Paweł Rajba <u>pawel@cs.uni.wroc.pl</u> <u>http://itcourses.eu/</u>

# Information Systems Security PKI and digital certificates

# Agenda

- Introduction
- Certificate Authority
- X.509 Certificates
  - Introduction
  - Structure
  - Extensions
  - Usages
- PKCS
- Encodings & formats

- Revoking certificates
- Getting a certificate
- Renewing a certificate
- Certificates on the market
- Digital signatures for the population
- Checking a certificate

## Introduction

- Public Key Infrastructure (PKI)
- Main components
  - Digital Certificates
  - Certificates Authorities (CAs)
  - Registration Authority (RA)
  - Certificate Repository
  - PKI Client Software
  - PKI-Enabled Applications
  - Policy
    - Certificate Policy & the Certification Practice Statement

### Introduction

- Why do we need PKI?
  - Control access to the network with 802.1x authentication
  - Approve and authorize applications with Code Signing
  - Protect user data with EFS
  - Secure network traffic IPSec
  - Protect LDAP-based directory queries Secure LDAP
  - Implement two-factor authentication with Smart Cards
  - Protect traffic to internal web-sites with SSL
  - Implement Secure Email

### Introduction

- Certificate is an electronic document which includes:
  - Public key of the subject
  - Identity description of the subject
  - Digital signature
    - of the trusted third party or
    - we consider self-signed certficate
  - Expiration date
- Main goal
  - Having a document which proves your identity in transactions
    - Something similar to driving licence in real life

### **Certificate Authority**

- Certificate Authority is a unit which everyone "trusts"
- Every CA has a set of Root CA's
  - https://www.symantec.com/page.jsp?id=roots
  - <u>https://www.symantec.com/content/en/us/about/med</u> <u>ia/repository/root-certificates.pdf</u>
- We consider
  - Root CA
    - self-signed certificates
  - Intermediate CA, Issuing CA
    - certificate signed by another CA

#### **Certificate Authority**



## X.509: Introduction

- Certificates systems
  - PGP, SPKI/SDSI
    - decentralized, based on WOT
  - X.509
    - based on hierarchy of certficate authorities
- In this presentation we will focus on X.509

## X.509: Introduction

- ITU-T standard which allows to create a hierarchical Public Key Infrastructure (PKI)
   Built on top of X.500 family
  - http://pl.wikipedia.org/wiki/X.500
- Currently X.509 usually refers to IETF's PKIX Certificate and CRL Profile of the X.509 v3 certificate standard, as specified in RFC 5280
  - <u>http://tools.ietf.org/html/rfc5280</u>
- PKIX Public Key Infrastructure X.509 Working Group (closed in 2013)

## X.509: Structure

- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
- Certificate Signature Algorithm
- Certificate Signature

## X.509: Extensions

- Give additional information about certificateUniquely identified by OIDs
  - Based on ASN.1 syntax
    - http://en.wikipedia.org/wiki/Abstract\_Syntax\_Notation\_One
  - Registry one can find here:
    - <u>http://www.oid-info.com/</u>
    - <u>http://www.alvestrand.no/objectid/</u>
- Extension may be
  - Critical, then certificate system must reject certificate if it is
    - Not recognized or
    - Cannot be processed
  - Not-critical, then certificate system
    - May ignore extension if it is not recognized and
    - Must process if it is recognized

### X.509: Extensions

#### Examples

- Subject Key Identifier (OID: 2.5.29.14)
  - A hash derived from the public key of certficate
- Authority Key Identifier (OID: 2.5.29.35)
  - A hash based on public key of an issuer cert (SKI)
  - or based on issuer name and serial number
- CRL Distribution Points (OID: 2.5.29.31)
  - A place when information about revocaton can be found
- Netscape Certificate Type (OID:2.16.840.1.113730.1.1)
  - Define certficate subject to be SSL client, SSL server or CA
- Basic Constraints (OID: 2.5.29.19)
  - Determine if subject can act as a CA
- Key Usage (OID: 2.5.29.15)
  - Determine set of allowed usages
- Full list of extensions is defined in RFC:
  - http://tools.ietf.org/html/rfc5280#section-4.2.1

