DANE – soumrak certifikačních autorit

Ondřej Surý, CZ.NIC

24.11.2012 – IT12, Praha

Stručný obsah

- Jak sčítáme procenta?
- Infrastruktura veřejných klíčů (PKI)
- Druhy certifikátů
- Trocha historie
- Protokol DANE
  - Struktura TLSA záznamu
  - Bezpečnost
  - Generování
  - Budoucnost
- Otázky

Infrastruktura veřejných klíčů (PKI)

Infrastruktura veřejných klíčů

- X.509 certifikáty
  - Zabezpečení komunikace
- Ověření validity certifikátů
  - Mluvím s tím, s kým chci mluvit?
  - Identifikace druhé strany

Certifikační autority

- „Důvěryhodné“ organizace
  - Vstupní body důvěry (Trust Anchor)
    - Nakonfigurovány výrobci OS, prohlížečů, i dalších aplikací...
- Musí existovat validní cesta mezi certifikátem a TA (PKIX validation path)
- CA potvrdí: „tento klíč patří www.nic.cz“

Proč model CA selhává?

- 2009: 3 zranitelnosti díky chybám CA
- 2010: důkazy o CA, které jdou na ruku vládám
- 2011,2012: další napadení CA

Proč model CA selhává?

- Všechny CA, kterým důvěřujete jsou si rovny
- Jakákoli CA může vydat certifikát pro libovolnou službu

