OASIS, Washington 2009

PKI implementation:
the good, the bad and the future

PrimeKey Solutions
Lars Bagnert
lars.bagnert@primekey.se

Background

- Swedish Police
  - 25.000 users
  - 400 offices over the country
  - From 5 to 1.000 users / office
  - 20 regional operation centres
- Demands for strong authentication
  - Swedish privacy act
  - Internal regulations
- *The goal*
  - *Making users countable for their actions*

Smart cards, 1st generation 1995-2002

- 3 different card to be used
  - Smart card with PKI for authentication
  - Smart card vendor delivered the PKI solution
  - ID-card for user identification

- Results
  - Many cards, many PIN-codes
  - Different processes to between the cards
  - Problem with temporary cards
  - Not user friendly

- *The goal*
  - *Technical focus: to implement strong authentication*

Smart cards, 2nd generation 2003-

- Organizational phase
  - One card, one process
  - In house centralized production
  - Decentralized issuing
  - Needed routines
- Technical phase
  - Standards
  - Vendors and products
  - Technical issues
  - Proof of Concept
- Implementation phase
  - Personal and responsibilities
  - Educations
  - Development, installation and implementation

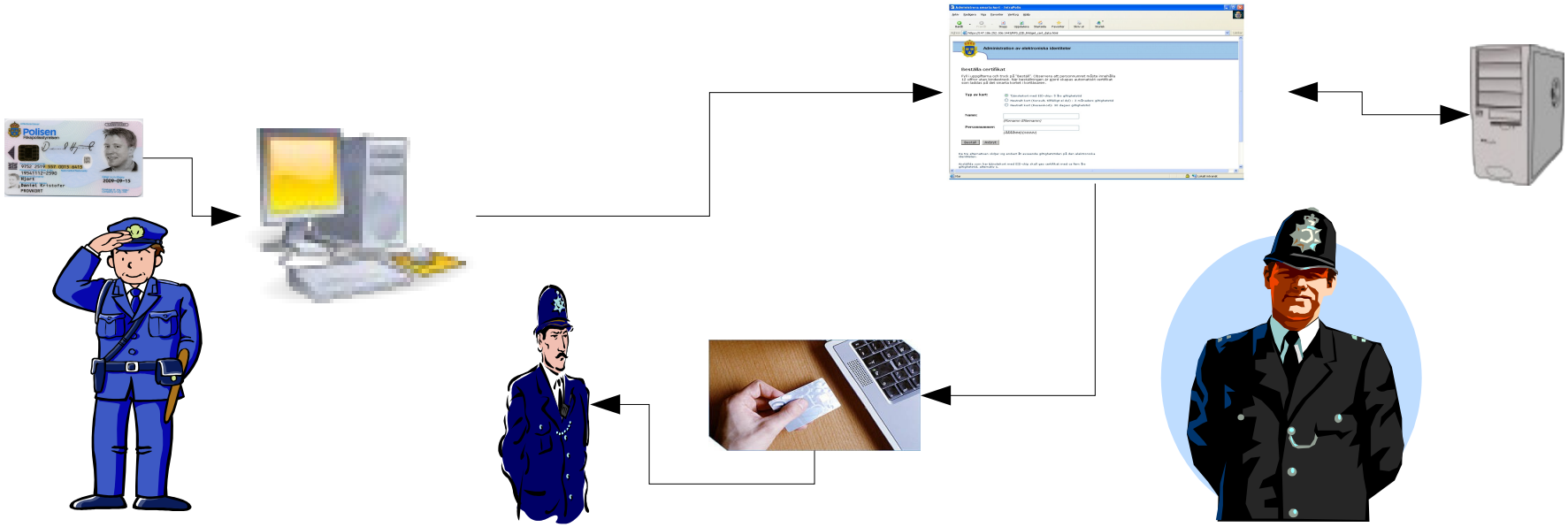
EJBCA PKI
PrimeKey
aep NETWORKS Secure Networking & Identity-Based Access
gemalto
hp

