SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security

Cryptography – Public Key Infrastructure

Lecture Twenty-two

Outline of Lecture

- Discussion of need for Public Key Infrastructure (PKI)
- Overview of technologies used in the implementation of PKI
- Digital certificates
- Digital certificate lifecycle
- Relevant PKI standards

Learning goals

- You should be able to explain
  - why we need PKI
  - what PKI is
  - what the main components of PKI are
  - what a digital certificate is
  - the digital certificate lifecycle
  - relevant PKI standards

Public Key Infrastructure

- Public key encryption solves the problem of securely communicating over an insecure channel with a party we have never communicated with before
- BUT still problem of linking identity to the key
  - How do you know who you are communicating with?
  - How do you know you are dealing with the real Amazon.com and not a spoofed website?
  - How can you implement some form of non-repudiation?
- Goal of PKI
  - reliably link the name of an organisation or person to a public key
  - make that linkage information available
  - be able to trust a public key without ever having had contact with its owner

PKI and digital signatures

- PKI relies on digital signatures
- Different entities issue and make use of Digital Certificates
- Digital Certificates contain an entity's public key (amongst other information)
- The Digital Certificate is digitally signed
- Digital signatures
  - Take a hash of digital data
  - Use private key to encrypt it
  - A digital signature
- Anyone with your public key can decrypt the data
  - Shows that you must have encrypted it

Certificate Authority

- A trusted third party who signs a digital certificate that contains an organisation or person's public key
- Examples of Certificate authorities are:
  - Specialist companies such as Verisign and Thawte who sell certificates used mainly to verify the identity of websites
  - Some banks and government departments who issue certificates to their customers to allow them to access services
  - Organisations who issue certificates to their employees to allow them to access corporate systems and services (perhaps through a VPN)

Trusted 3rd parties in IE

- Online trusted 3rd parties in Internet Explorer can be viewed by
  - Tools (* button) > Internet Options
  - Content tab > certificate
  - Trusted root certification authorities
- Your browser trusts digital certificates it receives so long as the certificate or intermediate certificates have been signed by one of the Certificate authorities in this list

Digital certificates

- A digitally signed data structure that contains a public key and the name of its owner
- The entity who signs the certificate guarantees (to some level) that the owner of the key is the person or organisation named in the certificate
- Main format of digital key is X.509
  - X.509 an ANSI standard
- Use in Internet is defined in IETF RFC 2459 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”
- IETF group developed PKI X.509 standards (PKIX)

Digital certificate

Version	Serial number	Signature algorithm	Issuer	Validity	Subject	Subject public key info	Issuer Unique ID	Subject Unique ID	Extens-ions	Signature algorithm	Signatur

Digital Certificate field (from technet.Microsoft.com)

Certificate Field	Description
Version	Version of the certificate format; for example, version 3.
Certificate Serial Number	The unique serial number that is assigned by the issuing CA. The CA maintains an audit history for each certificate so that certificates can be traced by their serial numbers. Revoked certificates also can be traced by their serial numbers.
Certificate Algorithm Identifier	The public key cryptography and message digest algorithms that are used by the issuing CA to digitally sign the certificate.
Issuer	The name of the issuing CA. The name can be listed in one or more of the following formats: X.500 directory name, Internet e-mail address, fully qualified domain name (FQDN), X.400 e-mail address, and URL.
Validity Period	The certificate's start and expiration dates. These define the interval during which the certificate is valid, although the certificate can be revoked before the designated expiration date.
Subject	The name of the subject (owner) of the certificate. The name can be listed in one or more of the following formats: X.500 directory name, Internet e-mail address, fully qualified domain name (FQDN), X.400 e-mail address, and URL.
Subject Public-Key Information	The public key and a list of the public key cryptography algorithms. The algorithms are for the tasks for which the public key set can be used, such as digital signing, secret key encryption, and authentication.
Issuer Unique Identifier	Optional information for uniquely identifying the issuer, when necessary.
Subject Unique Identifier	Optional information for uniquely identifying the subject, when necessary.
Extensions	Additional information that can be specified for optional use by public key infrastructures. Common extensions include a list of specific uses for certificates (for example, S/MIME secure mail or IPSec authentication), CA trust relationship and hierarchy information, a list of publication points for revocation lists, and a list of additional attributes for the issuer and subject.
Certification Authority's Digital Signature	The CA's digital signature, which is created as the last step in generating the certificate.

