

Public Key Infrastructures

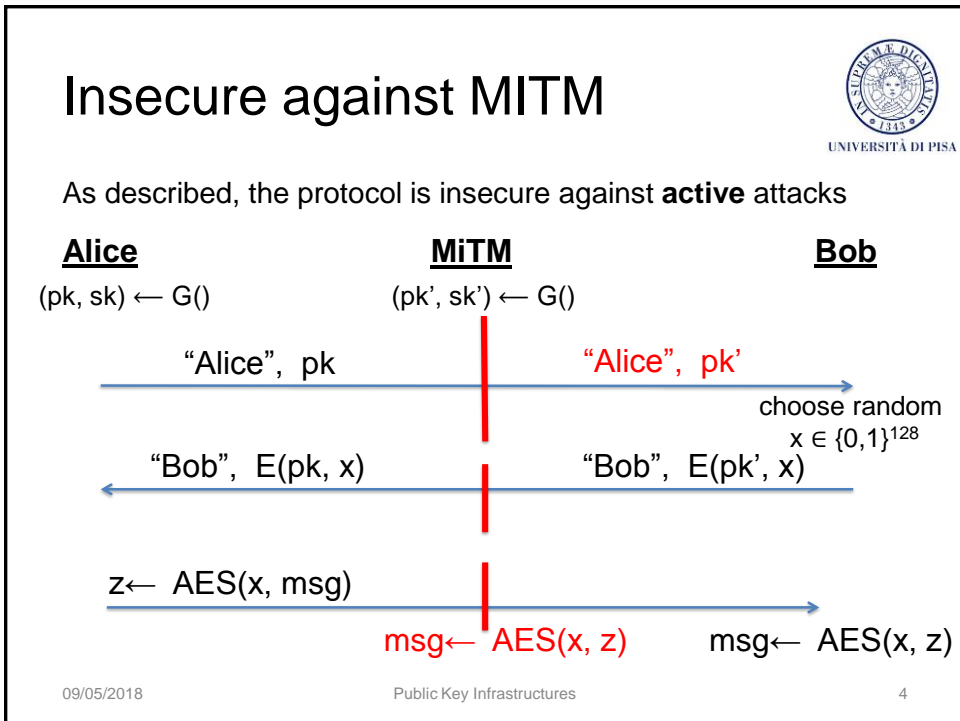
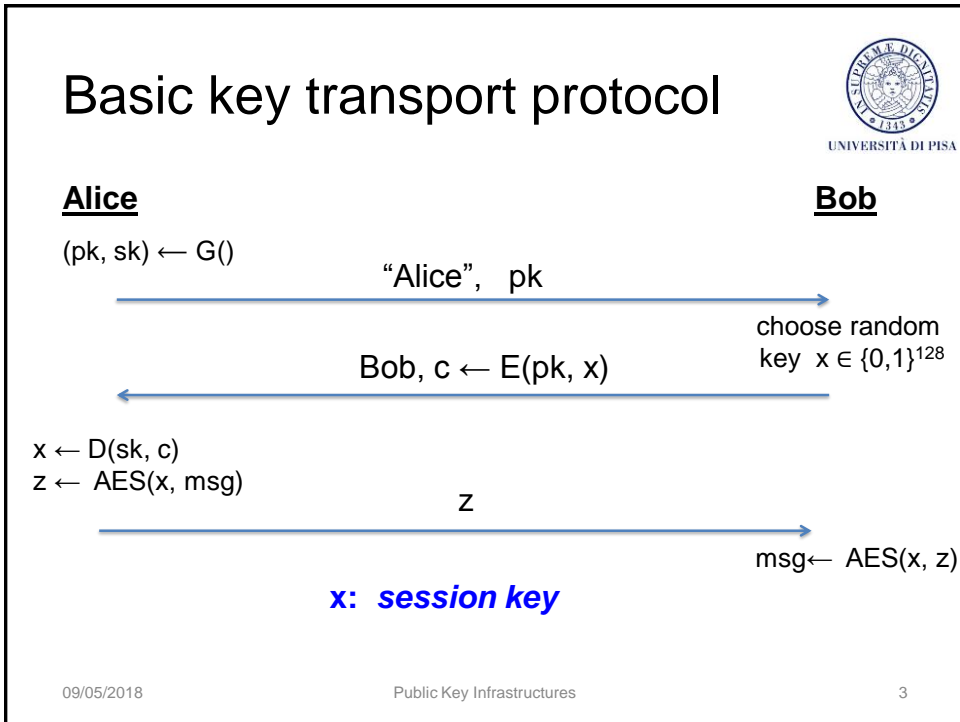
Security in Networked Computing Systems