## X.509: Usages

- Last 3 examples in previous slide define key usage limitation
- Let's see the definitione of Key Usage field:
  - KeyUsage ::= BIT STRING { digitalSignature (o),

nonRepudiation (1),

- -- recent editions of X.509 have
- -- renamed this bit to contentCommitment

keyEncipherment (2), dataEncipherment (3), keyAgreement (4), keyCertSign (5), cRLSign (6), encipherOnly (7), decipherOnly (8) }

- Good summary from IBM
  - https://www.ibm.com/support/knowledgecenter/SSKTMJ\_10.0.1/adm in/conf\_keyusageextensionsandextendedkeyusage\_r.html

Source: http://tools.ietf.org/html/rfc528o#section-4.2.1.3

# X.509: Usages

- Each certficate is intended to specific usages
  - E.g. Web servers, e-mails, code signing
- VeriSign introduces classes for types of certs:
  - Class 1 for individuals, intended for email.
  - Class 2 for organizations, for which proof of identity is required.
  - Class 3 for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority.
  - Class 4 for online business transactions between companies.
  - Class 5 for private organizations or governmental security.
     <u>https://www.symantec.com/page.jsp?id=roots</u>
     However, this is not a part of PKI standard

#### Some examples

#### Informacje o certyfikacie

#### Ten certyfikat jest przeznaczony do:

- Gwarantuje tożsamość zdalnego komputera
- Udowadnia Twoją tożsamość zdalnemu komputerowi
- 2.16.840.1.114412.2.1
- 2.23.140.1.1

\* Więcej informacji można znaleźć w oświadczeniu urzędu certyfikacji.

Wystawiony dla: allegro.pl

Wystawiony przez: DigiCert SHA2 Extended Validation Server CA

Ważny od 27.07.2018 do 01.08.2019

Informacje o certyfikacie

#### Ten certyfikat jest przeznaczony do:

- Gwarantuje tożsamość zdalnego komputera
- Udowadnia Twoją tożsamość zdalnemu komputerowi
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

\* Więcej informacji można znaleźć w oświadczeniu urzędu certyfikacji.

Wystawiony dla: \*.ii.uni.wroc.pl

Wystawiony przez: TERENA SSL CA 3

Ważny od 12.03.2018 do 16.03.2020

#### **PKCS Standards**

- A set of public-key cryptography standards
   Published by RSA Security Inc. in early 90s
  - Main goal was to promote cryptography techniques to which they had patents
  - Currently, most of them are in the public domain and taken care of organizations like IETF and PKIX
- Let's review shortly standards on the next slides
  - List can be found: <u>http://en.wikipedia.org/wiki/PKCS</u>

#### **PKCS Standards**

	Version	Name	Comments
PKCS #1	2.1	RSA Cryptography Standard <sup>[1]</sup>	See RFC 3447. Defines the mathematical properties and format of RSA public and private keys (ASN.1-encoded in clear-text), and the basic algorithms and encoding/padding schemes for performing RSA encryption, decryption, and producing and verifying signatures.
PKCS #2	-	Withdrawn	No longer active as of 2010. Covered RSA encryption of message digests; subsequently merged into PKCS #1.
PKCS #3	1.4	Diffie-Hellman Key AgreementStandard <sup>[2]</sup>	A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
PKCS #4	-	Withdrawn	No longer active as of 2010. Covered RSA key syntax; subsequently merged into PKCS #1.
PKCS #5	2.0	Password-based Encryption Standard <sup>[3]</sup>	See RFC 2898 and PBKDF2.
PKCS #6	1.5	Extended-Certificate Syntax Standard <sup>[4]</sup>	Defines extensions to the old v1 X.509 certificate specification. Obsoleted by v3 of the same.
PKCS #7	1.5	Cryptographic Message Syntax Standard <sup>[5]</sup>	See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is as of 2010 based on RFC 5652, an updated Cryptographic Message Syntax Standard (CMS). Often used for single sign-on.
PKCS #8	1.2	Private-Key Information Syntax Standard <sup>[6]</sup>	See RFC 5208. Used to carry private certificate keypairs (encrypted or unencrypted).

