Trau, schau, wem
Was sind Zertifikate und was macht die KNF-CA

Matthias Brüstle
<m@mbsks.franken.de>

Kommunikationsnetz Franken e.V.

Public Key Cryptography

- Schlüssel existieren immer als Paar:
  - Privater Schlüssel (private key)
  - Öffentlischer Schlüssel (public key)
- Verschlüsseln mit öffentlichem Schlüssel 1 Entschlüsseln mit privatem Schlüssel
- Unterschreiben mit privatem Schlüssel **1** Prüfen mit öffentlichem Schlüssel

Problematik bei der Public Key Cryptography

[67 A9 01 BC 89 EE 47 82 6F 90 6A 55 A2 E0 73
Dieser Schlüssel gehöhrt George Orwell.]

- Vorteil gegenüber herkömmlicher Verschlüsselung: Keine geheime Übermittlung von Schlüsseln nötig.
- Problem: Der öffentliche Schlüssel muß zweifelsfrei dem Eigentümer zuordenbar sein.

Schlüsselzertifikate

[67 A9 01 BC 89 EE 47 82 6F 90 6A 55 A2 E0 73
Dieser Schlüssel gehöhrt George Orwell.]
[Die Angaben in diesem Schlüssel sind korrekt. -Eric Arthur Blair]fnord

- Ein Zertifikat bestätigt den Eigentümer.
- Es ist mit dem Schlüssel der ausstellenden Person unterschrieben.

Schlüsselzertifikate (2)

[67 A9 01 BC 89 EE 47 82 6F 90 6A 55 A2 E0 73
Dieser Schlüssel gehört George Orwell.]
[Die Angaben in diesem Schlüssel sind korrekt. -Eric Arthur Blair]

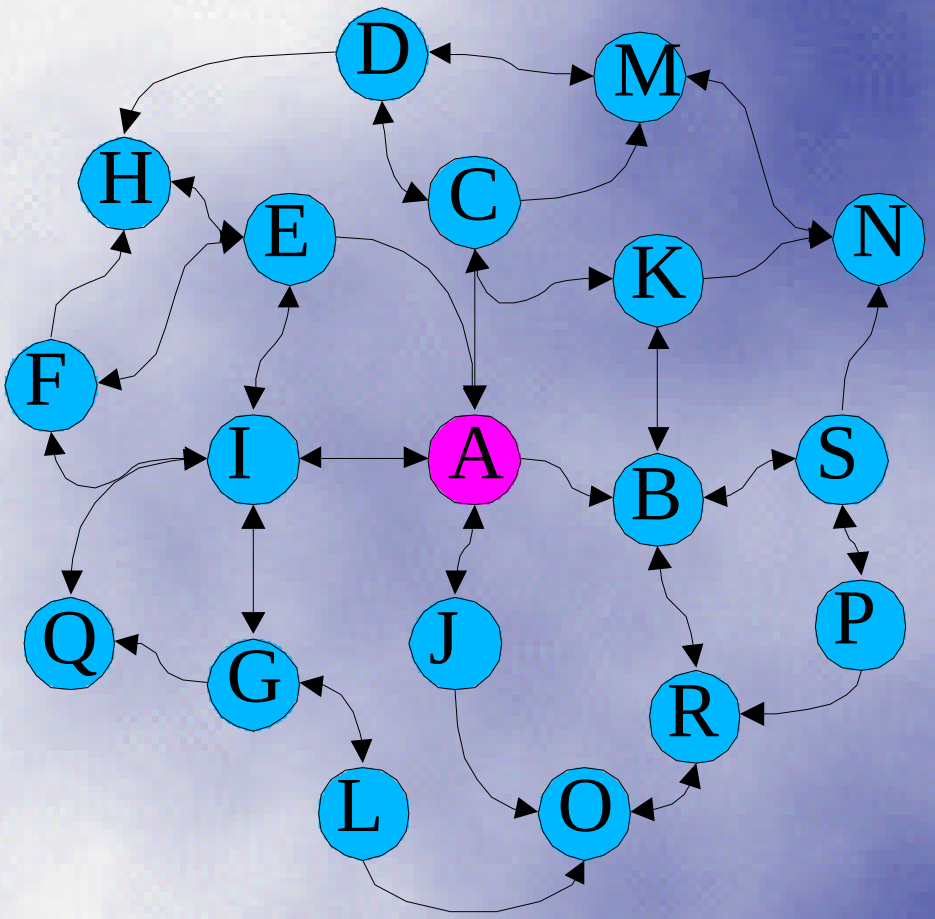
[82 62 A8 00 F0 37 55 C8 23 54 71 D2 C2 51 EA
Dieser Schlüssel gehört Eric Arthur Blair.]