Goals



UNIVERSITÀ DI PISA

- Understand how public keys can be distributed and revoked on a large scale
- Understand what a CA-based PKI is and what the problems are with their deployment
- Understand how multiple CAs can interoperate depending on their trust relationship



Public Key Authentication



UNIVERSITÀ DI PISA

- In Key Establishment using Asymmetric Techniques, the underlying problem of the MIM attack is that public keys are not authenticated
 - **Public-key schemes do not require secure channel but authenticated channels for the distribution of public keys**
- **Certificates** are the main mechanism to address the problem of public key authentication

09/05/2018

Public Key Infrastructures

5

Certificate



UNIVERSITÀ DI PISA

- A **Certificate** is a data structure that **cryptographically links** the identifier of a subject to the subject public key (and other stuff):


$$\text{Cert}_A = A, e_A, L_A, S_{CA}(A||e_A||L_A)$$

- **A**: identifier;
- **e_A**: public key;
- **L_A**: validity interval
- The link is represented by the digital signature by a trusted third party (certification authority)
- A **Certification Authority** is a TTP that attests the authenticity of a public key

09/05/2018

Public Key Infrastructures

6



UNIVERSITÀ DI PISA

Certificate-based DHP

$Y_A = g^a \text{ mod } p$
 $\text{Cert}_A = A, Y_A, L, S_{CA}(A||Y_A||L)$

Alice

$Y_B = g^b \text{ mod } p$
 $\text{Cert}_B = B, Y_B, L, S_{CA}(B||Y_A||L)$


Bob

- A certificate can be sent contextually to the public key

09/05/2018

Public Key Infrastructures

7



UNIVERSITÀ DI PISA

Certificate generation

User-provided Keys

Alice

Generate $\text{pub}K_A, \text{priv}K_A$

CA


1. Verify Alice identity
2. Run challenge-response
3. Choose L_A
4. $s_A = S_{CA}(\text{Alice}||\text{pub}K_A||L_A)$
5. $\text{Cert}_A = \text{Alice}||\text{pub}K_A||L_A, s_A$

CA gets certain that Alice holds the corresponding $\text{priv}K_A$

09/05/2018

Public Key Infrastructures

8



UNIVERSITÀ DI PISA

Challenge-response protocol

User-provided Keys

Alice

2. Compute the response
 $s_A = S_A(c)$

CA


1. Generate a random challenge c
3. Verify the response by means of $pubK_A$

- CRP can be implemented also with a cipher

09/05/2018

Public Key Infrastructures

9



UNIVERSITÀ DI PISA

Certificate generation

CA-Generated Keys

Alice

CA

1. Verify Alice identity
2. Generate $(pubK_A, privK_A)$
3. Choose L_A
4. $s_A = S_{CA}(Alice || pubK_A || L_A)$
5. $Cert_A = Alice || pubK_A || L_A, s_A$

REQ

REP, Cert_A, privK_A

09/05/2018

Public Key Infrastructures

10

On key generation at CA-side



UNIVERSITÀ DI PISA

Fatal crypto flaw in some government-certified smartcards makes forgery a snap
www.arstechnica.com



- Fatal flaw in the hw RNG
- Smartcards passed two international certifications
- Research paper at AsiaCrypt 2013

09/05/2018

Public Key Infrastructures

11

Key lifetime, backup & recovery



UNIVERSITÀ DI PISA


- If you use privK for decryption then you want to backup it or your encrypted data become inaccessible
 - Be able to decrypt even after key lifetime expiration
 - Government => backup of **citizen's** privK
 - This raises privacy issues
 - Company => backup of **employee's** privK
 - Encrypted data belong to the company
- What about backup of a signing privK?
 - Delete the key after key expiration
 - Adverse impact on non-repudiation
 - Expensive recovery in large scale apps
 - Threshold crypto (t out of n)