#### **PKCS Standards**

PKCS #9	2.0	Selected Attribute Types <sup>[7]</sup>	See RFC 2985. Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.
PKCS #10	1.7	Certification Request Standard <sup>[8]</sup>	See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.
PKCS #11	2.20	Cryptographic Token Interface <sup>[9]</sup>	Also known as "Cryptoki". An API defining a generic interface to cryptographic tokens (see also Hardware Security Module). Often used in single sign-on, public-key cryptography and disk encryption <sup>[10]</sup> systems. RSA Security has turned over further development of the PKCS#11 standard to the OASIS PKCS 11 Technical Committee.
PKCS #12	1.0	Personal Information Exchange Syntax Standard <sup>[11]</sup>	Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key. PFX is a predecessor to PKCS #12. This container format can contain multiple embedded objects, such as multiple certificates. Usually protected/encrypted with a password. Usable as a format for the Java key store and to establish client authentication certificates in Mozilla Firefox. Usable by Apache Tomcat.
PKCS #13	_	Elliptic Curve CryptographyStandard <sup>[12]</sup>	(Under development as of 2012.) <sup>[13]</sup>
PKCS #14	-	Pseudo-random Number Generation	(Under development as of 2012.) <sup>[13]</sup>
PKCS #15	1.1	Cryptographic Token Information Format Standard <sup>[14]</sup>	Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15. <sup>[15]</sup>

### **Encodings & formats**

#### PEM

- Encoded with Base64
- Doesn't support storing the whole path of certficates
- Doesn't support storing combination of cerficate and private key
- Extentions: .pem, .crt, .cer, .cert, .key
- Popular in open source solutions (e.g. Apache uses PEM)
- DER
  - Binary representation
  - Doesn't support storing the whole path of certficates
  - Doesn't support storing combination of cerficate and private key
  - Extensions: .cer, .der
- PKCS#7
  - Supports storing whole chain of certificates
  - Doesn't support storing private key
  - Extensions: .p7b, .p7c
- PKCS#12 (previously .pfx was predecessor of PKCS#12)
  - Supports storing whole path of certificates
  - Supports storing private key
  - Extensions: .p12, .pfx

# X.509: Revoking certificates

#### CERTIFICATE REVOCATION IS TO MAKE SURE WE DON'T USE CERTIFICATES WHICH ARE NOT TRUSTED ANYMORE

#### CRL

- Certificate Revocation List
- A file with a list of revoked certificates
- Location included as an extension field in certificate
- Signed by the CA's private key
  - Let's see sample list from <u>https://access.redhat.com/home</u>
    - http://crl3.digicert.com/ssca-sha2-g6.crl

#### OCSP

- Online Certificate Status Protocol
- A service which can answer about the status of certificate
- More efficient than parsing CRL lists
- Read more
  - <u>http://en.wikipedia.org/wiki/Online\_Certificate\_S</u> <u>tatus\_Protocol</u>
  - http://www.ietf.org/rfc/rfc2560.txt
- On lab you will be asked to play with this more <sup>(C)</sup>

#### **Getting a certificate**

#### The process overview



http://www.ibm.com/support/knowledgecenter/SSFKSJ\_8.o.o/com.ibm.mq.sec.doc/qoog87o\_.htm

