Public Key Infrastructure

Public Key Infrastructure

Motivation:

1. Numerous people buy/sell over the internet – hard to manage security of all possible pairs of connections with secret keys
2. US government subject to the Government Paperwork Elimination Act requiring electronic transactions with the public (from 2003)
3. Agencies are required to use electronic authentication technology to verify identity of the sender and the integrity of electronic content
4. This is especially important when doing classified work or working with contractors who do classified work
5. The Health Insurance Portability and Accountability Act of 1996 mandates security and privacy standards to protect health information that is exchanged electronically.

Public Key Infrastructure

A PKI:

1. binds public keys to entities
2. enables other entities to verify public key bindings
3. provides services for management of keys in a distributed system

Public Key Infrastructure

A PKI:

1. binds public keys to entities
2. enables other entities to verify public key bindings
3. provides services for management of keys in a distributed system

Goal:

protect and distribute information that is needed in a widely distributed environment, where the users, resources and stake-holders may all be in *different places* at different times

Public Key Infrastructure

A PKI:

1. binds public keys to entities
2. enables other entities to verify public key bindings
3. provides services for management of keys in a distributed system

Goal:

protect and distribute information that is needed in a widely distributed environment, where the users, resources and stake-holders may all be in *different places* at different times

Provides:

1. Data integrity
2. Data confidentiality
3. Authentication

Public Key Infrastructure

A PKI:

1. binds public keys to entities
2. enables other entities to verify public key bindings
3. provides services for management of keys in a distributed system

Goal:

protect and distribute information that is needed in a widely distributed environment, where the users, resources and stake-holders may all be in *different places* at different times

Provides:

1. Data integrity
2. Data confidentiality
3. Authentication

Integrates:

1. Digital certificates
2. Public key cryptography
3. Certification authorities

for an enterprise-wide network security architecture

Public Key Infrastructure

Components:

1. Certification Authority
   - issues certificates of ownership of a public key by named entity

Public Key Infrastructure

Components:

1. Certification Authority
   - issues certificates of ownership of a public key by named entity
2. Registration Authority
   - trusted by a CA to register or vouch for users of the CA
   - verifies user requests for a digital certificate and tells the CA to issue it

Public Key Infrastructure

Components:

1. Certification Authority
   - issues certificates of ownership of a public key by named entity
2. Registration Authority
   - trusted by a CA to register or vouch for users of the CA
   - verifies user requests for a digital certificate and tells the CA to issue it
3. Repository
   - database of active digital certificates for a CA
   - provides data that allows users to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages

Public Key Infrastructure

Components:

1. Certification Authority
   - issues certificates of ownership of a public key by named entity
2. Registration Authority
   - trusted by a CA to register or vouch for users of the CA
   - verifies user requests for a digital certificate and tells the CA to issue it
3. Repository
   - database of active digital certificates for a CA
   - provides data that allows users to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages
4. Archive
   - to store and protect sufficient information to determine if a digital signature on an "old" document should be trusted

Public Key Infrastructure

Components:

1. Certification Authority
   - issues certificates of ownership of a public key by named entity
2. Registration Authority
   - trusted by a CA to register or vouch for users of the CA
3. Repository
   - database of active digital certificates for a CA
   - confirm status of digital certificates for individuals and businesses
4. Archive
   - to store and protect sufficient information to determine if a digital signature on an "old" document should be trusted
5. Certificates
   - includes public key, information about the identity of the party holding the corresponding private key, the operational period for the certificate, and the CA's own digital signature
   - may contain other information about the signing party or information about the recommended uses for the public key

Public Key Infrastructure

X.509 certificate standard:

- version
- serial number
- algorithm ID
- issuer
- validity – not before, not after
- subject
- subject key key info – algorithm and public key
- extensions
  - basic constraints – includes public
  - key usage – crypto operations that key can be used for
    Ex: signing but not encryption
  - extended key usage – indicates allowed usage per application
    Ex: may be used on the server end of a TLS connection
    may be used to protect email
- certificate signature algorithm
- certificate signature

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI
2. Collection of hardware, software, and people who operate it

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI
2. Collection of hardware, software, and people who operate it
3. Performs four basic PKI functions:
   - issues certificates (creates and signs them)
   - maintains certificate status information and issues CRLs
   - publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services
   - maintains archives of status information about the expired certificates that it issued

