In: Horster, P. (Hrsg.): *Trust Center*. Proceedings der Arbeitskonferenz Trust Center 95, Vieweg-Verlag, Braunschweig 1995, S. 1-10.

Grundüberlegungen zu Trust Centern

Dirk Fox[1] · Patrick Horster[2] · Peter Kraaibeek[3]

[1]Universität - Gesamthochschule - Siegen
Institut für Nachrichtenübermittlung
fox@nue.et-inf.uni-siegen.de

[2]Technische Universität Chemnitz
Theoretische Informatik und Informationssicherheit
pho@informatik.tu-chemnitz.de

[3]Competence Center Informatik GmbH, Meppen
Fachbereich IT-Sicherheit
kbk@cci.de

Zusammenfassung

Gegenstand dieses Beitrags sind grundsätzliche, zunächst von Realisierungen und spezifischen Implementierungen unabhängige Überlegungen zu Trust Centern. Unter Trust Center wird eine Summe von Einheiten oder Instanzen verstanden, die eine wichtige Funktion in einer Sicherheitsinfrastruktur erfüllen und denen diesbezüglich (in der Regel) von den Nutzern Vertrauen entgegengebracht wird. Die technische und organisatorische Gestaltung eines solchen Trust Centers kann dabei sehr unterschiedlich ausfallen.

Trust Center werden nach der ihnen im Rahmen einer Sicherheitsinfrastruktur zugewiesenen Aufgabe klassifiziert. Dabei zeigt sich, daß abhängig von der dem Trust Center zugewiesenen Funktion Benutzervertrauen in unterschiedlicher Form und verschieden hohem Grad erforderlich ist. Es werden überblicksartig Maßnahmen vorgestellt, mit denen die jeweils gewünschte Qualität eines Trust Centers erreicht werden kann.

1 Einleitung

Je nach Anforderung an eine IT-Umgebung sind für den Schutz von Daten unterschiedliche Sicherheitsdienste zu erbringen, von denen einige wichtige in der ISO-Norm 7498-2 (OSI-Security Architecture) definiert wurden. Sie spielen inzwischen eine zentrale Rolle bei der Bewertung von sicheren und vertrauenswürdigen IT-Systemen. Für die Realisierung einiger dieser Dienste ist Vertrauen der Benutzer sowohl in eine informationstechnische Umgebung, bestehend aus Geräten und Implementierungen, als auch in unabhängige Instanzen erforderlich. Solche Geräte und Instanzen werden als *Trust Center* bezeichnet.

Die Vertrauenswürdigkeit solcher Trust Center spielt wegen ihrer meist herausgehobenen, oft zentralen Stellung in komplexen Sicherheitssystemen eine entscheidende Rolle für die Akzep-

tanz ganzer IT-Infrastrukturen. Aus diesem Grund erscheint die Bezeichung *Trusted Center* zutreffender.

Da Sicherheitsmechanismen vor Umgebungen schützen sollen, denen von einem Benutzer oder Betreiber prinzipiell Mißtrauen entgegengebracht wird, ist die Vertrauenswürdigkeit von Trust Centern besonders begründungsbedürftig. Vertrauenswürdigkeit ist zunächst ein sehr subjektives Bewertungskriterium. Sie kann aber durch die Aufstellung von Angreifermodellen, Risikoanalysen und eines organisatorische und technische Maßnahmen umfassenden Sicherheitskonzeptes transparent und damit objektiven Kriterien und Bewertungen zugänglich gemacht werden.

So lassen sich durch geeignete Sicherheitsmechanismen die Bereiche systematisch eingrenzen, denen Subjekte einer Infrastruktur Vertrauen entgegenbringen müssen. Auch die Art des erforderlichen Vertrauens mit unterschiedlicher Dauer oder Qualität kann durch technische Mechanismen begrenzt werden. Auf diese Weise kann blindes Vertrauen eines Benutzers in eine Umgebung durch eine vergleichsweise genau spezifizierte Form des Vertrauens ersetzt werden. Diese gibt Antworten auf die Fragen: *welche Art Vertrauen? in wen? zu welchem Zweck? wie lange? unter welchen Voraussetzungen? wie überprüfbar? wie zu entziehen?* Dadurch wird die Bewertung der Vertrauenswürdigkeit einer Umgebung anhand beschreibbarer Eigenschaften und Bedingungen möglich.