Digital certificate fields

- Version
  - Usually version 3 X.509.v3
- Serial Number
  - Unique integer identifier for the certificate
- Signature Algorithm
  - Algorithm id used to sign the certificate
- Issuer
  - Unique name of certificate issuer
- Validity
  - Not Before
  - Not After

Digital certificate fields

- Subject
  - Unique name of the owner (Distinguished Name)
- Subject Public Key Info
  - Public Key Algorithm
    - Algorithm used to generate the public key
  - Subject Public Key
    - The public key
- Issuer Unique Identifier (Optional)
  - Not used
- Subject Unique Identifier (Optional)
  - Not used

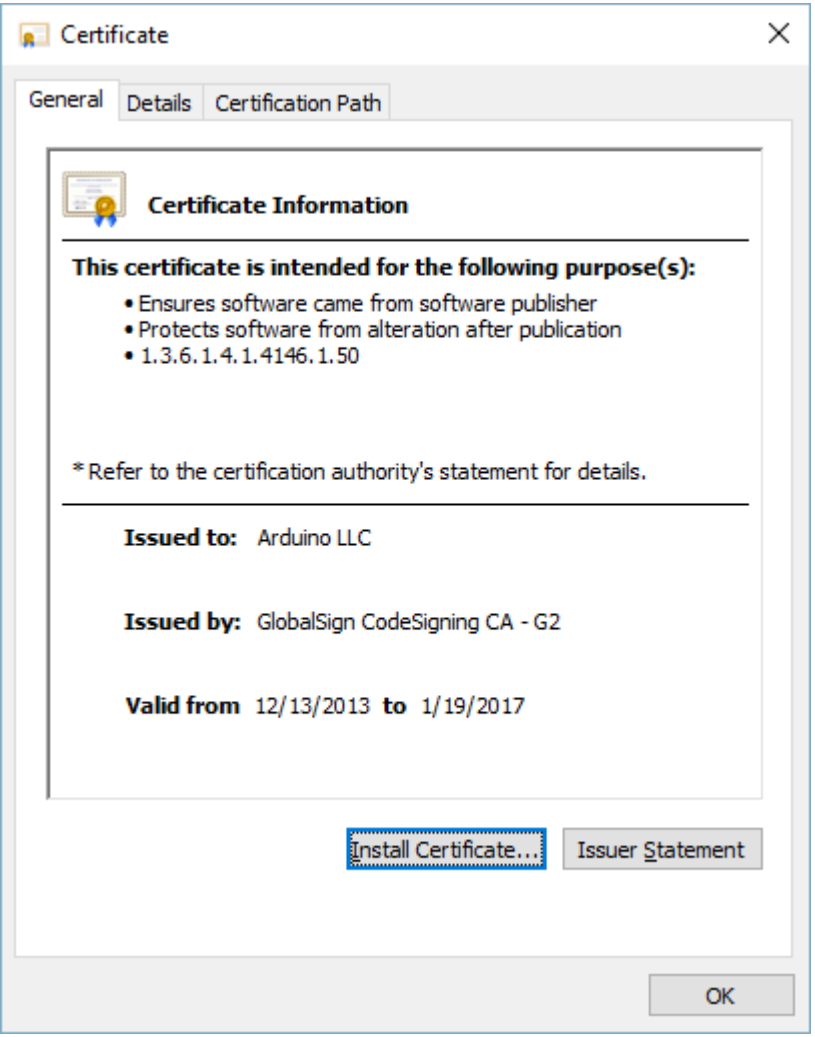
Digital certificate fields

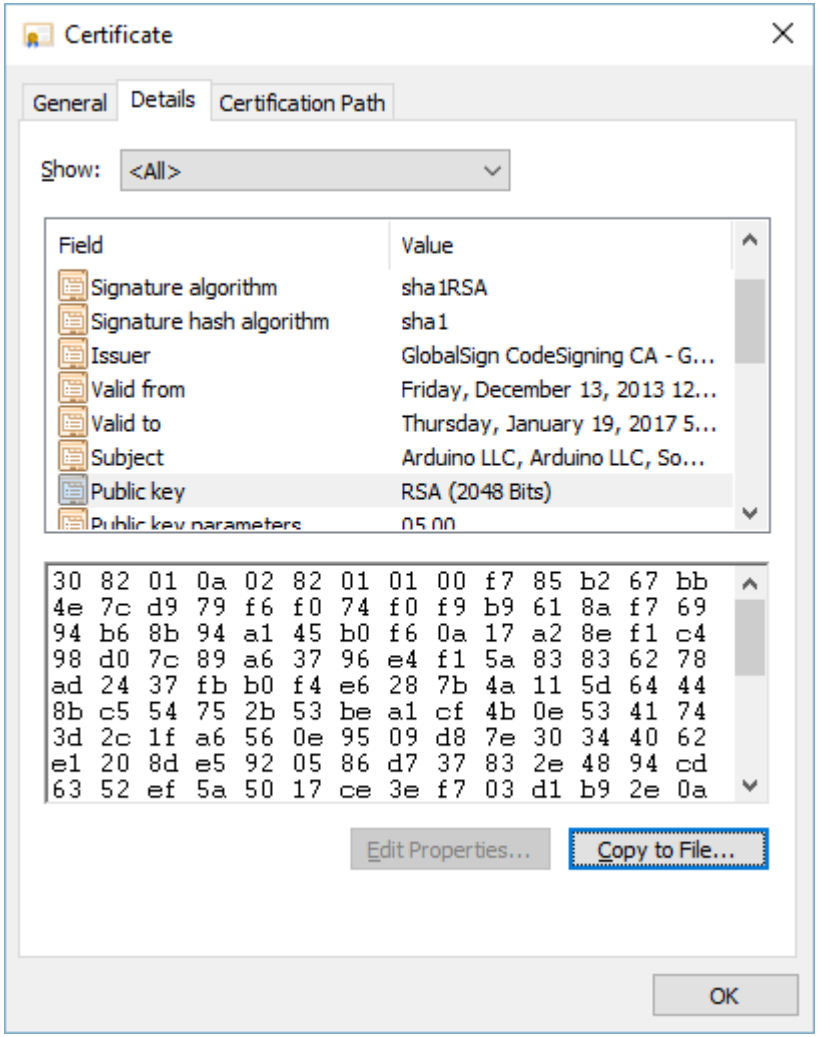
- Extensions (Optional)
  - Many optional fields specifying the purpose of the key, revocation information, policies and other information
- Certificate Signature Algorithm
  - How the signature was constructed
    - Usually a hash and an encryption algorithm
      - SHA-1 and RSA encryption
- Certificate Signature
  - The digital signature of the certificate

