

Electronic Identity

SwUPKI - Universitetens PKI



Torbjörn Wiberg

torbjorn.wiberg@adm.umu.se

www.umu.se/it/personal/tvw/pub/swupki011101.pdf



2001-10-17

©Torbjörn Wiberg, UmU

1

Electronic Identity

Public Key Cryptography? - Problems



- You have to make your key **known!**
- People getting your public key has to trust that it is **Your** key.
- There has to be a way of saying that your key shall no longer be used (revoke the key) when
 - Time has gone and you need a longer key
 - You suspect that your key has been compromised

2001-10-17

©Torbjörn Wiberg, UmU

15

PKI - Electronic Identity

Public Key Infrastructure



- The information about our electronic identity is distributed in a certificate issued by a Certification Authority (CA) in a PKI
 - An infrastructure!
- To be of any real use, the identity issued by the PKI must be trusted by "everyone"
 - The subscriber of the identity must trust the PKI
 - Those authenticating the subscriber must trust that the certificate distributed by the PKI is valid and belongs to the subscriber and noone else
- Compare with credit cards



2001-10-17

©Torbjörn Wiberg, UmU

16

Electronic Identity

Public Key Infrastructure



- An infrastructure for issuance, management, distribution and validation of certificates containing public crypto keys
- The PKI must earn trust among its users and peers. That is the users and peers must trust the organisation of the PKI:
 - work procedures and personnel
 - provisions
 - liability
 - level of cryptographic security chosen, etc

2001-10-17

©Torbjörn Wiberg, UmU

17

Electronic Identity

Issue Certificates



- A certificate states that the public crypto key belongs to the subscriber of the certificate
- The Certificate Authority (CA)
 - verifies that the subscriber owns the public crypto key
 - identifies the subscriber
 - decides whether the key is strong enough
 - gives the subscriber a unique name (within the CA) in the certificate
 - issues the certificate
 - decides for what period the certificate is valid
- The first two points may be delegated to a Registration Authority (RA)

2001-10-17

©Torbjörn Wiberg, UmU

18

Electronic Identity

Manage Certificates



- Certificates may be revoked
 - This shall be noted in a revocation list (CRL)
 - The CRL shall be digitally signed by the issuing CA
 - The CRL must be distributed and kept available for validation purposes
- Certificates expire and must be renewed
 - Perhaps the subscriber shall be offered a renewal automatically

2001-10-17

©Torbjörn Wiberg, UmU

19

Electronic Identity



SwUPKI

- A PKI whose members are Swedish universities and university colleges and associated authorities
- The responsibility is shared between Stockholm University and Umeå University
 - Policy Management Authority (SU)
 - Policy CA (UmU)
- Members are accepted by the PMA after inspection and approval of procedures, security and the CPS
 - UU, SU and UmU its first members
 - UU was inspected 2001-01-18
- There is a steering group appointed by the universities (-> the members)

2001-10-17

©Torbjörn Wiberg, UmU

28

Electronic Identity



SwUPKI - A PKI for the Swedish Universities and University Colleges

- Umeå universitet issues certificates for members of SwUPKI (is the Policy CA)
 - CA-certificate is issued after the PMA has accepted the member and a certificate request has arrived
 - Policy CA is up and running since February 2001 and will only issue CA-certificates and certificates for its own operation
 - I believe that just a few universities will operate their own CA - probably 5-10 CA operators
- We don't (yet) have technical systems for issuing large numbers of certificates
- We are cooperating with the tax authorities and Statskontoret to influence the current procurement of citizen's certificates

2001-10-17

©Torbjörn Wiberg, UmU

29

Electronic Identity



Citizen's Certificates

- The Tax authorities have been assigned the task by the government to provide means for and facilitate authorities to use digital signatures
- For communication with authorities
 - Not enough!
 - For communication!!
- Not ONE pki
 - Not good enough!
 - One national pki for certificates for persons!
 - National cooperation more important than academic
- Pki for internal use
 - Useless! Can't communicate with citizens

2001-10-17

©Torbjörn Wiberg, UmU

30

Electronic Identity



SwUPKI - A PKI for soft storage of the keys

- SwUPKI is a PKI for soft certificates of medium strength
- The public keys may be used for (in combination with the corresponding private keys)
 - Control of the integrity of documents
 - Nonrepudiation of documents
 - Authentication as the first step in authorization
 - Negotiation for session keys
- The strength is considered good enough for internal authentication, and for communication with students and other authorities