Im folgenden werden unterschiedliche Aspekte der Vertrauenswürdigkeit betrachtet, klassifiziert nach den Aufgaben, die Trust Centern übertragen werden können. Dabei werden auch die Interessen weiterer Beteiligter wie Ermittlungs- und Verfassungsschutzbehörden berücksichtigt, die die Vertrauensproblematik komplizieren können. Rechtliche Probleme und Fragestellungen werden an anderer Stelle in diesem Tagungsband ausführlich behandelt.

2 Aufgaben von Trust Centern

Die Aufgaben, die einem Trust Center in einer Sicherheitsinfrastruktur zugewiesen werden, lassen sich grob in drei Bereiche gliedern: *Schlüsselmanagement*, *Beglaubigungsleistungen* und *Serverfunktionen*. Diese Aufgaben können entweder von unter der Kontrolle des Benutzers arbeitenden *Personal Trust Centern* (PTCs), z.B. „intelligenten“ Sicherheitstoken wie SmartCards, als auch von vertrauenswürdigen dritten Instanzen, sogenannten *Trusted Third Parties* (TTPs) übernommen werden. PTCs und TTPs werden häufig in einer Sicherheitsarchitektur hierarchisch angeordnet; Kontrollmechanismen sorgen dabei für eine zuverlässige Diensterbringung. TTPs benötigen zur Begründung ihrer Vertrauenswürdigkeit eine veröffentlichte Policy, die eine klare Darstellung der Aufgaben und Sicherheitsanforderungen umfaßt und möglichst benutzerüberprüfbar realisiert ist.

Zwar können die Aufgaben auch in einem Trust Center konzentriert werden; eine solche Vermischung geschieht aber meist ohne Not und erschwert die Begründung der Vertrauenswürdigkeit oft erheblich. Denn je nach Aufgabe sind unterschiedliche Sicherheitsanforderungen an ein Trust Center zu stellen.

