NTNU

Innovation and Creativity

Large Scale Single Sign-on Scheme by Digital Certificates On-the-fly

Martin Eian [1] & Stig F. Mjølsnes

Department of Telematics

October 28, 2005

Background

- http://www.item.ntnu.no/~sfm/research/PKI/PKIprosjekt.pdf
- Public Key Infrastructure: provide certified public keys
- PKI deployment a lot slower than initially expected
- "The year of PKI" - announced annually for more than 10 years
- OASIS action plan for wide adoption of PKI
  - Lack of software support
  - High cost
  - Weak understanding of PKI technology
  - Interoperability problems
  - Lack of focus on user requirements

NTNU
Innovation and Creativity

Problem description

- X.509: top-down hierarchical view hard to adapt to the real world
  - No global top-level CA
  - More a political problem than a technological one
- Revocation problem: Keys are lost, stolen or compromised in other ways
  - Example: How are certificates revoked on the web?
  - Serious scalability issues
- Solutions to the revocation problem
  - Certificate Revocation Lists (including delta CRLs)
  - On-line Certificate Status Protocol
  - Short validity periods for certificates

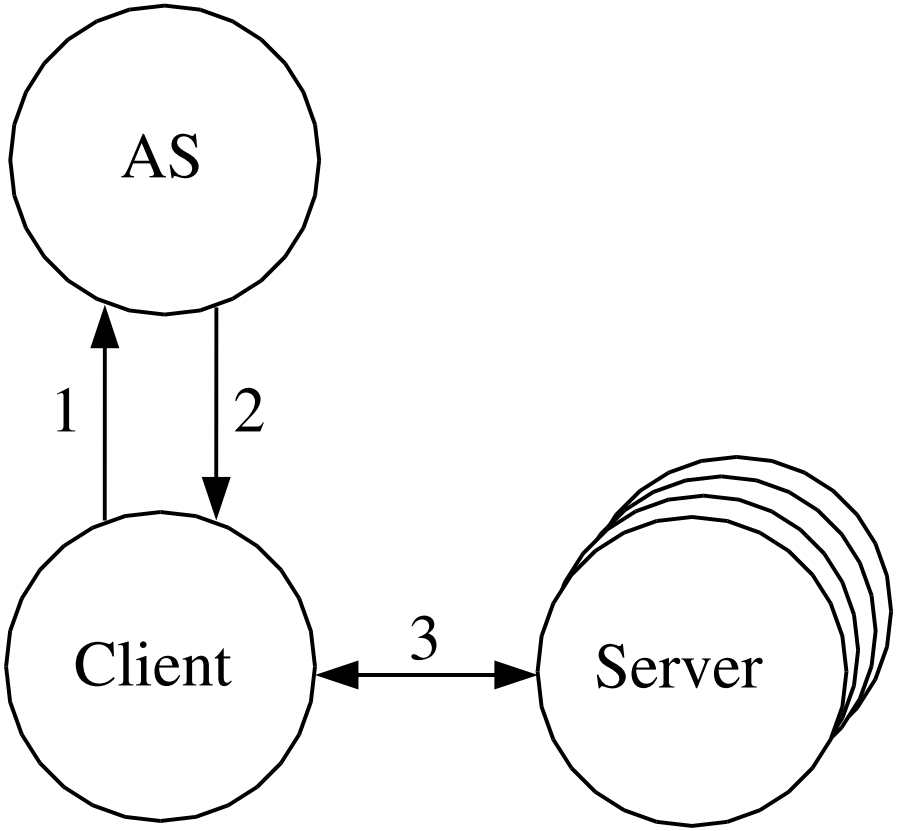
NTNU
Innovation and Creativity

Our approach

- Bottom-up, examine a single organization
- Large scale access authentication using PKI
  - Single sign-on
  - Revocation by short validity periods
  - Massive demand on certificate issuing
- Goals
  - Avoid high cost - keep it simple
  - Gain a better understanding of the technology
  - Use existing standards to ensure interoperability
  - Focus on a well-known user requirement

