INFORMATIONSTECHNIK UND ARMEE

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 2001/2002
Leitung:
Untergruppe Führungsunterstützung - Generalstab
Divisionär E. Ebert, Unterstabschef Führungsunterstützung

Public Key- und Smartcardinfrastruktur
Die Basis der e-Sicherheit

Referent: Willi Bühn

Public Key- und Smartcardinfrastruktur – die Basis der e-Sicherheit

Willi Bühn

Inhaltsverzeichnis

Zusammenfassung

Public-Key Verfahren gibt es seit über 20 Jahren, deren Einsatz im e-Business steht jedoch erst am Anfang. Die Public-Key Kryptographie bietet Lösungen an, die sich auch in grossen Gruppen bewähren können. Ein Blick auf die Grundlagen der Schlüsselverteilung zeigt die kritischen Stellen: Initialverteilung, Vertrauensanker und Geheimhaltung der Schlüssel (Smartcard), Publikation der öffentlichen Schlüssel (Verzeichnis). Eine Public Key Infrastruktur (PKI) hat die Aufgabe, Vertrauensbeziehungen (Trust) der Teilnehmer sicherzustellen. Die Smart-Crypto-Card Infrastruktur (SCI) ergänzt die PKI, indem sie die Geheimhaltung der privaten Schlüssel sicherstellt. Die Smartcard soll der einzige Sicherheits-Token in einem Unternehmen sein. Die SCI ist zudem ein Management Tool für die Verwaltung von zig-tausend Smartcards, indem sie die täglichen Benutzerprobleme wie Ersatzkarten, PIN vergessen, Karte verlegt, etc. auch in grossen Gruppen löst.

Adresse des Autors:

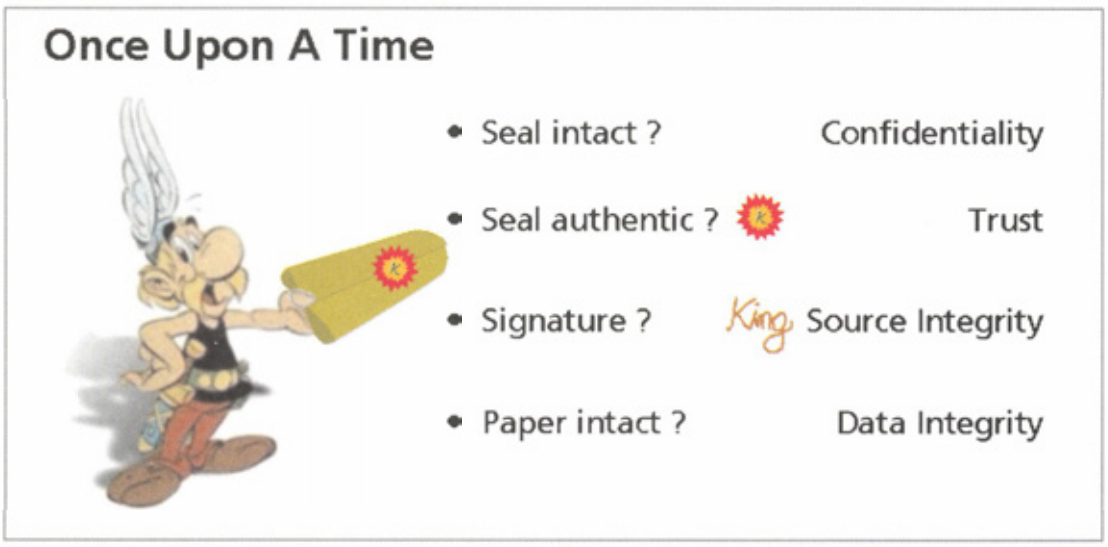
Willi Bühn
IT_SEC iT Security AG
8000 Zürich

Informationstechnik und Armee
41. Folge 2001/2002

1 Aus der Geschichte

Von altersher besteht das Bedürfnis, bestimmten Partnern geheime Mitteilungen zu senden. Das gilt vor allem im militärischen Bereich und in Krisenzeiten besonders. Seit die modernen elektronischen Mittel der Datenerfassung und Datenkommunikation eine lückenlose Personenüberwachung ermöglichen, entwickelt sich auch im zivilen Bereich vermehrt das Bedürfnis nach Vertraulichkeit oder Privatsphäre und damit nach Gesetzen zum Datenschutz.

Im einfachen einleitenden Satz sollten wir jedes einzelne Wort überdenken. Es gibt ein Bedürfnis, sich mitzuteilen. Die Mitteilung soll einen bestimmten Partner erreichen und andere nicht. Dieser ist nicht nebenan, sondern entfernt, und daher muss die Mitteilung transportiert werden und zwar so, dass sie andere nicht einsehen können. Den Empfänger wird interessieren, wer die Mitteilung verfasst hat und wie aktuell sie ist.



Ein reizvolles Gedankenspiel könnte den vertrauenswürdigen Schnellläufer, der einen unterzeichneten Brief in versiegeltem Umschlag von Athen nach Sparta bringt, mit einer entsprechenden Meldung vergleichen, die im Internet übertragen wird[1].

Verfolgen wir die Geheimhaltung kurz durch die Geschichte.

1.1 Geheime Verfahren

Zunächst bewährten sich geheime Verfahren ganz gut, bis sich erwies, dass Verfahren nur schwer geheim zu halten sind.

1.2 Geheime Schlüssel

Dann folgten Verfahren, die wohl bekannt sein durften, die aber einen Schlüssel verwenden, der geheim bleiben muss. Da der Schlüssel nicht mit der Nachricht zusammen transportiert werden darf, muss er separat zum Empfänger gebracht werden. Bei der symmetrischen Verschlüsselung[2] verwenden der Absender und der Empfänger denselben Schlüssel, meist für mehrere Nachrichten. Gute Verschlüsselung macht den Transport der Nachricht unbedenklich - umso grösserer Sorgfalt bedarf der Transport des Schlüssels. Das gilt nicht nur für symmetrische Verfahren, sondern auch für den privaten Teil eines asymmetrischen Schlüsselpaares.

[1] Alle Bilder zum Vortrag finden Sie unter http://www.it-sec.com/downloadfiles/pki-sci-esecurity.pdf.

[2] Zum Beispiel DES (Data Encryption Standard); wird abgelöst durch AES (Advanced Encryption Standard).

1.3 Authentizität

Neben dem Inhalt einer Nachricht interessiert auch der Urheber (zum Beispiel bei einem Befehl). Bei symmetrischer Verschlüsselung und unter der Voraussetzung, dass zwei Partner einen bestimmten Schlüssel exklusiv gebrauchen, von dem sie wissen, dass er authentisch ist, kann der Empfänger annehmen, dass der Schlüsselpartner die Nachricht verschlüsselt hat. Dass er sie auch verfasst hat, hängt davon ab, ob er den Schlüssel persönlich verwahrt und anwendet. Die Partner müssen sich davon überzeugen, dass diese beiden Anforderungen[3] (exklusiv und persönlich angewendet) erfüllt sind und strikt eingehalten werden. Der Nachricht selbst haftet nach wie vor kein Merkmal an, welcher der Partner sie verschlüsselt hat.

1.4 Verteilung symmetrischer Schlüssel

In einer Gruppe könnten sich zum Beispiel je zwei Partner treffen, den Schlüssel erzeugen und ihn sorgsam mit nach Hause nehmen (auf diese Weise transportiert ist der Schlüssel authentisch), ihn nie jemand anderem zugänglich machen und ihn nur selber anwenden. Ist die Gruppe gross, ist das ein sehr aufwändiges Verfahren, wenn nicht undurchführbar. Zudem fehlt jede Unterstützung des einzelnen bei der schwierigen Aufbewahrung der Schlüssel.

Eine Schlüsselzentrale, welche die Schlüssel vorschriftgemäss erzeugt, in Module schreibt, die sie schützen und ihre sichere Anwendung gewährleisten, kann einer solchen Gruppe helfen. Voraussetzung ist, dass alle der Zentralen vertrauen.

Neben dem bekannten $n^2/2$ Problem der Schlüsselanzahl (und ebenso vieler Vertrauensbeziehungen beim Schlüsseltransport), ist es in einem solchen System aufwändig, neue Partner aufzunehmen, weil alle Module der Partner des Neuen seinen Schlüssel speichern müssen.

Diese Schwierigkeiten vermeidet die Public-Key Kryptographie, indem jeder Teilnehmer seine eigenen Schlüssel besitzt und bewahrt, jene seiner Partner aber jederzeit von einem Verzeichnisdienst beziehen kann.

2 Public-Key Kryptographie

Mit Public-Key Kryptographie ist es möglich, mit dem einen Schlüssel zu verschlüsseln und mit dem anderen zu entschlüsseln, wobei die beiden Schlüssel einander eineindeutig zugeordnet sind und einer von beiden öffentlich bekannt sein kann, der andere aber geheim zu halten ist.

W. Diffie and M.E. Hellman[4] publizieren 1976 "New Directions in Cryptography." R. Rivest, A. Shamir und L. Adleman erfinden 1977 den RSA[5] Algorithmus. 1988 erscheinen die X.500[6] Standards "The Directory." In dieser Reihe sticht in diesem Zusammenhang die Empfehlung X.509 mit der Thematik Authentisierung[7] hervor. Um ihre Brauchbarkeit in der Internet Gemeinschaft macht sich seit 1995 die IETF Arbeitsgruppe PKIX[8] verdient.