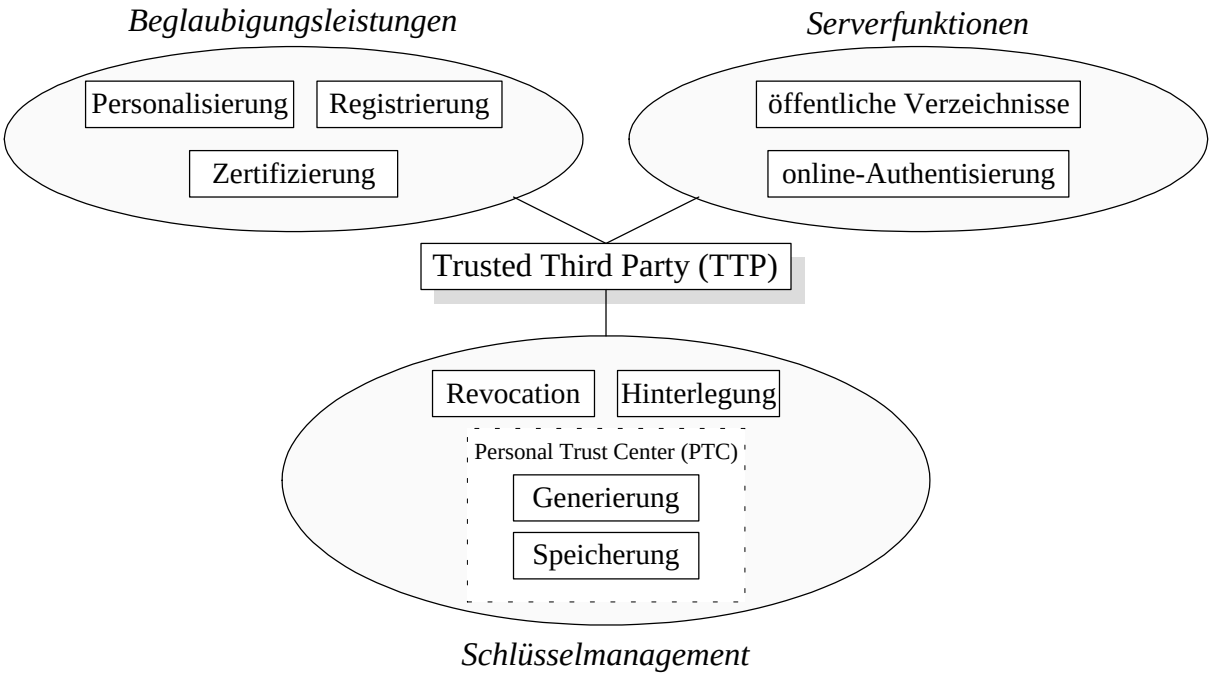

Bild 1: Zuordnung der Aufgaben von Trust Centern zu TTPs und PTCs

Im folgenden werden aus der Perspektive des Teilnehmers einer Sicherheitsinfrastruktur, d.h. eines „vertrauenden“ Subjekts die unterschiedlichen Aufgaben von Trust Centern diskutiert.

2.1 Schlüsselmanagement

Eine wichtige Aufgabe eines Trust Centers ist das Schlüsselmanagement. Dieses umfaßt als grundlegende Funktionen die Schlüsselgenerierung, die Speicherung und die Zurücknahme (Revocation) von Schlüsseln, ggf. auch deren Verteilung und Löschung.

2.1.1 Schlüsselgenerierung und Revocation

Besonders sensibel hinsichtlich der Vertrauenswürdigkeit ist jede Instanz, die mit der Generierung kryptographischer Schlüssel befaßt ist. Da die Kenntnis geheimer Schlüssel einen Zugriff auf später damit verschlüsselte Daten bzw. deren Fälschung erlaubt, muß die Generierungsinstanz hohen Sicherheitsanforderungen genügen. So ist zunächst zu fordern, daß kein Unberechtigter Kenntnis von geheimen Schlüsseln erlangen kann. Dies muß durch angemessene Maßnahmen sichergestellt sein. Die Generierung der Schlüssel darf zudem nicht nachvollzogen werden können. Das gelingt durch die Verwendung echter Zufallswerte, wenigstens als Startsequenz starker Pseudozufallsgeneratoren.

Häufig werden, auch aus staatlichem Schutzinteresse, zentrale behördliche Instanzen als TTP für die Schlüsselgenerierung vorgeschlagen. Diese besitzen mit der Kenntnis sämtlicher Schlüssel natürlich auch die Möglichkeit zum benutzerseitig nicht kontrollierbaren Zugriff auf verschlüsselt gespeicherte oder übertragene Daten. Sie erfordern erhebliches, weitgehend blindes Vertrauen des Benutzers in die Bereitschaft des Trust Centers, diese Kenntnisse nicht

zu mißbrauchen. Hier sind aus Gründen des allgemeinen Persönlichkeitsschutzes rechtliche Rahmenbedingungen erforderlich.

Aber auch dann, wenn die Speicherung der generierten Schlüssel im Trust Center nicht vorgesehen oder sogar die Löschung vorgeschrieben ist, besteht für den Benutzer keinerlei Gewähr, daß die Schlüssel nach Generierung auch tatsächlich gelöscht werden. Organisatorische Vorkehrungen, die öffentlich bekannt gemacht und diskutiert werden, können hier vertrauensbildend wirken, ermöglichen jedoch keine benutzerüberprüfbare Lösung.

Diesem Ansatz ist daher eine Schlüsselgenerierung beim Benutzer in einer von ihm vollständig kontrollierten Einheit, einem PTC vorzuziehen, realisiert als Chipkarte, Token oder Personal Digital Assistant (PDA). Schwierig ist bei einem solchen kleinen, wenig leistungsfähigen System zur Zeit noch die Erzeugung geeigneter Zufallswerte.