09/05/2018

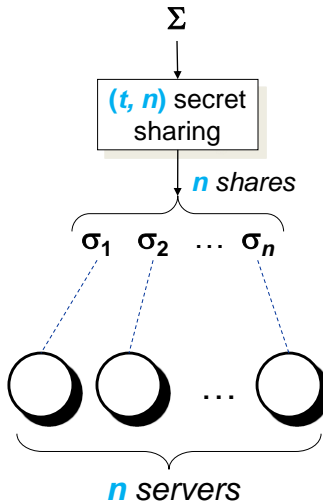
Public Key Infrastructures

12

Threshold crypto (intuition)



UNIVERSITÀ DI PISA



Σ

↓

(t, n) secret sharing

↓ n shares

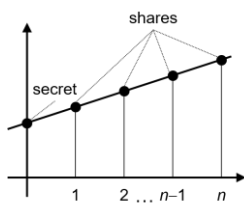
$\sigma_1 \quad \sigma_2 \quad \dots \quad \sigma_n$

↓

n servers

SECRET SHARING


- The secret (private key Σ) is split into n shares
- At least t shares are necessary to reconstruct the secret
- The system tolerates the compromise of $t-1$ nodes



Polynomial (2, n) secret sharing

09/05/2018
Public Key Infrastructures
13

CA's obligations



UNIVERSITÀ DI PISA

- **CA must be reliable**
 - CA must verify that the name (Alice) goes along with the key ($\text{priv}K_A$)
 - CA must verify that owner of ($\text{priv}K$, $\text{pub}K$) pair is really entitled to use that name
 - CA establishes rules/policies to verify that a person has rights to the name
 - *Identifying a subject is not easy; depends on country*
- **CA's certificate must be (immediately) available**
 - CA's certificate is released at user registration time
 - CA's certificate is published in newspapers
 - CA's certificate is embedded in a browser installation package (*is this secure?*)

09/05/2018
Public Key Infrastructures
14

Trust delegation



UNIVERSITÀ DI PISA

- Certification is based on **trust delegation** (trust transfer)
 - Bob **trusts** and **delegates** CA to verify Alice's identity and attest the authenticity of pubK_A
 - Bob **trusts** the authenticity of CA's pubK_{CA}

then

 - Through a certificate Cert_A signed by CA, Bob acquires trust in (believes) the authenticity of pubK_A

09/05/2018

Public Key Infrastructures

15

Just to recap



UNIVERSITÀ DI PISA

- **A certificate defines a indissoluble link between a subject's identifier and public key**
 - A certificate does not specify the meaning of that link
 - A certificate doesn't specify the possible uses of that key
 - A certificate doesn't make any statement on the trustworthiness of the subject

09/05/2018

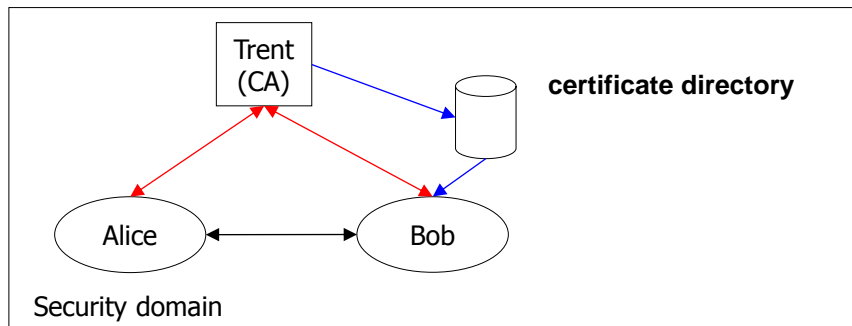
Public Key Infrastructures

16

Single CA Model



UNIVERSITÀ DI PISA



- **Security domain** under control of the CA
- **Certificate directory** is a read-only database that stores certificates

09/05/2018

Public Key Infrastructures

19

Expired vs revoked certificates



UNIVERSITÀ DI PISA

- A certificate is **expired** if the validity period is expired
- If the private key gets compromised before expiration, then the certificate must be **revoked**
 - The private key has been revealed
 - The subject has changed role or left the organization
- **Certificate revocation** must be
 - **correct**: it can be granted only to authorized parties, i.e., the owner or the issuer
 - **timely**: it must be disseminated to all interested parties as soon as possible