---

3 Es gibt nicht viele Anwendungen symmetrischer Verschlüsselung, die diese beiden Anforderungen einhalten.

4 Diffie & Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory IT-22, November 1976.

5 R. Rivest, A. Shamir and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM, 21(2), pp. 120-126, February 1978.

6 Ed.1 1988, Ed.2 1993, Ed.3 1997, Ed. 4 2001.

7 ITU-T, X.509 (03/2000) "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks." Gemeinsamer Standard mit ISO/IEC 9594-8.

8 Public-Key Infrastructure (X.509) (pkix): "The PKIX Working Group was established in the Fall of 1995 with the intent of developing Internet standards needed to support an X.509-based PKI." http://www.ietf.org/html.charters/pkix-charter.html.

2.1 Das RSA Schlüsselpaar

Das RSA Schlüsselpaar wird in PKCS#1[9] "RSA Cryptography Standard" definiert. Der Anhang A zitiert leicht angepasst wenige Abschnitte daraus um das Nachschlagen zu erleichtern.

2.1.1 Der öffentliche Schlüssel

Der öffentliche Schlüssel besteht aus zwei Komponenten, dem Modulus und dem öffentlichen Exponenten.

2.1.2 Der private und geheime Schlüssel

Der private Schlüssel besteht aus zwei Komponenten, dem selben Modulus (wie beim öffentlichen) und dem privaten Exponenten. Er wird so berechnet, dass öffentlicher und privater Schlüssel die Umkehrfunktion zueinander leisten.

2.2 Die Grundoperationen

Die Grundoperationen sollen anhand des RSA Algorithmus dargestellt werden. Beim RSA Schlüsselpaar kommt es nicht darauf an, ob der öffentliche oder der private Schlüssel zuerst angewendet wird, jeder leistet die Umkehrfunktion für den anderen.

PKCS#1 definiert vier Grundoperationen, zu Paaren geordnet: Verschlüsseln und Entschlüsseln; Signieren und Verifizieren. Das wichtige mathematische Verfahren jeder Operation ist Potenzieren.

2.2.1 Verschlüsseln und entschlüsseln

Verschlüsseln ist exklusiv für den Empfänger, nur er soll mit seinem privaten Schlüssel entschlüsseln können. Also wird der öffentliche Schlüssel zum Verschlüsseln benötigt.

Die RSA Berechnungen sind aufwändig im Vergleich zu symmetrischen Algorithmen. Deshalb werden die Daten mit einem symmetrischen Verfahren verschlüsselt. Nur der "ad hoc erzeugte" symmetrische Schlüssel (session key) wird mit RSA verschlüsselt und der Meldung beigelegt[10].

2.2.2 Signieren und verifizieren

Die Aktivität bei Authentisierung, Identitätsnachweis oder Unterschrift liegt exklusiv bei demjenigen, der den Nachweis erbringen will und dazu den privaten Schlüssel gebrauchen muss. Prüfen soll jeder können, wozu der öffentliche Schlüssel dient.

Bei der Authentisierung und dem Identitätsnachweis fordert der Prüfer dazu auf, zum Beispiel eine grosse Zufallszahl mit dem privaten Schlüssel zu verschlüsseln, damit er mit dem öffentlichen Schlüssel die Antwort prüfen kann und daher den Eigenschaften, die er damit verbindet (z.B. dem Namen), vertrauen kann.

Bei der Unterschrift bildet der Urheber nach fester Regel eine Quersumme[11] über den Text, verschlüsselt diese mit seinem privaten Schlüssel und legt diese "Signatur" bei (daher der Ausdruck "signieren"). Der Prüfer berechnet nach gleicher Regel die Quersumme über den erhaltenen Text und vergleicht sie mit jener, die er aus der Signatur zurückgewinnt (er entschlüsselt die Signatur mit dem öffentlichen Schlüssel des Urhebers). Von diesem Nachrechnen kommt der Ausdruck "verifizieren." Bei Übereinstimmung gilt der Text als unverändert und vom Absender stammend.

---

[9] In der gültigen Version ist das PKCS #1 v2.0. http://www.rsasecurity.com/rsalabs/pkcs/index.html.

[10] Das ist das sogenannte "hybride" Verfahren: die Menge wird symmetrisch, der angewandte Schlüssel asymmetrisch verschlüsselt.

[11] Solche Quersummen heissen je nach Anwendungsbereich Hash, Message Digest, u.a.m.

3 Handhabung der asymmetrischen Schlüssel

Im Falle der Verschlüsselung muss der Absender zweifelsfrei sicher sein, dass er mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Dabei ist unabdingbar, dass der Empfänger seinen privaten Schlüssel dauernd geheim hält und nur selber anwendet.

Im Falle der Nachweisprüfung muss der Prüfer zweifelsfrei sicher sein, dass er mit dem öffentlichen Schlüssel des Nachweiserbringers prüft. Dabei ist unabdingbar, dass der Nachweiserbringer seinen privaten Schlüssel dauernd geheim hält und nur selber anwendet.

Wer Public-Key Kryptographie anwendet, hat zwei Grundanforderungen: die privaten Schlüssel sind geheim, die öffentlichen Schlüssel sind auf eine verlässliche Art erhältlich. Wir haben es also mit Geheimhaltung und Vertrauen zu tun.

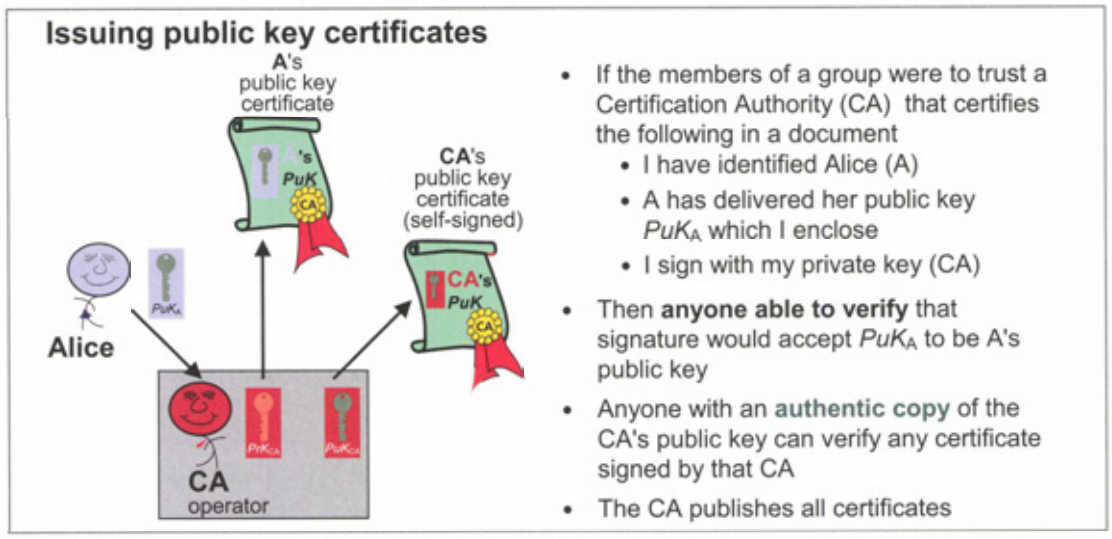
3.1 Vertrauen in den öffentlichen Schlüssel

Wer eine Nachricht verschlüsseln will, muss sicher sein, den öffentlichen Schlüssel des beabsichtigten Adressaten zu verwenden. Dieser soll von einem Verzeichnis erhältlich sein, zum Beispiel einem Adressbuch, das zu jedem Teilnehmer auch den öffentlichen Schlüssel ausweist. Diese einfache Lösung birgt die Gefahr, dass jeder, der im Verzeichnis Einträge vornehmen kann, auch Gelegenheit hat, Schlüssel auszutauschen mit dem Ziel, verschlüsselte Nachrichten anderen Personen als dem Adressaten in Klartext zugänglich zu machen. Es gilt als schwierig, solchen Missbrauch zu verhindern und deshalb gelten Verzeichnisse für die einfache Lösung als unsicher.

Besser sieht es aus, wenn den blossen Schlüssel ein nicht veränderbarer Text begleitet, der aussagt, zu wem der Schlüssel gehört und wozu er zu gebrauchen ist. Wird der Schlüssel zusammen mit dem Text unterzeichnet, ist auch die Nicht-Veränderbarkeit gewährleistet. Die Richtigkeit hängt von der Verlässlichkeit des Unterzeichners ab. Das so entstandene Dokument heisst Zertifikat und kann in einem als unsicher betrachteten Verzeichnis zur Verfügung gestellt werden. Wer verschlüsseln will, benutzt das Zertifikat, das auf den Adressaten ausgestellt ist, und entnimmt ihm den öffentlichen Schlüssel.

Die Frage, wer Zertifikate unterzeichnen soll, führt auf viele mögliche Antworten.

Es kann der Schlüsseleigentümer selber sein. In dem Falle braucht sein Partner einen verlässlichen Weg, wie er das Zertifikat aus "erster Hand" erhält. Damit ist für eine grössere Gruppe wenig gewonnen, weil solche Zertifikate nicht "verzeichnisfähig" sind und also jeder bei jedem das Zertifikat direkt abholen muss.



