PKI and OpenSSL part 1

X.509 from the user's and the client software's point of view

Version 0.5

Richard Levitte, LP

mailto:levittelp.se

November 18, 2003

A serie of lectures

PKI and OpenSSL part 1: codeX.509 from the user's and the client software's point of view.

PKI and OpenSSL part 2: `X.509` from the CA's point of view.

PKI and OpenSSL part 3: to set up a CA using OpenSSL and CSP.

References

Russ Housley, Tim Polk, *Planning for PKI: Best Practics Guide for Deploying Public Key Infrastructure*, ISBN 0-471-39702-4, 2001

R. Housley, W. Polk, W. Ford, D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 3280, 2002

Public Key Cryptography: a reminder

• PKC is performed with pairs of keys: one private, one public. Anything encrypted with one of the keys in the pair can be decrypted by the other key in the pair.

• The private key is only known by the owner. The public key is known by everyone.

• Signing is performed by encrypting with the private key. Verification is performed by decrypting with the public key. This is used to prove authenticity of the signed document.

• Encryption is performed by encrypting with the public key. Decryption is performed by decrypting with the private key. This is used to make sure only the intended recidpient can read the encrypted document.

PKI basics: what's the big deal?

- Q: Who owns the private key?
- Q: How is that proven?
- A: Tie the identity securely with the key!
- Q: How do I know this is still true?
- Q: How do I know it's safe to use?
- A: Require expiration and out-of-band checks.

PKI basics: real world certificates

• Business card with PGP key fingerprint or a complete public key. This loosely ties the name on the business card with a public key.

Problems:

• The card must be received in person, or there can be no trust. And still, everything on it may be a lie!

• The card can't realistically be taken back if the validity of the information changes. There's also no realistic way to check if the information is still valid.

PKI basics: real world certificates

• Credit card. Doesn't have a public key, so it isn't really a certificate in a PKI sense. Instead, it ties a name with an account number.

Pros compared to business card:

• Has a visible issuer. With hologram techniques and recognisable images, it's hard to forge, and is therefore considered secure.

• Has name, account number and expiration date printed in raised letters, which is hard to changed after the card has been issued.

• Thanks to magnetic stripe, it can be used electronically.

• It has an expiration date, so validity is limited.

PKI basics: the ideal certificates

1. Purely digital object.
2. Contains name of private key holder, includes contact info
3. Easy to determine if issued recently
4. Created by trusted party rather than key holder
5. Easy to tell certificates from same issuer apart
6. Easy to determine if the certificate is genuine or forged
7. Tamper-proof
8. We can immediately determine if the information is no longer current
9. Easy to determine from certificate which application it applies to

PKI basics: general public key certificates

Serial Number:	48
Certificate for:	Bob Burton
Company:	Fox Consulting
Issued by:	CertsRUs, Inc.
Email address:	bb@pleasantville.ca.us
Activation:	Jan 10, 2002
Expiration:	Jan 10, 2004
Public Key:	2421ab81fe61448a c6b88142056fde8c ba7527c96148cbe1 4682ade412ed8923
CertsRUs' Digital Signature:	83bd86124d90e16a d81e135671324bde 89c562d5ae182134 33de8ade19ed9143

PKI basics: CA vs. EE

- CA = Certificate Authority. They issue certificates.
- EE = End Entity. The use certificates for services, authentication, identity.
- The two should not be mixed. A CA certificate must not be used to certify a server or a person. An EE certificate must not be used to sign other certificates.

PKI basics: PKI architectures

Simple architectures

Single CA : one trust point. Real easy, not very interoperable.

Basic trust list : multiple trust points which are single CA's.

Enterprise architectures

Hierarchical PKI : a tree of CA's. The top of the tree is the normal trust point for everyone.

Mesh PKI : every department has it's own individual CA, and all of them cross-certify with each other. The trust point is usually your own CA.

