Secure Communication

with

Open Source Public Key Infrastructure

Johan Eklund, Tham Wickenberg
johan at primkey dot se, tham at primekey dot se

www.ejbca.org  www.signserver.org  www.hardtokenmgmt.org
Basic symmetric encryption

The old way of protecting data
Transform plaintext to encrypted data with a secret key
What is asymmetric encryption?

A pair of keys
- A public and a private
- Encryption w/ public key is easy
- Decryption w/o private key is hard

Diagram:
- Public key A
- Private key A
- Enc (encryption)
- Dec (decryption)
- Sign (signature)
- Ver (verification)
- Plain text
- Encrypted
- Signature
- Public key B
- Private key B
What is a X509 certificate?

Public key
Information about the owner of the private key
Usage
Validity
Verification information
Signature by CA guarantees the correctness of the information
The Trusted Root

"Self-signed" certificate
Signing other certificates
= certificate authority

RootCA's Certificate

Alice's Certificate

Bob's Certificate

Carol's Certificate

Signs

Signs

Signs
Verifying a certificate chain

Is certificate in trusted list?
Is signature for this certificate?
Is certificate valid (expired/revoked)?
Verify the issuer's certificate (recurse)
Authenticating a Person or Machine

Verify proof of possession
Verify certificate chain

RootCA A

Alice  Bob  Carol
Limit trust with SubCAs

High security
Offline, bunker, long validity, Hardware Security Module

Medium security
Online, limited validity

Lower security:
Soft token or smartcard, limited validity
What if you loose a key?

Revoke trust
- Certificate data invalid
- Compromised private key

Revocation checks
- Certificate Revocation List (CRL)
- Delta CRL
- Online Certificate Status Protocol (OCSP)
When is Public Key Infrastructure the solution

Asymmetric cryptography
  signatures, authentication, encryption
Entity trusted by everyone in context
  organisation, institution, company, person
Central management
  verification, revocation
..and when should you avoid it?

No single entity is trusted by everyone
GPG and the web of trust solves this better

Need for plausible deniability
Accurate identification hurts anonymity
Avoid unnecessary data in certificates
Use “selfsigned” certs or unpublished GPG-keys
The dark side of PKI

Trusted Computing
Only signed code is allowed to run
Digital Rights Management (DRM)
Defective by design
Separation of duties

Registration Authority (RA)
  Binds an entity to it's data
  CACert.org uses the community as a distributed RA

Certificate Authority (CA)
  Issues certificates based on input from RA

Validation Authority (VA)
  Revocation check service
OpenSource CAs

OpenSSL
  Still great for simple tasks
TinyCA
  Beta OpenSSL GUI
OpenCA / OpenXPKI
  First version recently released / Beta a SF
EJBCA
  Reliable and scalable enterprise solution
  Full featured
The demonstration

Client authenticated SSL
  Firefox and Apache
Encrypt and sign emails
  Thunderbird
Virtual Private Network with certificates
  OpenVPN
Signing code
  Jarsigner from Open JDK
Federation trends

Identities for different purposes
  Higgins project has X509 support

OpenID
  StartSSL has X509 support

Bridging PKIs
  Trusting another PKI for a purpose
Electronic signatures

Different rules in all EU member countries
  AES? DS? ES? EDI? ”Other means”
  Ask your local expert
  Need for standardisation
Upcoming EU proposal: BP might be sufficient
EU Passport PKI (1/2)

PKI with Card Verifiable Certificates
not X509
No revocation - short lifespan
Components:
  Country Verifying CA (CVCA)
  Document Verifier-Domestic
  Document Verifier-Foreign
  Inspection System
  Passport
EU Passport PKI (2/2)

The infrastructure located in Sweden
(only nordic DV-Fs shown)

CVCA.se
SHA256wRSA

DV-D.se
SHA256wRSA

DV-F.no
ECC-a?

DV-F.fi
ECC-b?

DV-F.dk
Alg?

DV-F.is
Alg?

IS

IS Cert.se
SHA256wRSA

IS Cert.no
ECC-a?

IS Cert.fi
ECC-a?

IS Cert.dk
ECC-a?

IS Cert.is
ECC-a?

Passport.se

Passport.no

Passport.fi

Passport.dk

Passport.is
Certificates and smartcards

SmartCard protects the private key
Short password/PIN
OpenSmartCard
   PKCS#11
   Don't invent card-specific support
No free cardriver with RSA2048 support?
Summary

Stable infrastructure
Useful in a context with a common trust
Benefits of centralized management
Simplifies authentication, signatures and encryption

johan at primekey dot se, tham at primekey dot se