09/05/2018

Public Key Infrastructures

21

How to verify a certificate



UNIVERSITÀ DI PISA

- **Bob verifies authenticity of pubK_A using Cert_A**
 - Bob obtains CA's public key e_T [**once at set-up**]
 - Bob verifies validity of CA's public key [**once at set-up**]
 - Bob verifies the digital signature in Cert_A by using CA public key
 - Bob verifies that certificate Cert_A is valid (within L_A)
 - Bob verifies that certificate Cert_A is not revoked
 - If all these checks are successful, then Bob accepts pubK_A as authentic key of Alice

09/05/2018

Public Key Infrastructures

22

Management of revoked certificates




UNIVERSITÀ DI PISA

- **Validity period** limits exposition of a compromised key
- **Out-of-band notification** doesn't scale
- **Certificate Revocation List (CRL)**, a public file that contains the list revoked certificate; *it must be checked before every usage of the key*

09/05/2018

Public Key Infrastructures

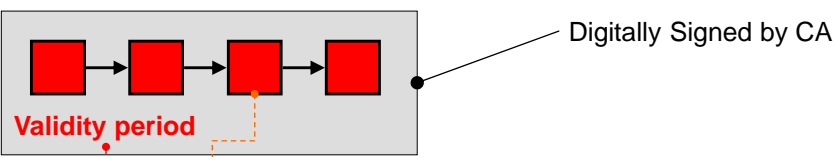
24



UNIVERSITÀ DI PISA


CRL

- A CRL is published periodically
- A revoked certificate lies in CRL until expiration



- serial number, revocation date, revocation reason
- **Validity period** dà indicazioni sulla freshness della CRL

09/05/2018 Public Key Infrastructures 25



UNIVERSITÀ DI PISA

An example: X.509


A data structure with several fields

1. Version	7. Subject public key information
2. Serial number	8. Issuer unique identifier (v=2,3)
3. Signature algorithm identifier	9. Subject unique identifier (v=2,3)
4. Issuer distinguished name	10. Extensions (v=3)
5. Validity interval	11. Signature
6. Subject distinguished name	

X.509 uses the Abstract Syntax Notation, ASN.1, (RFC 1422)
 X.509 has been conceived for X.400 mail standard
 X.509 uses Distinguished Names

09/05/2018 Public Key Infrastructures 26

Distinguished names


UNIVERSITÀ DI PISA

COUNTRY
CO=IT


ORGANIZATION
CO=IT, O=University of Pisa

ORGANIZATIONAL UNIT
CO=IT, O=University of Pisa, OU=Dipartimento di Ingegneria della Informazione

COMMON NAME
CO=IT, O=University of Pisa,
OU=Dipartimento di Ingegneria della Informazione, CN=Gianluca Dini

09/05/2018 Public Key Infrastructures 27

Example: <https://www.mps.it>



UNIVERSITÀ DI PISA


Certificate name
www.mps.it
Consorzio Operativo Gruppo MPS
Terms of use at www.verisign.com/rpa (c)00
Florence
Italy, IT

Issuer
VeriSign Trust Network
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

Details
Certificate version: 3
Serial number: 0x652D0F8ADAB4C7B168A27BBD1C3E9D9D
Not valid before: Mar 2 00:00:00 2004 GMT
Not valid after: Mar 2 23:59:59 2005 GMT
Fingerprint: (MD5) CA CA 88 08 EC D0 8E 49 A6 9A 66 C4 69 31 E0 AE
Fingerprint: (SHA-1) 82 64 CB 69 F0 43 86 43 FF B4 55 D4 25 EF 51 60 65 46 D3 87

contd

09/05/2018 Public Key Infrastructures 28



UNIVERSITÀ DI PISA

Example: https://www.mps.it

Public key algorithm: rsaEncryption
Public-Key (1024 bit):
Modulus:
 00: E1 80 74 5E E7 E5 54 8B DF 6D 00 95 B5 96 27 AC
 10: 66 93 E0 49 B9 6F 5B 73 53 1C BE 1C EB 47 64 B2
 20: 12 95 70 E6 CD 50 67 02 88 E3 EE 9D B1 91 49 C8
 30: 8D 58 19 4B 86 8F C0 2E 65 E8 F2 D4 82 CC 55 DB
 40: 43 BC 66 DA 44 2F 53 B3 48 4B 37 15 F3 AB 67 C1
 50: 69 B4 53 23 19 30 1A 19 23 7F 28 E0 E3 C0 6B 18
 60: FF 84 C4 AC A9 74 28 DB FF E9 48 CA 75 D5 35 D6
 70: 46 FB 7D D4 A7 3F A1 4B 00 60 14 DC D5 00 CF C7