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI
2. Collection of hardware, software, and people who operate it
3. Performs four basic PKI functions:
   - issues certificates (creates and signs them)
   - maintains certificate status information and issues CRLs
   - publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services
   - maintains archives of status information about the expired certificates that it issued
4. May delegate some functions to other components of the PKI

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI
2. Collection of hardware, software, and people who operate it
3. Performs four basic PKI functions:
   - issues certificates (creates and signs them)
   - maintains certificate status information and issues CRLs
   - publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services
   - maintains archives of status information about the expired certificates that it issued
4. May delegate some functions to other components of the PKI
5. By creating a certificate, CA asserts the subject of the certificate has the private key associated with the public key of the certificate

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI
2. Collection of hardware, software, and people who operate it
3. Performs four basic PKI functions:
   - issues certificates (creates and signs them)
   - maintains certificate status information and issues CRLs
   - publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services
   - maintains archives of status information about the expired certificates that it issued
4. May delegate some functions to other components of the PKI
5. By creating a certificate, CA asserts the subject of the certificate has the private key associated with the public key of the certificate
6. May assert that certificates issued by other CAs are trustworthy

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI
2. Collection of hardware, software, and people who operate it
3. Performs four basic PKI functions:
   - issues certificates (creates and signs them)
   - maintains certificate status information and issues CRLs
   - publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services
   - maintains archives of status information about the expired certificates that it issued
4. May delegate some functions to other components of the PKI
5. By creating a certificate, CA asserts the subject of the certificate has the private key associated with the public key of the certificate
6. May assert that certificates issued by other CAs are trustworthy
7. Signs every certificate

Public Key Infrastructure

Certification Authority:

1. Basic building block of the PKI
2. Collection of hardware, software, and people who operate it
3. Performs four basic PKI functions:
   - issues certificates (creates and signs them)
   - maintains certificate status information and issues CRLs
   - publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services
   - maintains archives of status information about the expired certificates that it issued
4. May delegate some functions to other components of the PKI
5. By creating a certificate, CA asserts the subject of the certificate has the private key associated with the public key of the certificate
6. May assert that certificates issued by other CAs are trustworthy
7. Signs every certificate
8. CA *must* provide adequate protection for its own private key

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert
   - examples (credit card company):
      a. drivers license
      b. recent pay stub
      c. data from a company's human resources department
      d. letter from a company official

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert
   - examples (credit card company):
     a. drivers license
     b. recent pay stub
     c. data from a company's human resources department
     d. letter from a company official
2. Information is collected and sent to the CA

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert
   - examples (credit card company):
     a. drivers license
     b. recent pay stub
     c. data from a company's human resources department
     d. letter from a company official
2. Information is collected and sent to the CA
3. Usually operated by a single person (CA is larger)

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert
   - examples (credit card company):
     a. drivers license
     b. recent pay stub
     c. data from a company's human resources department
     d. letter from a company official
2. Information is collected and sent to the CA
3. Usually operated by a single person (CA is larger)
4. A CA maintains a list of trusted (accredited) RAs

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert
   - examples (credit card company):
     a. drivers license
     b. recent pay stub
     c. data from a company's human resources department
     d. letter from a company official
2. Information is collected and sent to the CA
3. Usually operated by a single person (CA is larger)
4. A CA maintains a list of trusted (accredited) RAs
5. Is known to the CA by a name and public key

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert
   - examples (credit card company):
     a. drivers license
     b. recent pay stub
     c. data from a company's human resources department
     d. letter from a company official
2. Information is collected and sent to the CA
3. Usually operated by a single person (CA is larger)
4. A CA maintains a list of trusted (accredited) RAs
5. Is known to the CA by a name and public key
6. By verifying RA's signature, CA is sure info obtained is reliable

Public Key Infrastructure

Registration Authority:

1. Verify certificate contents for the CA
   - certificate contents can represent info presented by requester of cert
   - examples (credit card company):
     a. drivers license
     b. recent pay stub
     c. data from a company's human resources department
     d. letter from a company official
2. Information is collected and sent to the CA
3. Usually operated by a single person (CA is larger)
4. A CA maintains a list of trusted (accredited) RAs
5. Is known to the CA by a name and public key
6. By verifying RA's signature, CA is sure info obtained is reliable
7. RAs must provide adequate protection for their private keys