### **Getting a certificate**

- How to enroll?
  - I.e. prepare and send a Certificate Signing Request which ...
    - ... includes information about an applicant
    - ... is signed by the private key of the applicant
- There are several ways:
  - Autoenrollment
  - Manual Enrollment
  - Web Enrollment
  - Application Specific Enrollment
- For manual there many supporting tools, e.g.
  - CertReq cmd tool, IIS, OpenSSL, DigiCert SSL Utility
- Information Distinguished Name (DN) Business name / Organisation Department Name / Organisational Unit Town/City Province, Region, County or State Country An email address

### Renewing a certificate

- 1. If the expiration date come, a new certificate is required
- 2. To make it easier, CAs offer a renewal proces
- 3. Usually you can apply 90 days before the expiration date
- 4. If company data hasn't changed, it is very quick
  - If changed, a new verification is required
- 5. Once you obtain a certificate, you need install it in the desired place

Interesting comment: <u>http://serverfault.com/questions/554710/azure-web-service-ssl-renewal-procedure</u>

#### We consider 3 levels of validation

- DV Domain Validation
  - Only domain is checked in DNS systems
  - No information about organization is included
  - Available in a few minutes
- OV Full Organization Validation
  - Additionally organization is checked on the basis of organization documentation
  - Available in 1-2 days
- EV Extended Validation
  - More checks are performed: if company has a bank account, there is a phone call with set of questions, etc.
  - Available in 1-10 days
  - Only this type gives a green bar in a web browser
  - Guidelines: <u>https://cabforum.org/extended-validation/</u>

- What means a guarantee of certificate?
  - If something is wrong with a certificate or CA private key, an issuer is obliged to pay compensation
- There is a possibility to buy a wildcard certificate
  - \*.domain.com
    - However, you can consider SAN field

	-		COMPARE			
	Syr	nantec SS	SL/TLS Ce	ertificates		
	Internal Networks			Transactional	Muiti-Domain	Comprehensive
Features	Secure Site	Secure Site with EV	Secure Site Pro	Secure Site Pro with EV	Secure Site Wildcard	Complete Website Security
Norton Secured Seal	•	•	•	•	•	•
Green Bar in Browsers	×	•	×	•	×	•
ECC: Strongest Security	×	×	•	•	×	•
Multiple subdomains	×	×	×	×	•	×
Vulnerability Assessment	×	•	•	•	×	×
DDoS Protection	×	×	×	×	×	•
	from \$399/yr BUY	from \$995/yr виу	from \$995/yr BUY	from <b>\$1,499</b> /yr вич	from \$1,999/yr вич	Please Contact Sales

https://www.symantec.com/ssl-certificates/

- Who sells certificates
  - Symantec
  - Thawte
  - Geotrust
  - Comodo
  - GoDaddy
  - Certum (in Poland)

igicert <sup>®</sup> s	SL PKI IOT S	olutions About Supp	ort	% m 0 8
Standard SSL	EV SSL	Multi-Domain SSL	Wildcard SSL	Secure Site ™ Business Certificate
As low as	As low as	As low as	As low as	As low as
	\$284	\$340	\$625	\$379
BUY	BUY	BUY	BUY	BUY
Renew Learn	Renew Learn	Renew Learn chydr	Renew Learn	



#### GoDaddy @ EN -

Protect one website	Protect multiple websites	Protect all subdomains
	UCC/SAN SSL ()	Wildcard SSL 📀
As low as	As low as	As low as
\$59.99/vr	\$135.99/vr	\$279.99/vr
On sale - Save 20%	On sale - Save 20%	On sale - Save 20%
\$74.99/yr when you renew <sup>4</sup>	\$169.99/yr when you renew <sup>4</sup>	\$349.99/yr when you renew <sup>4</sup>
Add to Cart	Add to Cart	Add to Cart
Secures one website	Secures up to five websites 📀	Secures one website and all its sub-
Strong SHA2 & 2048-bit encryption	Strong SHA2 & 2048-bit encryption	domains
Available in DV, OV and EV SSL	Available in DV, OV and EV SSL	Strong SHA2 & 2048-bit encryption
Certificates 😢	Certificates 😝	Available in DV and OV SSL Certificate
EV SSL turns browser bar green 📀	EV SSL turns browser bar green 📀	•
		Reports come altain Grands condition

Comodo CA offers the quickest, most cost-effective way to protect your business and customer transactions. To maintain the highest levels of trust security and TLS/SSL encryption levels, you can choose from a variety of Comodo CA TLS/SSL certificates.