Exponent:
 01 00 01

Public key algorithm: sha1WithRSAEncryption
 00: 23 A6 FE 90 E3 D9 BB 30 69 CF 43 2C FD 4B CF 67
 10: D7 3C 46 22 9A 08 DB 05 1D 45 DC 07 F3 1E 4D 1F
 20: 4B 11 23 5B 42 91 14 95 25 88 1F BD 60 E5 6F 84
 30: 44 70 7A 95 EC 30 E4 46 4F 37 87 F1 B2 FA 45 04
 40: 6F 7C BE 97 25 C7 20 E7 F3 90 55 51 99 3A 72 35
 50: 40 F2 E8 E3 36 3A 7D 58 61 9C 91 D6 AC 34 E7 E8
 60: 09 27 64 4F 2C 4C C2 D2 A3 32 DB 2B 7E F0 B6 F3
 70: 69 96 E4 2B C3 2B 42 ED CA 2C 3C C8 F5 AA E6 71

09/05/2018

Public Key Infrastructures

cont'd
29



UNIVERSITÀ DI PISA

Example: https://www.mps.it

Extensions:

- X509v3 **Basic Constraints:** CA:FALSE
- X509v3 **Key Usage:** Digital Signature, Key Encipherment
- X509v3 **CRL Distribution Points:**
 URI: http://crl.verisign.com/Class3InternationalServer.crl
- X509v3 **Certificate Policies:**
 Policy: 2.16.840.1.113733.1.7.23.3
 CPS: https://www.verisign.com/rpa
- X509v3 **Extended Key Usage:** Netscape Server Gated Crypto, Microsoft Server Gated Crypto, TLS Web Server Authentication, TLS Web Client Authentication
- Authority Information Access:**
 OCSP - URI: http://ocsp.verisign.com
 Unknown extension object ID 1 3 6 1 5 5 7 1 12:
 0_.j.[0Y0W0U..image/gif0I0.0....+.....k...j.H.,{-0%.#http://logo.verisign.com/vslogo.gif

