diese Herausgeber haben unterschiedliche Anforderungen, was mit den Zertifikaten gemacht werden soll. Eine CMA kann eine automatische Akzeptierung anbieten, die Anfragen von einer KA und anderen Prozessen die zu verschiedenen Diensten jedes Herausgebers gehören. Sonst würde ein menschlicher Administrator zwischen den verschiedenen Herausgebern unterscheiden müssen und die weiteren Schritte durchführen müssen.

c) Die CMA muss online sein, um ihre Services anbieten zu können. Diese sind: veröffentlichen von Zertifikaten auf einem LDAP-Server, versenden von PSEs an deren Eigentümer.

d) Die grundlegendsten Sicherheitsziele sind Integrität und Authentizität. Beide können mit der digitalen Signatur realisiert werden. D.h., dass die KA alle Anträge an die CMA signieren muss. Damit kann man nachweisen, dass die Daten nicht verändert wurden und zusätzlich ist die CMA sicher, dass sie tatsächlich von der registrierten KA kommen, die für diese Services zugelassen wurde. Normalerweise werden Zertifikate, CRLs und geschützte Software PSEs von der KA zur CMA gesendet. Daher ist keine Vertraulichkeit nötig. In manchen Umgebungen ist auch dies notwendig. Z.B. wenn die KA die PIN einer PSE schickt oder die Daten aufgrund von

Datenschutzrichtlinien vertraulich bleiben müssen. Zusammengefasst sind die Sicherheitsziele: Integrität und Authentizität, manchmal auch Vertraulichkeit!

- e) CRLs, die von anderen Instanzen herausgegeben werden, als die, die die Zertifikate in der CRL signieren, werden indirekte CRLs genannt. Das ist immer der Fall, da die CMA niemals ein Zertifikat signiert. Daher wird sie auch immer indirekte CRLs erzeugen. Wie oben beschrieben ist der Unterschied, dass die CRLs, die von der KA herausgegeben werden, von der Instanz signiert werden, die auch die Zertifikate signiert hat.