Im Fall der Schlüsselgenerierung durch ein PTC des Benutzers muß dieser zwar nicht einer ihm möglicherweise unbekannten Instanz, dafür jedoch dem Hersteller von Soft- und Hardware seines PTC vertrauen. Dessen Vertrauenswürdigkeit kann durch eine Sicherheitszertifizierung verstärkt werden, die allerdings das Vertrauen des Benutzers in die Eignung der Zertifizierungskriterien, in die Sorgfalt, Kompetenz und Gründlichkeit der evaluierenden Instanz und die Vertrauenswürdigkeit des Herstellungsprozesses voraussetzt.

Kann – aus welchen Gründen auch immer – die Generierung der Schlüssel nicht vom Benutzer selbst vorgenommen werden, besteht die Möglichkeit, die Generierung auf mehrere Vertrauensinstanzen zu verteilen. Der Benutzer erhält seinen Schlüssel durch geeignete Kombination der Schlüsselteile. Für die Vertrauenswürdigkeit einer solchen verteilten Schlüsselgenerierung genügt die Vertrauenswürdigkeit einer Instanz, d.h. die Gewähr, daß wenigstens eine Instanz nicht mit anderen zusammenarbeitet, da ein Mißbrauch der Schlüssel nur mit Kenntnis aller Schlüsselteile möglich ist. Dies wurde ansatzweise im amerikanischen *Escrowed Encryption Standard* (EES) verwirklicht, der kontrovers diskutiert wird.

In jedem Fall sollte nicht nur bei zentraler Generierung von Schlüsseln deren Gültigkeit zeitlich begrenzt und durch Revocation Mechanismen benutzerseitig beendet werden können. Nur so kann Mißbrauch beschränkt und bei Feststellung gestoppt werden.

2.1.2 Schlüsselspeicherung

Zufällig gewählte oder erzeugte kryptographische Schlüssel kann sich ein Benutzer im allgemeinen nicht merken. Schlüssel müssen daher in einer geeigneten, insbesondere maschinenlesbaren Form gespeichert werden. Die speichernde Instanz ist aus der Sicht des Benutzers ein Trust Center, auch wenn es sich lediglich um eine Magnetstreifenkarte oder Diskette handelt.

Für bestimmte Sicherheitsdienste und Mechanismen wie Drei-Parteien-Protokolle ist außerdem die zentrale Speicherung geheimer Schlüssel in Trusted Third Parties unvermeidlich. So setzen beispielsweise symmetrische Authentifikationsprotokolle die Kenntnis eines gemeinsamen Geheimnisses von Authentifikationsserver und Benutzer voraus. Die zentrale Speicherung geheimer Schlüssel erfordert jedoch volles blindes Vertrauen des Benutzers in die

Sicherheit und Zuverlässigkeit dieser Instanz, denn ein Mißbrauch der geheimen Kenntnisse wie Weitergabe an Dritte oder Maskerade kann nicht benutzerüberprüfbar verhindert werden. Aus diesem Grund ist eine zentrale Instanz, die geheime Schlüssel speichert, eine der empfindlichsten Komponenten eines Sicherheitssystems. Häufig ist zudem eine hohe Verfügbarkeit dieser zentralen Instanz gefordert. Sie muß daher zwingend insbesondere durch bauliche Maßnahmen vor unberechtigtem Zugriff geschützt werden.

Dies läßt sich für die geheimen Schlüssel des Benutzers mit vergleichsweise geringem Aufwand durch die Verwendung von PTCs verwirklichen. Idealerweise sollte das Geheimnis das geschützte, persönliche Sicherheitstoken nie verlassen. Intelligente SmartCards mit Kryptochip erlauben die Durchführung kryptographischer Operationen wie zum Beispiel die Berechnung einer digitalen Unterschrift auf der Chipkarte. Damit müssen auf der Karte gespeicherte geheime Schlüssel nie mehr von der Karte gelesen werden.

Besonders kritisch ist die Behandlung von Schlüsseln für Digitale Signatursysteme. Die Rechtsverbindlichkeit Digitaler Unterschriften setzt insbesondere voraus, daß die geheimen, zur Erzeugung der Signatur erforderlichen Schlüssel ausschließlich der signierenden Person bekannt sind; eine Speicherung ist daher allein in einem vom Benutzer selbst kontrollierten PTC akzeptabel.