09/05/2018

Public Key Infrastructures

30

Public Key Infrastructure

TRUST MODELS

09/05/2018

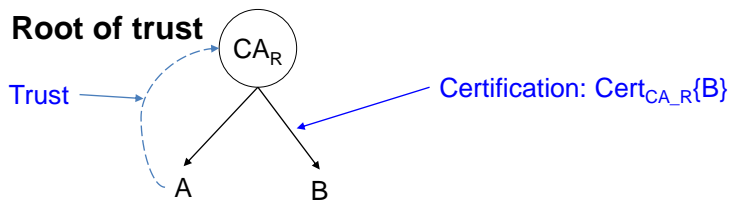
Public Key Infrastructures

31

Centralized Trust Model



UNIVERSITÀ DI PISA



The Model

- Every user trusts the root
- The root releases certificates

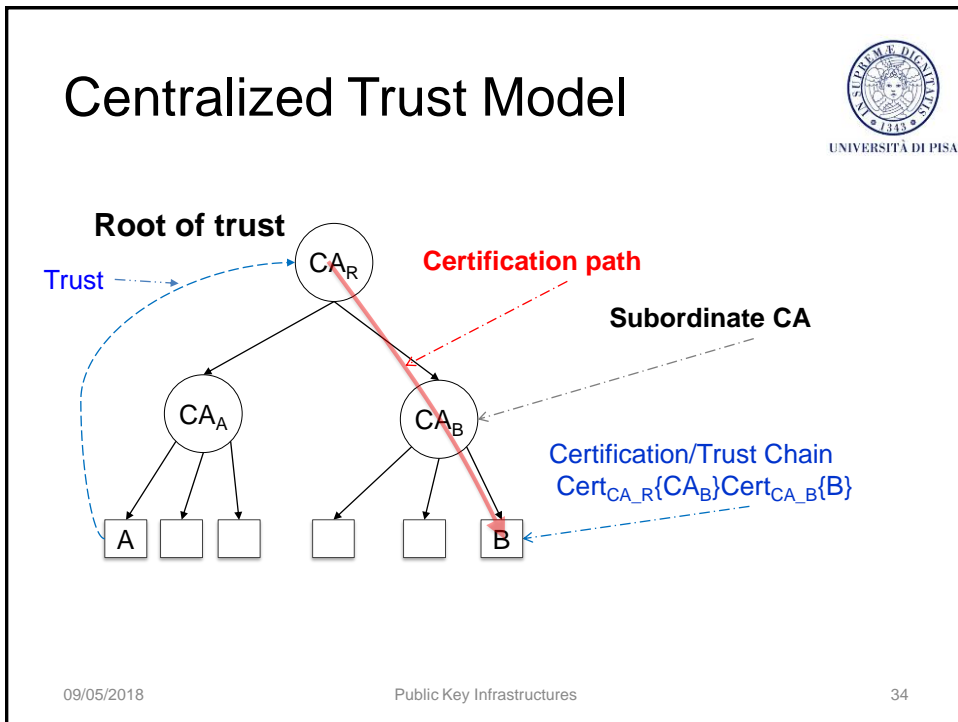
Inconvenient

- Users have to go to the root in order to get a certificate

09/05/2018

Public Key Infrastructures

33




Constraints on the certification path

UNIVERSITÀ DI PISA

- If CA_X certifies CA_Y , the trust that CA_X has in CA_Y transitively propagates to all CAs reachable from CA_Y
- CA_X may limit this propagation by posing constraints
 - **Constraint on the chain length.** The chain after CA_Y has a limited length
 - **Constraint on the set of domains.** CAs in the chain after CA_Y must belong to a predefined set of CAs

09/05/2018 Public Key Infrastructures 36



UNIVERSITÀ DI PISA


Esempio: <https://www.mps.it>

Certificate name
 VeriSign Trust Network
www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD.(c)97 VeriSign

Issuer
 VeriSign, Inc.
 Class 3 Public Primary Certification Authority
 US

Details
 Certificate version: 3
 Serial number: 0x254B8A853842CCE358F8C5DDAE226EA4
 Not valid before: Apr 17 00:00:00 1997 GMT
 Not valid after: Oct 24 23:59:59 2011 GMT
 Fingerprint: (MD5) BC 0A 51 FA C0 F4 7F DC 62 1C D8 E1 15 43 4E CC
 Fingerprint: (SHA-1) C2 F0 08 7D 01 E6 86 05 3A 4D 63 3E 7E 70 D4 EF 65 C2 CC 4F

09/05/2018
Public Key Infrastructures
37




UNIVERSITÀ DI PISA

Esempio: <https://www.mps.it>

Public key algorithm: rsaEncryption
Public-Key (1024 bit):
Modulus:
 00: 6F 7B B2 04 AB E7 34 4F 9C 53 A7 02 B2 90 4F 22
 10: F9 3A 3C 5A 8B 51 2B FE CB 42 95 30 70 FE 8A B2
 20: D3 1D C1 B8 5A 49 5C F7 39 4E 4D B7 F3 3B 09 F1
 30: FA E5 28 93 3E 30 F5 63 AA 43 71 27 56 FE A3 BB
 40: CA C4 6C 75 B2 32 C1 07 D9 DD 25 40 F5 5C A9 D4
 50: 15 0A 34 9A ED 42 97 EA BD F1 B2 55 45 73 3C AA
 60: E7 B6 5B 6C 4C F0 AA 3B 36 E6 BC D3 05 D4 BF E1
 70: 2B 65 A2 25 39 18 85 1F 7D 02 19 D6 E8 80 82 D8
Exponent:
 01 00 01
Public key algorithm: sha1WithRSAEncryption
 00: 08 01 EC E4 68 94 03 42 F1 73 F1 23 A2 3A DE E9
 10: F1 DA C6 54 C4 23 3E 86 EA CF 6A 3A 33 AB EA 9C
 20: 04 14 07 36 06 0B F9 88 6F D5 13 EE 29 2B C3 E4
 30: 72 8D 44 ED D1 AC 20 09 2D E1 F6 E1 19 05 38 B0
 40: 3D 0F 9F 7F F8 9E 02 DC 86 02 86 61 4E 26 5F 5E
 50: 9F 92 1E 0C 24 A4 F5 D0 70 13 CF 26 C3 43 3D 49
 60: 1D 9E 82 2E 52 5F BC 3E C6 66 29 01 8E 4E 92 2C
 70: BC 46 75 03 82 AC 73 E9 D9 7E 0B 67 EF 54 52 1A