- Problem: Gehört der Schlüssel, mit dem das Zertifikat unterzeichnet ist, wirklich der ausstellenden Person?

Modell 1: Web of trust (Netz des Vertrauens)

- Das normale PGP-Modell.
- Jeder zertifiziert 1 Zertifikate bilden ein Netz
- Ursprung ist man selbst.

Web of trust: Netzstruktur



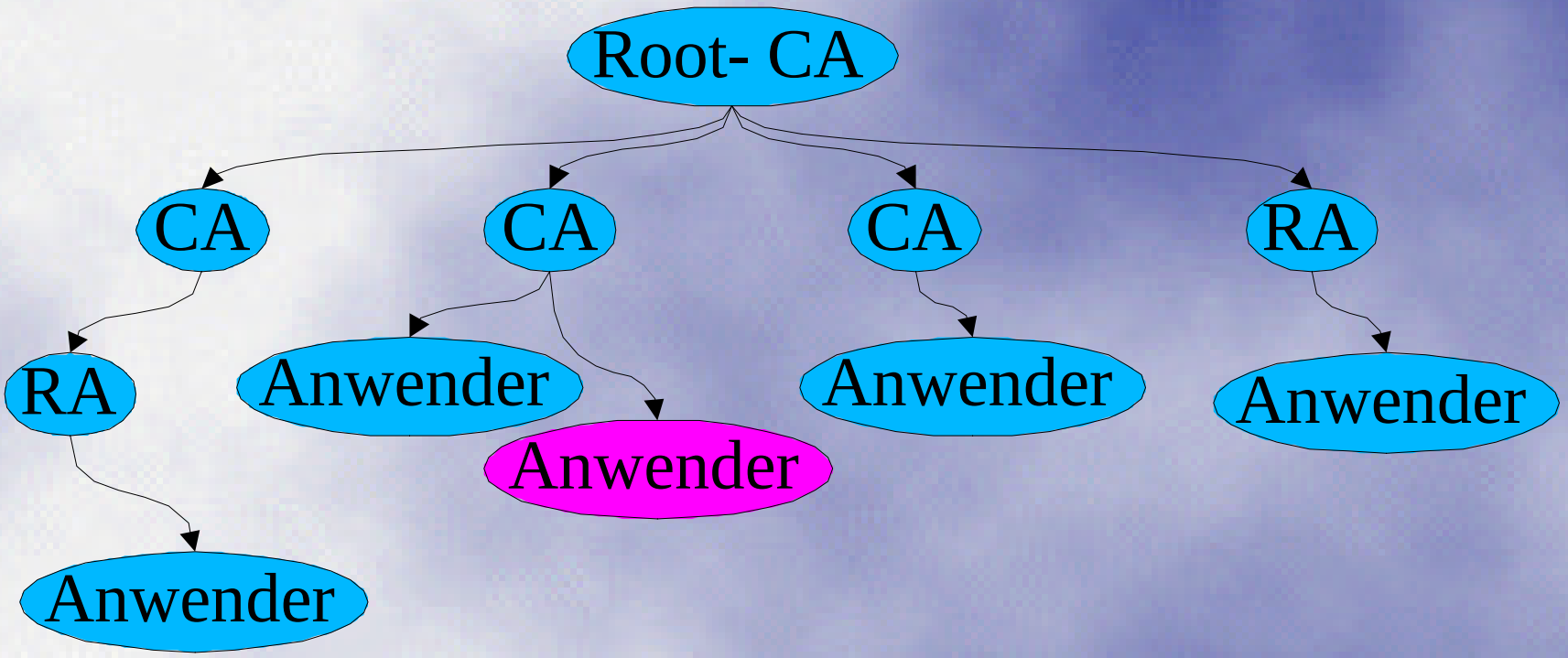
Web of trust: Vor-/Nachteile

- Vorteile:
  - Von keiner einzelnen Organisation abhängig.
  - Benutzer kann entscheiden, wem er vertraut.
- Nachteile:
  - Eventuell kein Zertifikatspfad zum Kommunikationspartner vorhanden.
  - Benutzer muß selbst Arbeit investieren. (Schlüssel zertifizieren, Schlüsseln Vertrauen zuweisen)
  - Vertrauenswürdigkeit unbekannter Personen eigentlich nicht abschätzbar.

