NTNU

Det skapende universitet

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

Martin Eian [1] & Stig F. Mjølsnes

Institutt for Telematikk

20 oktober 2006

Oversikt

- Terminologi
- Bakgrunn
- Problemformulering og tilnærming
- Systembeskrivelse
- Sikkerhetsanalyse
- Bruk i trådløse nett
- Ytelse
- Konklusjon

NTNU
Det skapende universitet

Terminologi

- Offentlige og private nøkler
- Digitale signaturer
- Digitale sertifikater
- PKI
- CA
- X.509
- Autentisering
- Autorisasjon
- Single sign-on (SSO)

NTNU
Det skapende universitet

Bakgrunn

- http://www.item.ntnu.no/~sfm/research/PKI/PKIprosjekt.pdf
- Public Key Infrastructure: sertifiserte offentlige nøkler
- Utrulling av PKI har gått langt tregere enn forventet
- "The year of PKI" — annonsert årlig i over 10 år
- OASIS — plan for storskala bruk av PKI
  - Manglende støtte i programvare
  - Dyrt
  - Ikke god nok teknologiforståelse
  - Problemer med interoperabilitet
  - For lite fokus på brukerbehov

NTNU
Det skapende universitet

Problemformulering

- X.509: globalt hierarki fungerer ikke i den virkelige verden
  - Ingen global CA
  - I hovedsak et politisk problem, ikke et teknologisk problem
- Ugyldiggjøring: Nøkler kommer før eller siden på avveie
  - Eksempel: Hvordan ugyldiggjøres nøkler i weblesere?
  - Store utfordringer mtp skalering
- Aktuelle løsninger
  - Certificate Revocation Lists (CRL)
  - On-line Certificate Status Protocol (OCSP)
  - Kort levetid for sertifikater