Sample digital certificate

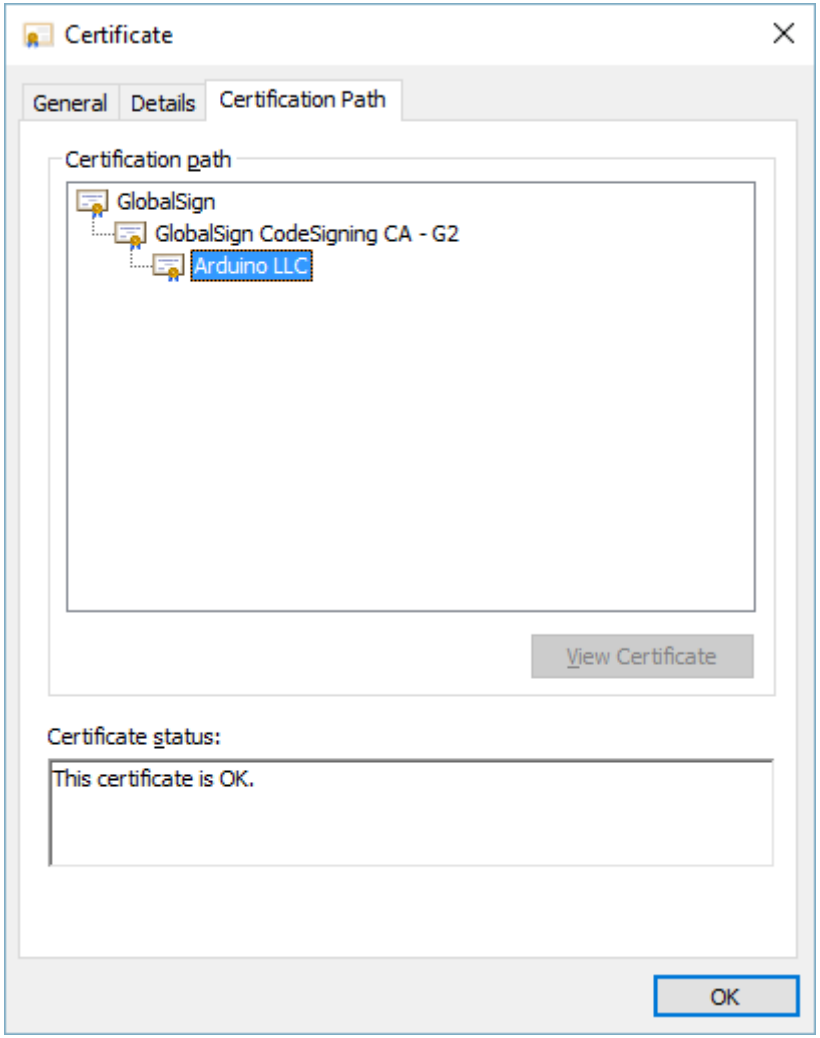
```
Version: V3
Serial number: 11 21 63 d5 cf 47 2f 1f e8 09 34 23 64 d5 26 10 ae cb
Signature algorithm: sha1RSA
Signature hash algorithm: sha1
Issuer:
  CN = GlobalSign CodeSigning CA - G2
  O = GlobalSign nv-sa
  C = BE
Valid from: Friday, December 13, 2013 12:25:31 AM
Valid to: Thursday, January 19, 2017 5:46:35 AM
Subject:
  CN = Arduino LLC
  O = Arduino LLC
  L = Somerville
  S = Massachusetts
  C = US
Public key:
30 82 01 0a 02 82 01 01 00 f7 85 b2 67 bb 4e 7c d9 79 f6 f0 74 f0 f9 b9 61 8a f7 69 94 b6 8b 94 a1 45
b0 f6 0a 17 a2 8e f1 c4 98 d0 7c 89 a6 37 96 e4 f1 5a 83 83 62 78 ad 24 37 fb b0 f4 e6 28 7b 4a 11 5d
64 44 8b c5 54 75 2b 53 be a1 cf 4b 0e 53 41 74 3d 2c 1f a6 56 0e 95 09 d8 7e 30 34 40 62 e1 20 8d e5
92 05 86 d7 37 83 2e 48 94 cd 63 52 ef 5a 50 17 ce 3e f7 03 d1 b9 2e 0a a7 ee 2e 8c f3 e8 2a 93 4f a4
eb e1 bc e9 ae 50 74 b8 f2 c7 9e 1f 4b 0f d3 d0 07 ef d1 73 dd 67 f0 cf 5f 2f 1f 6d d1 fe 00 32 48 80
61 cb 53 98 76 7d 9a b8 ae c3 9a 0c a8 c7 1a 78 50 7b 54 c5 a4 02 51 35 93 c6 d6 79 34 2a 53 b2 a9 62
9b 26 20 03 e1 21 c1 11 51 c0 ac 29 1c 8b ac 4f 23 1c 34 52 c5 ba 00 10 cb 0f 14 79 df 8f ec df e3 07
d0 ac 8a fa 57 55 99 9b 8e 96 c0 4d 0a ec de 40 79 28 6e b8 49 3b 7a 4f 5b 6a 67 02 03 01 00 01
Public key parameters: 05 00
Optional parameters: (not listed)
Digital signature:
  Thumbprint algorithm: sha1
  Thumbprint: 4d 1a 55 90 11 74 2e ba 43 f0 3a d8 83 5e 54 3c 3f f8 a2 2a
```