Public Key Infrastructure

Repositories:

1. Directory service for distribution of certificates and certificate status
   - provides means of storing and distributing certificates
   - manages updates to certificates
   - typically implementations of the X.500 standard

Public Key Infrastructure

Repositories:

1. Directory service for distribution of certificates and certificate status
   - provides means of storing and distributing certificates
   - manages updates to certificates
   - typically implementations of the X.500 standard
2. Directory servers work across international, company, system borders

Public Key Infrastructure

Repositories:

1. Directory service for distribution of certificates and certificate status
   - provides means of storing and distributing certificates
   - manages updates to certificates
   - typically implementations of the X.500 standard
2. Directory servers work across international, company, system borders
3. Suite of protocols is specified for different kinds of services needed in server-to-server communication
   - chaining
   - shadowing (replication, say near certificate expiration)
   - referral (if server cannot satisfy the request)

Public Key Infrastructure

Repositories:

1. Directory service for distribution of certificates and certificate status
   - provides means of storing and distributing certificates
   - manages updates to certificates
   - typically implementations of the X.500 standard
2. Directory servers work across international, company, system borders
3. Suite of protocols is specified for different kinds of services needed in server-to-server communication
   - chaining
   - shadowing (replication, say near certificate expiration)
   - referral (if server cannot satisfy the request)
4. Lightweight Directory Access Protocol (LDAP) for client-server communications

Public Key Infrastructure

Repositories:

1. Directory service for distribution of certificates and certificate status
   - provides means of storing and distributing certificates
   - manages updates to certificates
   - typically implementations of the X.500 standard
2. Directory servers work across international, company, system borders
3. Suite of protocols is specified for different kinds of services needed in server-to-server communication
   - chaining
   - shadowing (replication, say near certificate expiration)
   - referral (if server cannot satisfy the request)
4. Lightweight Directory Access Protocol (LDAP) for client-server communications
5. Directory servers need to be *interoperable* to be able to retrieve CRLs and certificates from remote sites for signature verification

Public Key Infrastructure

Archives:

1. Accepts responsibility for long term storage of data needed by CA

Public Key Infrastructure

Archives:

1. Accepts responsibility for long term storage of data needed by CA
2. Asserts information is good at the time it is received and has not been modified since it entered the archive

Public Key Infrastructure

Archives:

1. Accepts responsibility for long term storage of data needed by CA
2. Asserts information is good at the time it is received and has not been modified since it entered the archive
3. Information provided by the CA to the archive must be sufficient to determine if a certificate was actually issued by the CA as specified in the certificate, and valid at that time.

Public Key Infrastructure

Archives:

1. Accepts responsibility for long term storage of data needed by CA
2. Asserts information is good at the time it is received and has not been modified since it entered the archive
3. Information provided by the CA to the archive must be sufficient to determine if a certificate was actually issued by the CA as specified in the certificate, and valid at that time.
4. The archive protects that information through technical mechanisms and appropriate procedures while in its care.

Public Key Infrastructure

Archives:

1. Accepts responsibility for long term storage of data needed by CA
2. Asserts information is good at the time it is received and has not been modified since it entered the archive
3. Information provided by the CA to the archive must be sufficient to determine if a certificate was actually issued by the CA as specified in the certificate, and valid at that time.
4. The archive protects that information through technical mechanisms and appropriate procedures while in its care.
5. If a dispute arises at a later date, the information can be used to verify that the private key associated with the certificate was used to sign a document.

Public Key Infrastructure

Archives:

1. Accepts responsibility for long term storage of data needed by CA
2. Asserts information is good at the time it is received and has not been modified since it entered the archive
3. Information provided by the CA to the archive must be sufficient to determine if a certificate was actually issued by the CA as specified in the certificate, and valid at that time.
4. The archive protects that information through technical mechanisms and appropriate procedures while in its care.
5. If a dispute arises at a later date, the information can be used to verify that the private key associated with the certificate was used to sign a document.
6. This permits the verification of signatures on old documents (such as wills) at a later date.