China Internet Network Information Center EV Certificates Root

Root certificate authority

Expires: sobota, 31. srpna 2030 9:11:25 Středoevropský letní čas

This certificate is valid

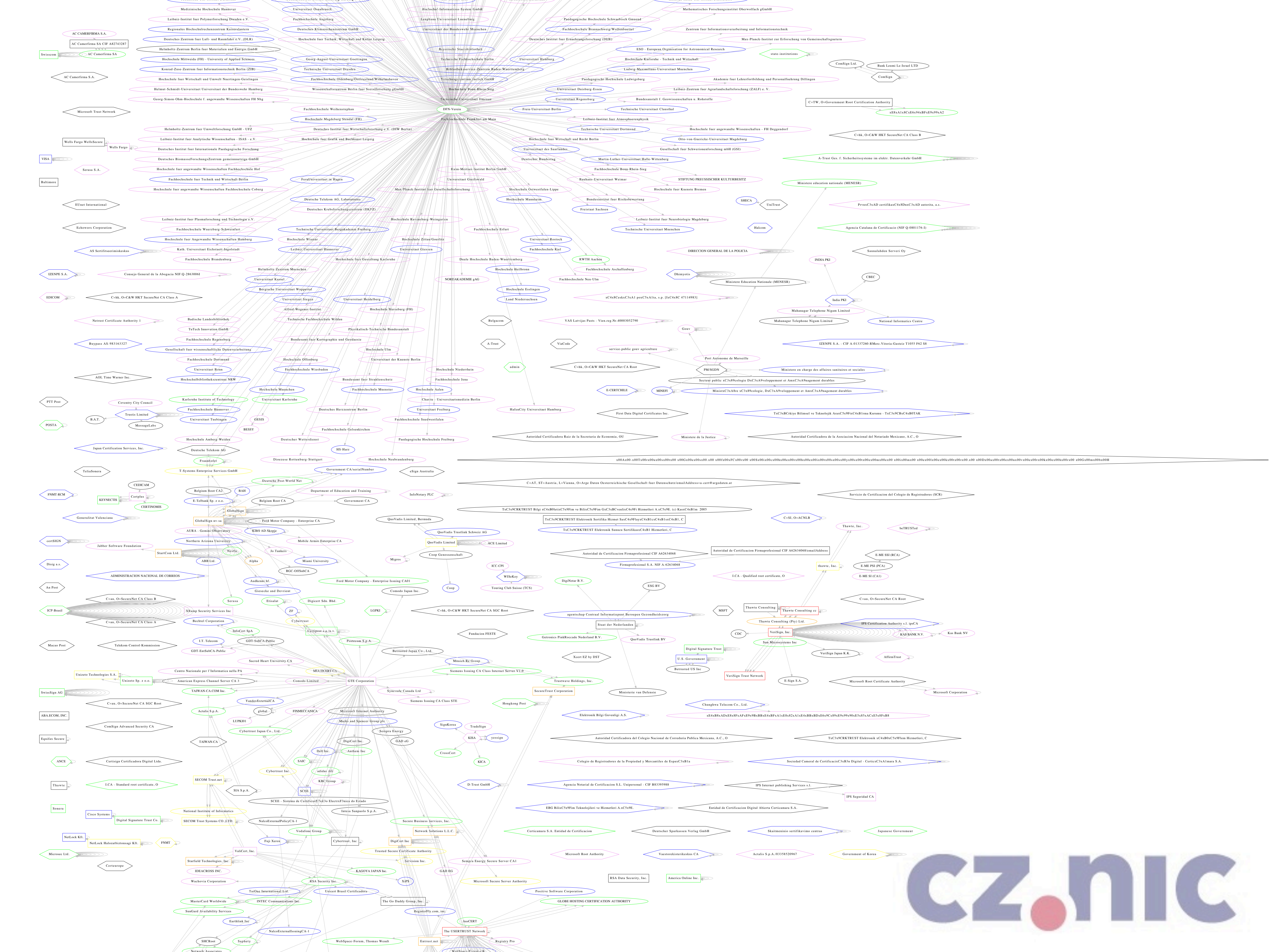
…třeba i Marťani

cz.nic

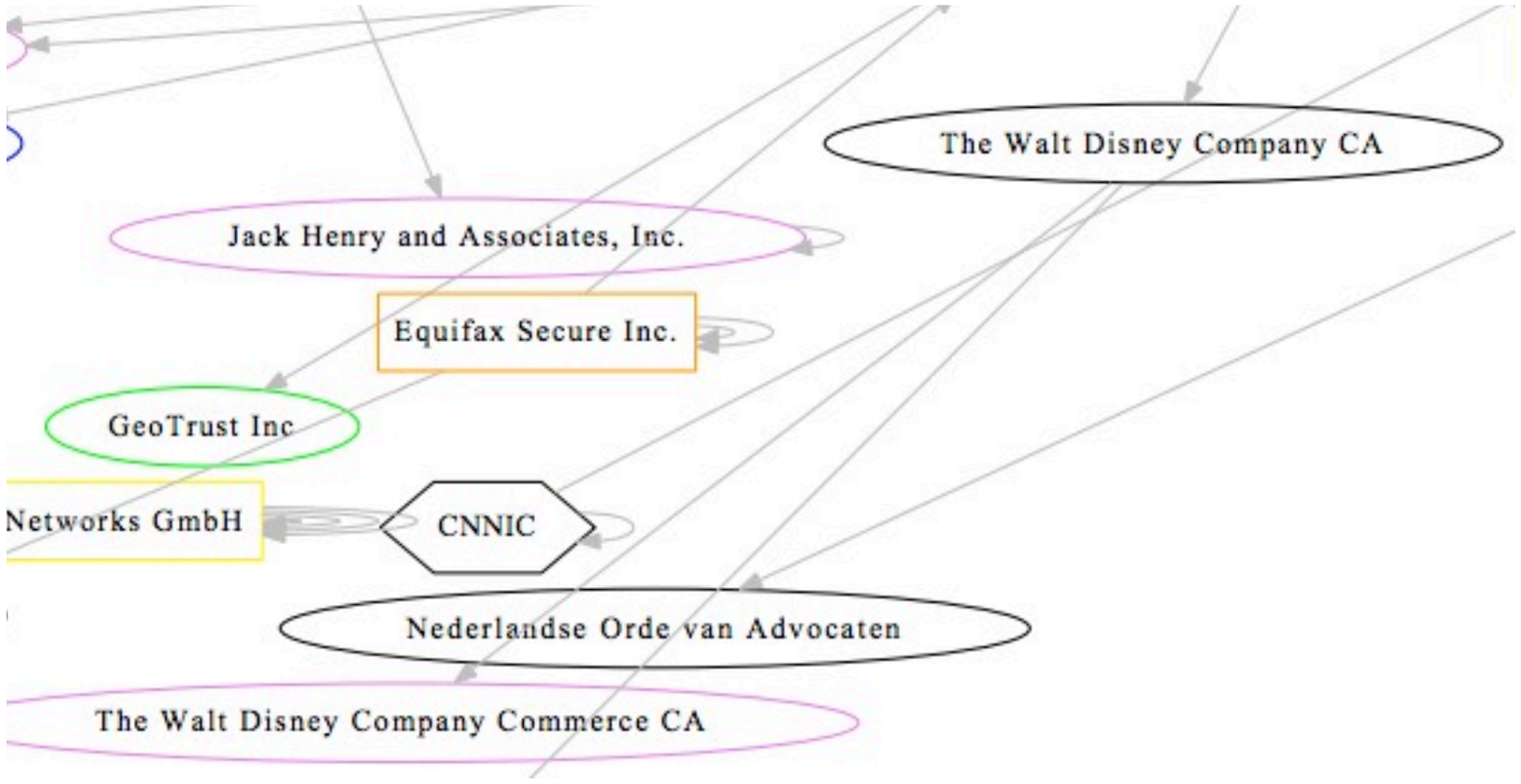
Intermediate CA

- CA může vystavit podřízený certifikát s BasicConstraints: CA: TRUE
- Intermediate CA je stejně důvěryhodná jako nadřízená CA

Zrcadlo, zrcadlo, řekni mi, kolik je certifikačních autorit?