Sample digital certificate





Sample digital certificate



Public Key Infrastructure

- PKI provides trusted and authenticated public key distribution
- Components of PKI
  - Certificate authority
  - Certificate repository
  - Certificate revocation
  - Key backup and recovery
  - Automatic key update
  - Key history
  - Cross certification
  - Support for non-repudiation
  - Time stamping
  - Client software

PKI solutions

- Authentication
  - The assurance that an entity is who he/she/it claims to be
- Non repudiation
  - Signatory to a digital document cannot later deny they signed
- Integrity
  - The assurance of non-alteration
- Confidentiality
  - The assurance of data privacy

PKI services

- Secure communication
- Secure timestamping
- Notarization
- Non-repudiation
  - relies on other services (secure time stamping) and secure archival
- Privilege management
  - authorisation, access control

PKI mechanisms

- Digital signatures, Hashes, MACs and ciphers
- Trusted time sources
- Privilege processing mechanisms

Certification and registration authority

- Certificate issuance and registration are often separate
- Certificate authority (or certification authority) (CA)
  - Issues digital certificates
- Registration authority (RA)
  - validates the user requesting the certificate
  - might be (or make use of) a business consultancy firm such as Dun and Bradstreet
  - might be a domain name service
  - might be a corporation who requests a CA to issue certificates to their customers
    - eg. a Bank

Certificate lifecycle

- A certificate has a limited life
  - usually 1 to 5 years
    - about the same length of time we can reasonably expect a key to remain uncompromised
- Life cycle of a certificate
  - Initialisation
  - Issuance
  - Cancellation

Certificate initialisation

- End-entity registration
  - End user registers their name with whatever process is appropriate
- Key pair generation
  - End user generates a private / public key pair
- Certificate creation
  - CA uses public key to generate certificate
- Certificate distribution
  - Certificate is sent to end-entity
- Certificate dissemination
  - End-entity (or CA) distributes certificate to other entities

Issuance

- Certificate is in regular use
- Certificate is retrieved
  - Entity wishes to make use of the certificate
    - Needs to obtain it from a certificate repository or the certificate owner
- Certificate is validated
  - End-user needs to check on the validity of the certificate
- Key is recovered
  - Public key is extracted from the certificate as needed
- Key is updated
  - End of life an automatic key pair generation can be issued

Cancellation

- Certificate expiration
  - natural expiry of the ticket
  - Certificate renewal
    - Same public key can be put into a new certificate
  - Certificate update
    - New key and new certificate
      - Should be part of Issuance
- Certificate revocation
  - action before natural expiry to revoke certificate
    - certificate compromised, end-entity defunct etc
- Key history and key archive
  - necessary to maintain key history so that encrypted and signed documents can be read after the certificate has expired

Certificate revocation

- Certificates sometimes need to be cancelled before their natural expiry date
- Certificates that have been revoked are recorded on a Certificate Revocation List (CRL) contained within the CA
- Access to the CRL can be via an online query protocol
  - Online Certificate Status Protocol (OCSP)

Different kinds of CRLS

- Complete CRLS
  - List of all certificates issued by this CA that have been revoked
- Authority Revocation Lists
  - List of certificates revoked by a higher CA
- Delta CRLs
  - Increment in CRL lists
- Others

Trust models

- Which certificates can you trust?
- How can trust be established?
- Under what circumstances and to what extent is this trust appropriate?