NTNU
Innovation and Creativity

Proposed system overview



1: Credential request
2: Credential response
3: PK based authentication

NTNU
Innovation and Creativity

Proposed system description

- Centralized authentication (AS)
- Local/distributed authorization and access control (Servers)
- Support for multiple authentication mechanisms
  - Passwords
  - Hardware tokens (public key based)
- Components used
  - Simple Password Exponential Key Exchange (SPEKE), DH key agreement with $g = H(P)^2$
  - Certificate Management Protocol (CMP)
- Security properties
  - Not vulnerable to server compromise
  - Not vulnerable to passive network attacks
  - At most one password guess per active network attack

NTNU
Innovation and Creativity

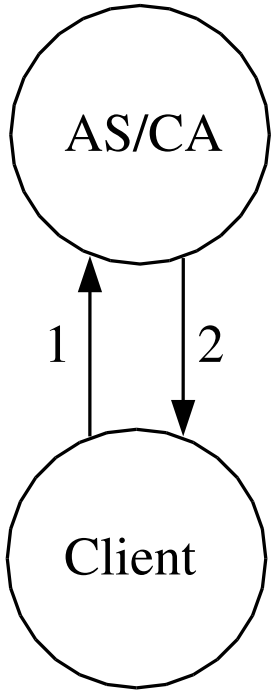
Issuing of certificate

— Password based

- Two messages (stateless)
- Certificate(s) encrypted with SPEKE key
- No message authentication
- AS does not verify identity

— Token based / renewal

- Two messages (stateless)
- Messages protected by digital signatures
- AS verifies identity

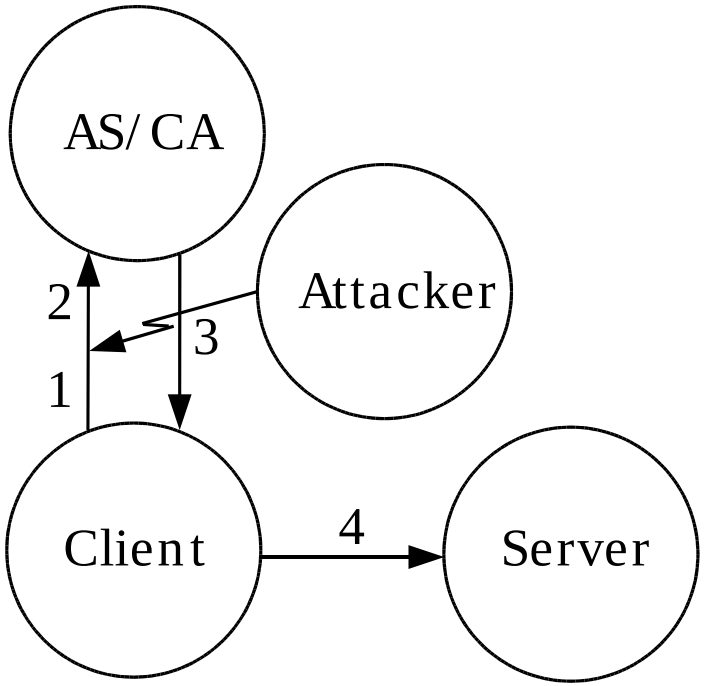


1: C, PK_C, g^{R_C}

2: $g^{R_{CA}}$,
$\{CERT(C, PK_C, SIG_{CA})\}g^{R_C R_{CA}}$,
$[\{CERT(CA, PK_{CA}, SIG_{CA})\}g^{R_C R_{CA}}]$

NTNU
Innovation and Creativity

Active attack on password authentication



1: C, PK_C, g^{R_C}
2: C, PK_A, g^{R_C}
3: $g^{R_{CA}}$, $\{CERT(C, PK_A, SIG_{CA})\}g^{R_C R_{CA}}$
4: $CERT(C, PK_A, SIG_{CA})$

NTNU
Innovation and Creativity

Lessons learned

- AS is not a proper CA in password-only mode
  - does not certify that the public key belongs to the correct identity
- Client must verify the certificate contents
  - public key
  - identity
  - any other data provided by the client
- Client should verify anyhow

