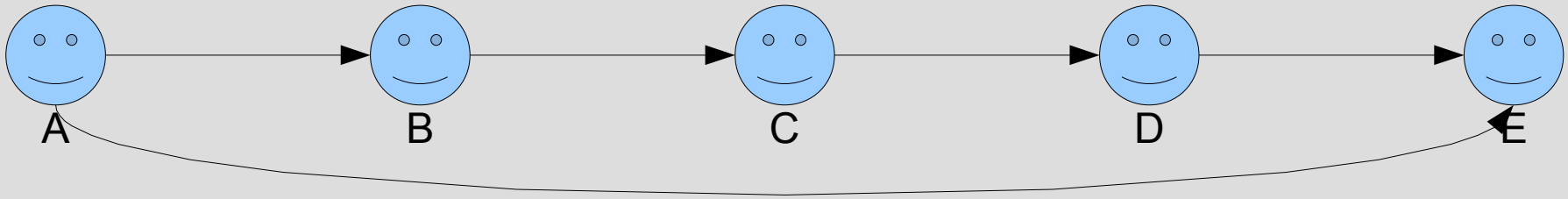
„Die Zertifizierungsstelle der Community“

Probleme der virtuellen Welt des Internets

- Privatsphäre durch Verschlüsselung
  - Warum verwenden die meisten Leute noch immer das elektronische Gegenstück der Postkarte?
- Sicherheit durch Authentifizierung
  - Wie kann ich sicher sein, wer auf der “anderen Seite” der Leitung ist?
- Vertrauen in das Internet
- Kostengünstige Lösung für jedermann

Der Evergreen : PGP web of trust

- A vertraut B, B vertraut C, C vertraut D, D vertraut E, also vertraut A auch E und kann ihm verschlüsselte Nachrichten schicken



- Vorteil : keine Zentrale Stelle, jeder kann mitmachen

Nachteil bei PGP

- Was, wenn D ein Bösewicht ist?
  - Wie kann ich sicher sein, dass E wirklich E ist?
    - Beispiel: Chinesischer Dissident schreibt an Obama
    - In Wirklichkeit liest der Geheimdienst und verhaftet ihn
  - Wie kann ich sicher sein, dass D meine Nachricht an E nicht verfälscht?
    - Beispiel: Exil-Kubaner schreibt an JFK:

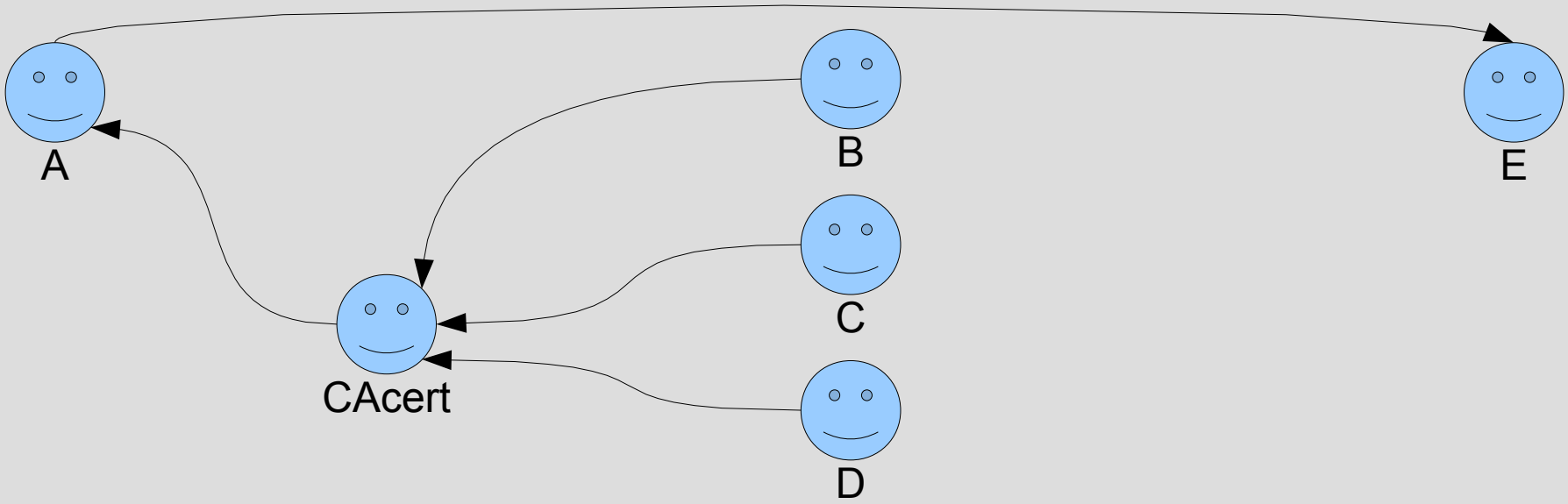
      „in der Schweinebucht NICHT landen“
- Jeder bestätigt die Schlüssel wie er es mag