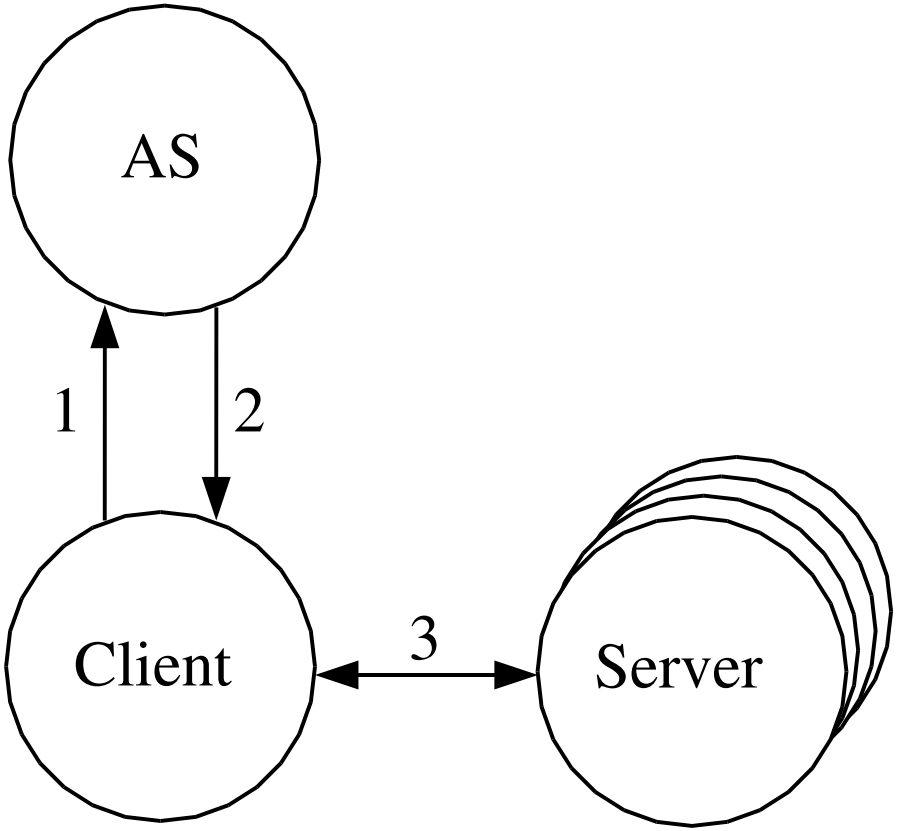
NTNU
Det skapende universitet

Vår tilnærming

- Start nedenfra, se på en enkelt organisasjon
- Storskala tilgangskontroll med bruk av PKI
  - Single sign-on (SSO)
  - Ugyldiggjøring ved kort levetid på sertifikater
  - Svært mange sertifikater må utstedes
- Mål
  - Billig og enkelt
  - Få en bedre forståelse av teknologien
  - Bruk eksisterende standarder — interoperabilitet
  - Fokus på et velkjent brukerbehov

NTNU
Det skapende universitet

Systemskisse



1: Forespørsel om sertifikat
2: Sertifikat
3: PK-basert autentisering

NTNU
Det skapende universitet

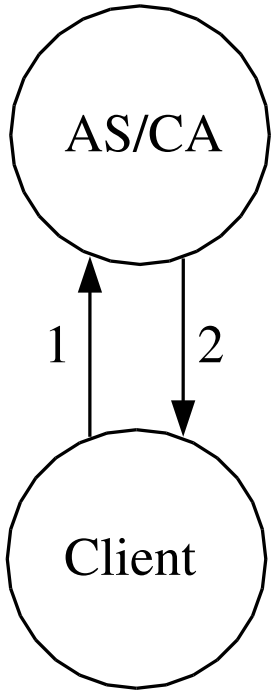
Systembeskrivelse

- Sentralisert autentisering (AS)
- Lokal/distribuert autorisasjon og tilgangskontroll (Server)
- Støtte for forskjellige autentiseringsmetoder
  - Passord
  - Hardware token (public key)
- Byggeklosser
  - Simple Password Exponential Key Exchange (SPEKE), Diffie-Hellman med $g = H(P)^2$
  - Certificate Management Protocol (CMP)
- Sikkerhetsmessige egenskaper
  - Ikke sårbar for kompromittert server
  - Ikke sårbar for passive nettverksangrep
  - Maksimalt ett forsøk på å gjette passord per aktivt nettverksangrep

NTNU
Det skapende universitet

Sertifikatutstedelse (1)

- Passordbasert
  - To meldinger (tilstandsløst)
  - Sertifikatet kryptert med nøkkelen fra SPEKE
  - Ingen meldings-autentisering
  - AS verifiserer ikke brukerens identitet



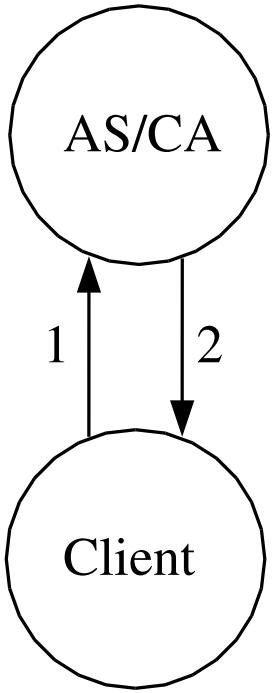
1: C, PK_C, g^{R_C}

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
Det skapende universitet

Sertifikatutstedelse (2)

- Hardware token / fornye sertifikat
  - To meldinger (tilstandsløst)
  - Digitale signaturer som meldings-autentisering
  - AS verifiserer brukerens identitet