The project

- The project organization
  - Small but flexible
  - Right people involved, early
  - Support from upper management
- Involvement
  - Information to the organization
  - Guidelines and routines
  - Training
- Implementation phase
  - Smart card issuing organization
  - Educations
  - Installation and implementation
  - Support organization

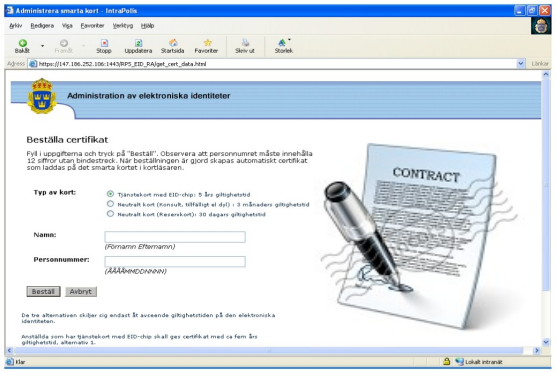
The Solution

- Temporary smart card
  - User 1, applies for temporary card for User 2
  - User 2 , puts a new smart card in the reader
  - Senior officer grants the request
  - User 2's ordinary card is suspended
  - Everything is log



The benefits

- For the users
  - One card, one PIN-code
  - Functions for personal temporary cards
  - One easy process for all functions
  - One local function to turn to



- The organization
  - Higher efficiency
  - Lower cost
  - Better control
  - Better security

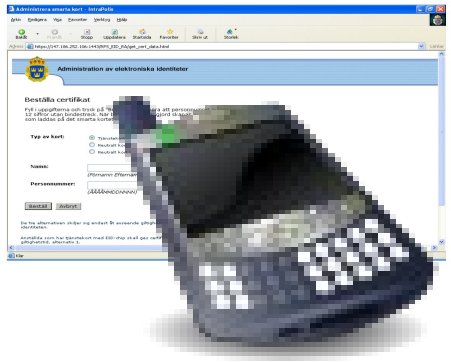
- *An example*
  - *600 user per month had log-on problems*
  - *4 application represented 50 % of the problems*

PKI today

- Easy to extend the PKI
  - New CA for every needed function
    * Server certificates
    * VPN certificates
    * Qualified signature certificates
    * ePassport certificates (generation 1 & 2)
    * Encryption certificates

The future

- User administration portal
  - Self administration of user certificates for mobile devices, based on users smart card
  - Apply for applications and rights
  - Reset password in applications
  - Administer personal information



- Electronic signature workflow
  - Internal documents
  - Between governments

- Other Swedish governments
  - Similar approach
  - Cooperation between governments
  - Cross certification between governments

Tullverket

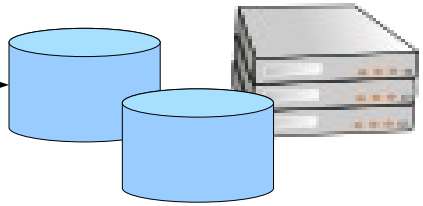
Skatteverket

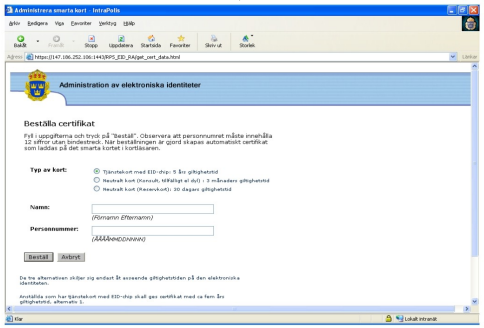
Arbetsförmedlingen

KUSTBEVAKNINGEN
SWEDISH COAST GUARD

Police Administration Portal (PAP)