Modell 2: Zertifizierungsinstanz (Certification Authority, CA)

- Normales Modell für X.509 (SSL, S/MIME, SigG).
- Der Ursprung ist hier eine Root-CA, die der Anwender - oder die Software (vgl. in Browser eingebaute CAs) - für vertrauenswürdig erklären muß

CAs: Baumstruktur



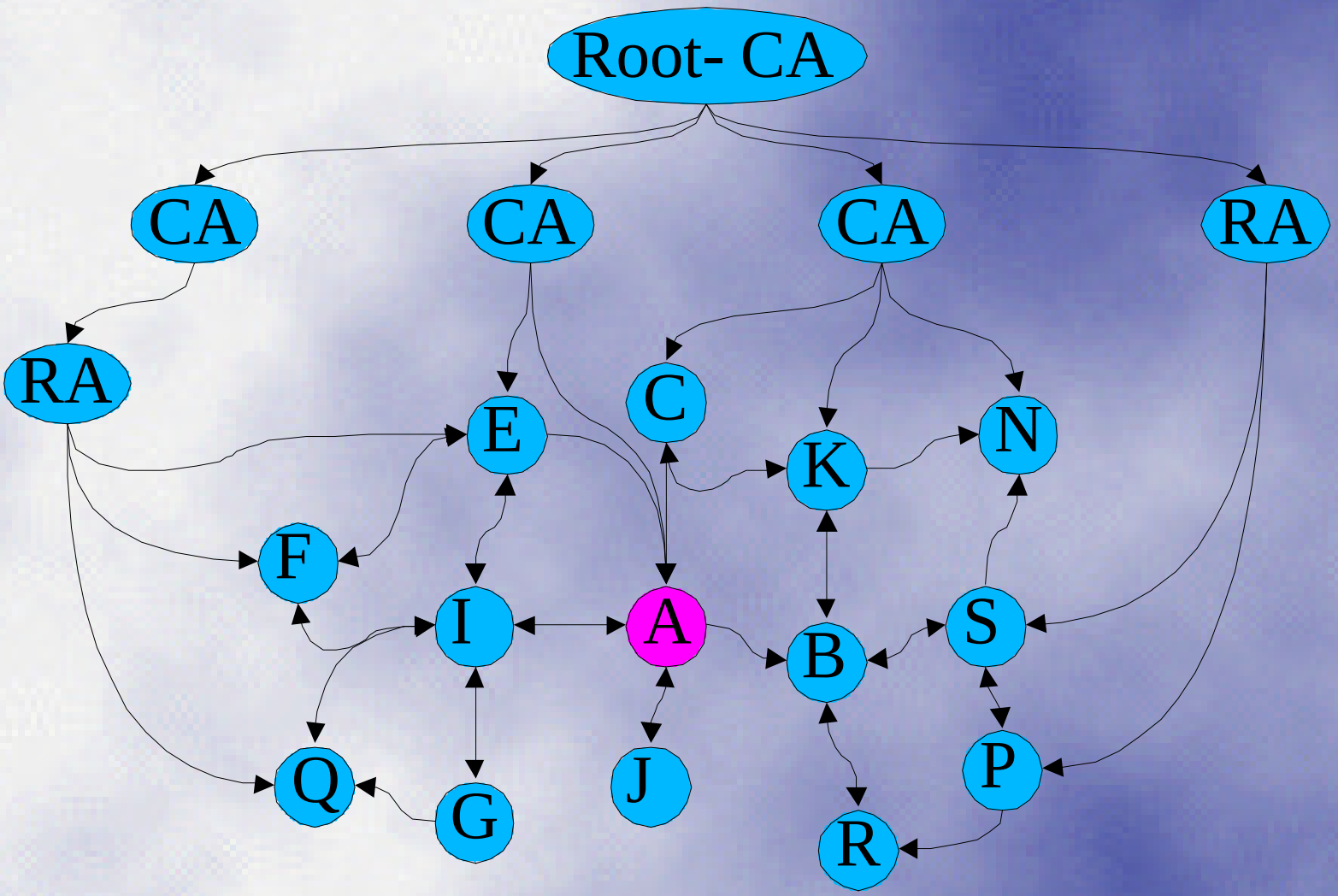
CAs: Vor-/ Nachteile

- Vorteile:
  - Weniger Arbeit für den Anwender.
  - Zertifikatswege leichter handhabbar.
  - Bekannte Zertifizierungsrichtlinien.
- Nachteile:
  - Starre Struktur.
  - Von zentralen Instanzen abhängig.
  - Fest im Browser eingebaut == vertrauenswürdig

PGP meets CAs

- Um auch unter PGP die Vorteile von CAs nutzen zu können wurden CAs für PGP geschaffen.
- z.B.:
  - c't-CA
  - DFN-CA
  - KNF-CA (ehem. IN-CA)

Parallelbetrieb von Web of Trust und CA



Vor-/Nachteile der zusätzlichen CA

- Vorteile:
  - Definierte Zertifizierungsrichtlinen.
  - Verknüpfung auch von nicht miteinander bekannten Personen.
  - Nicht von zentralen Instanzen abhängig, da das Web of Trust weiterhin vorhanden ist.
- Nachteile:
  - Zertifikatsverwaltung ist für den Anwender trotzdem nicht so einfach wie bei X.509.