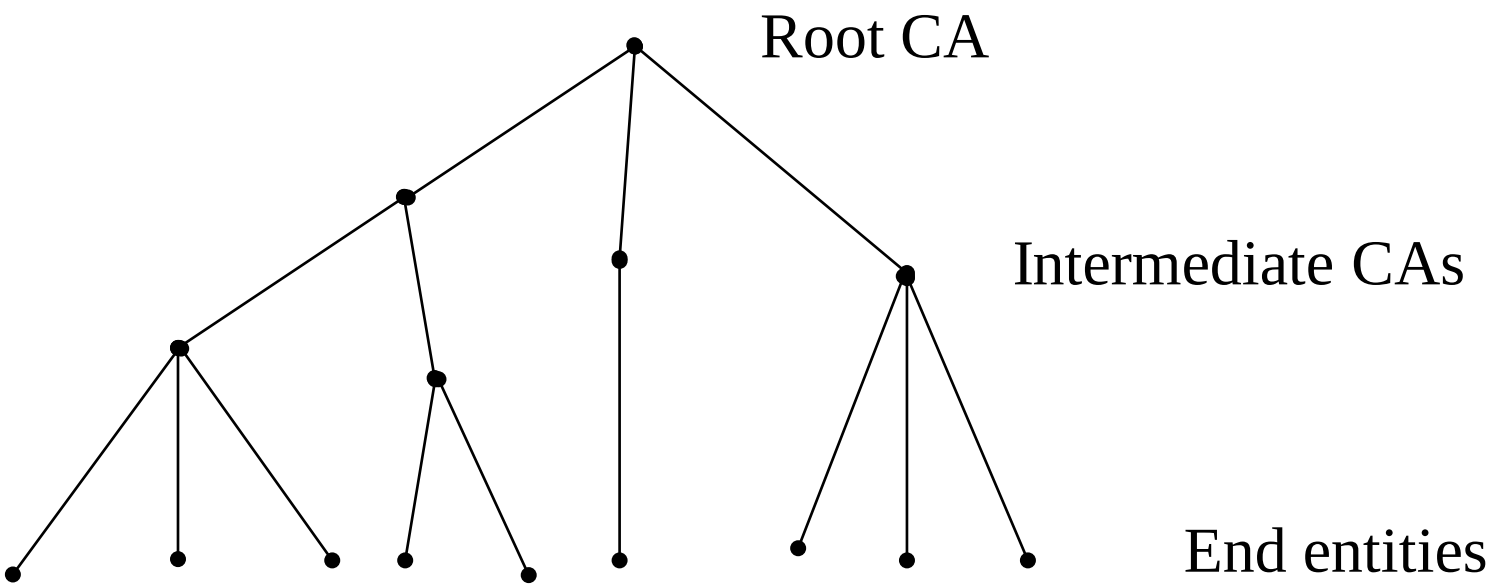
Trust models

- Not all certificates originate from the one source
- If we set up a website here in Melbourne to sell something we will probably use a local supplier of certificates
  - eg Verisign Australia
    - They know the appropriate local procedures for issuing a certificate
- However, we would like people from anywhere in the world to be able to use our website
  - We need them to be able to trust our server certificate