Der CAcert Ansatz

- Nicht nur die E-Mail Adresse sondern auch die Identität wird überprüft
  - „Vertrauenspunkte“ werden vergeben
  - Postident-ähnliches Verfahren
  - Aber Mehraugenprinzip: es müssen mindestens 2 Personen Punkte vergeben
  - Punkte System: wer mehr Erfahrung hat, darf auch mehr Vertrauenspunkte vergeben
- Festgelegtes, verpflichtendes Verfahren

Der CAcert Ansatz in der Praxis

- B, C und D („Assurer“) haben E gesehen, seine Identität festgestellt („Assurance“) und an CAcert berichtet
- A vertraut dem CAcert System und kann sich sicher sein, dass E die richtige Person ist



CAcert Zertifikate : Anwendungsfelder

- Verschlüsselung von E-Mail & Dokumenten
  - Sowohl PGP als auch S/MIME (X509) Format
- Digitale Signatur von Dokumenten, E-Mails …
  - Echtheit und Ursprung von Rechnungen
  - Echtheit & Datum von Erfindungen
  - Integrität von Testamenten
- SSL-Zertifikate für Webseiten
- Auto-Login per Browser-Zertifikat
- SSL-basierte VPNs
- SSL/TLS-abgesicherte Übertragungen

Vor- und Nachteile

- Zertifikate sind kostenlos
- Einmalige Identitätsfeststellung – gilt lebenslang
- Unbegrenzte Anzahl an Zertifikaten

- Zentrale Anlaufstelle, der man vertrauen muss
- Root-Zertifikate nicht standardmäßig installiert

Assurance

- Konto bei CAcert anlegen
- Ausreichend Assurer besuchen, je nach Punktebedarf
  - Mind. 1 amtlichen Ausweis mit Foto, besser 2
  - Formular (korrekt) ausfüllen
- Assurer bestätigt Identität an CAcert und vergibt Vertrauenspunkte
- Features werden entsprechend bei CAcert freigeschaltet

Punktesystem

- Jeder Assurer vergibt Punkte je nach Erfahrung
  - maximal 10 bis 35, kann auch weniger

- Name nicht im Zertifikat enthalten.
- Man kann Client- und Server-Zertifikate mit 6 Monaten Gültigkeit erhalten.

- Maximal von anderen Assurern erhältliche Punktzahl.
- Code-Signing kann beantragt werden.
- Man kann Assurer werden.

- Name kann im Zertifikat enthalten sein.
- Server-Zertifikat ist 2 Jahre gültig.
- PGP/GPG Key kann von CAcert signiert werden.

- Maximale Punktezahl, die durch das Assuren erreicht werden kann
- Als Assurer kann man die maximale Zahl von 35 Punkten vergeben.

Die CAcert AGB:
CAcert Community Agreement (CCA)

- Rechte ...
  - Begrenzung von Schadensersatzforderungen gegen Assurer
  - CAcert und Ausstellung von Zertifikaten bleiben frei
  - Datenschutz
- … und Pflichten
  - CAcert Regeln anerkennen
  - Streitigkeiten nur über CAcert, nicht gerichtlich
  - Angaben müssen wahrheitsgemäß sein
  - Keinen Einsatz in „mission critical“ Systemen

Organisation Assurance: für Betriebe

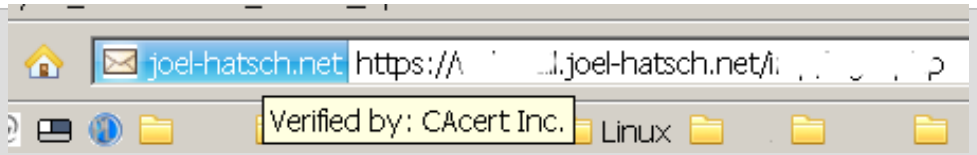
- Firma als solche wird assured
  - Anschließend kann deren Sysadmin selbst die Mitarbeiter assuren
  - Die Mitarbeiter können sich Zertifikate erstellen
- Firma kommt kostengünstig zu sicheren Kommunikation und kann ihre Dokumente digital signieren (Archivierung, Rechnungswesen ...)
- Mehr Infos : direkt bei CAcert anfragen