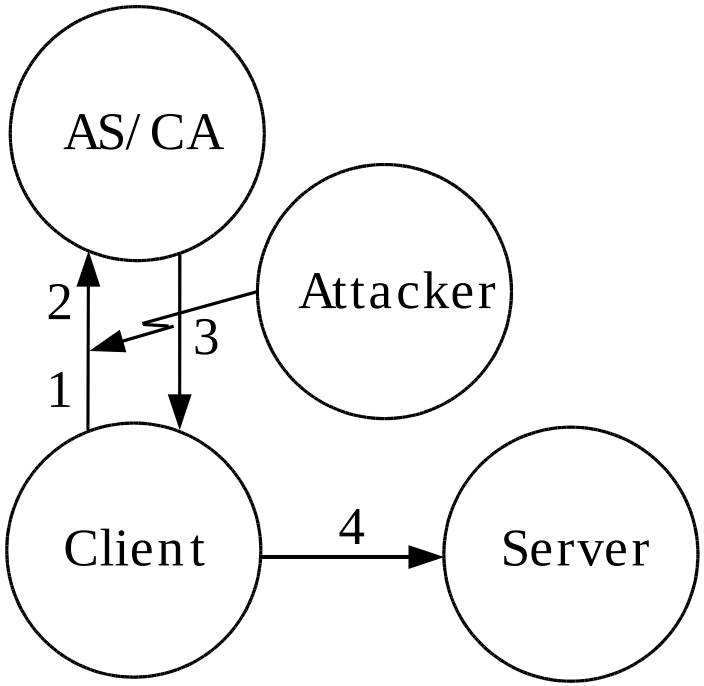


1: $C, PK_C, SIG'_C,$
$CERT(C, PK'_C, SIG_{CA})$

2: $CERT(C, PK_C, SIG_{CA}), SIG_{CA}$

NTNU
Det skapende universitet

Aktivt angrep på passordbasert autentisering



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
Det skapende universitet

Resultater av sikkerhetsanalysen

- AS er ikke en CA når passordbasert autentisering brukes
  - verifiserer ikke bindingen mellom nøkkel og identitet
- Klienten må sjekke innholdet i sertifikatet
  - nøkkel
  - identitet
  - andre data fra klienten
- Klienten bør uansett verifisere innholdet i sertifikatet