Weit weniger problematisch ist die Speicherung von öffentlichen Schlüsseln. Diese müssen lediglich authentisch, vor unerlaubten Modifikationen geschützt abgelegt werden. Üblicherweise werden öffentliche Schlüssel zusammen mit ihrem Zertifikat, dem von einer Zertifizierungsinstanz ausgestellten Gültigkeitsstempel, in einem öffentlichen Verzeichnis abgelegt (siehe Abschnitt 2.3.2). Anhand des Zertifikats kann die Unverfälschtheit des Schlüssels und damit die Vertrauenswürdigkeit der speichernden Instanz vom Benutzer jederzeit überprüft werden.

2.1.3 Treuhänderfunktion

Anders sieht es aus, wenn mit den geheimen Schlüsseln Daten geschützt werden sollen, die zwar vom Benutzer generiert und bearbeitet werden, nicht aber ihm allein gehören, beispielsweise im Rahmen seiner beruflichen Tätigkeit. Für den Schutz dieser Daten ist eine zentrale Hinterlegung der geheimen Schlüssel bei einem *Treuhänder* erforderlich, um dem Unternehmen oder der Behörde bei Tod oder Ausscheiden des Mitarbeiters einen Zugriff auf die Daten zu ermöglichen.

Ein ähnliches Vorgehen wurde zur Ermöglichung staatlichen Zugriffs auf verschlüsselt kommunizierte Daten in den USA als Escrowed Encryption Standard genormt. Durch treuhänderische Hinterlegung von geheimen Benutzerschlüsseln soll ein Abhören bei Vorliegen einer gerichtlichen Anordnung ermöglicht werden. Dabei werden die geheimen Schlüssel zerlegt und auf mehrere Treuhänder verteilt, um die Gefahr eines Schlüsselmißbrauchs durch die Treuhänder zu verringern.

Natürlich können neben geheimen Schlüsseln auch andere, z.B. personenbezogene Daten treuhänderisch bei einer Trusted Third Party hinterlegt werden. Darunter fallen auch

Referenzdaten für Unverfälschtheitsnachweise. Dabei sind die Voraussetzungen für eine Herausgabe dieser Daten ebenso wie die bei einer Anfrage greifenden Authentisierungs- und Identifikationsverfahren exakt festzulegen. Deren praktische Unumgehbarkeit begründet neben den ergriffenen physischen Schutzmechanismen des Trust Centers die Vertrauenswürdigkeit einer solchen Treuhänder-Instanz.

2.2 Beglaubigungsleistungen

Unter Beglaubigungsleistungen werden alle Aufgaben eines Trust Centers zusammengefaßt, die der Bezeugung der Authentizität von Daten oder Vertrauenswürdigkeit von Instanzen dienen. Dazu zählen die Ausstellung von Zertifikaten, die Personalisierung von TTPs und PTCs und die Registrierung von Nutzern einer Sicherheitsinfrastruktur.

2.2.1 Zertifizierungsinstanz

Asymmetrische Protokolle für den Austausch von Sitzungsschlüsseln (Session Keys) und die Authentisierung eines Kommunikationspartners erfordern Instanzen für die Ausstellung von Zertifikaten, d.h. unfälschbaren Gültigkeitsnachweisen für die verwendeten öffentlichen Schlüssel. Wesentliche Eigenschaft einer solchen Zertifizierungsinstanz ist deren Vertrauenswürdigkeit hinsichtlich der korrekten Ausstellung der Zertifikate.

Selbstzertifizierende Schlüsselaustauschprotokolle erfordern Zertifikate, die keinen öffentlichen Schlüssel, sondern die Identität des Benutzers bestätigen. Zertifikate können auch für Policies oder in Form von Berechtigungsnachweisen für Trusted Third Parties in einer Sicherheitsinfrastruktur ausgestellt werden. Zertifikate können darüberhinaus als Authentizitätsnachweise bzw. Beglaubigungen für Daten aller Art dienen, die einer Zertifizierungsinstanz vorgelegt werden.