Es kann auch eine vertrauenswürdige Institution sein, die Zertifikate ausstellt. Mit der Unterschrift bestätigt diese, dass sie nach bestimmten Regeln der Sorgfalt geprüft hat, dass der Schlüssel zum benannten Teilnehmer gehört und zu einem bestimmten Zweck gebraucht werden soll. Solche Zertifikate sind "verzeichnisfähig" und gelten für alle Teil-

nehmer, welche dieser Institution vertrauen. Der übliche Name für eine solche Institution ist Zertifizierungsstelle oder Certification Authority. Im folgenden sei unter Zertifikat immer eine sich selbst beschreibende Datenstruktur verstanden, die nach der ITU-T X.509 Norm[12] gebildet ist.

Bei der Handhabung der Schlüssel spielen Zertifizierungsstellen und Verzeichnisse eine wichtige Rolle, ja sie dominieren die Projektarbeit, wenn Public-Key Kryptographie eingeführt wird.

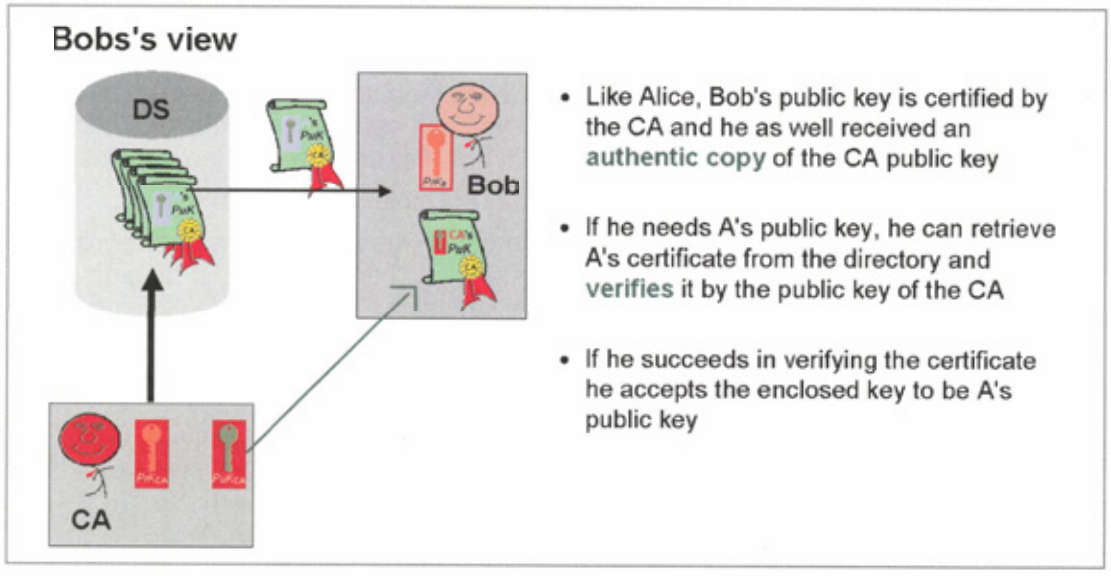
3.1.1 Zertifizierungsstellen

Das gemeinsame Vertrauen in die Unterschrift der Zertifizierungsstelle bildet die Anwendergruppe.

Der öffentliche Prüfschlüssel der Zertifizierungsstelle ist dabei das wichtigste kryptographische Element: ist er nicht mehr zuverlässig, fällt alles in sich zusammen. Er ist in einem selbst unterzeichneten Zertifikat enthalten mit weiteren Angaben. Dieses Zertifikat ist nur dann vertrauenswürdig, wenn man sich vergewissert[13] hat, dass es von jener Zertifizierungsstelle erstellt wurde, der man vertraut.

Eine wichtige Aufgabe der Zertifizierungsstelle ist die Publikation der gültigen Zertifikate und der Liste der ungültig erklärten Zertifikate (Certificate Revocation List, CRL,vergleiche auch 3.1.3.) im Verzeichnis. Sie kann in den Zertifikaten ausserdem[14] angeben, wo und wie sich der Benutzer informieren kann über die angewandten Zertifizierungsrichtlinien, ob und wie on-line Anfragen über Zertifikatsgültigkeit erhältlich sind und allenfalls mit welchen Zertifizierungsstellen sie zusammenarbeitet.

3.1.2 Verzeichnisdienste



X.500 Verzeichnisse[15] bieten eine Fülle von Diensten an, mit angemessenen Zugriffsrechten und Verbreitungsmechanismen. Darin ist das Directory Access Protocol (DAP) das Instrument für Abfragen.

Die Internet-Gemeinschaft zieht für Abfragen dem X.500 Directory Access Protocol (DAP) allerdings das "Lightweight" Directory Access Protocol[16] (LDAP, IETF) vor.

---

[12] ITU-T, X.509 (03/2000) "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks." Gemeinsamer Standard mit ISO/IEC 9594-8.

[13] Zum Beispiel durch direktes, persönliches Abholen.

[14] Authority Information Access certificate Extension, IETF, PKIX Working Group, RFC 2459.

[15] ITU-T X.500, ISO/IEC 9594-1: "Information Technology – Open Systems Interconnection – The Directory: Overview Of Concepts, Models, And Services"

PKI geschützte Anwendungen (typischerweise eMail) befragen Verzeichnisse, wenn der öffentliche Schlüssel in einem Zertifikat gesucht wird (zum Verschlüsseln einer Meldung oder zur Prüfung einer Unterschrift).

3.1.3 Missbrauch und Prüfung

Um dem Missbrauch von öffentlichen Schlüsseln zu begegnen, sind zwei Massnahmen für das zugehörige Zertifikat vorgesehen: die Verifikation und die Gültigkeitsprüfung (Validierung).

Bei der Verifikation geht es einfach darum, gestützt auf die im Zertifikat verfügbaren Informationen zu prüfen, ob damit alles in Ordnung ist, insbesondere dass es korrekt unterschrieben ist (Nachrechnen der Unterschrift) und innerhalb seiner Gültigkeitsdauer benutzt wird.

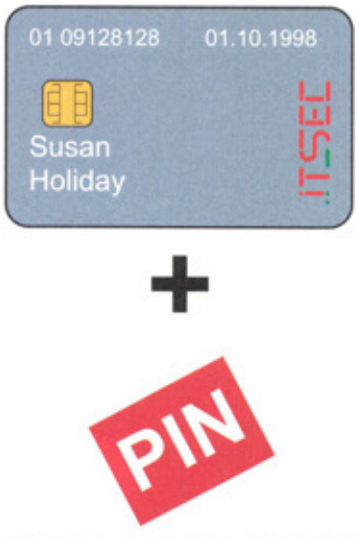
Danach geht es darum, ob der Unterzeichner vertrauenswürdig ist; allenfalls ist eine ganze Kette von füreinander bürgenden Zertifizierungsstellen zu prüfen, bis das Glied, dem man traut, gefunden ist. Dabei ist es wichtig, bei jedem verwendeten Zertifikat sicher-zustellen, dass es vom Unterzeichner nicht widerrufen wurde (Validierung, siehe 4.3).

3.2 Geheimhaltung des privaten Schlüssels

Es ist eine anspruchvolle Aufgabe, die privaten Schlüssel immer geheim zu halten und sie exklusiv zu gebrauchen. Dabei muss der Anwender unterstützt werden.

Software Token helfen dadurch, dass die kryptographischen Elemente in die Form eines strukturierten Datenpakets gegossen werden und dieses verschlüsselt wird mit Hilfe einer längeren Zeichenkette (Passphrase), die nur der Eigentümer kennt. Der Nachteil von Software Token besteht darin, dass sie unbemerkt kopiert werden können. Damit sind sie einer unbeschränkten Zahl von Versuchen ausgesetzt, die Passphrase herauszufinden, um schliesslich die Geheimelemente zu missbrauchen.

Hardware Token[17], zum Beispiel Kryptokarten (das sind Smartcards mit kryptographischem Koprozessor) speichern die geheimen Elemente unter Schutzrechten, die erlauben, sie auf der Karte anzuwenden, aber verunmöglichen, sie auszulesen. Somit verlassen sie die Karte nie, von der Einpflanzung bis zur Zerstörung.



- Cryptocards enhance security twice
  - security based on knowledge (PIN) and possession (card)
  - the secret keys never leave the card: all secret-based operations are performed on the card
- Portability of the personal security environment: just use your card at a different workstation
- Secure "initial path" from the party you trust (CA/RA) directly in your hands
- Your primary secrets are tamper-protected by the smart cryptocard during their entire lifecycle

[16] Die Grundlage dazu bilden: "Lightweight Directory Access Protocol" RFC 1777; "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2" RFC 2559; "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security" RFC 2830.

[17] Verbreitete Zugriffschnittstellen auf Hardware Token sind PKCS#11 und der Crypto Service Provider (CSP, Microsoft). PKCS#15 beschreibt eine Struktur, welche interoperable Implementierunge erlauben soll (im gleichen Sinne auch der Entwurf ISO/IEC DC 7816-15 "Cryptographic Information Application", 2001.08.27).