2001-10-17

©Torbjörn Wiberg, UmU

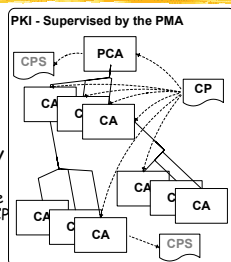
31

SwUPKI is a PKI - Identity



www.swupki.su.se

- Certification Authority (CA)
 - Trusted to issue & manage certificates
- Certificate Policy (CP)
- Policy CA (PCA)
 - At the top of the CP hierarchy
- Policy Management Authority (PMA)
 - Manages the CP and makes sure that the CAs comply with the CP
- Certification Practice Statement (CPS)



2001-10-17

©Torbjörn Wiberg, UmU

32



SwUPKI

Welcome to the PKI for Universities and University Colleges in Sweden (SwUPKI). SwUPKI is operated by Stockholm University and Umeå University. Detailed information, root certificates and policy is available by selecting links on the left. Please note that some resources are only available to members in SwUPKI.

The SwUPKI staff can be contacted by the following email addresses:

- PMA
 - Contact: info@swupki.su.se
 - Organization: membership@swupki.su.se
 - Certificate Policy: cp@swupki.su.se
 - Issues SwUPKI: issues@swupki.su.se
- PCA
 - PCA Certification Practice Statement: cps@swupki.su.se
 - PCA Repository: repository@swupki.su.se
 - PCA CRL: crl@swupki.su.se
- Resources
 - PKI Resources: resources@swupki.su.se

2001-10-17

©Torbjörn Wiberg, UmU

33

Electronic Identity

Men - För att dra verklig nytta av en PKI



- PKI-tekniken måste fungera även i våra applikationer (egna och standard)
 - installation av egna certifikat
 - installation av certifikat för PKIer man har förtroende för
 - användning av egna certifikat
 - access till och validering av andras certifikat
- Våra användare måste förstå och kunna använda tekniken på rätt sätt
 - generera tillförlitliga krypteringsnycklar
 - Begära att få, ta emot, kunna installera och använda certifikat - det egna certifikatet och PolicyCA-certifikat för de PKIer man har förtroende för

Electronic Identity

Vad uppnår vi?



- Framför allt en så säker autentisering (identifiering) av IT-system och personer som den valda krypteringstekniken medger
- Brasklapp! Våra användare måste förstå och kunna använda tekniken på rätt sätt
 - generera tillförlitliga krypteringsnycklar
 - bevara den privata nyckeln skyddad och hemlig
 - kunna begära, ta emot, installera och använda certifikatet

Electronic Identity

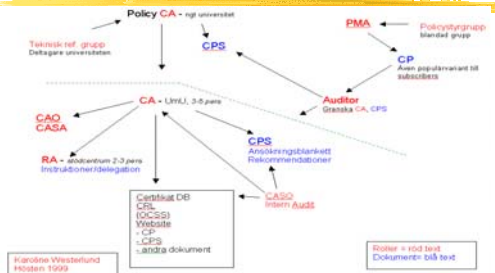
Goals Guiding Positions Taken



- Ease of use
- Interoperability and trust
 - Between PKIs
 - Between IT-systems
- Support of eWhatever (priority on national cooperation instead of academic)
- SwUPKI - ONE PKI for Swedish Universities and University Colleges

SwUPKI

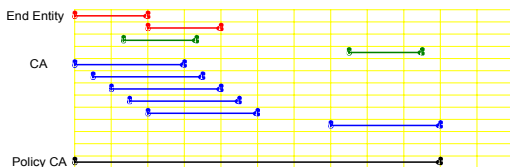
Roller och dokument



Nycklars och certifikats livslängder enligt SwUPKI CP



- Certifikat
 - End Entity - 2 år
 - CA - 3 år
 - PCA - 10 år
- Privata nycklar
 - End Entity - 2 år
 - CA - 6 månader
 - PCA - 7 år



Electronic Identity

SwUPKI - A PKI for Swedish Universities and University Colleges



- A PKI based on open standards - IETF-pkix standards
- Soft certificates of medium strength
- Strong enough for internal authentication and for correspondence with students and other authorities

Electronic Identity

Why a PKI Based on Open Standards?