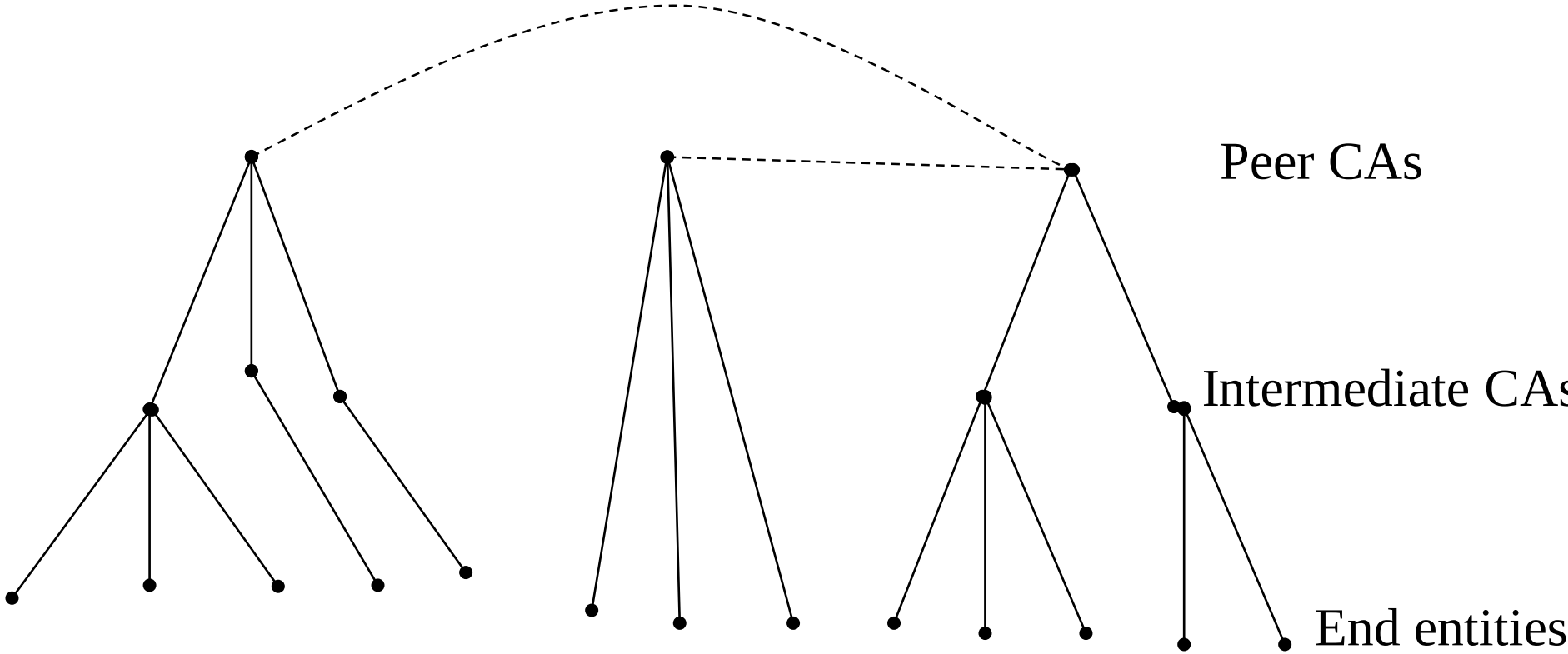
Different approaches to Trust in PKI

- Different networks of trust
- Strict hierarchy of Certification Authorities
  - An inverted tree with the root at the top
  - All entities in the tree trust the root
- Distributed trust architecture
  - Trust is distributed between multiple roots
  - Users roots trust each other
- Web model
  - multiple root CAs installed in the browser
  - Web browser implicitly trusts all the Root CAs installed in their browser
- Mesh, hub and spoke