	BUY NOW	BUY NOW	BUY NOW	BUY NOW
L	Compare   Learn More	Compare Learn More	Compare   Learn More	Compare Learn More
	e couver https://www.	https://www.	https://www.	
	Extended Validation Prices starting from: \$249	Organization Validation Prices starting from: \$179	Domain Validation Prices starting from: \$99	UCC Multi- Domain Prices starting from: \$285



#### Do we always need a certificate from a trusted CA?

# **Digital signatures for population**

- Qualified signature (podpis kwalifikowany)
  - A digital dignature based on qualified certificate
    - Usually, if you buy a qualified signature, you get a package
      - Certificate
      - Device with private key
      - Software intended to make signatures
  - In Poland only National Certification Center is allowed to decide who should be able to issue such certificates
    - But it doesn't issue them on its own
    - Let's see their website: <u>http://www.nccert.pl/</u>
  - Read more:

http://pl.wikipedia.org/wiki/Podpis\_kwalifikowany

Let's see a short list o applications there

# **Digital signatures for population**

- Trusted profile and ePUAP
  - A cheaper alternative for quilified signatures
  - Allows making a lot interactions with many departments of Polish Government
  - Author of the solution discourages the use of it  $\bigcirc$ 
    - http://www.computerworld.pl/news/382785/Nie-uzywam-profilu-zaufanego-na-ePUAP.html

#### How browser knows whether to trust a CA?

#### Katalog główny konsoli

- Certyfikaty bieżacy użytkownik 📋 Osobisty
  - Zaufane główne urzędy certyfikacji Certyfikaty
  - Zaufanie przedsiębiorstwa >
  - Pośrednie urzedy certyfikacji >
  - Obiekt użytkownika Active Directory >
  - Zaufani wydawcy >
  - > Certyfikaty niezaufane
  - Główne urzędy certyfikacji innych firm >
  - Zaufane osoby >
  - Wystawcy uwierzytelniania klienta >
  - > Inne osoby
  - Local NonRemovable Certificates >
  - MSIEHistoryJournal >
  - Zaufane certyfikaty kart inteligentnych >

#### Wystawiony dla

AddTrust External CA Root AffirmTrust Commercial Baltimore CyberTrust Root Certum CA Certum Trusted Network CA 🗔 Class 2 Primary CA COMODO RSA Certification Au... Copyright (c) 1997 Microsoft C... STATEST DESKTOP-JMMF46M Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA 🔄 DigiCert Global Root CA 🔄 DigiCert High Assurance EV Ro... DST Root CA X3 Entrust Root Certification Auth... Entrust Root Certification Auth... Entrust.net Certification Author... Equifax Secure Certificate Auth... GeoTrust Global CA GeoTrust Primary Certification ... GeoTrust Primary Certification ... 🔄 GlobalSign 🔄 GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification ... Go Daddy Root Certificate Auth... GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 🗔 Kaspersky Anti-Virus Personal R... 🔄 Kaspersky Anti-Virus Personal R...

Microsoft Authenticode(tm) Ro... Microsoft Authenticode(tm) Root...