KNF-CA

- Ursprünglich in die Zertifizierungshierarchie des Individual Network e.V. eingebunden.
- Seit der Auflösung des IN weiterbetrieb als KNF-CA.

KNF-CA: Zertifizierungsrichtlinie (Policy)

- Identifikation:
  - Persönliches Treffen, Verifikation des Ausweises oder Passes
  - Bei gut bekannten Personen alternativ auch eine Verifikation per Telefon
- Schlüssel der KNF-CA:
  - Schlüssellänge mind. 1536bit (1.5kbit)
  - Getrennte Schlüssel für Signatur und Verschlüsselung
  - Begrenzte Gültigkeit (max. 2 Jahre, Signaturen max. 1.5 Jahre)

KNF-CA: Zertifizierungsrichtlinie (2)

- Sicherheitsanforderungen:
  - Schlüssel auf einem Wechseldatenträger (Floppy, Chipkarten, ...), der nur bei Verwendung in Kontakt mit dem CA-Rechner ist.
  - CA-Rechner unvernetzt. Einzige Möglichkeit zum Datenaustausch ist die Floppy.
  - Regelmäßiges Backup und Überprüfung der Integrität der Software (tripwire).
  - Protokollierung der Vorgänge in einem Buch.

KNF-CA: PGP2

- Für den Betrieb einer CA fehlen in PGP2 wichtige Funktionen:
  - Gültigkeitszeiträume von Schlüsseln.
  - Widerruf von Schlüsselzertifikaten.
  - Separate Schlüssel für Signatur und Verschlüsselung.
- Erweiterung von PGP2 um diese Funktionen 1 PGP 2.6.3in

KNF-CA: GnuPG

- GnuPG unterstützt alle für die KNF-CA nötige Funktionalität.
- Wegen der Mindestlänge des Schlüssels wird ein ElGamal-Schlüssel verwendet.
- Sollte Aufgrund der Kopatibilität mit OpenPGP auch mit PGP5/6/7 funktionieren.

KNF-CA: X.509

- Bisher im Testbetrieb.
- Testschlüssel für wwws.franken.de, pop-n.franken.de, shell.franken.de.
- Ungeklärte Fragen:
  - Unterstützung von Schlüsseln länger als 1024bit?
  - Widerruf von Schlüsseln?
  - Schlüsselerzeugung beim Anwender?

Weiterführende Informationen

- KNF-CA: http://www.franken.de/crypt/inca.html
- c't-CA: http://www.heise.de/ct/pgpCA/
- DFN-CA: http://www.cert.dfn.de/dfnpca/
- GnuPG: http://www.gnupg.org
- PGP2: ftp://ftp.iks-jena.de/pub/mitarb/lutz/crypt/software/pgp/pgp263in/
- Crypto-Mirror: ftp://www.franken.de/pub/crypt/mirror/

Schlüssel der KNF-CA

- PGP2: 2048/3E826309 "CA des Kommunikationsnetz Franken e.V. <ca@franken.de> (SIGN EXPIRE:2001-12-31)" FP = AC 81 26 98 D1 98 BD 1F C0 FC A6 4C A4 12 A6 E5
- PGP2: 2048/B3E0EA79 "CA des Kommunikationsnetz Franken e.V. <ca@franken.de> (ENCR EXPIRE:2001-06-30)" FP = BB 62 37 46 92 19 8B EB A1 F6 EB 83 8F 70 50 70
- GnuPG: 2048G/1041DD34 "CA des Kommunikationsnetz Franken e.V. (CERTIFICATION KEY 2001) <ca@franken.de>" FP = E9B7 CCD7 5D60 D183 F654 92CF B7DB 966D 1041 DD34
- GnuPG: 2048G/B9C058A4 "CA des Kommunikationsnetz Franken e.V. (COMMUNICATION KEY 2001) <ca@franken.de>" FP = 13AC 05CF 3D31 2F98 C309 333E 9A2B 7C3F B9C0 58A4

Mahlzeit