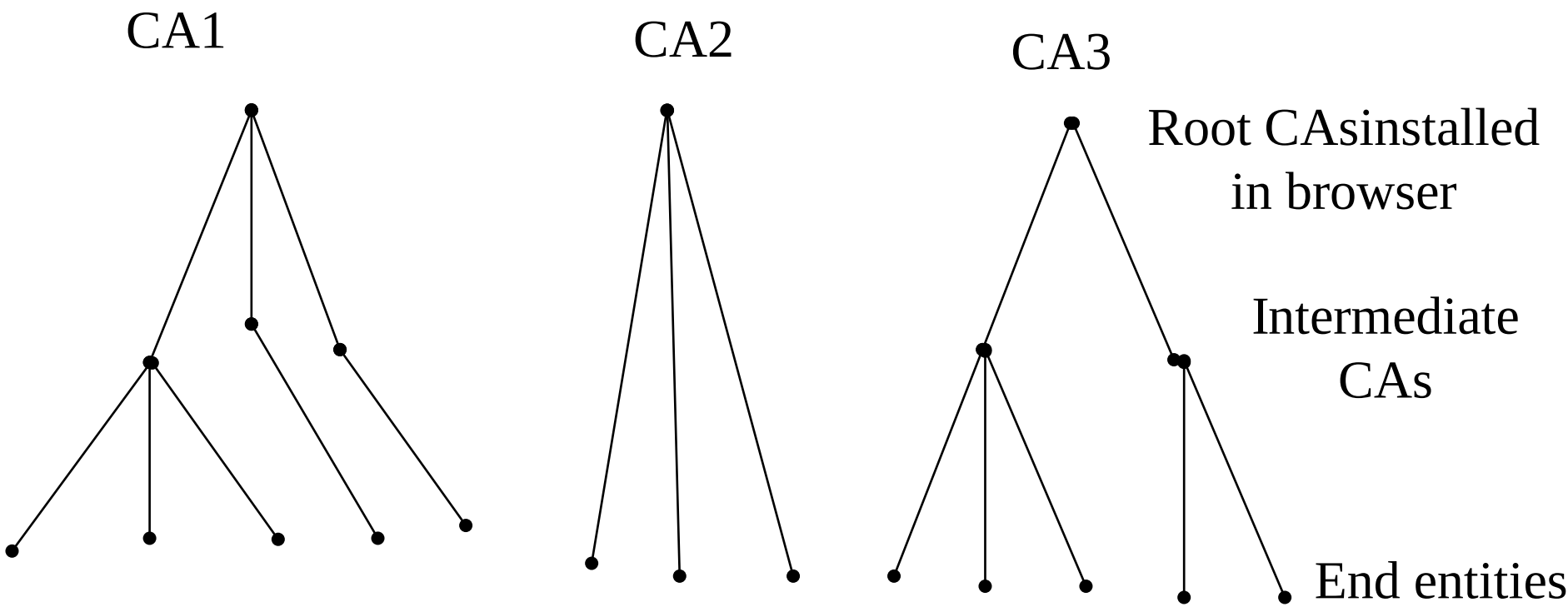
Strict hierarchy of CAs trust model



Distributed trust architecture



Web model


CA1
CA2
CA3
Root CAsinstalled in browser
Intermediate CAs
End entities

Certificate path processing

- Goal is to find an unbroken path of certificates between a given target and a trusted key
- Need to aggregate certificates to form a complete path
- Then validate each certificate in the path in turn to determine whether or not it can be trusted to the appropriate level

PKI information dissemination

- How do we distribute certificates?
- Private dissemination
  - hand delivery
  - delivery as an attachment to an email
- Repositories
  - LDAP servers
  - X.500 directory system agents (DSAs)
  - OCSP (revocation information only)
  - DNS can support certificate information (RFC 2583)
  - Web servers can support dissemination of certificate information (RFC2585)
  - FTP, corporate databases

PKI standards

- X.509
  - Defines certificate format and PKI entities
- PKIX
  - Developed by RSA
  - All RFCs
  - Specifies X.509v3 protocols
  - Operational protocols
  - Management protocols
  - Certificate policies

PKI standards

- X.500
  - Directory services
- LDAP
  - Light weight directory services
  - Originally intended as a simple subset of X.500
- ISO TC68
  - Financial industry PKI
- S/MIME
  - Industry consortium
  - S/MIME v3 incorporates X.509v3 certificates
- IPSec, TLS, DNSSec, OpenPGP all support X.509v3 certificate and PKI

Conclusion

- PKI
  - Overview of technologies
  - Digital certificates
- Digital certificate lifecycle
- Relevant PKI standards