Wystawiony przez 30.05.2020 AddTrust External CA Root AffirmTrust Commercial 31.12.2030 Baltimore CyberTrust Root 13.05.2025 Certum CA 11.06.2027 Certum Trusted Network CA 31.12.2029 Class 2 Primary CA 07.07.2019 🔄 Class 3 Public Primary Certificat... Class 3 Public Primary Certificatio... 02.08.2028 COMODO RSA Certification Auth... 19.01.2038 Copyright (c) 1997 Microsoft Corp. 31.12.1999 DESKTOP-JMMF46M 29.12.3014 Deutsche Telekom Root CA 2 10.07.2019 DigiCert Assured ID Root CA 10.11.2031 DigiCert Global Root CA 10.11.2031 DigiCert High Assurance EV Root ... 10.11.2031 DST Root CA X3 30.09.2021 Entrust Root Certification Authority 27.11.2026 07.12.2030 Entrust Root Certification Authori... Entrust.net Certification Authority... 24.07.2029 Equifax Secure Certificate Authority 22.08.2018 GeoTrust Global CA 21.05.2022 GeoTrust Primary Certification Au... 17.07.2036 GeoTrust Primary Certification Au... 02.12.2037 18.03.2029 GlobalSign GlobalSign 15.12.2021 GlobalSign Root CA 28.01.2028 Go Daddy Class 2 Certification Au... 29.06.2034 Go Daddy Root Certificate Author... 01.01.2038 14.08.2018 GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 08.12.2043 01.07.2026 Kaspersky Anti-Virus Personal Ro... Kaspersky Anti-Virus Personal Ro... 29.08.2026

Data wygaśnie... Zamierzone cele Przyjazna nazwa Uwierzytelnienie ser... The USERTrust Net... Uwierzytelnienie ser... Trend Micro Uwierzytelnienie ser... DigiCert Baltimore ... Uwierzytelnienie ser... Certum Uwierzytelnienie ser... Certurn Trusted Net... CertPlus Class 2 Pri... Bezpieczna poczta ... Bezpieczna poczta ... VeriSign Class 3 Pu... COMODO SECURE™ Uwierzytelnienie ser... Sygnatura czasowa Microsoft Timesta... Uwierzytelnienie ser... <br/>
<br/>
hrak> Bezpieczna poczta ... Deutsche Telekom ... Uwierzytelnienie ser... DigiCert Uwierzytelnienie ser... DigiCert Uwierzytelnienie ser... DigiCert Bezpieczna poczta ... DST Root CA X3 Uwierzytelnienie ser... Entrust Uwierzytelnienie ser... Uwierzytelnienie ser... Bezpieczna poczta ... Uwierzytelnienie ser... Bezpieczna poczta ... Uwierzytelnienie ser... <Wszyscy>

Uwierzytelnienie ser...

Bezpieczna poczta ...

01.01.2000

Entrust.net Entrust (2048) GeoTrust GeoTrust Global CA GeoTrust GeoTrust Primary C... GlobalSign GlobalSign GlobalSign Go Daddy Class 2 C... Go Daddy Root Cer... DigiCert Global Root Hotspot 2.0 Trust R... <brak> <br/>
<br/>
hrak> Microsoft Authenti...





Check validity period and verify that this is

CA is trusted, verification stops here.

signed by Engineering CA. Since Engineering



Certificate Issued by Engineering CA



Trusted Authority



Untrusted Authority

- There 2 parts of certificate validation process
  - Path Discovery
  - Path Validation
    - http://tools.ietf.org/html/rfc3379
  - Let's see main points of an algorithm
    - http://en.wikipedia.org/wiki/Certification\_path\_validation\_algorithm
- Trust is based on Trusted Store Certificate in the system
- A mess around SHA-1 vs. SHA-2 based signatures
  DEMO
  - Let's see the list of trusted certificates in IE
  - Let's see the chain of certificates for
    - https://www.symantec.com/index.jsp