Die exklusive Anwendung wird ermöglicht, indem die Karte nur funktioniert, wenn eine auf der Karte überprüfbare Identifikation geliefert wird (PIN, eine persönliche Identifikationsnummer), die nur der Eigentümer kennt und die er jederzeit auch wechseln kann. Ein weiterer Vorteil liegt darin, dass man immer weiss, wo die Schlüssel sind (in der Karte) und dass sie am Ende zuverlässig zerstört werden können (Einziehen der Karte). Ausprobieren der PIN kann auf wenige Fehlversuche eingeschränkt werden, wobei die Karte weiteren Gebrauch selber sperrt, wenn zu viele Fehlversuche unternommen werden. Damit unterstützt eine solche Karte den Eigentümer weit besser als es das Software Token je kann. Zudem bieten Vorkommnisse beim Kartengebrauch (zum Beispiel Verlust, Diebstahl, etc.) frühe Warnsignale dafür, dass Schlüssel in Gefahr sein können und erlauben damit rechtzeitige Schutzmassnahmen.

3.3 Schlüsselwechsel - Key Lifecycle

Es gibt reguläre und ausserordentliche Gründe, das Schlüsselpaar zu wechseln. Vorsicht bestimmt den regulären und regelmässigen Schlüsselwechsel. Damit wird die Schadenwirkung mengenmässig begrenzt, die entstehen kann, wenn der private Schlüssel in Gefahr gerät. Treten während der regulären Gebrauchsdauer keine ausserordentlichen Ereignisse auf, beendet der Schlüsselwechsel eine sichere Anwendungsperiode, falls der weitere Gebrauch des alten Schlüssels mit Sicherheit[18] ausgeschlossen werden kann.

Die Bedrohung ist je nach Anwendungszweck der Schlüssel unterschiedlich. Im Fall der Verschlüsselung kann mit dem missbrauchten Private Key gestohlene oder aufgezeichnete Information entschlüsselt werden. Im Fall der Unterschrift können mit dem missbrauchten Private Key Dokumente nachträglich verändert oder neue in Umlauf gebracht werden. Im Fall der Authentisierung wird es mit dem missbrauchten Private Key möglich, eine falsche Identität vorzutäuschen und zusätzliche Rechte zu erschleichen. Erst der Gebrauch neuer Schlüssel verhindert weiteren Schaden.

Gibt es Hinweise auf Schlüsselmissbrauch, ist ein ausserordentlicher Schlüsselwechsel nötig. Er kommt in der Regel zu spät, verhindert aber weiteren Schaden. Nur mit geeigneten Hardware Token (zum Beispiel Kryptokarten) können rechtzeitige Meldungen über Verlust oder Diebstahl des Tokens Massnahmen[19] veranlassen, die möglicherweise Schaden ganz verhindern. Das trifft insbesondere dann zu, wenn der Schutz über die PIN durch pflichtgemässe Handhabung stark ist.

Selbstverständlich gelten diese Aussagen nicht nur für die Anwenderschlüssel, sondern auch für die Schlüssel, welche die Zertifizierungsstelle[20] selber gebraucht. Der neue öffentliche Prüfschlüssel muss allen Anwendern authentisch mitgeteilt werden. Das ist nur bei regulärem Wechsel[21] auf einfache Art möglich; sonst ist die Zertifizierung von Grund auf neu einzurichten.

3.3.1 Öffentlicher Schlüsselteil

Wird ein neues Schlüsselpaar gebraucht, ist auch ein neues Zertifikat für den neuen öffentlichen Schlüssel zu erstellen und zu publizieren. Wird der Schlüsselwechsel vorgenommen, weil das alte Zertifikat bald abläuft, sind keine weiteren Massnahmen nötig. Erfolgt der Wechsel vorzeitig, kann der Widerruf (Revocation) des alten Zertifikats angezeigt sein. Er muss erfolgen, wenn Zweifel am ordentlichen Gebrauch des alten Schlüsselpaares bestehen.

---

[18] Das trifft zu für die Private Keys, die für Authetnisierung oder Signatur verwendet werden, wenn die Kryptokarte eingezogen und dabei diese Schlüssel gelöscht werden (nicht möglich mit Software Token).

[19] Das zeigt deutlich, dass Hardware Token ein Public-Key System erheblich sicherer machen als ein vergleichbares reines Software System.

[20] Als Beispiel kann die KrypTIC CA dienen; http://www.kryptic.de/index.htm.

[21] Der alte Prüfschlüssel muss verlässlich sein während der ganzen Dauer des Wechsels, bis die Gültigkeitsdauer aller alten Zertifikate abgelaufen und nur noch neue in Gebrauch sind.

Es kann auch sein, dass ein neues Zertifikat für den bestehenden öffentlichen Schlüssel benötigt wird. Dabei geht es darum, die den Schlüssel begleitende Information zu verändern, zum Beispiel bei Namenswechsel infolge Heirat, Zusatzinformationen zu Gunsten einer neuen Anwendung oder Anpassen anderer zertifizierter Information[22] an neue Umstände. Bei geschuldeter Vorsicht kann auch einfach der Gebrauch des bestehenden Schlüsselpaares verlängert[23] werden. Ob in diesen Fällen das alte Zertifikat zu widerrufen ist oder nicht, hängt vom verfolgten Zweck und der Ausgangslage ab.

3.3.2 Privater Schlüsselteil

Die Erzeugung des neuen Schlüsselpaares muss auf sichere Weise vorgenommen werden und dasselbe gilt für die allfällige Lieferung, wenn es zum Beispiel zentral erzeugt wird. Anderenfalls sind die Schlüssel von Anfang an Gefahren ausgesetzt.

Reine Softwarelösungen (mit Software Token) beziehen bestimmte Gefahren a priori in die allgemeine Risikobetrachtung mit ein, wie zum Beispiel die Schlüsselerzeugung beim Anwender auf einer relativ unsicheren Maschine oder die Lieferung privater Schlüssel unter Passphraseverschlüsselung.

Advantages of Cryptocards in Comparison to Software Tokens

- impossible to copy
- impossible to read secrets
- private key functions execute on card
- inspire confidence in private key handling
- key integrity by a secure initial path
- authentic trust anchor
- dictionary attack on PIN impossible
- tangible key container: know where the keys are
- realize loss or theft immedia-tely: take measures early
- reduced administration
- reduced training

– hardware required

Lösungen mit Hardware Token (Kryptokarten) unterscheiden sich darin, wie die Karte ausgestellt wird: gut geschützt in sicherer Umgebung oder beim Anwender in relativ unsicherer Umgebung, allenfalls mit Lieferung privater Schlüssel unter Passphraseverschlüsselung. Beide Verfahren können auch neue Schlüssel zum Anwender bringen.

3.3.3 Gültigkeitsdauer der Zertifikate

Die Gültigkeitsdauer ist in allen X.509 Zertifikaten festgeschrieben.

Im Falle der Verschlüsselung bestimmt die Gültigkeitsdauer, wie lange Partner den öffentlichen Schlüssel im Zertifikat zum Verschlüsseln gebrauchen sollen. Der Schlüsseleigentümer kann den privaten Schlüssel uneingeschränkt zur Entschlüsselung benutzen und wird dies in aller Regel auch noch nach Ablauf des zugehörigen Zertifikates tun.

---

[22] Die Begleitinformation zum Schlüssel in Zertifikaten soll auf stabile Werte ausgerichtet sein: häufig wechselnde Information (zum Beispiel die Anschrift) verkürzt die Gebrauchsdauer unnötig. Auch betriebsorganisatorische Angaben (organisational unit) stören in Zertifikaten eher, es sei denn, die Autorisierung stützt darauf ab (zum Beispiel mittels Gruppenberechtigungen).

[23] Das sollte vermieden werden, ausser bei besonderem Schutz der privaten Schlüssel (zum Beispiel in Kryptokarten) und nach sorgfältiger Beurteilung der Sicherheit des verwendeten Algorithmus.

Im Falle der Unterschrift bestimmt die Anwendungsdauer für den privaten Schlüssel, wie lange der Schlüsseleigentümer gedenkt mit dem privaten Schlüssel, der zum Zertifikat[24] gehört, zu unterzeichnen. Der öffentliche Schlüssel dient zur Prüfung innerhalb der Anwendungsdauer geleisteter Unterschriften und seine Anwendung zu diesem Zweck wird mit der Gültigkeitsdauer des Zertifikats eingeschränkt. Ohne weitere Massnahmen sind solche Prüfungen später nicht mehr möglich.

Der Fall der Authentisierung ist technisch analog zur Unterschrift mit der Auflage, dass der Zeitpunkt, in welchem sie stattfindet, im Deckungsbereich von Gültigkeitsdauer des Zertifikats und Anwendungsdauer des Schlüssels liegt und ausserdem das Zertifikat gültig ist.

Die unterschiedliche Handhabung in den drei Fällen empfiehlt, für jeden Zweck ein eigenes Schlüsselpaar zu verwenden. Der Abschnitt 3.3.4 zeigt auf, warum ausserdem das Paar für Verschlüsselung nur zu diesem und keinem anderen Zweck gebraucht werden soll.

3.3.4 Alte Dokumente

In einer Unternehmung kann es auch nach langer Zeit nötig werden, ein verschlüsselt abgelegtes Dokument zu entschlüsseln. Dazu müssen die privaten Schlüssel für Verschlüsselung von Anfang an in einem sicheren Archiv abgelegt werden, zusammen mit klaren Regeln, wer sie wiederverwenden darf und wie dies zu erfolgen hat.

Alte Verträge zum Beispiel stellen ein analoges Problem mit der Unterschriftenprüfung, die aber des öffentlichen Schlüssels für Signatur bedarf. So späte Nachprüfungen sind in den üblichen Standards nicht geregelt und brauchen daher fallweise besondere Massnahmen[25], die möglicherweise die aktive Mithilfe der Zertifizierungsstelle erfordern bei der Wiederbeschaffung alter Zertifikate.