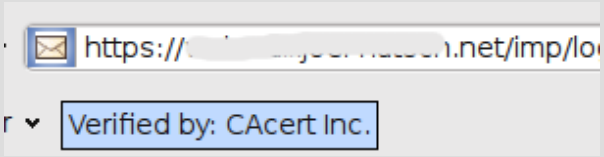
Wermutstropfen : Browser-Integration

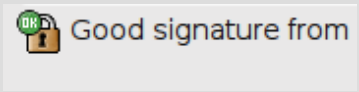
- CAcert Root-Zertifikat nicht standardmäßig bei den Browsern dabei
  - daher: von CAcert ausgestellte Zertifikate nicht als gültig erkannt
- Audit läuft. Wenn erfolgreich: Aufnahme bei der Mozilla Foundation
- Bis dahin: Zertifikat per Hand auf den Clients installieren
  - Bei den meisten Linux Distributionen als Paket

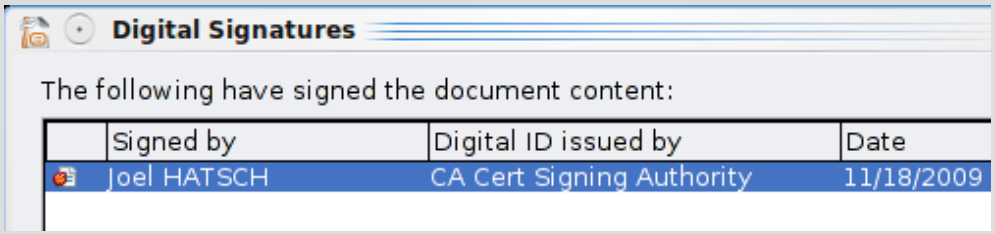
Zusammenspiel mit anderen OSS-Tools

- Browser
  - Firefox, Epiphany, Konqueror
- Mailprogramme
  - Thunderbird, Evolution, Kmail ...
- OpenOffice.org : Datei digital Signieren
- OpenVPN
- Fetchmail / Postfix / ...



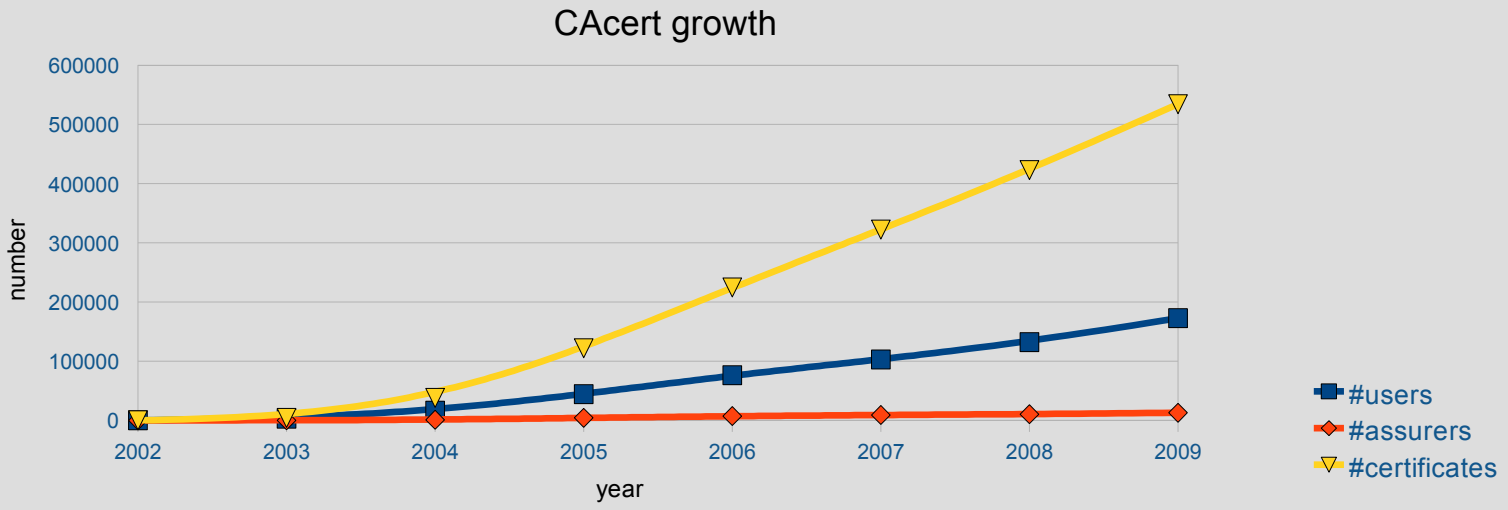






CAcert lebt nur durch die Community

- ~157.000 User, ~3000 Assurer
- >200.000 E-Mails
- >115.000 Domains
- > 517.000 certs in use
- Deutschland #1 bei CAcert