Mit der Ausstellung eines Zertifikats nimmt ein Trust Center zugleich eine Identitätsbestätigung vor: Die digital unterschriebenen Daten (z.B. der öffentliche Schlüssel eines Nutzers oder eine Berechtigung) werden einem (eindeutigen) Namen oder einem Pseudonym zugeordnet. Die Vertrauenswürdigkeit einer Zertifizierungsinstanz hängt daher auch von der Qualität des zur zweifelsfreien Feststellung der Nutzeridentität verwendeten Verfahrens ab.

Dieses Vertrauen kann technisch und organisatorisch sehr leicht benutzerüberprüfbar erreicht werden. Die Korrektheit eines Zertifikats ist für den Nutzer selbst ebenso wie für Dritte unmittelbar überprüfbar.

2.2.2 Registrierung

Revocation Mechanismen, Gebühren-Abrechnungsverfahren und pseudonyme Protokolle machen eine Registrierung von Benutzern einer Sicherheitsinfrastruktur erforderlich. Dazu werden ausgestellte Identitätsbeglaubigungen gesammelt und treuhänderisch hinterlegt (siehe Abschnitt 2.1.3). Bei Vorliegen einer berechtigten Anfrage werden diese Daten autorisierten Stellen ausgehändigt.

2.2.3 Personalisierung

Eine wichtige Aufgabe von Trust Centern ist schließlich die Personalisierung von untergeordneten Instanzen, z.B. Personal Trust Centern. Diese Personalisierung umfaßt unterschiedliche Teilaufgaben. Untergeordnete PTCs erhalten im Rahmen des Personalisierungsvorgangs zertifizierte persönliche Schlüssel sowie den öffentlichen Schlüssel der Instanz, die die Zertifikate ausstellt. Untergeordnete TTPs erhalten eine zertifizierte Policy und spezielle Berechtigungen.

Werden Zertifizierung und Personalisierung von unterschiedlichen TTPs durchgeführt, muß die personalisierende Instanz mit geeigneten, möglichst benutzerüberprüfbaren Berechtigungen ausgestattet werden, um die Authentizität des öffentlichen Zertifikats-Prüfschlüssels zu gewährleisten.

Werden PTCs der Benutzer personalisiert, so sind nach Übertragung geheimer oder authentischer Daten an das PTC, beispielsweise eine SmartCard, diese durch Paßwörter, Personal Identification Number (PIN) oder ähnliches vor unberechtigtem Zugriff zu schützen. Durch eine abschließende Löschung aller geheimen Daten in der Personalisierungsinstanz sollten Mißbrauchsmöglichkeiten weiter eingeschränkt werden.

2.3 Serverfunktionen

Einige Aufgaben von Trust Centern erfordern die Bereitstellung von Informationen in einer Sicherheitsinfrastruktur. Solche Serverfunktionen werden üblicherweise von online-verfügbaren zentralen Instanzen erbracht. Deren Verfügbarkeit ist daher durch geeignete redundante Auslegung sicherzustellen.

2.3.1 Authentisierungsserver

Die Authentizität eines Kommunikationspartners wird üblicherweise durch ein kryptographisches Protokoll erbracht. Viele symmetrische und hybride Authentisierungs- und Schlüsselaustauschprotokolle, beispielsweise in dem Sicherheitssystem Kerberos, arbeiten dabei mit einem online verfügbaren Authentifikationsserver. Als symmetrische Authentisierungsinstanz muß ein solches Trust Center auch eine Speicherfunktion für geheime Schlüssel umfassen. Ein zentraler Authentisierungsserver ist daher vor allem von Angriffen auf die Vertraulichkeit bedroht.