3.4 Abstecher in den Cyberspace

Namen sind im virtuellen Raum des Worl Wide Web (Cyberspace) nicht verlässlich, weil sie nicht mit Kirchtürmen, Herkunftsgeschichten und erworbenem gutem Ruf verbunden werden können. Nur der öffentliche Schlüssel für Signatur (Prüfschlüssel) ist sichtbar und bei Lesern in Gebrauch. Es entwickelt sich eine Identität und ein Ruf im Hyperspace, die einzig darauf gründen, dass der Handelnde und nur er den zugehörigen privaten Schlüssel besitzt und anwendet, diesen also insbesondere geheimhält[26]. Regeln gegen Missbrauch (HyperLaws), eine zugehörige Rechtsprechung (HyperJurisdiction) und Strafverfolgung (HyperProsecution) fehlen weitgehend. Und natürlich treten vielfältige Schwierigkeiten an allen Berührungsstellen mit dem realen Raum auf. Gegenwärtig versucht die Internet Gemeinschaft, vom realen (Wirtschafts[27]-) Raum aus in einen verlässlichen Cyberspace hineinzuwachsen – und tut sich schwer damit.

4 Die Vertrauensfrage

Vertrauen ist unteilbar. Welche Vertrauensbeweise für den verfolgten Zweck und unter einer bestimmten Risikobereitschaft erforderlich sind, kann von der Applikation abhängen, die gesichert werden soll.

---

[24] Die Gültigkeitsdauer des privaten Schlüssels kann in der Zertifikatserweiterung "privateKeyUsagePeriod" festgelegt werden (RFC 2549).

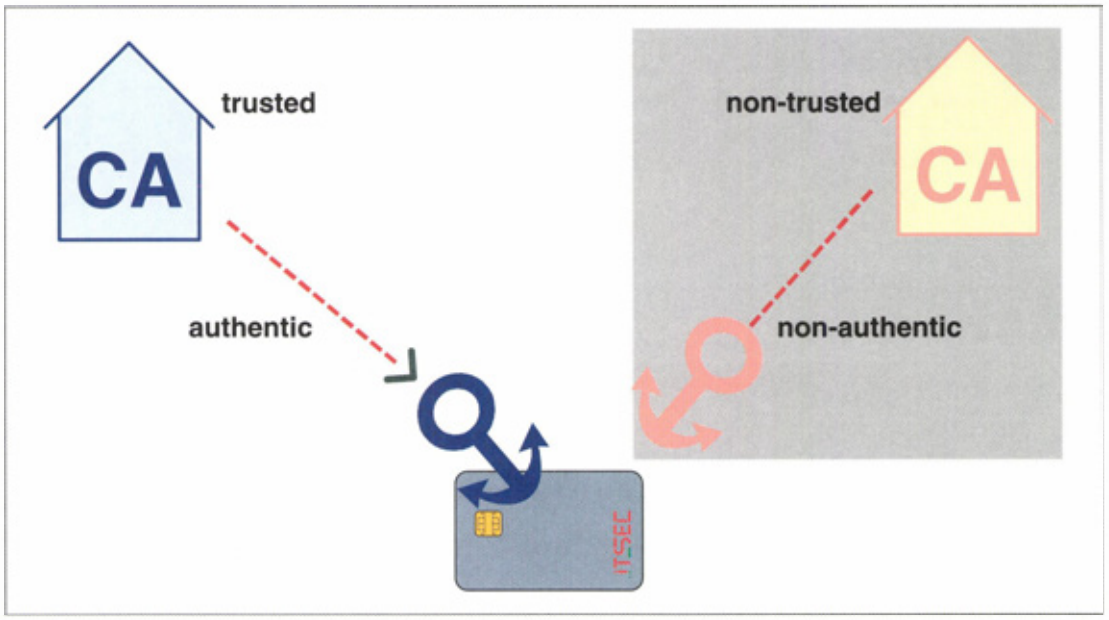
[25] Die bedecken ein weites Feld, das den Rahmen dieser Betrachtungen sprengt.

[26] In diesem Zusammenhang ergeben sich auch interessante Aspekte, wenn eine (Arbeits-) Gruppe denselben privaten Schlüssel gebraucht.

[27] Darin liegt die Schwierigkeit - immaterielle Werte haben weniger kritische Berührungsstellen mit dem realen Raum (zum Beispiel in der Wissenschaft).

4.1 Vertrauen in den ersten Schritt

In jedem PKI System ist genau zu verfolgen, wie das Vertrauen von Anfang an Schritt für Schritt aufgebaut wird.



Jedem Anwender muss klar sein, welchen Zertifizierungsstellen er vertrauen will. Von diesen benötigt er erwiesenermassen unverfälschte Prüfschlüssel.

Diese öffentlichen Prüfschlüssel bilden die Verankerung des Vertrauens (trust anchors) in PKI Systemen. Der Anwender sollte sie genau so sorgfältig hüten[28] wie seine privaten Schlüssel.

4.2 Vertrauen in den Partner

Der Partner ist genau so vertrauenswürdig, wie es ihm gelingt, seine privaten Schlüssel geheim zu halten und nur selber anzuwenden. Partner, die Kryptokarten verwenden, sind deshalb vertrauenswürdiger als andere weil ihnen das leichter gelingt.

4.3 Validierung der Zertifikate

Wer immer sich auf den Inhalt eines Zertifikates stützt, muss sicherstellen, dass es nicht widerrufen ist und dass der Unterzeichner sein Vertrauen geniesst. Der Vorgang heisst Validierung.

Dass das Zertifikat nicht widerrufen ist, kann sein Fehlen auf der aktuellen Rückrufliste des Unterzeichners nachweisen.

Ist der Unterzeichner eines zu Validierung benötigten Zertifikates nicht direkt vertrauenswürdig, wird es nötig, eine Kette von für einander bürgenden Zertifizierungsstellen zu finden, die bei einer direkt vertrauenswürdigen endet. Je nach dem zu Grunde liegenden Modell der Vertrauensbildung (Abschnitt 4.5) ist diese Aufgabe leichter oder schwerer lösbar. Die Glieder dieser Kette bilden eine Reihe von Zertifikaten[29], von denen je einzeln festzustellen[30] ist, dass sie nicht widerrufen sind.

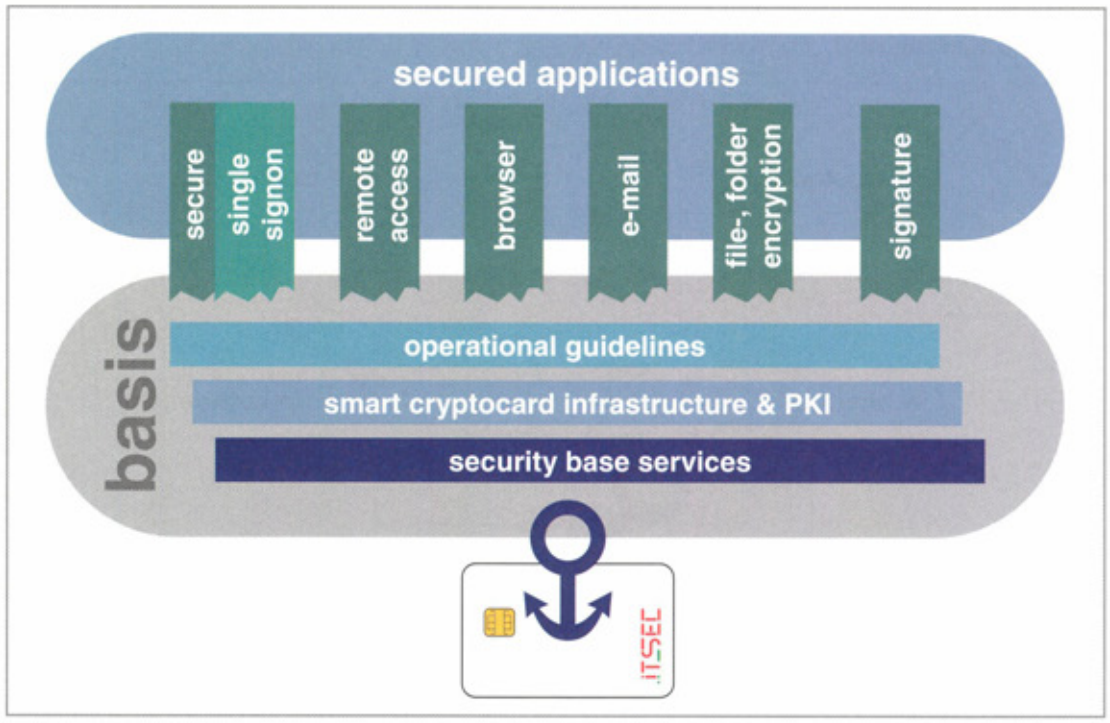
---

[28] Das bedeutet durchaus, dass bei Gebrauch von Kryptokarten diese Prüfschlüssel in der Karte festsitzen sollen und nur mit ebenso sorgfältigen Verfahren gewechselt werden können wie die privaten Schlüssel.

[29] "Certificate chain" und "chain validation" sind die damit verbundenen Stichworte.

[30] Ausser dem Fehlen eines Widerrufs kann es bei der Validierung nötig werden, auch die Zertifizierungsrichtlinen (Policy), welche die jeweiligen Unterzeichner anwenden, dem Zweck entsprechend vergleichend zu werten.