Medizinische Hochschule Hannover
Universitaet Osnabrueck
Hochschul-Informations-System GmbH
Paedagogische Hochschule Schwaebisch Gmuend
Mathematisches Forschungsinstitut Oberwolfach gGmbH
Leibniz-Institut fuer Polymerforschung Dresden e.V.
Fachhochschule Augsburg
Leuphana Universitaet Lueneburg
AC CAMERFIRMA S.A.
AC Camerfirma SA CIF A82743287
Regionales Hochschulrechenzentrum Kaiserslautern
Deutsches Klimarechenzentrum GmbH
Universitaet der Bundeswehr Muenchen
Fachhochschule Braunschweig/Wolfenbuettel
Zentrum fuer Informationsverarbeitung und Informationstechnik
Deutsches Zentrum fuer Luft- und Raumfahrt e.V. (DLR)
Hochschule fuer Technik, Wirtschaft und Kultur Leipzig
Deutsches Institut fuer Ernaehrungsforschung (DIfE)
Max-Planck-Institut zur Erforschung von Gemeinschaftsguetern
Swisscom
AC Camerfirma SA
Helmholtz-Zentrum Berlin fuer Materialien und Energie GmbH
Bayerische Staatsbibliothek
ESO - European Organisation for Astronomical Research
state-institutions
Hochschule Mittweida (FH) - University of Applied Sciences
Georg-August-Universitaet Goettingen
Technische Fachhochschule Berlin
Universitaet Hamburg
Hochschule Karlsruhe - Technik und Wirtschaft
ComSign Ltd.
Bank Leumi Le-Israel LTD
Konrad-Zuse-Zentrum fuer Informationstechnik Berlin (ZIB)
Technische Universitaet Dresden
Bibliotheksservice-Zentrum Baden-Wuerttemberg
Ludwig-Maximilians-Universitaet Muenchen
ComSign
AC Camerfirma S.A.
Hochschule fuer Wirtschaft und Umwelt Nuertingen-Geislingen
Fachhochschule Oldenburg/Ostfriesland/Wilhelmshaven
Forschungszentrum Juelich GmbH
Paedagogische Hochschule Ludwigsburg
Akademie fuer Lehrerfortbildung und Personalfuehrung Dillingen
Helmut-Schmidt-Universitaet Universitaet der Bundeswehr Hamburg
Wissenschaftszentrum Berlin fuer Sozialforschung gGmbH
Hochschule Bonn-Rhein-Sieg
Universitaet Duisburg-Essen
Leibniz-Zentrum fuer Agrarlandschaftsforschung (ZALF) e. V.
Georg-Simon-Ohm-Hochschule f. angewandte Wissenschaften FH Nbg
Technische Universitaet Ilmenau
Universitaet Regensburg
Bundesanstalt f. Geowissenschaften u. Rohstoffe
C=TW, O=Government Root Certification Authority
Microsoft Trust Network
Fachhochschule Weihenstephan
DFN-Verein
Freie Universitaet Berlin
Technische Universitaet Clausthal
Hochschule Magdeburg-Stendal (FH)
Fachhochschule Frankfurt am Main
Leibniz-Institut fuer Atmosphaerenphysik
Helmholtz-Zentrum fuer Umweltforschung GmbH - UFZ
Deutsches Institut fuer Wirtschaftsforschung e.V. (DIW Berlin)
Technische Universitaet Dortmund
Hochschule fuer angewandte Wissenschaften - FH Deggendorf
C=hk, O=C&W HKT SecureNet CA Class B
Wells Fargo WellsSecure
Leibniz-Institut fuer Analytische Wissenschaften - ISAS - e.V.
Hochschule fuer Grafik und Buchkunst Leipzig
Hochschule fuer Wirtschaft und Recht Berlin
Otto-von-Guericke-Universitaet Magdeburg
Wells Fargo
Deutsches Institut fuer Internationale Paedagogische Forschung
Universitaet des Saarlandes
Gesellschaft fuer Schwerionenforschung mbH (GSI)
VISA
Deutsches BiomasseForschungsZentrum gemeinnuetzige GmbH
Deutscher Bundestag
Martin-Luther-Universitaet Halle-Wittenberg
A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Serasa S.A.
Hochschule fuer angewandte Wissenschaften Fachhochschule Hof
Hahn-Meitner-Institut Berlin GmbH
Fachhochschule Bonn-Rhein-Sieg
Baltimore
Fachhochschule fuer Technik und Wirtschaft Berlin
FernUniversitaet in Hagen
Universitaet Greifswald
Bauhaus-Universitaet Weimar
STIFTUNG PREUSSISCHER KULTURBESITZ
Ministere education nationale (MENESR)
Hochschule fuer angewandte Wissenschaften Fachhochschule Coburg
Max-Planck-Institut fuer Gesellschaftsforschung
Hochschule Ostwestfalen-Lippe
Hochschule fuer Kuenste Bremen
Deutsche Telekom AG, Laboratories
Hochschule Mannheim
Bundesinstitut fuer Risikobewertung
SHECA
UniTrust
EUnet International
Deutsches Krebsforschungszentrum (DKFZ)
Freistaat Sachsen
Leibniz-Institut fuer Plasmaforschung und Technologie e.V.
Hochschule Ravensburg-Weingarten
Leibniz-Institut fuer Neurobiologie Magdeburg
Echoworx Corporation
Fachhochschule Wuerzburg-Schweinfurt
Technische Universitaet Bergakademie Freiberg
Fachhochschule Erfurt
Technische Universitaet Muenchen
Halcom
Agencia Catalana de Certificacio (NIF Q-0801176-I)
Hochschule fuer Angewandte Wissenschaften Hamburg
Hochschule Wismar
Hochschule Zittau/Goerlitz
Universitaet Rostock
AS Sertifitseerimiskeskus
Kath. Universitaet Eichstaett-Ingolstadt
Leibniz Universitaet Hannover
Universitaet Giessen
Fachhochschule Kiel
DIRECCION GENERAL DE LA POLICIA
Sonera
Saunalahden Serveri Oy
Fachhochschule Brandenburg
Hochschule fuer Gestaltung Karlsruhe
Duale Hochschule Baden-Wuerttemberg
RWTH Aachen
INDIA PKI
Helmholtz Zentrum Muenchen
Hochschule Heilbronn
Fachhochschule Aschaffenburg
IZENPE S.A.
Consejo General de la Abogacia NIF:Q-2863006I
Universitaet Kassel
NORDAKADEMIE gAG
Dhimyotis
Ministere Education Nationale (MENESR)
CBEC
Fachhochschule Neu-Ulm
Bergische Universitaet Wuppertal
Hochschule Esslingen
EDICOM
C=hk, O=C&W HKT SecureNet CA Class A
Universitaet Siegen
Universitaet Heidelberg
Land Niedersachsen
India PKI
Alfred-Wegener-Institut
Hochschule Merseburg (FH)
Mahanagar Telephone Nigam Limited
Netrust Certificate Authority 1
Badische Landesbibliothek
Technische Fachhochschule Wildau
Belgacom
VAS Latvijas Pasts - Vien.reg.Nr.40003052790
National Informatics Centre
TuTech Innovation GmbH
Physikalisch-Technische Bundesanstalt
Gouv
Fachhochschule Regensburg
Bundesamt fuer Kartographie und Geodaesie
Buypass AS-983163327
A-Trust
VisCode
IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Gesellschaft fuer wissenschaftliche Datenverarbeitung
service-public gouv agriculture
Fachhochschule Dortmund
Hochschule Offenburg
Hochschule Ulm
Universitaet der Kuenste Berlin
Port Autonome de Marseille
Universitaet Bonn
Fachhochschule Wiesbaden
Hochschule Niederrhein
admin
C=hk, O=C&W HKT SecureNet CA Root
PM/SGDN
Ministere en charge des affaires sanitaires et sociales
AOL Time Warner Inc.
Hochschulbibliothekszentrum NRW
Bundesamt fuer Strahlenschutz
Fachhochschule Jena
Hochschule Muenchen
Fachhochschule Muenster
Hochschule Aalen
E-CERTCHILE
MINEFI
PTT Post
Karlsruhe Institute of Technology
Universitaet Karlsruhe
Charite - Universitaetsmedizin Berlin
Coventry City Council
Fachhochschule Hannover
Deutsches Herzzentrum Berlin
Universitaet Freiburg
HafenCity Universitaet Hamburg
First Data Digital Certificates Inc.
Trustis Limited
B.A.T.
Universitaet Tuebingen
GESIS
Fachhochschule Suedwestfalen
MessageLabs
POSTA
BESSY
Fachhochschule Gelsenkirchen
Autoridad Certificadora Raiz de la Secretaria de Economia, OU
Ministere de la Justice
Autoridad Certificadora de la Asociacion Nacional del Notariado Mexicano, A.C., O
Hochschule Amberg-Weiden
Deutscher Wetterdienst
Paedagogische Hochschule Freiburg
Japan Certification Services, Inc.
Deutsche Telekom AG
HS Harz
Diozese Rottenburg-Stuttgart
Hochschule Neubrandenburg
Fraunhofer
T-Systems Enterprise Services GmbH
Government CA/serialNumber
eSign Australia
TeliaSonera
CEDICOM
Deutsche Post World Net
Servicio de Certificacion del Colegio de Registradores (SCR)
Belgium Root CA2
BAH
Department of Education and Training
FNMT-RCM
Certplus
InfoNotary PLC
KEYNECTIS
E-Telbank Sp. z o.o.
Belgium Root CA
Government CA
CERTINOMIS
GlobalSign
Generalitat Valenciana
GlobalSign nv-sa
Ford Motor Company - Enterprise CA
QuoVadis Limited, Bermuda
C=SI, O=ACNLB
Thawte, Inc.
beTRUSTed
AURA - Gemini Observatory
KIBS AD Skopje
QuoVadis Trustlink Schweiz AG
certSIGN
Northern Arizona University
Mobile Armor Enterprise CA
QuoVadis Limited
ACE Limited
Jabber Software Foundation
StartCom Ltd.
Nestle
Jo Tankers
Coop Genossenschaft
Autoridad de Certificacion Firmaprofesional CIF A62634068
Autoridad de Certificacion Firmaprofesional CIF A62634068/emailAddress
E-ME SSI (RCA)
ABB Ltd.
Alpha
Miami University
Migros
Firmaprofesional S.A. NIF A-62634068
thawte, Inc.
E-ME PSI (PCA)
Disig a.s.
BGC-OfiSubCA
ICC-CPI
I.CA - Qualified root certificate, O
E-ME SI (CA1)
ADMINISTRACION NACIONAL DE CORREOS
Ford Motor Company - Enterprise Issuing CA01
WISeKey
DigiNotar B.V.
ESG BV
An Post
Audkenni hf.
Comodo Japan Inc.
Touring Club Suisse (TCS)
Coop
Giesecke and Devrient
C=au, O=SecureNet CA Class B
Serasa
Etisalat
Digicert Sdn. Bhd
ICP-Brasil
XRamp Security Services Inc
ZF
LGPKI
C=hk, O=C&W HKT SecureNet CA SGC Root
agentschap Centraal Informatiepunt Beroepen Gezondheidszorg
MSFT
Thawte Consulting
Thawte Consulting cc
C=au, O=SecureNet CA Root
C=au, O=SecureNet CA Class A
Bechtel Corporation
Cybertrust
Thawte Consulting (Pty) Ltd.
IPS Certification Authority s.l. ipsCA
Certipost s.a./n.v.
Fundacion FESTE
Staat der Nederlanden
InfoCert SpA
CDC
VeriSign, Inc.
KAS BANK N.V.
Kas Bank NV
Macao Post
I.T. Telecom
GDT-SubCA-Public
Postecom S.p.A.
Getronics PinkRoccade Nederland B.V.
QuoVadis Trustlink BV
Sun Microsystems Inc
Telekom-Control-Kommission
GDT-EntSubCA-Public
Betrusted Japan Co., Ltd.
Digital Signature Trust
VeriSign Japan K.K.
Sacred Heart University CA
Munich Re Group
Xcert EZ by DST
U.S. Government
AffirmTrust
Unizeto Technologies S.A.
Centro Nazionale per l'Informatica nella PA
MULTICERT-CA
Siemens Issuing CA Class Internet Server V1.0
Betrusted US Inc
VeriSign Trust Network
Unizeto Sp. z o.o.
American Express Channel Server CA 3
Comodo Limited
GTE Corporation
Trustwave Holdings, Inc.
E-Sign S.A.
Microsoft Root Certificate Authority
SwissSign AG
Syncrede Canada Ltd
SecureTrust Corporation
Ministerie van Defensie
Microsoft Corporation
TAIWAN-CA.COM Inc.
Siemens Issuing CA Class STE
C=au, O=SecureNet CA SGC Root
YandexExternalCA
Hongkong Post
Chunghwa Telecom Co., Ltd.
Actalis S.p.A.
global
FINMECCANICA
Microsoft Internet Authority
Elektronik Bilgi Guvenligi A.S.
ABA.ECOM, INC
LUPKI01
Marks and Spencer Group plc
SignKorea
TradeSign
Cybertrust Japan Co., Ltd.
Sempra Energy
KISA
yessign
ComSign Advanced Security CA
GAD eG
DigiCert Inc.
Autoridad Certificadora del Colegio Nacional de Correduria Publica Mexicana, A.C., O
Equifax Secure
TAIWAN-CA
Dell Inc.
Anthem Inc
CrossCert
SAIC
KICA
ANCE
Certisign Certificadora Digital Ltda.
adidas AG
Colegio de Registradores de la Propiedad y Mercantiles de Espa=C3=B1a
Sociedad Cameral de Certificaci=C3=B3n Digital - Certic=C3=A1mara S.A.
KBC Group
Cybertrust Inc
D-Trust GmbH
Thawte
I.CA - Standard root certificate, O
SECOM Trust.net
SCEE
Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988
IPS Internet publishing Services s.l.
SIA S.p.A.
SCEE - Sistema de Certifica=C3=A7=C3=A3o Electr=C3=B3nica do Estado
IPS Seguridad CA
Sonera
Intesa Sanpaolo S.p.A.
Cisco Systems
National Institute of Informatics
Digital Signature Trust Co.
NalcoExternalPolicyCA-1
EBG Bili=C5=9Fim Teknolojileri ve Hizmetleri A.=C5=9E.
Entidad de Certificacion Digital Abierta Certicamara S.A.
SECOM Trust Systems CO.,LTD.
Secure Business Services, Inc.
Certicamara S.A. Entidad de Certificacion
Deutscher Sparkassen Verlag GmbH
Skaitmeninio sertifikavimo centras
Japanese Government
NetLock Kft.
Vodafone Group
Network Solutions L.L.C.
FNMT
NetLock Halozatbiztonsagi Kft.
Fuji Xerox
Cybertrust, Inc
DigiCert Inc
ValiCert, Inc.
Trusted Secure Certificate Authority
Microsec Ltd.
Microsoft Root Authority
Vaestorekisterikeskus CA
Actalis S.p.A./03358520967
Government of Korea
Starfield Technologies, Inc.
Servision Inc.
Sempra Energy Secure Server CA1
Certeurope
IDEACROSS INC.
KAGOYA JAPAN Inc.
GAD EG
Wachovia Corporation
RSA Security Inc.
XiPS
Microsoft Secure Server Authority
RSA Data Security, Inc.
America Online Inc.
TaiOne International Ltd.
Unicert Brasil Certificadora
Positive Software Corporation
MasterCard Worldwide
INTEC Communications Inc.
The Go Daddy Group, Inc.
GLOBE HOSTING CERTIFICATION AUTHORITY
SunGard Availability Services
RegisterFly.com, inc.
Earthlink Inc
AusCERT
NalcoExternalIssuingCA-1
The USERTRUST Network
SHCRoot
Saphety
WebSpace-Forum, Thomas Wendt
Entrust.net
Registry Pro
Network Associates
cz.nic