Public Key Infrastructure

Trust Models:

Monopoly model: One organization is trusted by all others to issue certificates. All software contains public key of that CA

Monopoly + Registration Authorities: Use other organizations to check identities and vouch for public keys

Delegated CAs: Trust anchor (TA) issues certificates to other CAs. Users can get a certificate from one of the other CAs.

Oligarchy (Browsers): Many trust anchors, certificate from one is sufficient

Anarchy (PGP): Each user responsible for configuring TAs.

Public Key Infrastructure

Monopoly:

There is no one universally trusted organization
Infeasible to change the key in all software if it is compromised
CA could charge whatever it wants to issue certificates

Monopoly + RAs:

More convenient than above – many places to get certified

Delegated CAs:

Recipient may see a chain of certificates vs. one for Mon+RAs

Oligarchy (e.g. browsers):

Worse than monopoly since *any* of trust anchors could be comp.
Trust anchors may be trusted by vendor but not user!
It is easy to trick a naive user into accepting a bogus trust anchor
Users do not understand what's up: ex: use of public terminal
Unlikely a user will check trust anchor list to see if it's tampered

Anarchy (PGP):

Trust of a single certificate varies so create a trust score from several then make a decision

Public Key Infrastructure

Name Constraints:

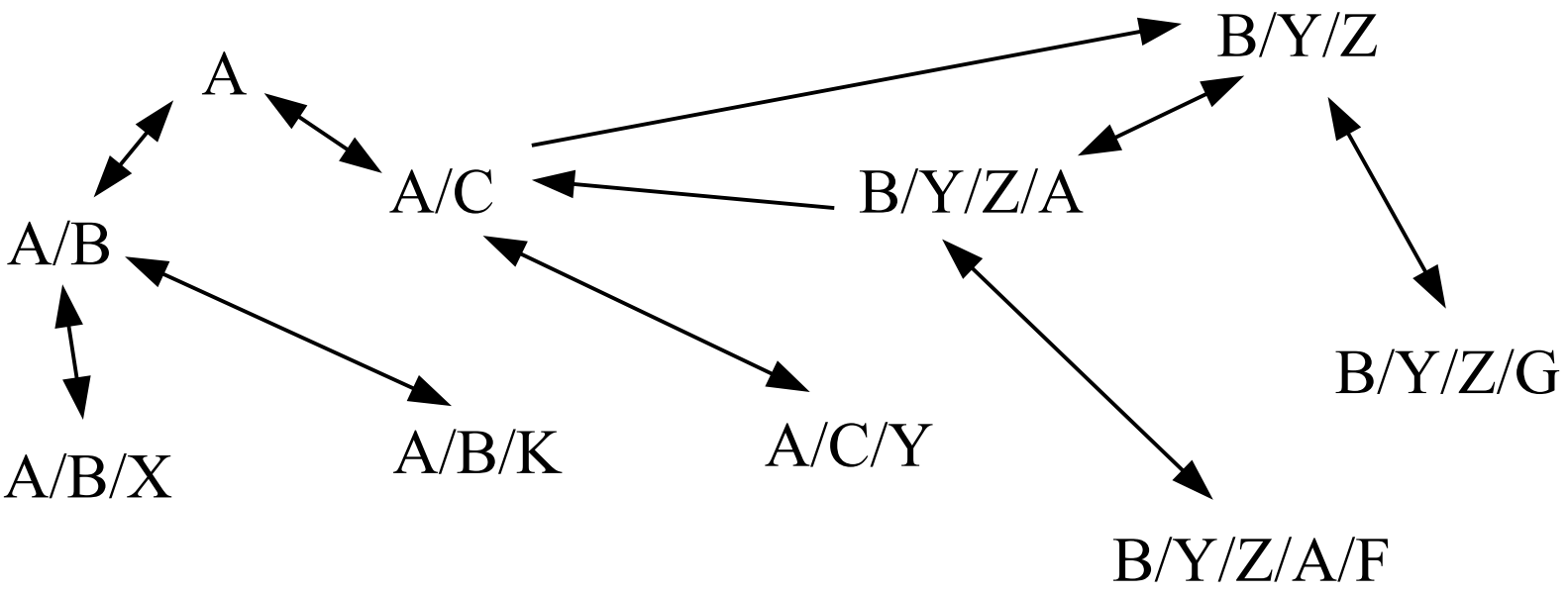
Assume CA trusted to issue certs for only some users or domains

Top-Down with Name Constraints:

Tree of CAs, each can only issue certs in their domain.