4.4 Die Anwendungen entscheiden



Die folgenden Beispiele deuten an, dass neben zuverlässigen Zertifikaten weitere Dienste gefordert sind.

Zum Beispiel ein Dienst, der den Zeitpunkt zu dem ein bestimmtes Faktum vorliegt überprüfbar festhält, oder ein Dienst, der es den Anwendungen erleichtert, Zertifikate zu validieren, oder ein Dienst, der dafür sorgt, dass Unterschriften in archivierten Dokumenten nicht verfallen. Die Einzelheiten sind in diesem Zusammenhang nicht wichtig, aber die Erkenntnis, dass es die Anwendungen sind, die entscheiden, welche Zusatzdienste nötig sind.

4.4.1 On-line Verbindungen

Browser-Sicherheit im Web (https)

Browser Sicherheit im Web stützt sich auf das Transport Layer Security[31] (TLS) Protokoll, das auf der Transportschicht Sicherheitsdienste zwischen Client und Server einrichtet, insbesondere Verbindungsverschlüsselung und allenfalls Authentisierung. Dabei dienen Public-Key Techniken zur Vereinbarung gemeinsamer Geheimelemente. Die ein- oder gegenseitige Authentisierung verwendet Zertifikate. Das Protokoll übergibt die benötigten Zertifikate - Verzeichnisdienste werden nur bei der Validierung beansprucht.

Geschäftsabwicklung (Transaktion)

Die on-line Abwicklung eines Geschäfts verlangt weit mehr. Gegenseitige Authentisierung ist Voraussetzung. Verbindliche Unterschrift ist zwingend. Eine zuverlässige Bestätigung des Abschlusszeitpunktes und Mittel sind gefordert, die verhindern, dass der eine oder andere Partner abstreitet, das Geschäft verlangt beziehungsweise den Auftrag angenommen zu haben. Validierung ist nicht mehr eine Option, sondern Pflicht. Verzeichnisdienste werden mehrfach beansprucht. Dabei werden Zeitstempel- und Notariatsdienste möglicherweise von vertrauenswürdigen Dritten erbracht, die neben den Zertifizierungsstellen arbeiten.

[31] Das Transport Layer Security (TLS) Protokoll nach IETF RFC 2246 stützt sich auf Netscape's Secure Socket Layer (SSL) Protokoll [A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996] und entwickelt es weiter.

Virtual Private Network (VPN)

Die Dienste gegenseitige Authentisierung und Vereinbarung eines Verbindungsschlüssels für die Verschlüsselung ermöglichen es, zwei oder mehrere Intranets über das Internet so miteinander zu verbinden, dass das Ganze unter dem Gesichtspunkt der Datensicherheit wie ein einziges aussieht. Die Sicherheitsdienste (IPsec[32]) werden in der Schicht des Internet Protokolls angeboten.

4.4.2 Store-and-forward Transport oder eMail

Am Beispiel sicherer elektronischer Post (eMail) ist leicht einzusehen, dass der Adressat mit seinen Zertifikaten nicht aushelfen kann wie im Fall einer on-line Verbindung. So muss beispielsweise das Zertifikat für Verschlüsselung des Adressaten im Verzeichnis (Adressbuch) abgeholt werden. Das gilt auch für das Prüfzertifikat für die Unterschrift (es wäre denn, dass es der Absender beilegte). Gegenüber der Browser Sicherheit im WEB sind hier Verzeichnisdienste von Anfang an gefordert.

Ganz ähnlich liegen die Verhältnisse beim Unterzeichnen und Gegenzeichnen von Verträgen.

Die Einträge in ein elektronisches Grundbuch stellen wegen ihrer Dauerhaftigkeit weitere besondere Anforderungen.

4.5 Modelle der Vertrauensbildung

4.5.1 Virtual Root

BrowserHersteller liefern mit dem Programm auch die Prüfzertifikate weltläufiger Zertifizierungsstellen, denen vertraut werden soll. Diese Versammlung von Prüfzertifikaten wirkt als ob eine (virtuelle) Wurzel (Root) der Zertifizierung bestünde, die der Hersteller führt. Den unbekümmerten Benutzer freut es, denn die "Sicherheitsdienste" seines Browsers funktionieren.

Besser steht es um die Vertrauenswürdigkeit, wenn die Liste[33] von Prüfzertifikaten anderer Zertifizierungsstellen von einer direkt vertrauenswürdigen Zertifizierungsstelle unterzeichnet und aktuell gehalten wird. Eine solche Liste lässt sich immerhin in die Validierung einbeziehen.

4.5.2 Hierarchie

Der Zertifizierungsstelle an der Spitze der Hierarchie[34] vertrauen alle - sie bildet den Ankerpunkt. Diese Tatsache definiert auch schon die Anwendergruppe als abgeschlossen. Die Validierung irgend eines Zertifikats verfolgt dabei eine Kette von einander untergeordneten Prüfzertifikaten sozusagen rückwärts bis zur Spitze. Vom Benutzer aus gesehen liegt die vertrauenswürdige Zertifizierungsstelle an der Spitze allerdings gefühlsmässig weit weg.

4.5.3 Netzwerk

Zertifizierungsstellen können auch gleichrangig[35] zusammenarbeiten. Dabei entsteht ein Netzwerk. Die Benutzer vertrauen der Zertifizierungsstelle, die ihre Zertifikate ausstellt und ihnen daher gefühlsmässig nahe liegt. Die Validierung muss sich von der Zertifizierungsstelle des Partners bis zu jener mit anerkanntem Vertrauen die Zertifikatskette zusammensuchen, was im Netz auf mehreren Pfaden möglich ist.

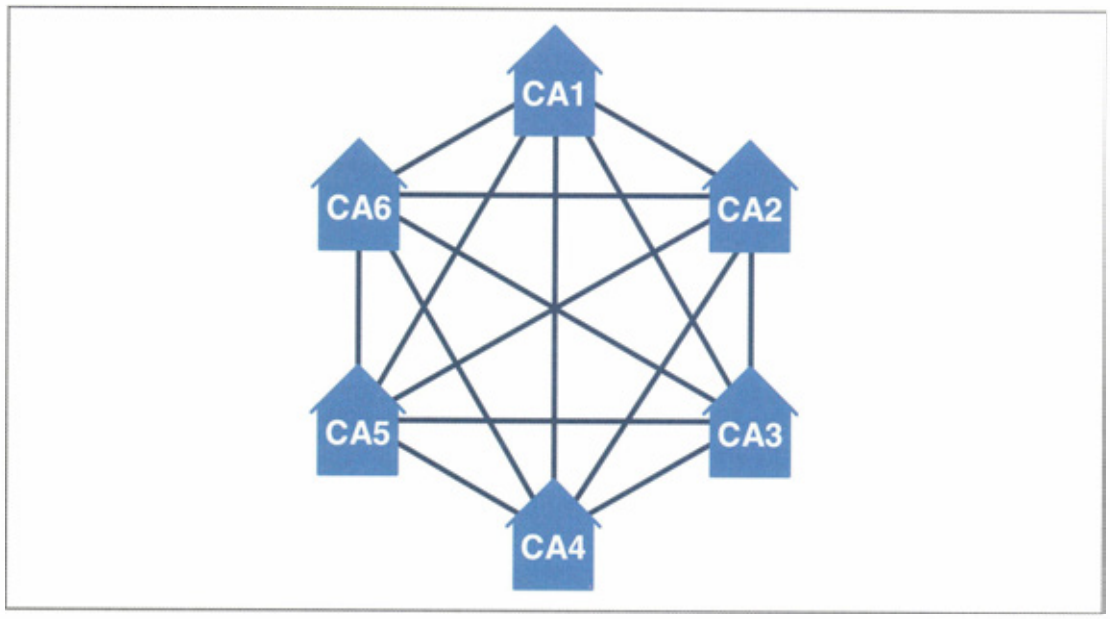
---

[32] Die Grundlagen für die Internet Protokoll Sicherheit IPsec wird in den RFCs 2401 bis 2412 gelegt; RFC 2411 "IP Security Document Roadmap" beschreibt die zugehörigen Dokumente und ihren Zusammenhang.

[33] Mit solchen Listen kann beispielsweise Windows 2000 umgehen.

[34] Das ist der Ansatz von "Privacy Enhancement for Internet Electronic Mail (PEM)" RFC 1422, RFC 1421, RFC 1423. Es ist zu vermuten, dass sich PEM gerade wegen der hierarchischen Struktur nicht hat durchsetzen können.