PKI basics: more PKI architectures

Hybrid PKI architectures

Extended trust list : like the trust list, but each entry may point at any kind of architecture. This is the most common way in web browsers.

Cross-certified Enterprise PKIs : many enterprises cross-certify with their partners, and form a mesh PKI at a higher level.

Bridge CA Architecture : when many enterprises cross-certify, the number of certificates to keep track of gets quite large. A bridge CA is an intermediate CA that cross-certifies with every enterprise. The bridge is never used as a trust point.

X.500: The directory

• In the beginning, there was the directory (X.500). It was designed to become a gigantic global on-line phone directory.

• The directory needed security. Public Key cryptography was chosen, and the certificate was created (X.509, 1988).

• The directory never became a reality except in some enterprises and communities. They never got connected together.

• The certificate was still cool, and got used as a general authentication tool for some protocols. The most popular are still SSL and TLS.

• PKIX (a working group of IETF) started working on standardising the use of X.509 certificates on the Internet. Today, the result is RFC 3280 and a bunch more.

X.509: certificates

version	v1
serialNumber	48
signature	DSA with SHA-1
issuer	C=US; L=CA; O=CertsRUs, Inc.; CN=CA1
validity	020110120000Z to 040110120000Z
subject	C=US; O=Fox Consulting, Inc.; OU=R&D; CN=Bob Burton
subjectPublicKeyInfo	RSA, 2421ab81fe61448a c6b88142056fde8c ba7527c96148cbe1 4682ade412ed8923
signatureAlgorithm	DSA with SHA-1
signature	83bd86124d90e16a d81e135671324bde 89c562d5ae182134 33de8ade19ed9143

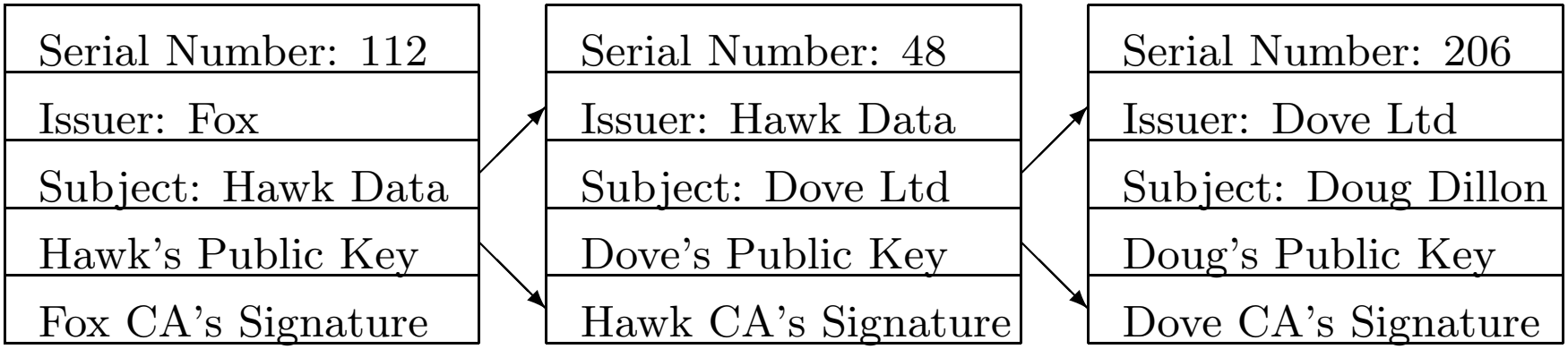
X.509: certificates

version	v2
serialNumber	48
signature	DSA with SHA-1
issuer	C=US; L=CA; O=CertsRUs, Inc.; CN=CA1
validity	020110120000Z to 040110120000Z
subject	C=US; O=Fox Consulting, Inc.; OU=R&D; CN=Bob Burton
subjectPublicKeyInfo	RSA, 2421ab81fe61448a c6b88142056fde8c ba7527c96148cbe1 4682ade412ed8923
issuerUniqueID	(usually omitted)
subjectUniqueID	(usually omitted)
signatureAlgorithm	DSA with SHA-1
signature	83bd86124d90e16a d81e135671324bde 89c562d5ae182134 33de8ade19ed9143