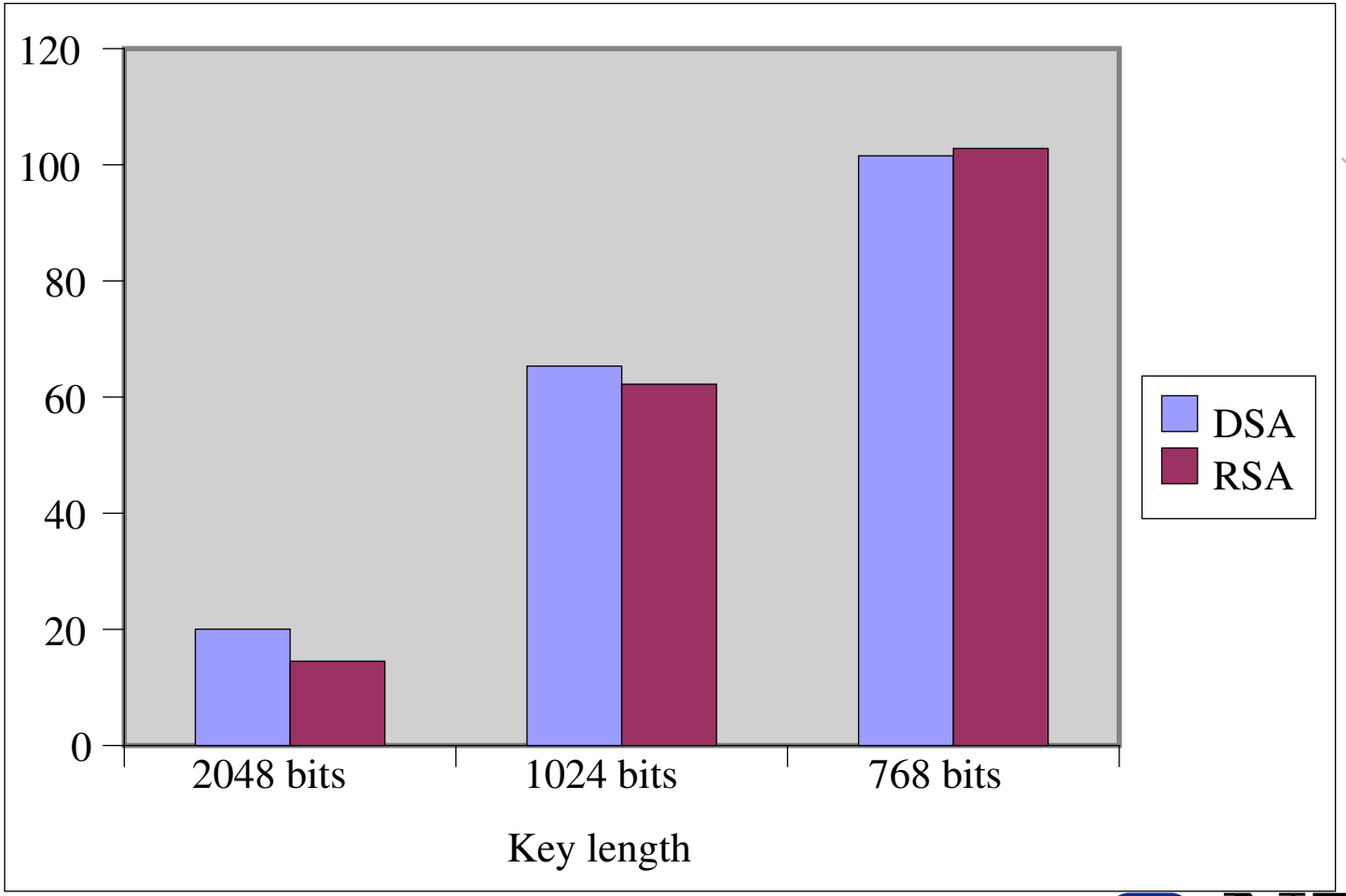
NTNU
Innovation and Creativity

Performance test setup

- 2 * Intel Xeon 2.8GHz
- 2 GB RAM
- SuSE Linux Enterprise Server 9
- Server (Servlet) and client written in Java (J2SE 1.5.0_02)
- Bouncy Castle Crypto APIs (1.27)
- Novosec CMP implementation (Release 101)
- Jakarta Tomcat 5.5.9 - CMP over HTTP