Use the force, Mickey...

Jaké certifikační autority používáte vy?

Těžko říct…

- Firefox: Společně s aktualizací prohlížeče (http://www.mozilla.org/projects/security/certs/policy/)
- Linux: balíček (Debian: ca-certificates)
- Mac OS X: Aktualizace operačního systému / (http://www.apple.com/certificateauthority/ca_program.html)
- Windows Vista, 7, 8: Automaticky kontroluje Microsoft Update pro neznámé certifikáty: http://support.microsoft.com/kb/931125

Druhy certifikátů

Druhy certifikátů

- Domain-validated
  - Stačí mít přístup k emailu
- Personal-validation
  - Složitější...třeba vám i zavolají na číslo z telefonního účtu, který... jim pošlete v PDF (ehm...)
- Organizational-validated

Malý kvíz…

https://www.qq.com

https://www.sury.org

www.yahoo.com/?s=https&r287=1351775988

https://blu154.mail.live.com/

https://www.ietf.org

https://en.wikipedia.org/wiki/Fail

https://www.muni.cz

https://www.linkedin.com/

https://www.facebook.com

https://en.wikipedia.org/wiki/Fail

https://www.vutbr.cz/

https://www.google.com

https://www.youtube.com

cz.nic

A ono je nakonec vlastně jedno…

Extended Validation

- Výrazné odlišení od DV, OV, ...
- CA/Browser Forum
- Důkladnější ověřování
  a důvěryhodnější (čti dražší) certifikáty

