NTNU
NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Reducing the Cost of Certificate Revocation for improved scalability: A Case Study

Mona Holsve Ofigsbø

10 Dec 2009

The Goal

How to reduce the number of revoked certificates and the bandwidth consumption in order to achieve better scalability

The Analysis

Based on empirical data in UNINETT and we analyze the revocation mechanisms based on three requirements for different user groups.

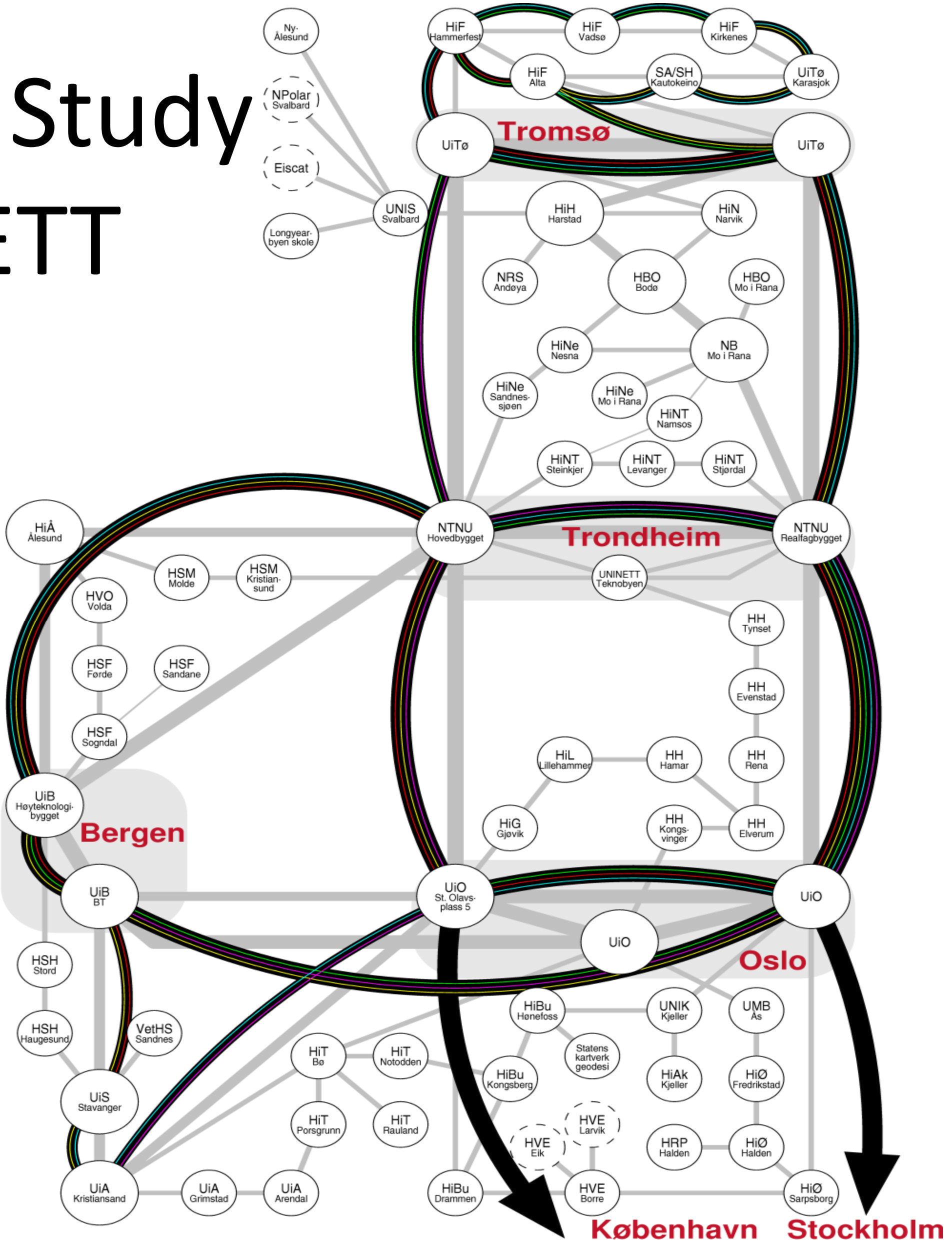
Outline

- The study case: UNINETT and Feide
- The revocation mechanisms
- The user groups
- The requirements
- The Analysis
  - Revocation mechanisms for each user group based on the requirements
- Conclusion

The case study: UNINETT and Feide

- UNINETT
  - The Internet of Norwegian Universities and Colleges.
- Feide
  - Project in UNINETT.
  - Identity management system on a national level for the educational system.
  - Members: 6 universities, 42 colleges, 82 research establishments and 7 high schools.