X.509: certificates

version	v3
serialNumber	48
signature	DSA with SHA-1
issuer	C=US; L=CA; O=CertsRUs, Inc.; CN=CA1
validity	020110120000Z to 040110120000Z
subject	C=US; O=Fox Consulting, Inc.; OU=R&D; CN=Bob Burton
subjectPublicKeyInfo	RSA, 2421ab81fe61448a c6b88142056fde8c ba7527c96148cbe1 4682ade412ed8923
issuerUniqueID	(usually omitted)
subjectUniqueID	(usually omitted)
extensions	
signatureAlgorithm	DSA with SHA-1
signature	83bd86124d90e16a d81e135671324bde 89c562d5ae182134 33de8ade19ed9143

PKI basics: X.509 certification



PKI basics: older X.509 certificate formats, the horrors!

- Misuse of certificates (for applications it wasn't meant for)
- Anyone can sign any certificate!
- Everyone must rely on the same certification policy
- So, what address does this person have? Is *alice@fox.com* the same as *C=US; O=Fox Consulting, Inc; CN=Alice Adams*? Is *www.fox.com* the same as *C=US; O=Fox Consulting, Inc; CN=Web Server*?
- The latter was solved with subject names like *C=US; O=Fox Consulting, Inc; CN=Alice Adams; emailAddress=alice@fox.com* and *C=US; O=Fox Consulting, Inc; CN=www.fox.com*, which is ugly and counterproductive

PKI basics: X.509 v3 certificates extensions

Subject type : is the certificate a CA or EE certificate?

Identity information : DNS names, email addresses

Key attributes : can this key be used for key transport? Can it also be used to verify a digital signature?

Policy information : can I trust Alice's certificate? Is it appropriate for large value transactions?

Additional information where can I find the CA certificate for the issuer of this certificate? Where can I find the certificate revocation list for that issuer?

PKI basics: X.509 v3 certificates extensions

• Extensions can be critical. If it is, it must be recognised, or the certificate is invalid. If it isn't critical, it can safely be ignored.

Subject type extensions

Basic Constraints : CA, a boolean that is true if this is a CA certificate.
pathLenConstraint, an integer that contains the number of steps further one may walk along the certificate chain.

PKI basics: X.509 v3 certificates extensions

Name Extensions

Subject Alternative Name : may contain extra identifiers, like DNS names (for servers, for example), IP addresses (useful in IPsec), e-mail addresses (for persons), and other types of data (Microsoft uses this to contain Kerberos data).

Name Constraints : used in CA certificates to constrain what names may be verified with it. This applies both to the basic subject name and the names gven in the subject alternate name. It's composed of a serie of permitted and excluded subtrees.

PKI basics: X.509 v3 certificates extensions

Key Attributes

Key Usage : identifies the security services that the public key can be used for. They include:

keyCertSign : the public key may be used to verify signatures on certificates.

cRLSign : the public key may be used to verify signatures on CRLs

non-Repudiation : the public key may be used to verify signature on documents and protects against the signer falsely denying some action.

digitalSignature : the public key may be used to verify signatures in other cases than the three given above.

keyEncipherment : the public key may be used for key transport and key management.

dataEncipherment : the public key may be used to encrypt data other than cryptographic keys.

PKI basics: X.509 v3 certificates extensions

Key Attributes

Key Usage : identifies the security services that the public key can be used for. They include:

keyAgreement : the public key may be used for key agreement. This is used when a DH key must be used for key management.

encipherOnly : the symmetric key resulting from key agreement may only be used for encrypting data.