2.3.2 Öffentliche Verzeichnisse

Zertifikatsbasierte asymmetrische Authentisierungsprotokolle benötigen den Zugriff auf zertifizierte öffentliche Benutzerschlüssel. Diese können über eine Zertifizierungshierarchie wie den X.500 Directory Information Tree oder auch über regelmäßig aktualisierte öffentliche Verzeichnisse auf dezentralen TTPs zugänglich gemacht werden. Eine dezentrale Lösung kann dem Erfordernis hoher Verfügbarkeit vergleichsweise leicht genügen. Eine Mißbrauchsmöglichkeit besteht in der Mißachtung von Revocation Lists, die ihrerseits wiederum durch befristete Gültigkeitsstempel und regelmäßige Aktualisierung zeitlich begrenzt werden kann.

3 Sicherheitsanforderungen an Trust Center

Unabhängig davon, welche Form von Vertrauen ein Trust Center im Hinblick auf seine Aufgaben erfordert und welche Gestalt ein Trust Center besitzt, ob SmartCard, Personal Digital Assistant (PDA) oder Behörde, müssen in jedem Fall Zugriffe Unberechtigter verhindert werden. Natürlich hängt der zu diesem Zweck zu treibende Aufwand von der Bedeutung der Aufgaben des Trust Centers und vom Grad des Vertrauens ab, das dem Trust Center entgegenzubringen ist. Im Lebenszyklus von Trust-Center-Komponenten einer Sicherheitsinfrastruktur können dabei drei Phasen unterschieden werden, in denen üblicherweise unterschiedliche Maßnahmen zur vertrauenswürdigen Realisierung ergriffen werden.

3.1 Der Entwicklungsprozeß

Die in einem Trust Center eingesetzte Hard- und Software sollte Gewähr dafür bieten, daß sie genau die Dienste korrekt und fehlerfrei erbringt, für die sie entwickelt wurde. Dies kann durch eine Vielzahl von unterschiedlich formalen und kostspieligen Evaluationsmaßnahmen erreicht werden: diversitäre Entwicklung, Redundanzmechanismen, Walk Throughs oder formale Verifikation. Durch Hinzuziehung unabhängiger Dritter für eine Evaluation und die Durchführung einer Zertifizierung nach öffentlich bekannten Kriterien ist ggf. eine weitere Steigerung der Vertrauenswürdigkeit möglich. Voraussetzung ist jedoch erstens eine anerkannt hohe Qualifikation der evaluierenden und zertifizierenden Instanz und zweitens die Existenz allgemein anerkannter, umfassender und anwendbarer Kriterien für die Zertifizierung.

Unter Umständen kann es erforderlich sein, die am Entwicklungsprozeß beteiligten Entwickler oder Firmen einer Untersuchung auf persönliche Integrität und Vertrauenswürdigkeit zu unterziehen.

Wünschenswert ist es darüber hinaus, sicherzustellen, daß die entwickelten Komponenten auch nicht mehr als das Spezifizierte ausführen können. Bis heute sind weder formale noch semiformale Verfahren bekannt, mit denen eine solche Form der Verifikation für komplexe Systeme möglich wäre. Es darf auch bezweifelt werden, daß ein solches Verfahren existiert, denn es würde zugleich das Problem der Existenz verdeckter Kanäle lösen. Allerdings kann der Evaluationsprozeß auf die verwendeten Werkzeuge und deren Herstellung und Hersteller ausgedehnt werden, um beispielsweise die Existenz von trojanischen Pferden auszuschließen.

3.2 Die Installationsphase

In der Installationsphase eines Trust Centers muß sichergestellt werden, daß die gut untersuchten oder sogar extern evaluierten und zertifizierten Komponenten nicht während der Einrichtung manipuliert oder modifiziert werden. Bei Personal Trust Centern wie SmartCards ist der dafür erforderliche Aufwand gering; hier muß nur verhindert werden, daß das Trust Center gegen ein manipuliertes Gerät ausgetauscht wird. Bei Trusted Third Parties steigt der Aufwand allerdings erheblich. Dort sind möglicherweise zusätzliche Maßnahmen wie Zugangskontrollen, Abstrahlschutz und Abhörsicherungen erforderlich, um Schutz vor Manipula-

tionen zu erreichen. In jedem Fall muß, wenn die eingesetzten Hard- und Software-Komponenten nicht ihrerseits schon eine manipulationssichere Einheit bilden, mit physischen Schutzmechanismen gearbeitet werden.