I to je nakonec vlastně jedno…

Další malý kvíz…

Ceskoslovenska obchodni banka, a.s. [CZ] https://maxibps.postovnisporitelna.cz

https://ibs.volksbank.cz/

Air Bank a.s. [CZ] https://ib.airbank.cz

Citigroup Inc. [US] https://production.citibank.cz/

Raiffeisen banka a.s. [CZ] https://klient4.rb.cz/

https://moje.zuno.cz/

https://klient4.rb.cz/ebts/version_02/cz/banka3.html

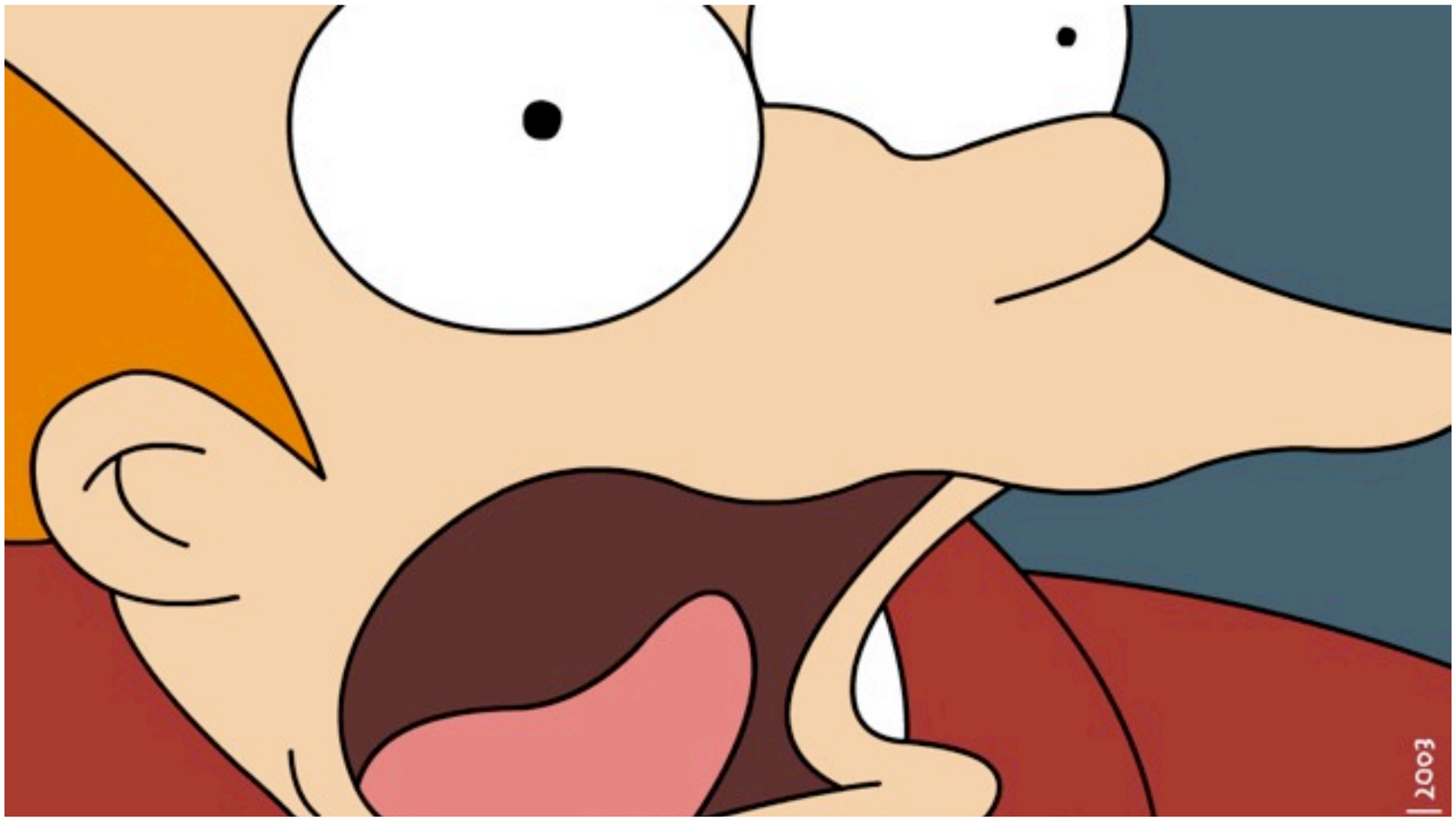
BRE Bank SA [PL] https://cz.mbank.eu

https://www.fio.cz/

Ceskoslovenska obchodni banka, a.s. [CZ] https://ib24.csob.cz

Ceska sporitelna, a.s. [CZ] https://www.servis24.cz/

https://cz.unicreditbanking.net/



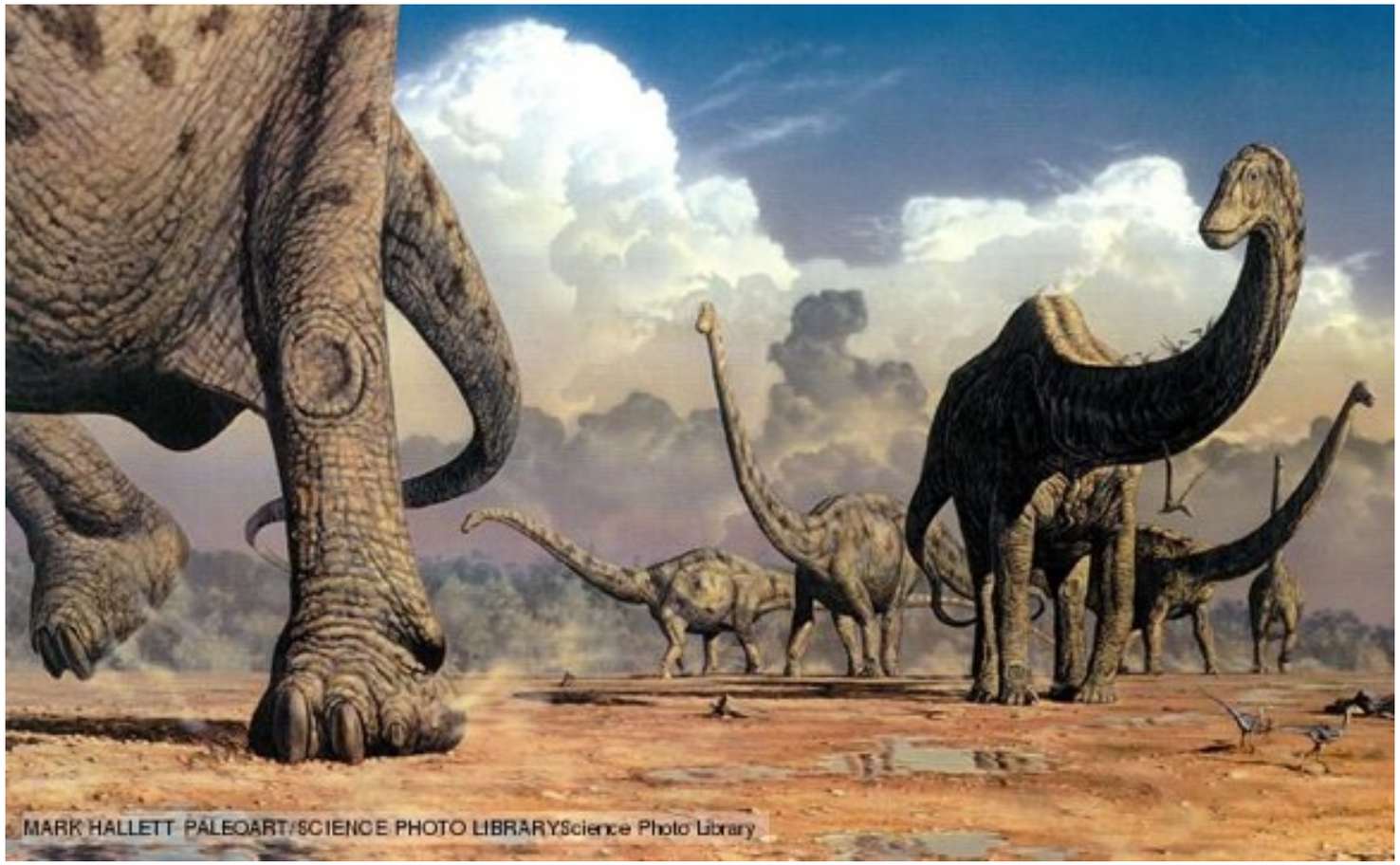
Jak z toho ven?

Jak z toho ven?

- Vrátit kontrolu zpátky tam, kam patří

Jednoduchá myšlenka

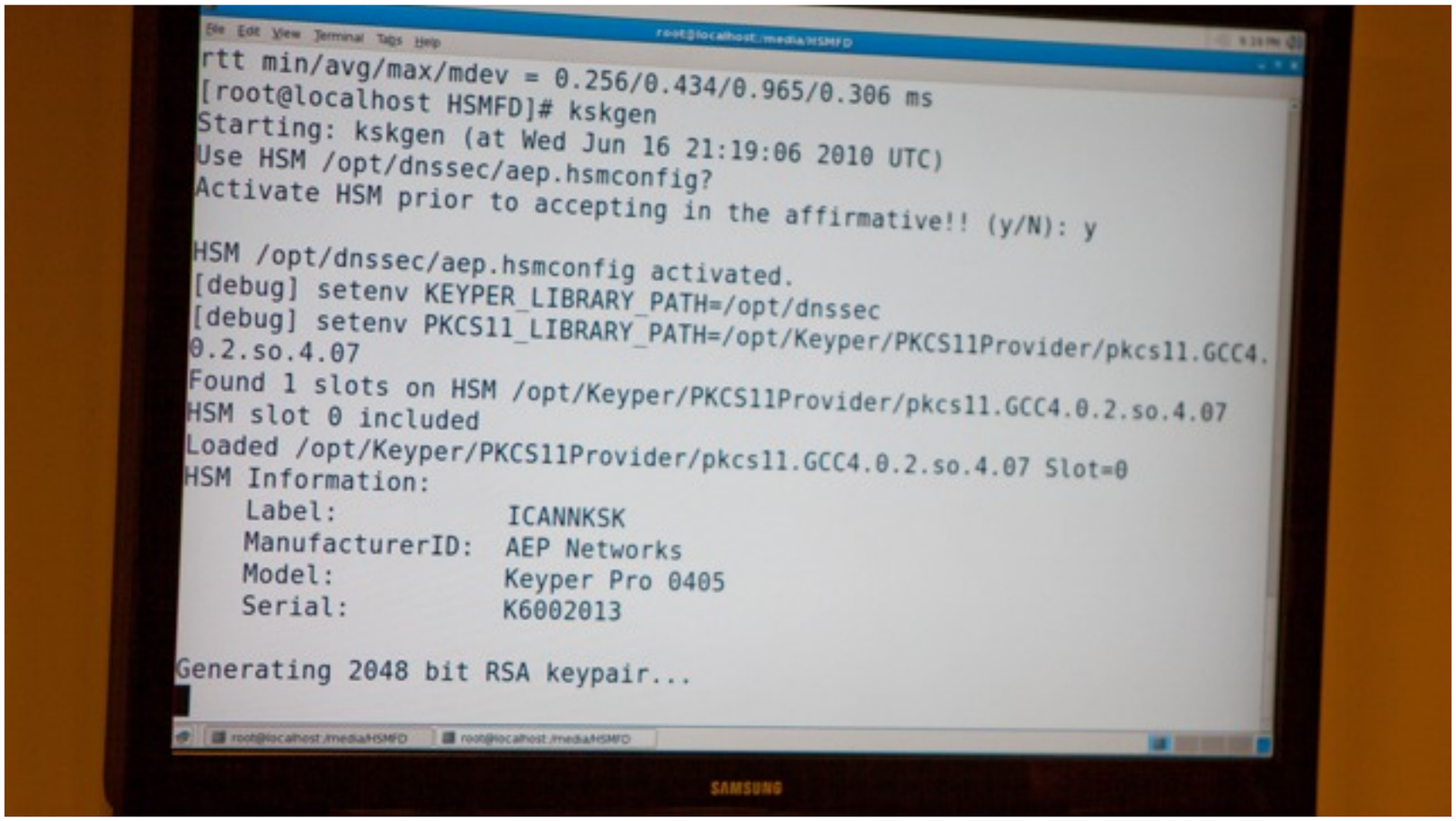
- Jedině vlastník domény (provozovatel služby) ví, jaký certifikát má být použit
- Vložíme identifikaci certifikátu do DNS