PWD reset
User info





Request
certificate

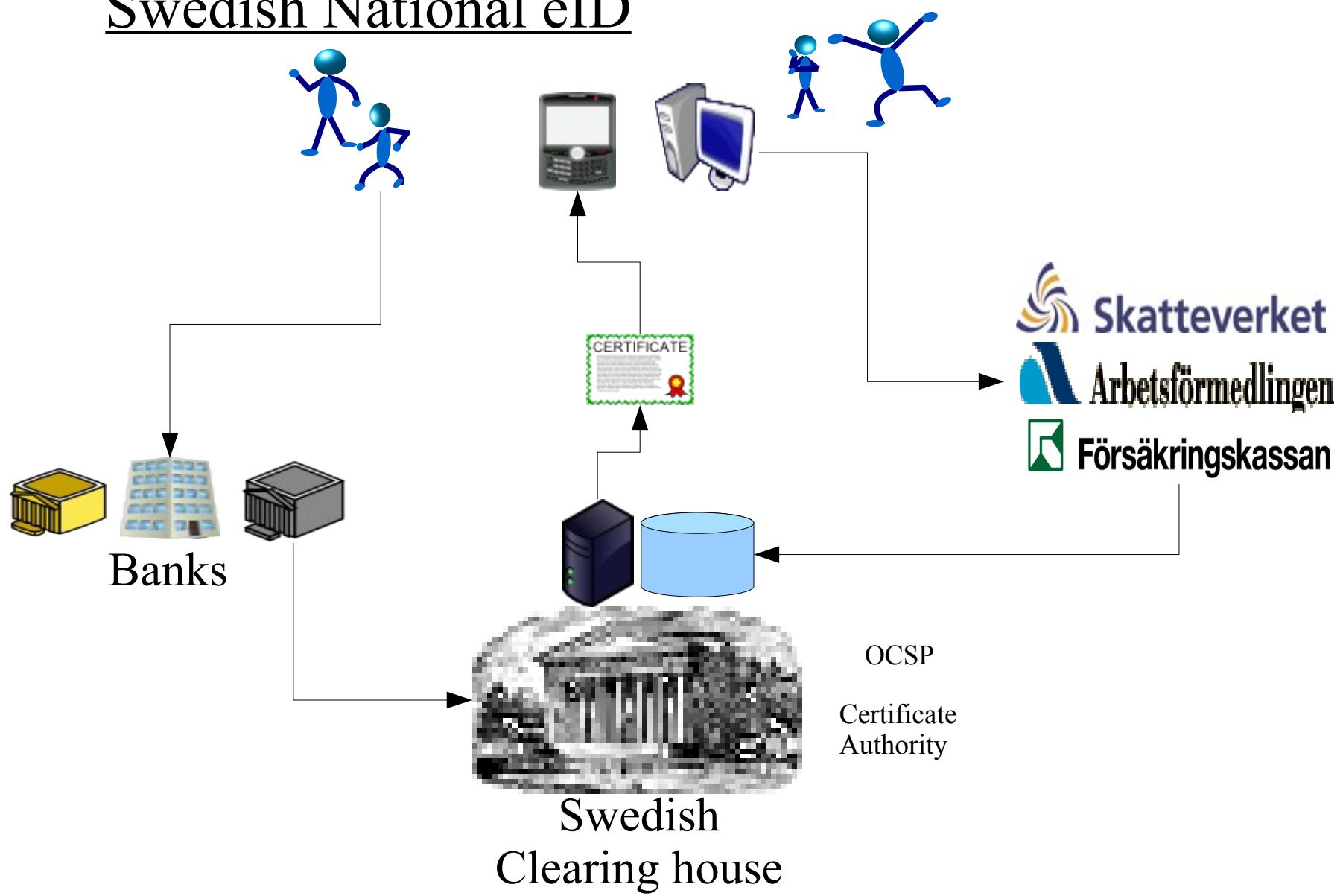
PKCS#12

Swedish national PKI

- The Swedish banks
  - Has the business relation with the citizen
  - Identifies the user
  - Provides the user with enrolment credentials
- The Swedish clearing house, BGC
  - Issues the user certificate
- Business model
  - Based on the use of the service
  - Banks and governments accept the certificates

Skatteverket Arbetsförmedlingen Försäkringskassan

Swedish National eID



Questions ?

PrimeKey Solutions
Lars Bagnert
lars.bagnert@primekey.se