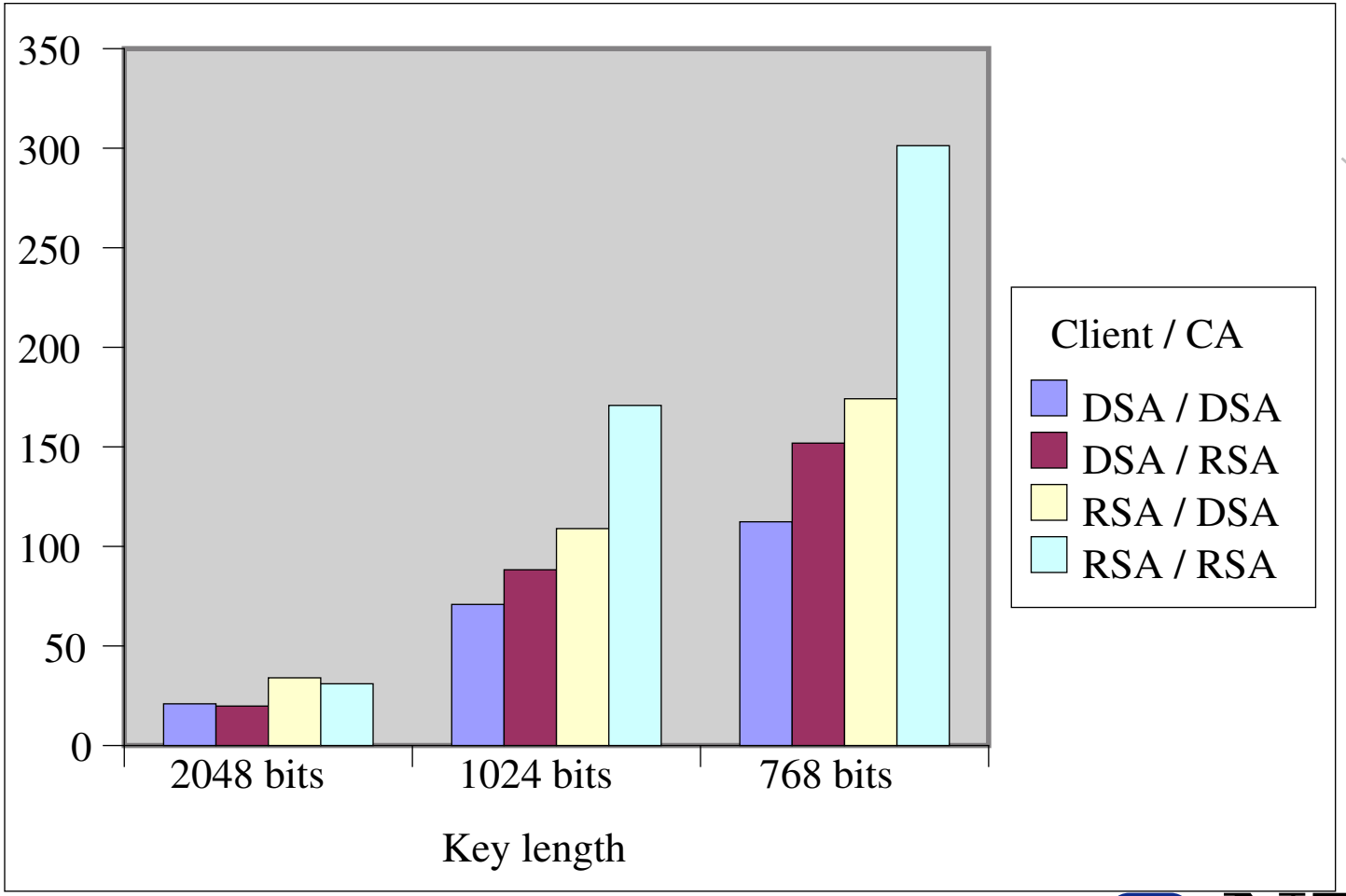
NTNU
Innovation and Creativity

Issued certificates per second (initial)



NTNU
Innovation and Creativity

Issued certificates per second (renew)



NTNU
Innovation and Creativity

Conclusions

- System performance good enough for organizations with tens of thousands of users
- Experimental implementation handles certificate issuing
- Client application support uncertain, should be investigated further
- More information
  - Paper
  - http://www.stud.ntnu.no/∼eian/paper/LargeScalePKI.pdf
  - Master's Thesis
  - http://www.stud.ntnu.no/∼eian/master/Masteroppgave_Martin_Eian.pdf
  - Experimental implementation
  - http://www.stud.ntnu.no/∼eian/master/sso_software_martin_eian.tar.gz
  - http://www.stud.ntnu.no/∼eian/master/sso_software_martin_eian.zip

NTNU
Innovation and Creativity