Auch diese Phase kann durch unabhängige Dritte, seien es Beobachter oder Evaluatoren, und durch den Einsatz überprüften Personals unterstützt werden. Die Erstellung authentischer Installationsprotokolle kann auch nachträgliche Kontrollen ermöglichen.

3.3 Die Betriebsphase

Die Vertrauenswürdigkeit des Betriebs von Trusted Third Parties ist abgesehen von der Qualität der bei der Einrichtung des Trust Centers getroffenen Maßnahmen insbesondere von vier Faktoren abhängig:

- dem eingesetzten Betriebspersonal,
- den organisatorischen und technischen Maßnahmen, die den Zugang zum Trust Center regeln, wobei biometrische Zugangskontrollen, Kameraüberwachungen und eine konsequente Umsetzung des „Vier-Augen-Prinzips“ zur Anwendung kommen können,
- Vorkehrungen für den Betrieb unter kritischen Bedingungen (Bedrohung durch Feuer, Stromausfall oder Blitzeinschlag) wie geeignete Fehlertoleranzmechanismen (fail safe), und
- der Existenz eines Auditing, das nicht nur abschreckend wirkt, sondern auch - in Kürze vielleicht auf rechtlicher Grundlage - beweisunterstützend eingesetzt werden kann.

Da sinnvollerweise nicht alle Trust Center-Aufgaben von einer einzigen zentralen Trusted Third Party erbracht sondern einer TPP-Hierarchie übertragen werden, sind auch die Übertragungskanäle, auf denen TTPs Daten austauschen, durch geeignete Maßnahmen zu schützen. Auch eine Überwachung untergeordneter Trust Center durch übergeordnete, die an jene Aufgaben delegieren, ist zu ermöglichen.

Im Fall eines PTC ist der Benutzer selbst Betreiber seines Trust Centers und muß sicherstellen, daß das Trust Center nicht zusammen mit dem für den Betrieb erforderlichen Wissen wie Paßwort oder PIN in die Hände eines Unberechtigten fällt.

4 Fazit

Aus den vorstehenden Überlegungen lassen sich paradigmatische Forderungen an die Konstruktion von Trust Centern ableiten. Nach dem Prinzip von Checks and Balances sollte Vertrauen niemals einer einzigen (all)mächtigen Instanz übertragen, sondern durch Kontrollmechanismen benutzerüberprüfbar gehalten werden. Das bedeutet konkret:

- *Verteilte Geheimnisse* sind zentral gehaltenen vorzuziehen, denn das betrügerische Zusammenarbeiten mehrerer Vertrauensinstanzen ist unwahrscheinlicher als der Mißbrauch durch eine Instanz.

- Geheime Schlüssel sollten einen physisch geschützten Bereich nie verlassen (müssen) und keiner Instanz außer dem Eigentümer bekannt sein. Damit ist *dezentralen, asymmetrischen Lösungen* der Vorzug vor symmetrischen zu geben, *aktiven Sicherheitstoken* wie Smart-Cards als PTC der Vorzug vor passiven wie Disketten oder Magnetstreifenkarten.
- Unterschiedliche Aufgaben eines Trust Centers sollten nicht ohne Not in einer Instanz konzentriert werden. *Aufgabentrennung* reduziert die Mißbrauchsmöglichkeiten einer Instanz und ermöglicht gegenseitige Kontrolle. Vertrauen kann dann benutzerseitig zweckgebunden und befristet entgegengebracht werden.
- Vertrauen sollte *immer nur befristet* ausgesprochen werden, um Mißbrauch zeitlich begrenzen zu können. Es sollte darüberhinaus *jederzeit entzogen* werden können; dies ermöglicht u.a. die Integration von Revocation Mechanismen in die Sicherheitsarchitektur.
- Schließlich sollte Vertrauen nie ohne *Kontrollmöglichkeit* ausgesprochen werden. Es sollte also solchen Mechanismen der Vorzug gegeben werden, die möglichst jederzeit eine Kontrolle durch den Benutzer erlauben.