NTNU
Det skapende universitet

Bruk av systemet i trådløse nett

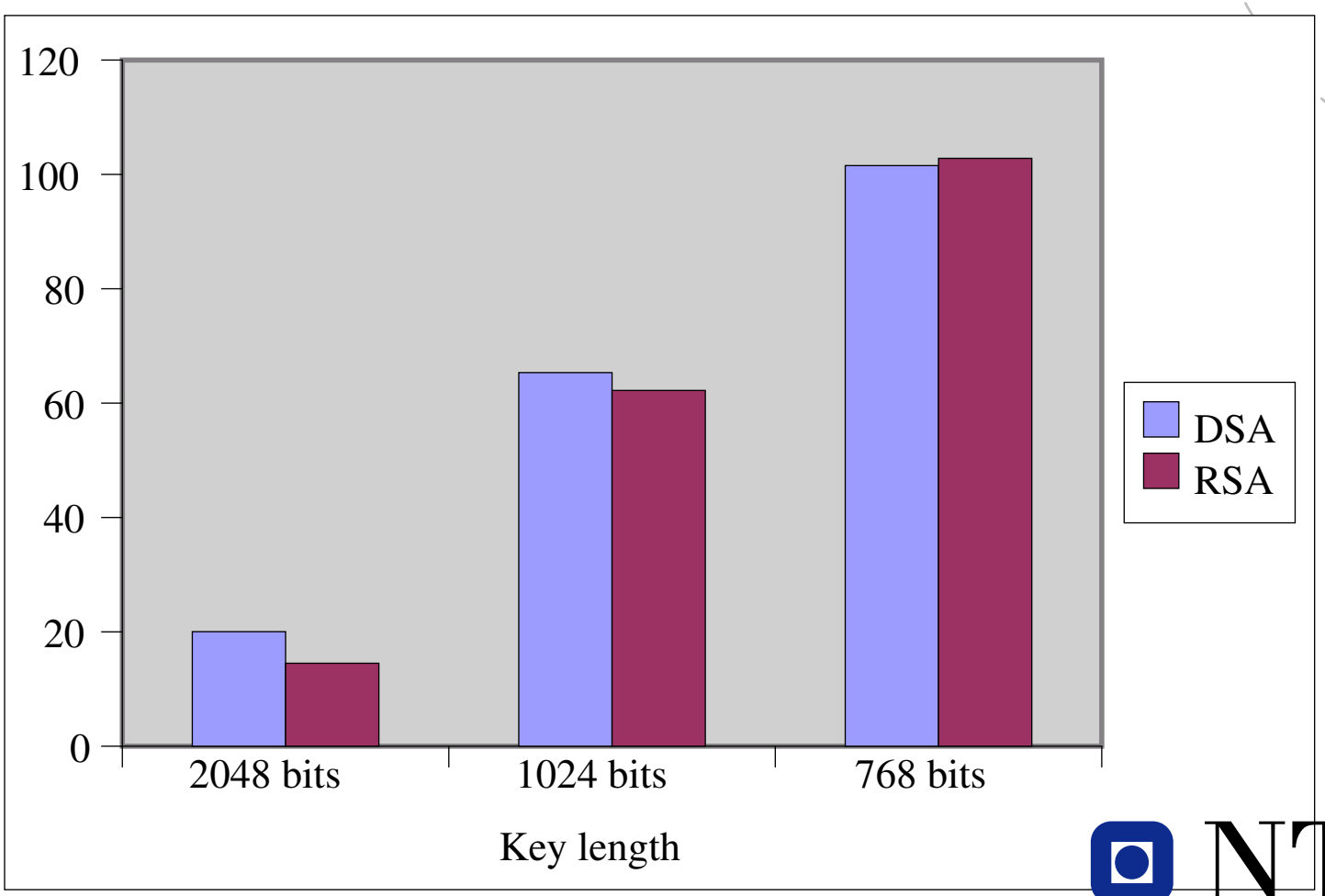
- 802.1x EAP-TLS brukt i WPA og RSN
- TLS/SSL generelt
  - HTTP, IMAP, POP, LDAP, SMTP, ...
  - Autentisert ende-til-endekryptering i åpne nett
- Klientsertifikater i mobile adhocnett
  - Feiltolerant, kan miste kontakt med AS i korte perioder
  - Lite trafikk, sertifikatene ugyldiggjør seg selv
  - Tåler segmentering (frem til sertifikatene ugyldiggjøres)
- Dynamisk tjenestetilbud
  - Skille mellom autentisering og autorisasjon
  - Enkelt å legge til nye tjenesteleverandører
  - Sikret mot tap av autentiseringsdata fra tjenesteleverandør