Trocha historie

Trocha historie

- Myšlenka kolovala v IETF delší dobu
  - 1997–1999, 2005–2006(bis): Storing Certificates in the Domain Name System (DNS) (RFC 4398)
  - 2002: DNS as X.509 PKIX Certificate Storage (draft-schlyter-pkix-dns-02)
  - 2009: Žádost o nový RRTYPE – TLSFP (Surý)



2010: podpis kořenové zóny

2010

- Červenec 2010: Podpis kořenové zóny
  - Možnost získání out-of-band podepsané informace o certifikátu
- První setkání budoucí pracovní skupiny DANE – barBoF na IETF 78
- Vývoj názvu (aneb to nejdůležitější)
  - Keyassure → KIDNS → DANE

cz.nic

DANE WG

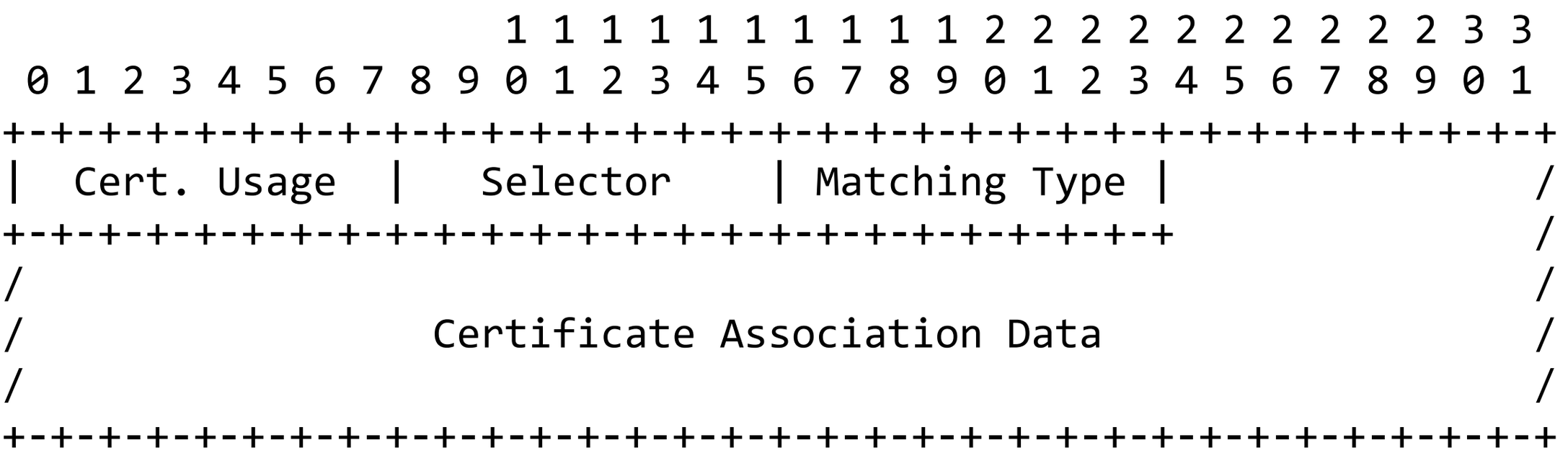
- Listopad 2010: BoF na IETF 79
  - Dnes již skoro nutná podmínka pro založení pracovní skupiny
  - Cca 200 účastníků
- Prosinec 2010: Založení pracovní skupiny DANE WG

Protokol DANE

Protokol DANE

- Nový RR typ – #52, mnemonika TLSA
- Definuje:
  - Způsob tvorby doménového jména
    - _<port>._<ipproto>.<domena>
  - Interpretaci získaných dat

Základní struktura RR záznamu



Selector

- Otisk generován z celého certifikátu (selector 0)
- Otisk generován pouze z klíče – SubjectPublicKeyInfo (selector 1)

Selector

- Doporučený Selector 1
  - Klíč se nemění při obnově certifikátu
  - TLSA záznam může zůstat stejný

Matching Type

- Celý certifikát

  (matching type 0)
- Hashovací funkce SHA-256

  (matching type 1)
- Hashovací funkce SHA-512

  (matching type 2)

Certificate Usage

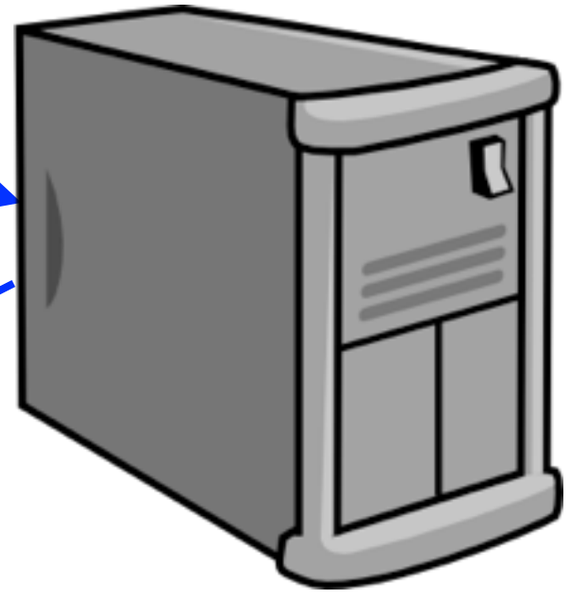
- Omezení na konkrétní CA
  (certificate usage 0)
- Omezení na konkrétní CA certifikát
  (certificate usage 1)
- Vložení neznámého kořene důvěry
  (certificate usage 2)
- Vlastní self-signed certifikát
  (certificate usage 3)

Certificate Usage

0 • Binární data kódují certifikát CA • Serverový certifikát musí projít PKIX validací • Libovolná PKIX validační cesta mezi serverovým certifikátem a kořenem důvěry musí obsahovat certifikát specifikovaný v TLSA záznamu	1 • Binární data kódují end-entity certifikát • Serverový certifikát musí odpovídat tomuto EE certifikátu • Serverový certifikát musí projít PKIX validací k existujícímu kořenu důvěry
2 • Binární data kódují libovolný certifikát CA • Tento certifikát je použij jako nový kořen důvěry • Mezi serverovým certifikátem a novým kořenem důvěry musí projít PKIX validací	3 • Binární data kódují EE certifikát • Serverový certifikát musí odpovídat tomuto EE certifikátu