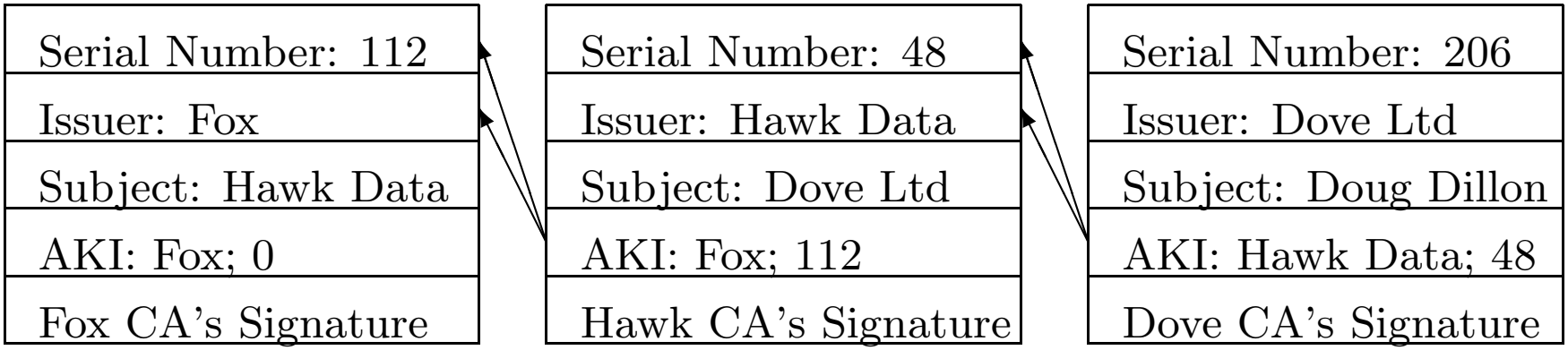
decipherOnly : the symmetric key resulting from key agreement may only be used for decrypting data.

PKI basics: X.509 v3 certificates extensions

Key Attributes

Subject Key Identifier : a hash value of the private key connected to this certificate. That makes it easier to keep track of which private key corresponds to which certificate.

Authority Key Identifier : a hash value of the private key connected to the issuer's certificate, or the issuer name and serial number from the issuer's certificate. That makes it easier to find the issuer's certificate when it has more than one, and thereby helps in certification path construction.



PKI basics: X.509 v3 certificates extensions

Policy Information

Certificate policies : a number of identities for the policy or policies that this certificate has been issued under.

Policy Mapping : when several CA's cross-certify, they usually don't have the same policy identifiers. However, they may agree that some of their policies are similar enough to be considered equal. The issued cross-certificates will then contain the mapping between those policies.

Policy Constraints : can be used to require that each certificate in the path has a valid policy identity, and can be used to prohibit policy mapping. For both these cases, there is a counter that says in how many steps this restriction starts to apply.

PKI basics: X.509 v3 certificates extensions

Additional Information

CRL Distribution point : in a CA cerificate, says where to find the CRL generated by that issuer.

Authority Information Access : points at other validation resources, for example an OCSP responder.

PKI basics: X.509 v3 certificates extensions

As you can imagine, there are many more extension, some standardised, some not.

There are also many ways to abuse them (for example, setting the critical flag on non-standard), and most likely, we have not seen the end of creativity in this department.

PKI basics: X.509 v2 Certificate Revocation List

version	v2
signature	DSA with SHA-1
issuer	C=US; L=CA; O=CertsRUs, Inc.; CN=CA1
thisUpdate	021101120000Z
nextUpdate	021108120000Z
revokedCertificates	(see next page])
crlExtensions	
signatureAlgorithm	DSA with SHA-1
signature	83bd86124d90e16a d81e135671324bde 89c562d5ae182134 33de8ade19ed9143

userCertificate	48
revocationDate	021012042234Z
crlEntryExtensions	

PKI basics: X.509 Certificate Path Construction

The best source here is `draft-ietf-pkix-certpathbuild-01.txt`, until it becomes and RFC...

PKI basics: X.509 Certificate Path Validation

The best source here is RFC 3280.