Mitmachen

- Mitglied werden – sich assuren lassen
- CAcert benutzen
  - PGP Schlüssel von CAcert signieren lassen
  - SSL Zertifikat von CAcert bestätigen lassen
- Assurer werden
  - 100 Punkte & Assurer Test ablegen
- An Treffen teilnehmen
- Technisch mitwirken (Code-Entwicklung, Doku ...)

Die „Konkurrenz“

- Verisign (& Thawte)
  - Ganz große **kommerzielle** Anbieter
- Thawte Free Web of Trust → R.I.P.
- PGP
  - Nur RSA Verschlüsselung, kein S/Mime, kein SSL
- StartSSL
  - Freie Zertifikate, SSL nur 1 Jahr
  - Volle Features (code signing, wildcard domains) nur entgeltlich

Hiiiiilfe ! Wo gibt's Support ?

"Offizielle" Anfragen

- support@cacert.org

"Inoffizielle" und triviale Sachen

- cacert-support@lists.cacert.org
- cacert-de@lists.cacert.org
- irc://irc.cacert.org/cacert.ger
- http://wiki.cacert.org/GettingSupport

Assurance beim OpenSource Treffen

- Es sollten ausreichend Assurer im Raum sein
- 100 Punkte problemlos erreichbar
- Formulare vorhanden
- Ausweis & Führerschein wird wohl jeder dabei haben

Let's assure !

BACKUP

How to join the community

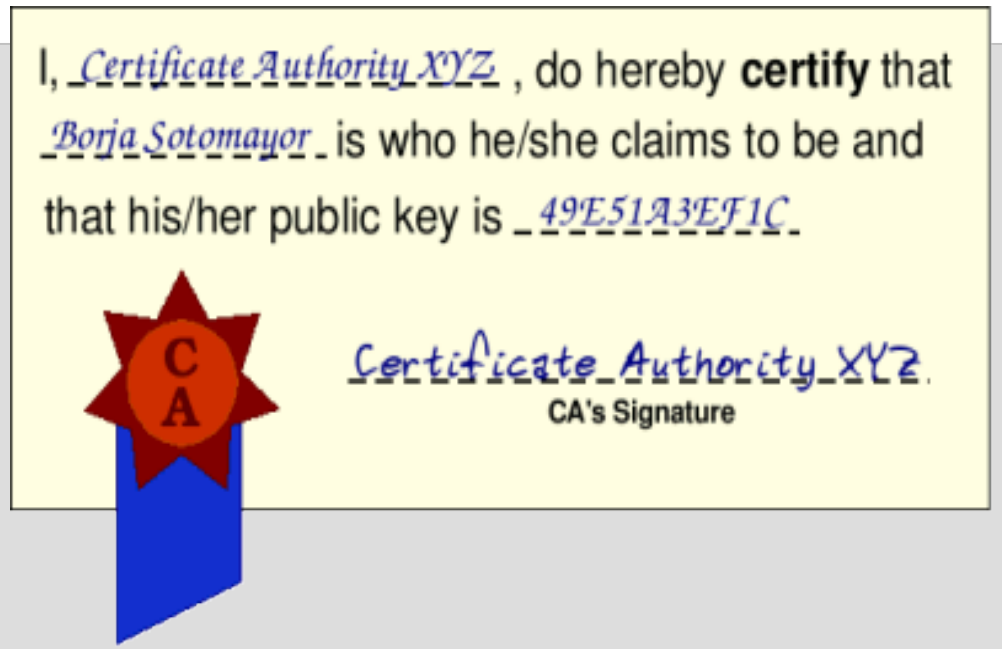
HowTo register

- read, agree CCA
- create
  - a CAcert account

    primary email address
  - password/phrase
  - five Q/A's
- remember them!

What is a CA?