NTNU
Det skapende universitet

Oppsett av ytelsestest

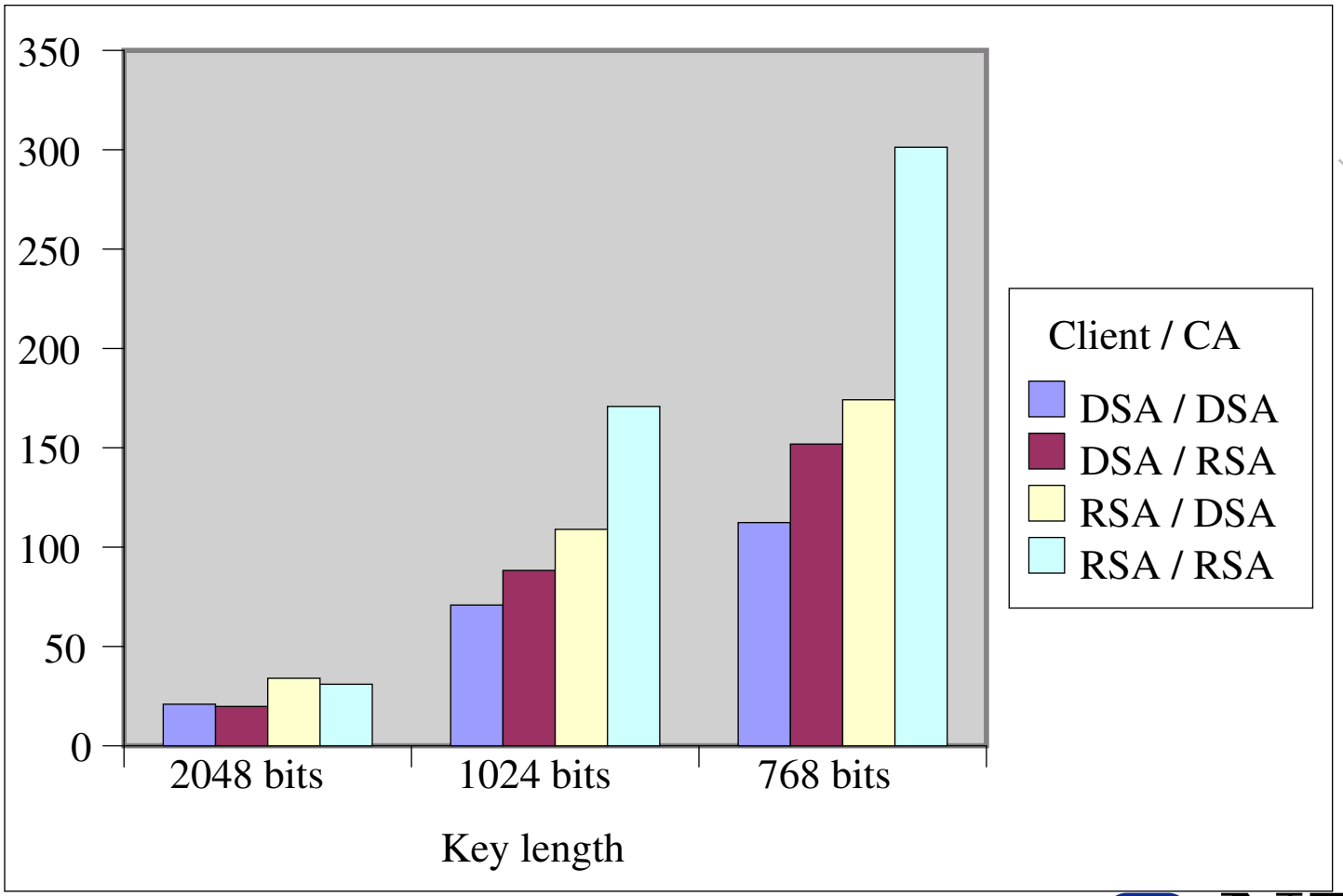
- 2 * Intel Xeon 2.8GHz
- 2 GB RAM
- SuSE Linux Enterprise Server 9
- Server (Servlet) og klient skrevet i Java (J2SE 1.5.0_02)
- Bouncy Castle Crypto APIs (1.27)
- Novosec CMP-implementasjon (Release 101)
- Jakarta Tomcat 5.5.9 - CMP over HTTP

Sertifikater per sekund (førstegangsutstedelse)



NTNU
Det skapende universitet

Sertifikater per sekund (fornye)



NTNU
Det skapende universitet

Konklusjon

- Ytelsen god nok for organisasjoner med flere titalls tusen brukere
- Eksperimentell implementasjon håndterer sertifikatutstedelse
- Programvare på klientsiden bør utforskes videre
- Ytelse på små mobile terminaler bør testes (ECC)
- Mer informasjon
  - Artikkel
  - http://www.uninett.no/nettforskning/nnrs2005/LargeScalePKI.pdf
  - Masteroppgave
  - http://home.samfundet.no/~eian/master/Masteroppgave_Martin_Eian.pdf
  - Eksperimentell implementation
  - http://home.samfundet.no/~eian/master/sso_software_martin_eian.tar.gz
  - http://home.samfundet.no/~eian/master/sso_software_martin_eian.zip

NTNU
Det skapende universitet