09/05/2018
Public Key Infrastructures
38

Esempio: <https://www.mps.it>



UNIVERSITÀ DI PISA


Certification Practice Statement

Extensions:

- X509v3 **Basic Constraints:** CA:TRUE, pathlen:0
- X509v3 **Certificate Policies:**
 - Policy: 2.16.840.1.113733.1.7.1.1
 - CPS: <https://www.verisign.com/CPS>
- X509v3 **Extended Key Usage:** TLS Web Server Authentication, TLS Web Client Authentication, Netscape Server Gated Crypto, 2.16.840.1.113733.1.8.1
- X509v3 **Key Usage:** Certificate Sign, CRL Sign
- Netscape Cert Type:** SSL CA, S/MIME CA
- X509v3 **CRL Distribution Points:**
 - URI:<http://crl.verisign.com/pca3.crl>

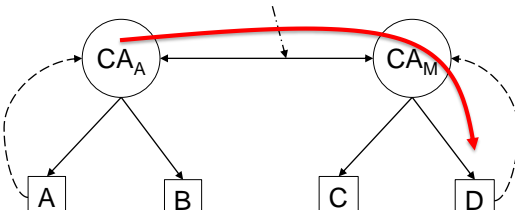
09/05/2018
Public Key Infrastructures
39

Cross-certification (enterprise model)



UNIVERSITÀ DI PISA

Cross-certification




Certification/Trust Chain
 $Cert_{CA_A}\{CA_M\}Cert_{CA_M}\{D\}$

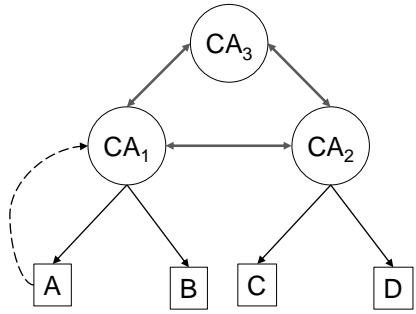
- Technology-wise is «easy»
- What about Legal implications?

09/05/2018
Public Key Infrastructures
42

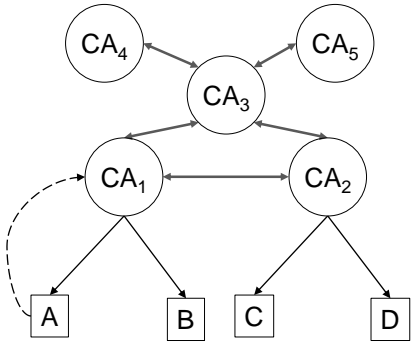
Enterprise model



UNIVERSITÀ DI PISA



Hub-and-spoke




Business requirements make certification complex

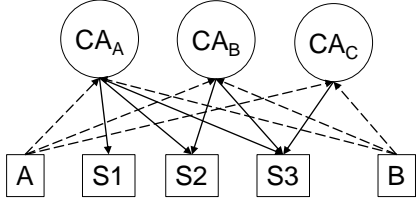
- No hierarchy anymore but mutual agreement
- Customers trust local CAs

09/05/2018
Public Key Infrastructures
43

Browser model



UNIVERSITÀ DI PISA



Trusted CA list in browsers

- More levels are possible
 - Subordinate CAs
- A user trusts **all** CAs in his browser
 - There are 650 CAs but many of them are related => 75

09/05/2018
Public Key Infrastructures
44

The CA Mess on the Web



UNIVERSITÀ DI PISA

- **Recommended reading**

- An Observatory for the SSLiverse, Peter Eckersley, Jesse Burns, [Defcon 18](#), Las Vegas, USA, July, 2010 ([pdf](#), [video](#))

09/05/2018

Public Key Infrastructures

45

Incidents



UNIVERSITÀ DI PISA

- March 2011 – Comodo
 - 9 fraudulent certs
- Summer 2011 – DigiNotar
 - 500+ fraudulent certs
 - [FOX-IT final report \(long\)](#)
 - [ENISA's resume \(short\)](#)
- January 2013 – Turktrust
 - 100+ fraudulent certs

09/05/2018

Public Key Infrastructures

46

Countermeasures (intuitions)