- We want to use standard software in our applications
- We need general means to authenticate IT users and systems
- We want to cross-certify with other PKIs

2001-10-17

©Torbjörn Wiberg, UmU

42

Electronic Identity

- A Personal View



- ITU
 - X.509v3 (->v4) - certificate format
- IETF - pkix - internet infrastructure aspects
 - Profile for the use of X.509v3
 - Protocols for management of structures
 - Policy and practises framework
 - Protocols for accessing certificates - LDAP f.ex.
- ETSI - realisation of eEurope
 - Requirements around Qualified Certificates
 - Electronic signature formats
 - Use in eBusiness

2001-10-17

©Torbjörn Wiberg, UmU

43

Electronic Identity

IETF-pkix - Open Issues



- The pkix working group of the IETF proposes standards for the PKI area.
- Some open/discussed issues in pkix:
 - Certificate validation paths and policy mapping
 - Online certificate status checking
 - Attribute certificates
 - Qualified certificates
 - Time stamping
- In addition pkix has entered a revision phase

2001-10-17

©Torbjörn Wiberg, UmU

44

Electronic Identity

- what else to wish for



- I believe more work has to be done on the organisation of the PKI infrastructure
- It is essential that people like myself understand the task at hand when starting a PKI
- RFC2527 - Certificate policy and certification practices framework
 - Important for PKI builders
 - The certificate policy is common for the PKI
 - The certification practices statement is local for each CA
- RFC2527 is informational
 - perhaps in the IETF margin
 - IETF is us

2001-10-17

©Torbjörn Wiberg, UmU

45

Electronic Identity

SwPKI - Vad fick vi då den 23 februari 2001?



- En infrastruktur med PMA och Policy CA som kan
 - acceptera lärosäten som medlemmar i PKIn och därvid
 - utfärda certifikat för lärosätets CA
- Flera lärosäten har redan en CA-verksamhet som modifierad kommer att kunna föras in i SwUPKI
 - den används för att utfärda certifikat för IT-system (autentisering av IT-system) ffa webb-servrar
- Med policyn i handen kan vi starta diskussioner om samarbete med andra PKIer
- Vi har en grund för användning av elektroniska signaturer i vår verksamhet som myndigheter

2001-10-17

©Torbjörn Wiberg, UmU

56

Electronic Identity

Läget i SwUPKI



- Policy CAn är igång sedan 23 februari 2001
- Stockholms universitet, Uppsala universitet och Umeå universitet är medlemmar
- Ett par universitet till har aviserat att de blir medlemmar innan årsskiftet
- Ett par universitet och högskolor har sagt att de vill utkontraktera driften av CAn (5 pers i driftorg)
- SwUPKI utfärdar hittills i huvudsak certifikat för servrar. Det förebereads vissa experiment med personcertifikat.
- Vi har (ännu) inte tekniska system för utfärdande i av certifikat i stor skala

2001-10-17

©Torbjörn Wiberg, UmU

57

Electronic Identity

Vad bör vi använda elektroniska identiteter till?



- Autentisering av IT-system som används i vår myndighetsutövning.
 - Webb-servrar, antagningssystem, diaries etc
 - Medför inte stora kostnader i PKIn
- Signering av e-post och elektroniskt publicerade dokument
 - Kräver personliga certifikat för alla
 - Kostar nog som identitetskort
- Autentisering av användare av våra IT-system
 - Lägst prioriterat (vi har redan behörighetssystem baserade på användarnamn och lösenord)
 - Behövs för personliga portaler

2001-10-17

©Torbjörn Wiberg, UmU

58

Electronic Identity

Vad vilar på lärosätet?



- Att skriva en CPS, anhänga om medlemskap i SwUPKI och starta en CA (som ev drivs av ett annat lärosäte).
- Att besluta för vilka/vad man ska utfärda certifikat
 - Certifikat överlämnas alltid till en person som måste kunna styrka att hon har de befogenheter i organisationen hon vill ska framgå av certifikatet
 - Certifikat utfärdas för en person, roll eller ett IT-system
- Att ta ställning till hur elektroniska identiteter ska användas i lärosätets verksamhet
- Att välja IT-system som kan använda certifikat och signaturer
- Att modifiera sina IT-system så att de kan använda certifikat och signaturer

2001-10-17

©Torbjörn Wiberg, UmU

59

Electronic Identity

Organisationen av en CA



- Utse en person som skulle kunna vara
 - CA-operatör att utvärdera teknik
 - CA-säkerhetsansvarig att sätta sig in i policyn och ta ställning till hur certifikat ska användas inom organisationen
- Välj teknik
- Utarbeta lokala rutiner och skriv en CPS i dialog med PMAAn
 - CA:n bör drivas i en "datacentralsliknande" miljö
- Begär inspektion från PMAAn
- Starta med några webb-servercertifikat
 - Brister rutinerna dras CA-certifikatet in

2001-10-17

©Torbjörn Wiberg, UmU

60

Electronic Identity

SwUPKI - Universitetens PKI (or: I Will Do This Only Once)



Torbjörn Wiberg

torbjorn.wiberg@adm.umu.se

www.umu.se/it/personal/tvw/pub/swupki011101.pdf



2001-10-17

©Torbjörn Wiberg, UmU

61