- Certificate Authority



- The CA Root Key is added into “your” CA-list
  - On which authority?
- Signs your X.509 public certificate
  - When signed you might be trusted?

Bestandteile eines digitalen Zertifikats

Herausgegeben für	
Allgemeiner Name (CN)	Jens Paul
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	02:A3:BA
Herausgegeben von	
Allgemeiner Name (CN)	CA Cert Signing Authority
Organisation (O)	Root CA
Organisationseinheit (OU)	http://www.cacert.org
Validität	
Herausgegeben am	05.09.2006
Läuft ab am	05.09.2007
Fingerabdrücke	
SHA1-Fingerprint	CA:BB:B8:8D:F1:B1:9C:6E:B5:BC:E2:0C:B6:64:BF:89:AB:38:7C:59
MD5-Fingerprint	55:55:63:67:F2:27:73:5C:FB:E9:C4:17:B4:39:94:D4

- Informationen über den Besitzer
- Informationen über die ausstellende Institution
- Fingerabdrücke zur Validierung des Zertifikates und des Besitzers
- Ausstellungs- und Ablaufdatum des Zertifikats

Öffentlicher Schlüssel

```
30 82 01 0a 02 82 01 01 00 b2 d8 fb 99 f5 07 a9
6e ee 2d 8a 97 c0 de 60 40 bb 64 a7 ec 04 b6 01
be 3c 5c 8e 41 8c d1 6f c6 bb 72 81 b7 15 52 dc
a2 fe 96 64 04 79 6c 88 01 94 21 74 63 55 cc c4
d8 07 46 60 45 93 65 d1 ce a6 b2 39 8a 9b b8 7d
49 7d 81 54 bb 20 07 95 b9 a1 86 37 d1 31 28 2b
0b 7a c1 c0 07 3b 96 6b 48 ab 25 0d 74 77 33 03
22 ae 6f fd 09 6b 6a 68 dd 4f 2b 5c 9d 7a 7f a9
17 50 fe 4c 3b 6f a5 fd b4 26 d8 16 b8 32 b3 ad
89 7b 27 14 d0 01 98 48 57 41 0d 9d fc 91 50 1c
83 ce 5c 95 ff 53 ff 13 40 bd 2c 6a e9 41 56 6a
c9 46 b2 51 87 94 55 39 1b 62 48 cb bb 10 a2 a8
0a 09 20 67 7c 7d 73 a6 79 72 6c 58 51 5c 5f 54
09 63 df a6 7e f3 0c a0 e0 07 ba 48 bf 3b 2f 4b
84 1d 7b fb 67 35 0d b0 51 77 fa 26 e6 5a 6f d8
f8 c6 ca dc 74 70 92 e1 66 52 88 8e c5 30 06 09
bb 33 d1 2c 4f 45 f1 61 27 02 03 01 00 01 11
```

Privater Schlüssel

...

- Ein öffentlicher Schlüssel, welcher es dem Kommunikationspartner ermöglicht, Hash-Werte (Fingerabdrücke) zu entschlüsseln und Nachrichten an den Besitzer zu verschlüsseln.
- Ein privater Schlüssel, welcher es dem Besitzer erlaubt, an ihn adressierte Nachrichten zu entschlüsseln und Hash-Werte zu verschlüsseln.

Zertifikatstypen

Typ		*Einsatzmöglichkeiten*	
Allgemein	Protokoll	Beschreibung	Anmerkungen
Server	TLS	Webserver-Verschlüsselung	Ermöglicht die Verschlüsselung
	Embedded	Authentifizierung auf embedded servern	Mailserver, Instant-Messaging
Client	S/MIME	E-Mail-Verschlüsselung	“Digitale Signaturen” innerhalb von S/MIME sind keine händischen Unterschriften, vielmehr gestatten Sie die Verschlüsselung der Nachrichteninhalte.
	TLS	Authentifizierung am Client	Verbesserung der Client Sicherheit
	TLS	Authentifizierung an Web basierten Signaturanwendungen	Das Zertifikat dient lediglich der Authentifizierung. Details siehe CPS.
	Advanced Signing	Signierung von Dokumenten	Bitte beachten Sie hierzu die Detailregelungen der CPS sowie die geltenden Gesetze Ihre Landes.
Code		Signierung von Quellcodes	Die Signaturen dienen lediglich zur Identitätsfeststellung.
PGP	OpenPGP	Schlüsselsignierung	Die Signaturen dienen lediglich zur Identitätsfeststellung.