#### Many services, the most popular ones

- https://www.ssllabs.com/ssltest/
- https://cryptoreport.websecurity.symantec.com/checker/
- <u>https://www.digicert.com/help/</u>

u are here: <u>Homa &gt; Projects</u> > SSL S	erver Test				
SL Server Test					
is free online service perform formation you submit here II.	is a deep analys is used only to	is of the configuration of any SSL w provide you the service. We don'	eb server on th t use the dom	e public Internet. Please note that t ain names or the test results, and	he we never
	Hostname:			Submit	
		Do not show the results on the boards			
Recently Seen		Recent Best		Recent Worst	
fyinghazard.com		meeting rg zoho.com	٨٠	mailers.zohosites.com	т
cabinmap.com		msk.tech	A+	ted of	E.
kruma.m		meetzoho.com	٨٠	£360help.manageengine.com	- E
www.leslado.cz		medicalmine.com	A+	helpdesk1 thandora.com	т
meeting2-ro.zoho.com	Α	me zoho com	A+	icm.leice-microsystems.com	E.
meeting-ro.zoho.com	A+	meeting2-ro.zoho.com	Α	devmalle-press aam.com	т
newserver.pumprescriptions	Α.	m.manageengine.com	Α	forms.zohocreator.com	т
doloi nu		newserver.pureprescriptions	A	de-licensing manageengine.co	т
izacromplus.ru		www.plannedparenthood.org	Α	campaigns nucleusfinancial.c	F.
meetzoho.com	۸۰	payroll cloard.com	в	customer-ro-wms.zoho.com	т
Report of 27.3					
C Program P Later of					











#### References

- SPKI
  - http://pl.wikipedia.org/wiki/SPKI
- PGP
  - <u>http://pl.wikipedia.org/wiki/Pretty\_Good\_Privacy</u>
- X.509 & PKI
  - http://en.wikipedia.org/wiki/X.509
  - http://technet.microsoft.com/en-us/library/cc737264(v=ws.10).aspx
- Encoding & formats
  - http://myonlineusb.wordpress.com/2011/06/19/what-are-the-differences-between-pem-der-p7bpkcs7-pfxpkcs12-certificates/
  - http://serverfault.com/questions/9708/what-is-a-pem-file-and-how-does-it-differ-from-other-openssl-generated-key-file
  - https://support.ssl.com/Knowledgebase/Article/View/19/0/der-vs-crt-vs-cer-vs-pem-certificates-and-how-to-convert-them
- Sample files
  - http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI-html/sample-openssl-usage.htm
- Calculating hashes (very good)
  - http://certificateerror.blogspot.com/2011/02/how-to-validate-subject-key-identifier.html
- Good Knowledge Base
  - <u>https://access.redhat.com/site/documentation/en-US/Red\_Hat\_Certificate\_System/8.o/html/Admin\_Guide/Standard\_X.509\_v3\_Certificate\_Extensions.html</u>
  - https://certyfikatyssl.pl/faq.html
  - https://blogs.technet.microsoft.com/askds/2009/09/01/designing-and-implementing-a-pki-part-i-design-and-planning/
- Checking trust chain of certificates
  - http://www.oasis-pki.org/pdfs/Understanding\_Path\_construction-DS2.pdf
  - http://www.herongyang.com/PKI/HTTPS-IE-8-View-Server-Certificate-Path.html
  - http://technet.microsoft.com/en-us/library/cc962065.aspx
  - http://en.wikipedia.org/wiki/Extended\_Validation\_Certificate
  - http://blog.securism.com/2009/01/summarizing-pki-certificate-validation/
- Managing and obtaining certificates
  - http://msdn.microsoft.com/en-us/library/windowsazure/gg981929.aspx
- Related RFC documents
  - <u>http://tools.ietf.org/html/rfc5280, http://tools.ietf.org/html/rfc3279, http://tools.ietf.org/html/rfc3280, http://tools.ietf.org/html/rfc4055, http://tools.ietf.org/html/rfc4491</u>
- Standard list (good review)
  - https://www.entrust.com/about-us/certifications-standards/standards-pki-standards-compliance-summary/