Omezení na konkrétní CA (bez DANE)

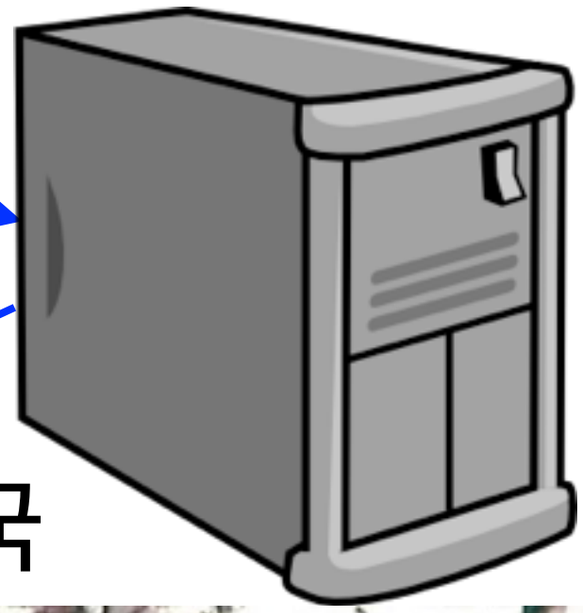
TLS spojení
mail.google.com



Issuer: Symantec
(Verisign/Thawte)

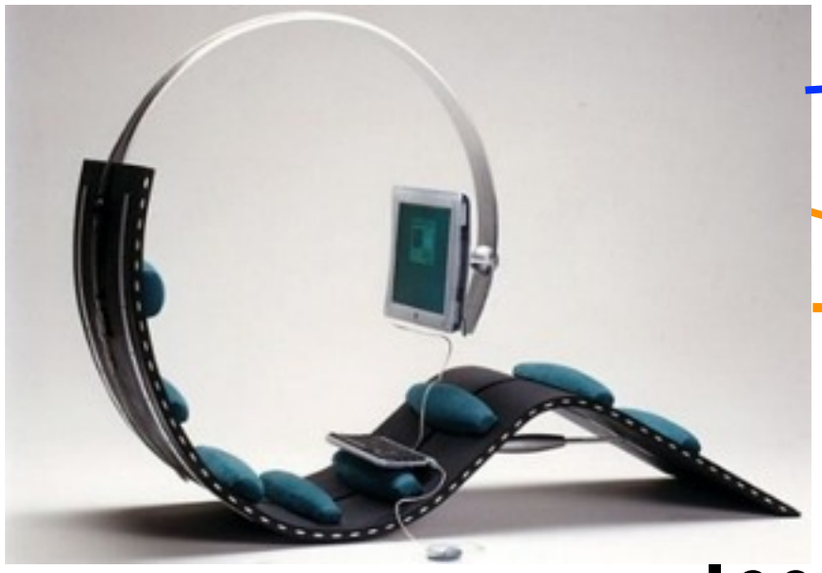
Omezení na konkrétní CA (bez DANE)

TLS spojení
mail.google.com



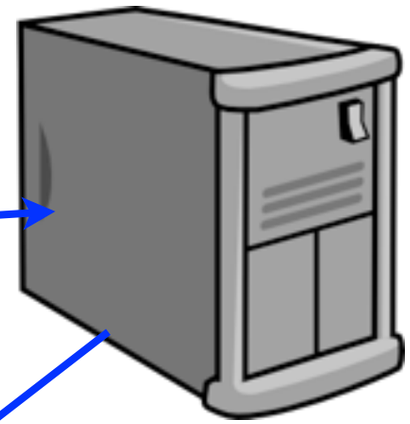
Issuer:
조선민주주의인민공화국

Omezení na konkrétní CA (s DANE)



TLS spojení

mail.google.com



TLSA dotaz

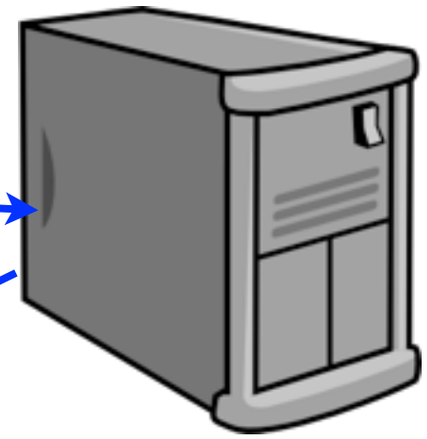
Issuer: DigiNotar

TLSA 0 1 1 [Thawte]

cz.nic

Self-signed certifikát (bez DANE)