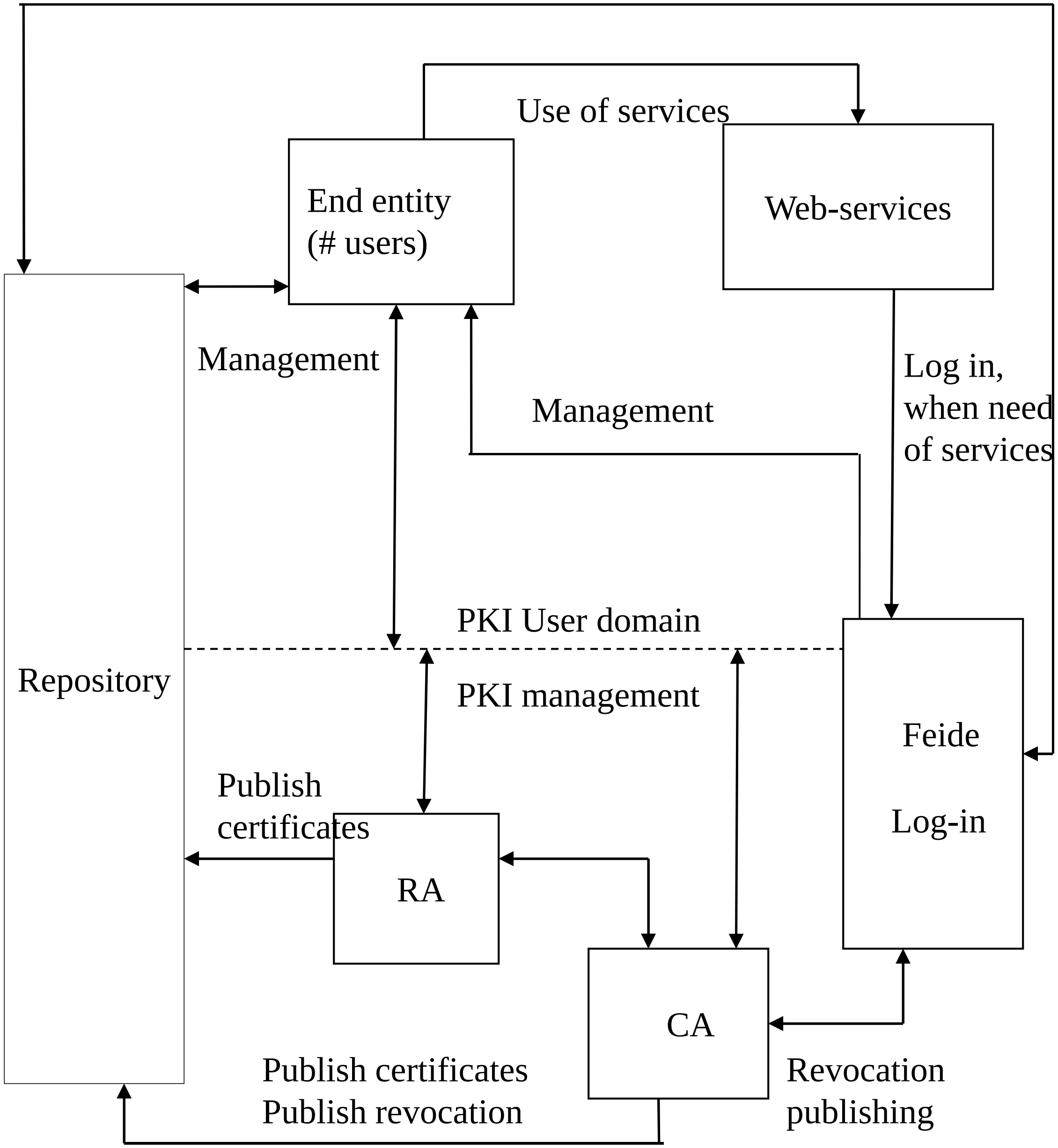
The Case Study UNINETT



The Internet of Norwegian Universities and Colleges.

Feide

- Refer to RFC5280.
- Central log-in services which authenticate users.
- End entity is institutions such as universities, colleges etc



The three revocation mechanisms

- Classify revocation methods into three categories:
  - Push mechanisms
    - Provide retrieving of revocation information lists (e.g. CRLs, delta CRLs, segmented CRLs)
  - Pull mechanisms
    - On-demand validation of certificates (e.g OSCP, NOVOMODO)
  - Short validity period
    - Certificates with short lifetime without any validation of the certificates.