UNIVERSITÀ DI PISA

- Public key pinning
 - List of presumed-good CAs and list of known-good certs
 - Chrome
- Certificate transparency
 - To make public that a CA issued a cert
 - Resistance from business
- Convergence
 - Download a cert directly and from a set of trusted CAs and compare them
- DANE (DNS-based Authentication of Name Entities)
 - Store a pubK in a DNS record; require DNSSEC
- Extended Validation certificates
 - Prove the legal entity controlling the website or sw package...
 - ...promise what we were promised a decade ago and we never got ([The inevitable collapse of the certification model](#), Hagai Bar-EI)

09/05/2018

Public Key Infrastructures

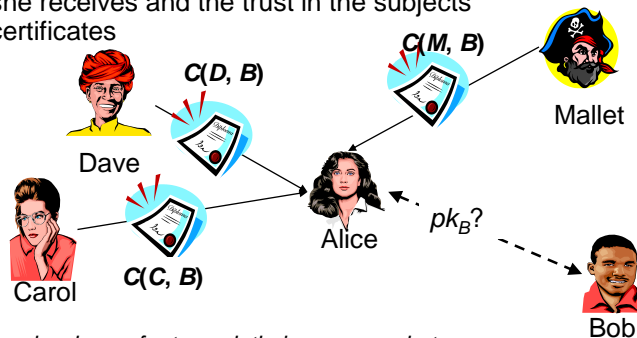
47

Personal trust model (PGP model)



UNIVERSITÀ DI PISA

- The user decides how much trust to put in a certificate
 - Alice determines the trust in pk_B according to the number of certificates she receives and the trust in the subjects issuing the certificates




PGP is for people who prefer to pack their own parachutes
[P. Zimmerman]

09/05/2018

Public Key Infrastructures

48



UNIVERSITÀ DI PISA


PGP model - Validity and trust level

- Trust level in a key
 - Own key
 - Implicit trust
 - Others' keys
 - Complete trust
 - Marginal trust
 - No trust

} *The user defines the trust to put in a key*

- A key may be
 - Valid
 - Marginally valid
 - Invalid
- A key is valid if it has been signed by a completely trusted key or by two marginally trusted keys

09/05/2018
Public Key Infrastructures
49



UNIVERSITÀ DI PISA

PGP vs X.509

- Number of signatures
 - X.509 – A key is signed just once
 - PGP – A key may be signed multiple time
- Trust level
 - X.509 – A certificate is implicitly associated to a certain trust level
 - Depend on the CA policy
 - PGP – Every signature is associated to an explicit trust level
 - Signatures on the same key may have different trust levels
 - The meaning of a trust level depend on the context

09/05/2018
Public Key Infrastructures
50

Personal Trust Model – PGP cons



UNIVERSITÀ DI PISA

- Hard to understand if you're not an expert
- Key revocation is a nightmare

09/05/2018

Public Key Infrastructures

51

Revocation options: OCSP




UNIVERSITÀ DI PISA

- CRL – offline
- OCSP – online
 - Online Certificate Status Protocol
- Protocol sketch
 - Alice -> OCSP: OCSP Request Bob's cert serial nr.
 - OCSP -> Alice: <OCSP Response OK|KO>_{OCSP}
- Protocol Pros
 - Lighter and simpler than CRL protocol
 - Effective if the adversary is not a MIM
- Protocol Cons
 - In the clear => confidentiality
 - Exposed to replay attack (nonces are an extension ☹)
 - Browsers silently ignore OCSP if the query times out (=>MIM)

09/05/2018

Public Key Infrastructures

52




UNIVERSITÀ DI PISA

Browser behaviour

- Idealized model
- Reality
 - Revocation is blocking information (latency)
 - What if revocation infrastructure is unreachable?
 - Browsers have been forced to ignore revocation information when unavailable
 - Types of server certificates
 - DV, OV => not checked by default
 - EV => checked but, if unavailable, response is browser-dep

[Defective By Design? - Certificate Revocation Behavior In Modern Browsers, SpiderLabs Blog, Apr. 4, 2011](#)

09/05/2018 Public Key Infrastructures 53



UNIVERSITÀ DI PISA

In-house or external CA?

- Implement your own CA or exploit a commercial one?
 - Cost-convenience ratio
 - High quality certification => high costs
 - Low quality certification => high risks
 - In-house
 - Pros – Complete control of the certification process
 - Cons – Cost of the infrastructure; limited scale
 - Commercial
 - Pros – Large scale
 - Cons – Trust delegation; no liability

09/05/2018 Public Key Infrastructures 56



09/05/2018

Public Key Infrastructures

58