Bottom-Up with Name Constraints:

Each org creates its own PKI and links to the WWW of PKIs



Public Key Infrastructure

Top-Down with Name Constraints:

Like Monopoly with delegated CAs where delegates are restricted to parts of the name hierachy

Public Key Infrastructure

Bottom-Up with Name Constraints:

1. Easy to determine whether path exists
2. Hierarchy corresponding to the name of the principal is intuitive
3. PKI can be deployed in any org, no need to pay someone to do it
   Can have a PKI in your org even if lots of other orgs do not
4. Damage due to compromised CA is limited to that org
   No one can impersonate you from a compromised CA outside of your org
5. Configuration is easy: all CAs can be reached beginning with your key pair - new employee gets a key just like a badge

Public Key Infrastructure

Relative Names:

Certificates carry relative names, not absolute names
e.g. Use *cs* instead of *cs.uc.edu*

If an entire subtree of names has to be moved, no certificates need to be reissued

Do not use name A/B/C/D but only D on certificates from A/B/C - then if that moves to H/Y, say, only certificates between H/Y and ancestors need be reissued.

Public Key Infrastructure

Relative Names:

Certificates carry relative names, not absolute names
e.g. Use *cs* instead of *cs.uc.edu*

If an entire subtree of names has to be moved, no certificates need to be reissued

Do not use name A/B/C/D but only D on certificates from A/B/C - then if that moves to H/Y, say, only certificates between H/Y and ancestors need be reissued.

Name Constraints in Certificates:

Field in certificate stating names

Allows issuer to specify names that subject is trusted to certify

Can also disallow names.

Public Key Infrastructure

Policies in Certificates:

Statement of how carefully the identity of requester is checked.
If not obeyed, no certificate is issued.
Can deny certificates to users not at high level of security.

Example of policy: certificate can be used only for signing

Public Key Infrastructure

Expiration and Revocation:

Revocation important – someone may realize their key is stolen.

Public Key Infrastructure

Expiration and Revocation:

Revocation important – someone may realize their key is stolen.

Expiration important – many orgs do not bother with revocation
companies collecting money for issuing certs want to issue
lots of them

Public Key Infrastructure

Expiration and Revocation:

Revocation important – someone may realize their key is stolen.

Expiration important – many orgs do not bother with revocation
companies collecting money for issuing certs want to issue
lots of them

If certificates of web service providers expire or are revoked, then
new ones have to be issued - thus, down time

Public Key Infrastructure

Expiration and Revocation:

Revocation important – someone may realize their key is stolen.

Expiration important – many orgs do not bother with revocation
companies collecting money for issuing certs want to issue lots of them

If certificates of web service providers expire or are revoked, then new ones have to be issued - thus, down time

So, browsers typically do not check certificates for revocation

Public Key Infrastructure

Expiration and Revocation:

Revocation important – someone may realize their key is stolen.

Expiration important – many orgs do not bother with revocation companies collecting money for issuing certs want to issue lots of them

If certificates of web service providers expire or are revoked, then new ones have to be issued - thus, down time

So, browsers typically do not check certificates for revocation

Verisign demands are so high, people do not get new certificates from them - depending on browsers not to check

Public Key Infrastructure

Expiration and Revocation:

Revocation important – someone may realize their key is stolen.

Expiration important – many orgs do not bother with revocation companies collecting money for issuing certs want to issue lots of them

If certificates of web service providers expire or are revoked, then new ones have to be issued - thus, down time

So, browsers typically do not check certificates for revocation

Verisign demands are so high, people do not get new certificates from them - depending on browsers not to check

Hence, security is down the tubes.

Public Key Infrastructure

Certificate Revocation Lists (CRL):

CA periodically issues a timestamped, signed list of revoked certs

Delta CRL – just the changes since a particular time/day

On-Line Revocation Server (OLRS):

System that can be queried over the net

Can this service be trusted?

Not security-sensitive -
Contains no vulnerable database of secrets
Worst thing it can do is to claim an invalid cert is still valid
– damage from this is limited