The three user categories

- User groups behave differently:
  - Stay in the system for various periods
  - Apply different Web-services
  - Different reason for revocations
- Classify the end users into three categories:
  - Students
  - Temporary employee (e.g. visiting lectures, PhD students)
  - Permanent employee (e.g. adm staff, teachers, professors etc)

The Requirements

- Must be relevant for our PKI environment
  - Security
    - No weaker than the rest of the system.
    - Authenticity, integrity, freshness must be fulfilled. (Freshness is the time between the actual revocation and when the revocation information is available.)
  - Cost
    - Bandwidth and operating cost.
  - Scalability
    - Must scale to European countries.
    - Wield the number of certificates users, end entities, revocation information and prevent bottlenecks.

Analysis

revocation mechanisms for each user group based on the requirements

	Students	Temp. employees	Employees
Push rev. schemes	Security Cost Scalability	Security Cost Scalability	Security Cost Scalability
Pull Rev. schemes	Security Cost Scalability	Security Cost Scalability	Security Cost Scalability
Short lifetime validation	Security Cost Scalability	Security Cost Scalability	Security Cost Scalability

Analysis

revocation mechanisms for each user group based on the requirements

	Students	Temp. employees	Employees
Push rev. schemes	Security Cost Scalability	Security Cost Scalability	Security Cost Scalability
Pull Rev. schemes	Security Cost Scalability	Security Cost Scalability	Security Cost Scalability
Short lifetime validation	Security Cost Scalability	Security Cost Scalability	Security Cost Scalability

The Analysis of Students

- Approximately 210,000 students in Norway (10 million in European Student Union)
- Study programs: Master, Bachelor, two-years and annual programs
- Revocation reasons
  - Quit before graduating, approximately 18,000 – 19,000
  - Change IDs, approximately 1000

The analysis of Push mechanisms for Students

- Security
  - Freshness depends on how often the end entities retrieve the revocation information
- Scalability
  - Retrieve voluminous lists from CA cause bottlenecks in the networks, Improvements:
    - Reduce certificates, optimize the lifetime
      - Example: Worst case,if revocation occurs in the first year after being issued.
        - » With lifetime on 5 years for all students.

$$\#\mathrm{Rev}_i = \sum_{n=1}^{5} \left(\mathrm{rev}_{A_{(i-n+1)}} + \mathrm{rev}_{o_{(i-n+1)}} + \mathrm{rev}_{B_{(i-n+1)}} + \mathrm{rev}_{M_{(i-n+1)}}\right)$$

The number of revoked certificates is 98,822 in 2008.

- » With lifetime is the same length as the length of the study program.

$$\#\mathrm{Rev}_i = \mathrm{rev}_{A_{(i-n+1)}} + \sum_{n=1}^{2} \mathrm{rev}_{o_{(i-n+1)}} + \sum_{n=1}^{3} \mathrm{rev}_{B_{(i-n+1)}} + \sum_{n=1}^{5} \mathrm{rev}_{M_{(i-n+1)}}$$

The number of revoked certificates is 50,424 in 2008

- Multicast groups reduce the load of multiple revocations lists on the link at the CA.
- Segmented CRL need more bandwidth than traditional CRLs, because of overhead and a digital signature on each segment.

The analysis of Push mechanisms for Students cont.

- Cost
  - Bandwidth cost is high if end entities retrieve the revocation lists often, Improvements:
    - Multicast groups.
      - Example. If the 147 end entities retrieve the 50424 revoked certificates :
        - » With Unicast addressing. Data amount on the link at CA will be 191 MB (147 end entities *1.3MB)
        - » With 6 Multicast groups. Data amount on the link at CA will be 7.8 MB (6 relying parties *1.3MB)
    - Reduce unnecessary revocation information, optimize numbers of CA
      - Example. Students in Norway request normally Web-services at Norwegian universities/colleges and the Italian students requesting normally at Italian universities/colleges.
        - » One CA per member/country reduces number of revocation distribution.

          $\sum^{49}_{n=1}\sum^{E}_{m=1}$ End Entity$_{(n,m)}$ -> $\sum^{E}_{m=1}$ End Entity$_{(m)}$
      - Example.
        - » 547350 revoked certificates per year or 2.5 mill in 5 years in Europe student union
        - » 10947 revoked cert per year or 50424 in 5 years in Norway

          => CA per country reduces BW consume compared to Delta CRL in European student Union.

Revocation model for Students

- Pull mechanisms suffer from the scalability. Propose to combine Short lifetime certificates and CRLs with improvements:
  1. The architecture
     a. A CA domain per member/country in European stud. Union
  2. The policies
     a. The lifetime should be equal to the semester period.
     b. Issue the certificates after semester registration fee is paid
  3. The network aspects
     a. distribute the revocation lists using Multicast addressing
     b. Multicast groups is preferred to be large and manageable

Conclusion

- CRL does not scale itself, but with cost reduction it does. We propose to:
  - Reduce the number of certificates issuing by policies
  - Optimize the number of CA domains
  - Different lifetime to different user groups
  - Multicast groups