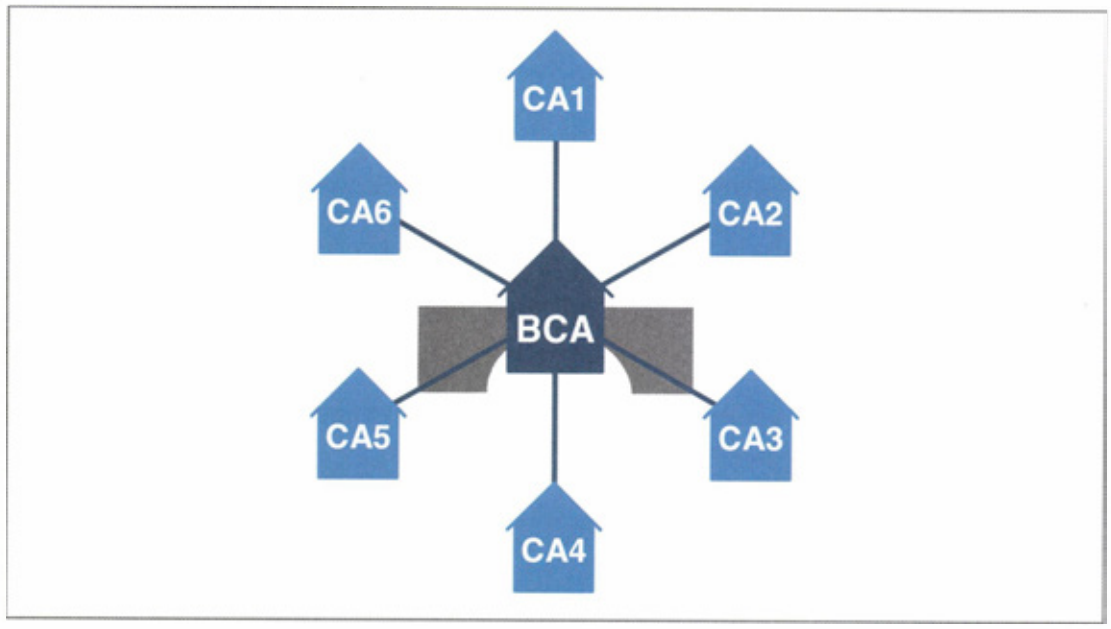
[35] Das heisst, dass sie sich gegenseitig (peer-to-peer) und für ihre Benutzer verbindlich als vertrauenswürdig anerkennen (cross-certification).



Vorteilhaft ist, dass mehrere Vertrauensanker für je ihre Benutzer bestehen. Das macht das Netzwerk robust beim Versagen einer einzelnen Zertifizierungsstelle. Soll eine Zertifizierungsstelle neu hinzutreten, muss sie allerdings Partnerschaften mit allen bestehenden eingehen.

4.5.4 Brückenbildung

Der Einsatz einer Zertifizierungsstelle, die eine Brücke (Bridge Certification Authority, BCA[36]) bildet zwischen den Zertifizierungsstellen eines Netzwerks (sie zertifiziert keine Benutzer), ermöglicht es, die Netzwerkstruktur deutlich dadurch zu vereinfachen, dass die einzelnen Stellen nicht mehr direkt, sondern nur noch über die Brücke zusammenarbeiten.



Die Vorteile der Nertzwerkstruktur bleiben erhalten und die Validierungspfade werden eindeutig.

[36] Zum Beispiel gilt für die (U.S.) "Federal Bridge Certification Authority (FBCA)": "The FBCA, as of June 7, 2001 is open and ready for business." http://www.cio.gov/fbca/

4.5.5 Vertauen in sehr grossen Gruppen

Menschlich Schwächen reduzieren die Vertrauenswürdigkeit, wenn die Gruppe zunimmt.

5 Lösungen

Die Anwendung von Public-Key Kryptographie stellt zwei Aufgaben, die letztlich auf der Eigenart der zwei Schlüssel des Schlüsselpaares beruhen: Vertrauen herzustellen in den öffentlichen Schlüssel und Geheimhaltung des privaten Schlüssels. Diese Aufgaben können kombiniert wahrgenommen werden, aber auch getrennt.

5.1 Zertifizierungsstellen

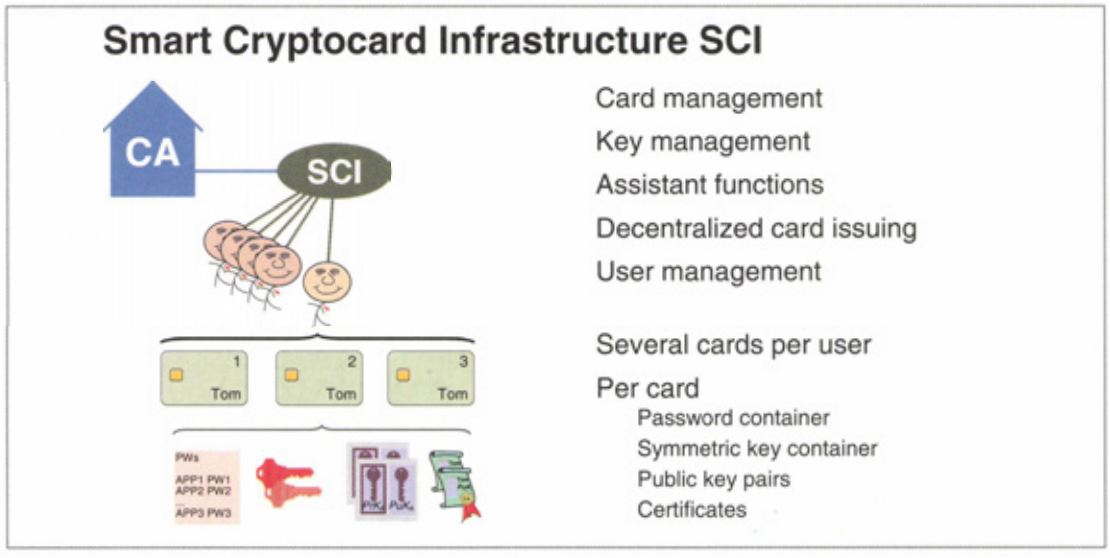
Im einfachsten Fall ist eine Zertifizierungsstelle die Institution, deren Zertifikaten alle vertrauen. Die Publikation erstellter Zertifikate und die Handhabung der Massnahmen, die es erlauben, unzuverlässig gewordene Zertifikate zu widerrufen, sind feste Aufgaben jeder Zertifizierungsstelle.

Soll ein Verband von Zertifizierungsstellen gebildet werden, um beispielsweise einen Marktplatz einzurichten, sind auch Instrumente für die wechselseitige Anerkennung erforderlich.

Wird auch noch Schlüsselverwaltung und allfällige Wiederbeschaffung von Schlüsseln gefordert, müssen Schlüsselerzeugung und ihre sichere Aufbewahrung einbezogen werden.

5.2 Kartenverwaltung

Sind Kryptokarten eingesetzt, um die Sicherheitsanforderungen zu erfüllen, leisten diese ihren starken Beitrag bei der Geheimhaltung. Karten- und Schlüsselverwaltung zu kombinieren vereinfacht die Prozesse bei Schlüsselwechsel und Wiederbeschaffung von Schlüsseln (Smart Cryptocard Infrastructure, SCI).



Derart ausgelegte Kartenverwaltungen gewinnen das Vertrauen in die öffentlichen Schlüssel von Zertifizierungsstellen[37]; sie übernehmen aber die ganze Schlüsselverwaltung.

Der Kartengebrauch lokalisiert die Schlüssel. Das hat zwei Vorteile. Ereignisse, welche die Karte betreffen, wie etwa ihr Verlust, ergeben rasch Hinweise auf mögliche Gefahren für die Schlüssel und erlauben frühzeitige Schutzmassnahmen. Daneben fördert der physische Behälter für die Schlüssel die gefühlsmässige Beziehung des Benutzers zu seinen Nachweisinstrumenten, sie werden greif- und begreifbar.

[37] Es kann eine sein, aber auch mehrere. Darunter sind auch öffentlich anerkannte denkbar, wenn sie bereit sind, mit Kartenverwaltungen zusammenarbeiten.

Andererseits muss eine Kartenverwaltung sicherstellen, dass die Benutzer unter allen Umständen eine Karte nutzen oder wiederbeschaffen können, bei Versagen, Vergessen, Diebstahl oder Problemen mit der PIN.

6 Zusammenfassung

Asymmetrische, d.h. Public-Key Verfahren erleichtern die Schlüsselverteilung und die Verwaltung von Gruppen, wenn Teilnehmer hinzukommen und weggehen.

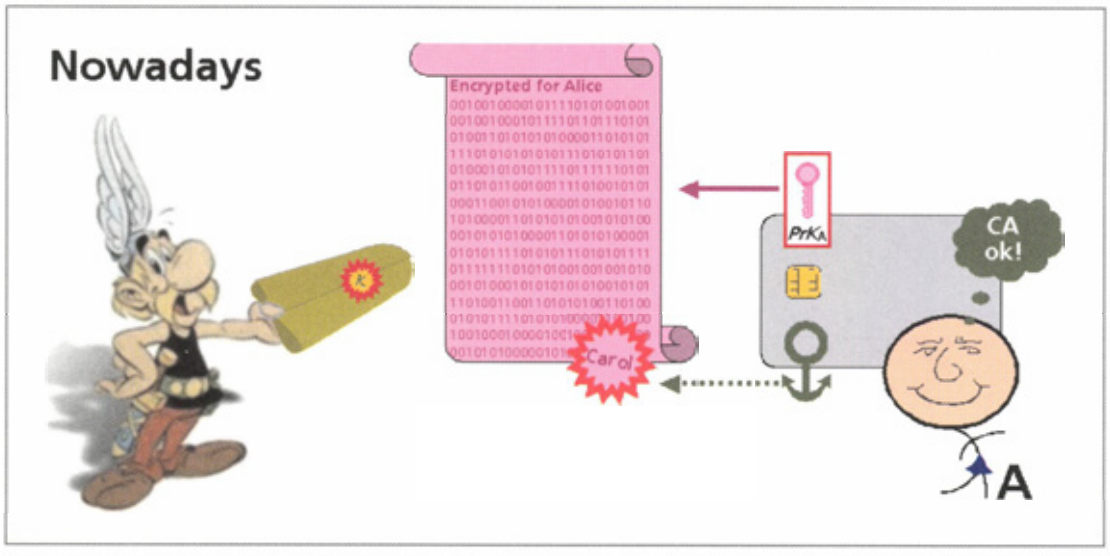
Zertifizierungsstellen ermöglichen die Bewirtschaftung der Vertrauensfrage und der öffentlichen Schlüssel, sei es als einzelne Zertifizierungsstelle oder in einem strukturierten Verband.