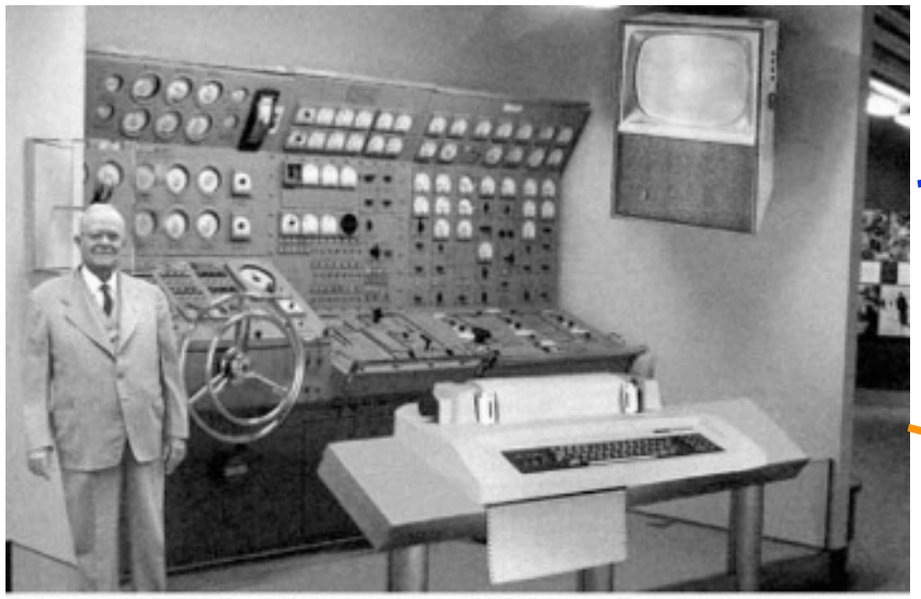
TLSA spojení na lists.debian.org



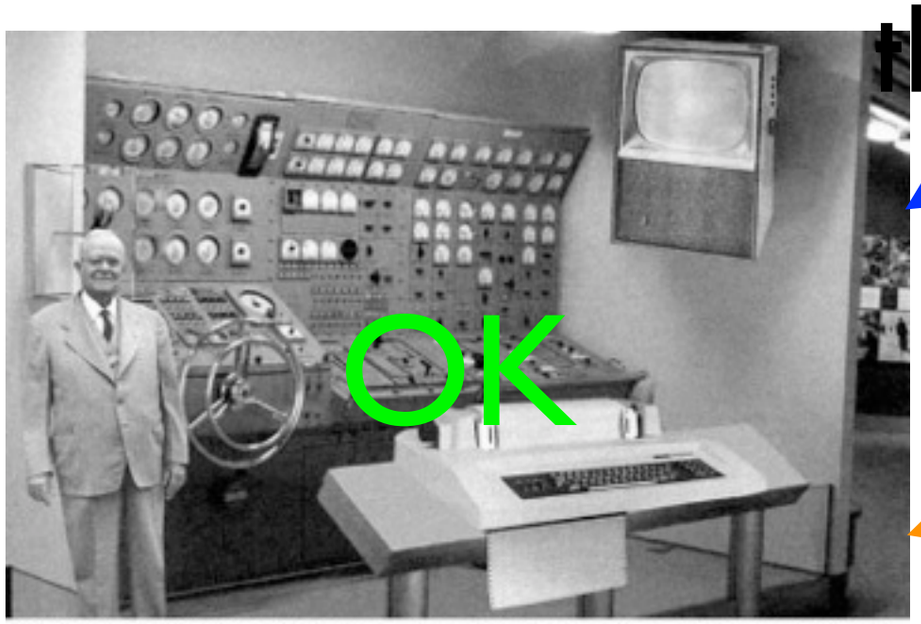
Issuer: Software in the Public Interest

cz.nic

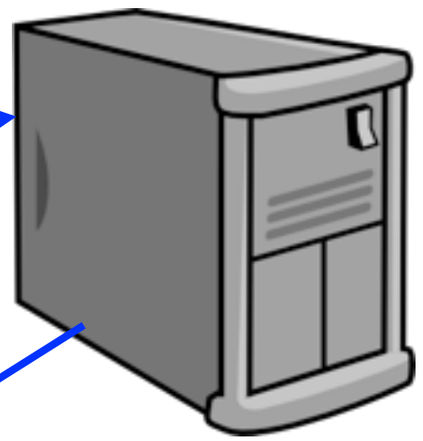
Self-signed certifikát (s DANE)



Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 30 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.



TLSA spojení na lists.debian.org



TLSA dotaz

Issuer: Software in the Public Interest

TLSA 3 1 1 [SPI]

cz.nic

Bezpečnost protokolu DANE

Bezpečnost DANE

- Povinný DNSSEC!
  - Bezpečná poslední míle
- Závislost na DNS

Povinný DNSSEC

- Certificate usage 0/1
  - Šlo by i bez něj
  - Maximální problém – odmítnutí přístupu při nesouladu certifikátu s TLSA záznamem
- Certificate usage 2/3
  - Pokud záznamy nezískáme bezpečně, tak máme problém
  - Útočník přes TLSA záznam může vsunout nový trust-anchor nebo self-signed certifikát
- „Zabezpečení“ je zapotřebí po celé cestě až ke konzumentovi (aplikaci)

Závislost na DNS

- Pokud dojde k napadení DNS
- Můžu si nechat vystavit DV certifikát
- Běžný uživatel nepozná rozdíl mezi DV a OV
- Běžný uživatel ani nepozná rozdíl mezi DV a EV!
  - Kde zjistíte, že druhá strana má používat EV certifikát?

Zhorší se něco?

- Ne, už dnes je vystavení certifikátů závislé na správné funkci DNS

Generování DANE záznamů

Generování DANE záznamů

- Utilita *swede*
- https://github.com/pieterlexis/swede
- Umí záznamy generovat i ověřovat

Příklady

- Omezení na DigiCert pro www.nic.cz

```
_443._tcp.www.nic.cz. IN TLSA 0 1 1
5a889647220e54d6bd8a16817224520bb5c78e
58984bd5705063 88b9de0f075f
```

Příklady

- Přidání Debian CA pro lists.debian.org

```
_443._tcp.lists.d.o. IN TLSA 2 1 1
9b55fd1f30494eac7ba21d7662b94e6468fa9a
5c2ae2dd6f6f2f90ab26273376
```

Budoucnost DANE protokolu

Další protokoly

- Další protokoly s komplexním DNS lookupem
  - S/MIME – draft-ietf-dane-smime
  - SMTP – draft-fanf-dane-smtp
  - MUA – draft-fanf-dane-mua
  - XMPP – draft-miller-xmpp-dnssec-prooftype

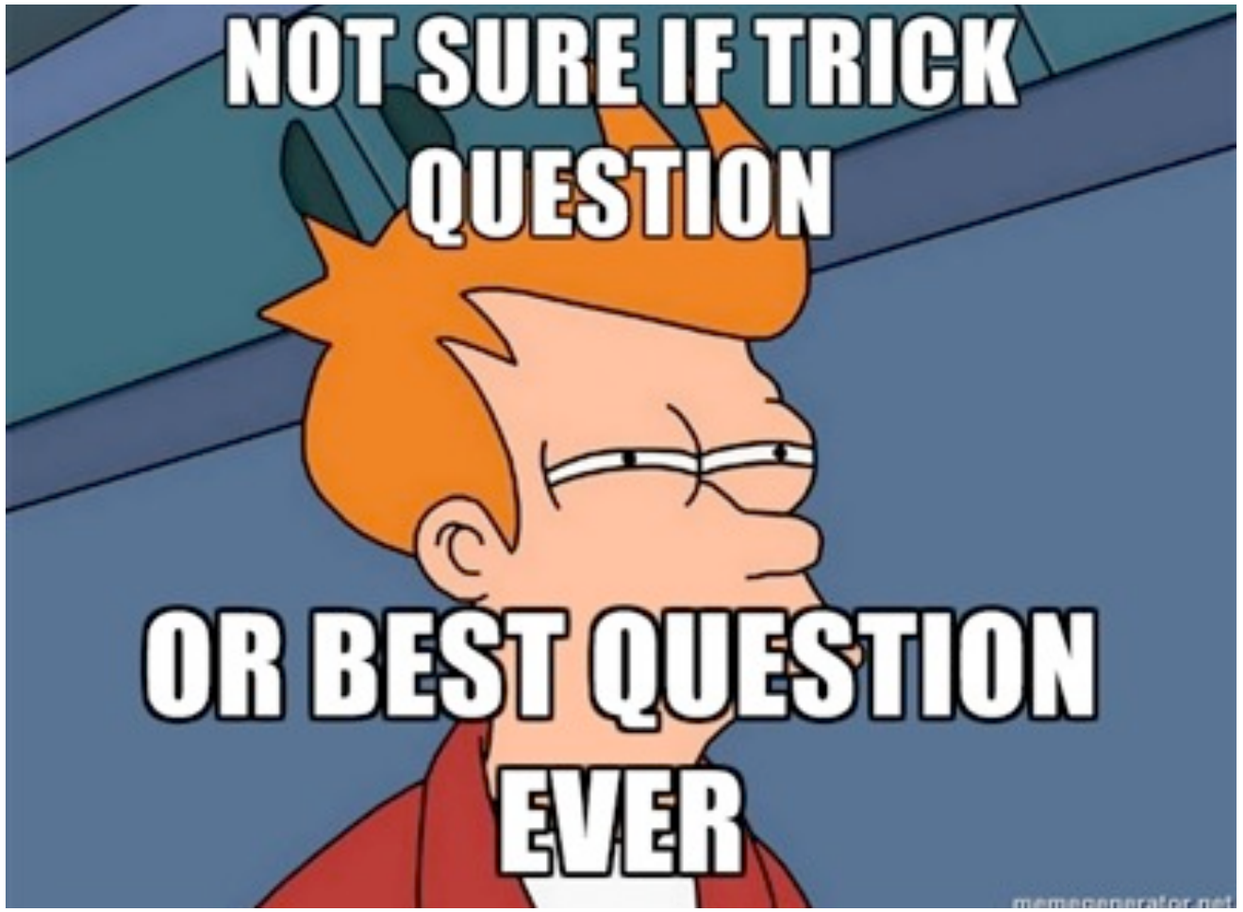
Podpora v DNS serverech

- Bind 9.8.3
- NSD 3.2.11
- Knot DNS 1.0.4

Podpora v jiném software

- GnuTLS 3.1.3 – http://nikmav.blogspot.cz/2012/10/some-thoughts-on-dane-protocol.html
- DANE Patrol (Firefox Add-On) – https://labs.nic.cz/page/1207/dane-patrol/
- OpenSSL – pracuje se na tom

cz.nic



Děkuji za pozornost!