Kryptokarten helfen, die privaten Schlüssel geheim zu halten. Auch sie brauchen eine Bewirtschaftung, die Kartenverwaltung.

Beide Komponenten sind für die sichere und dauerhafte Anwendung von Public-Key Verfahren wie Geschwister erforderlich. Beide nehmen den Charakter von Infrastrukturen an, wenn bedacht wird, wie viel Spezialwissen erforderlich ist, um eine korrekte Handhabung zu gewährleisten. Bei PKIs verbreitet sich diese Erkenntnis, bei Kartenverwaltungen (Smart Cryptocard Infrastructure, SCI) muss sie sich erst noch durchsetzen.

Gegenwärtig schwierig ist, dass ein grosses Geschrei um Zertifikate gemacht wird. Es breiten sich Softwarelösungen aus, die Kartenbedürfnissen nicht angemessen gerecht werden (W2K, Entrust). Dabei wird der gebührenden Sorgfalt für den privaten Schlüssel nicht die erforderliche Beachtung geschenkt. Es steht zu hoffen, dass die Architekten von Lösungen (auch grosser Herstellerfirmen) der Kenntnis kartenspezifischer Bedürfnisse bald angemessen Rechnung tragen.

Für die Zusammenarbeit zwischen Unternehmen bieten Brückenzertifizierungsstellen ein partnerschaftliches Vertrauensmodell an, das alternativ zu Diensten von Dritt-Anbietern (zum Beispiel Identrus[38]) erfolgreich genutzt werden kann.



So wird es möglich, dass Alice den Brief von Carol entschlüsseln und Carol's Unterschrift prüfen kann. Dabei ist sie sicher, dass erstens niemand sonst den Brief gelesen hat, weil sie ihren privaten Schlüssel gut geschützt weiss, und zweitens, dass Carol den Inhalt genau so gewollt hat, weil sie die Unterschrift mit dem Prüfschlüssel der Zertifizierungsstelle ihres Vertrauens validiert.

[38] http://www.identrus.com.

A Quotations from RSA Cryptography Standard PKCS#1

Two key types are employed in the primitives and schemes defined in this document[39]: RSA *public key* and RSA *private key*. Together, an RSA public key and an RSA private key form an *RSA key* pair.

...

An **RSA public key** consists of two components:

- n, the modulus, a nonnegative integer
- e, the public exponent, a nonnegative integer

In a valid RSA public key, the modulus n is a product of f distinct odd primes r_i, i = 1, 2,..., f, where f≥2 and the public exponent e is an integer between 3 and n–1 satisfying

GCD (e, λ(n)) = 1, where $\lambda(n) = LCM (r_1 - 1, \ldots, r_f - 1)$.

By convention, the first two primes r_1 and r_2 may also be denoted p and q respectively.

...

An **RSA private key** may have either of two representations.

The first representation consists of the pair (n, d), where the components have the following meanings:

- n, the modulus, a nonnegative integer
- d, the private exponent, a nonnegative integer

In a valid RSA private key with the first representation, the modulus n is the same as in the corresponding public key and is the product of f distinct odd primes r_i, i = 1, 2, ..., f, where f≥2. The private exponent d is a positive integer less than n satisfying

$e \cdot d \equiv 1 \pmod{\lambda(n)}$,

where e is the corresponding public exponent and λ(n) is as defined above.

...

Four types of primitive are specified in this document, organized in pairs:

- encryption and decryption; and
- signature and verification.

The main mathematical operation in each primitive is exponentiation.

...

Encryption primitive RSAEP ((n, e), m)

Input:
(n, e) RSA public key
m message representative, an integer between 0 and n–1
Output:
c ciphertext representative, an integer between 0 and n–1
Steps:
1. If the message representative m is not between 0 and n–1, output "message representative out of range" and stop.
2. Let $c = m^e \bmod n$.
3. Output c.

Decryption primitive RSADP (K, c)

Input:
KRSA private key, where K has the first form: a pair (n, d)
C ciphertext representative, an integer between 0 and n–1
Output:
m message representative, an integer between 0 and n–1
Steps:
1. If the ciphertext representative c is not between 0 and n–1, output "ciphertext representative out of range" and stop.
2. If the first form (n, d) of K is used: Let $m = c^d \bmod n$.
3. Output m.

...

[39] PKCS #1 v2.0. Http://www.rsasecurity.com/rsalabs/pkcs/index.html

Signature primitive RSASP1 (K, m)
Input:
KRSA private key, where K has the form (n, d)
m message representative, an integer between 0 and n–1
Output:
s signature representative, an integer between 0 and n–1
Steps:
1. If the message representative m is not between 0 and n-1, output "message representative out of range" and stop.
2. If the first form (n, d) is used: Let $s = m^d \bmod n$.
3. Output s.

Verification primitive RSAVP1 ((n, e), s)
Input:
(n, e) RSA public key
s signature representative, an integer between 0 and n–1
Output:
m message representative, an integer between 0 and n–1
Steps:
1. If the signature representative s is not between 0 and n–1, output "signature representative out of range" and stop.
2. Let $m = s^e \bmod n$.
3. Output m.

B Bridge Certification Authorities

By William T. Polk and Nelson E. Hastings[40]

... "**How the bridge certification authority enables business-to-business E-commerce**

Telecommuting, electronic mail, and web-based document delivery are commonplace in today's business operations. These applications help businesses streamline their processes, but they can also place sensitive information and assets at risk. To mitigate these threats, many organizations are implementing PKIs to secure internal operations. By deploying PKIs, organizations can protect their assets and still achieve the cost and time savings of electronic processing.

Most organizations have business partners and a desire to extend their electronic processing capability beyond their organizational boundaries. Businesses wish to leverage existing PKIs to support electronic processing with their business partners. However, these economic alliances are inherently dynamic. An organization may purchase widgets from one supplier today; if a new supplier can offer decreased cost or increased quality, they may select a new supplier tomorrow. Establishing or terminating peer-to-peer relationships each time business partners change is impractical given the dynamic nature of today's business relationships. In addition, the relationships between partnering organizations do not lend themselves naturally to support a hierarchical PKI.

The Bridge Certification Authority (BCA) architecture is ideally suited to support business-to-business (B2B) relationships. While each company has a limited set of business partners at any given moment, this set is very fluid. Companies establish and terminate these relationships with astonishing speed. However, the companies within a particular industry are not so dynamic. To illustrate this point, consider companies that manufacture sailboats.

[40] Excerpt from "Bridge Certification Authorities: Connecting B2B Public Key Infrastructures" http://csrc.nist.gov/pki/documents/B2B-article.pdf.

Sailboat manufacturers include either a gasoline or diesel engine in their boats. They don't build engines; they buy them from marine engine suppliers and install them in the boat. Sailboat manufacturers may change engine suppliers to obtain more powerful, lighter or less expensive engines as new products emerge. However, there is a limited set of sailboat manufacturers and a limited set of marine engine manufacturers. While we cannot predict which sailboat and engine manufacturers will partner in the future, we can identify the two pools of candidates – the set of engine suppliers and the set of sailboat manufacturers.

In general, sailboat manufacturers are competitors, but they all buy the same kinds of products from the same set of vendors. They need fiberglass cloth and epoxy resin for hulls, wood for the interior, aluminum tubing for spars and masts, and engines for calm days. Sailboat manufacturers compete on design, quality, and appearance as well as price. Where opportunities exist to increase efficiency and reduce prices across the board, they have an incentive to work cooperatively.

Electronic commerce with consumers has limited appeal for sailboat manufacturers because sailboat buyers want to see and touch a sailboat for themselves before they make a purchase. However, B2B electronic commerce between sailboat manufacturers and their suppliers has significant promise to increase construction efficiency and reduce the overall cost of a sailboat. A sailboat builder does not want to maintain a large inventory of expensive marine engines. On the other hand, they lose money if they stop production while they wait for a new engine to be delivered. Electronic commerce could help the manufacturer maintain just the right level of inventory by placing and filling orders efficiently.

However, a sailboat manufacturer cannot always predict which engines will be used in their boats. Building a PKI that links a sailboat manufacturer with the engine supplier they use today is useful, but the sailboat manufacturer may have to repeat the process next year if they decide to change suppliers. To complicate the situation, if an engine supplier's workers go on strike, a sailboat manufacturer may have to change suppliers even sooner. If a sailboat manufacturer does not establish a PKI with an engine supplier, the advantages of B2B electronic commerce are lost.

This type of situation is the motivating factor for establishing BCAs for specific economic industries. The sailboat industry (the manufacturers and their suppliers) would benefit as a whole from electronic commerce by deploying a BCA. By pooling resources, the sailboat industry could establish a BCA that would link all the sailboat builders and the parts manufacturers. The BCA would establish peer-to-peer relationships, eliminating arguments about sailboat manufacturer superiority. The BCA would have relationships with all the marine engine builders, so the sailboat manufacturers could order engines and check delivery dates regardless of which supplier is chosen."
