

# WPKI Project and Infrastructure

## Presentation

# WPKI Project – Why?

- Stimulate/enable a whole market of services that require a secure identification of the user and enables legally accepted signing
  - banking
  - “citizen services” from government, authorities etc.
  - enterprise services
  - gambling
  - etc.
- A hard key WPKI solution can provide increased security compared to both soft key and other hard key PKI-solutions
- A WPKI solution using mobile telephones increases mobility for PKI
  - no restriction to a particular PC with a downloaded client/certificate
  - no need for dedicated hardware (card readers etc)
- A WPKI-solution is an infrastructure
  - Requires coordination of several player’s assets and motives/incentives
  - Standardised interfaces – both technical and business

# WPKI Project – Who?

The parties are:

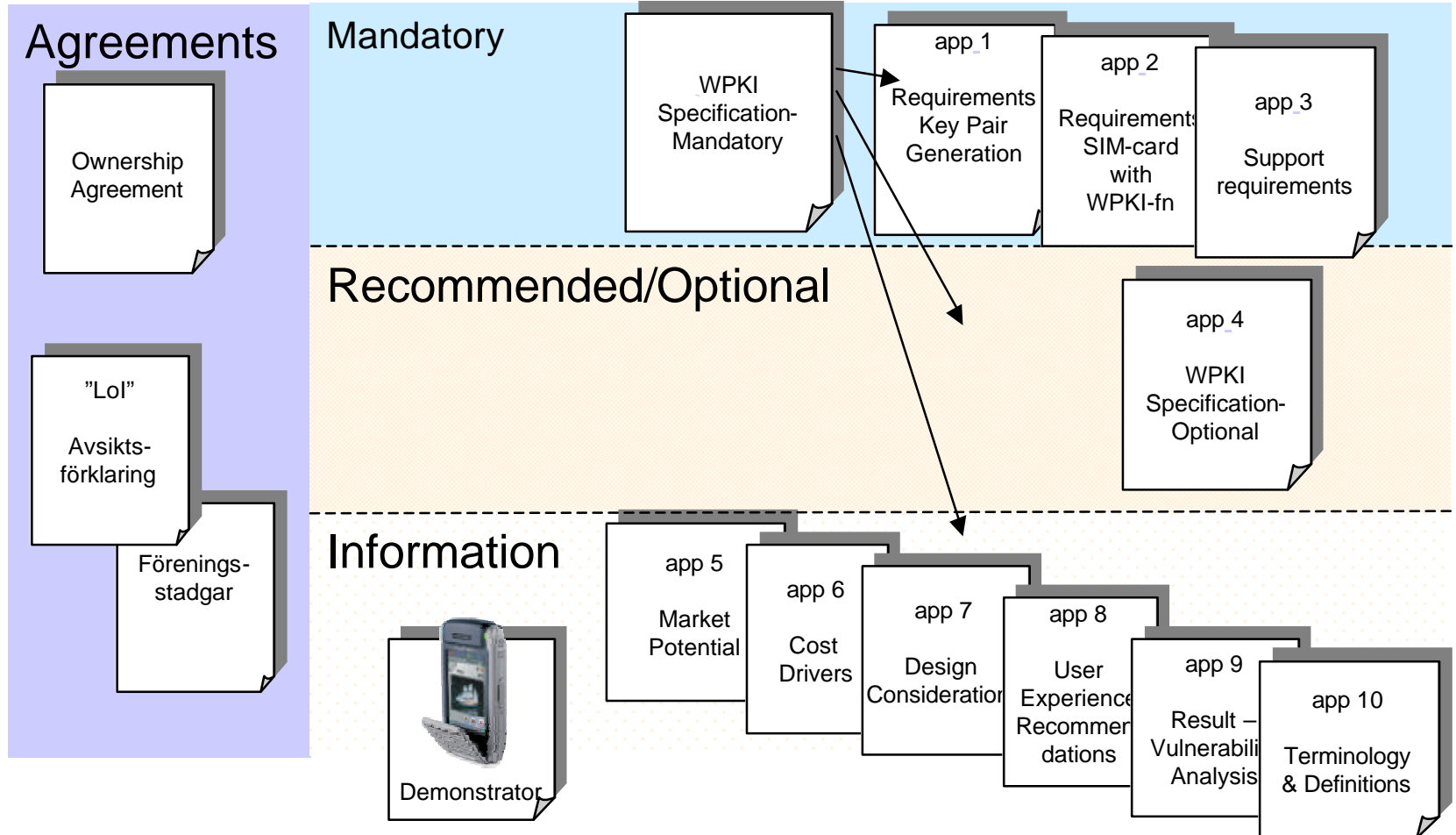
- BankID (BID)
- All "BID-banks" (Handelsbanken, Förenings Sparbanken, Danske Bank etc)
- Mobile Operators (TeliaSonera, Tele2, Vodafone)
- Ericsson

# WPKI Infrastructure – What?

- A standardised infrastructure with well-defined roles and agreed interfaces for RA/CAs, Mobile Operators, Relying Parties and End Users
- A hard key PKI-solution based on
  - existing infrastructure (mobile phones, SIM-cards, mobile Internet access)
  - open and widely accepted standards from OMA (Open Mobile Alliance) on WAP, WIM etc.
- Making the mobile telephone a personal trusted device in a variety of contexts and for a multitude of services
  - the mobile telephone is always playing the role as "security channel"
  - the "information channel" can be a PC, a digital TV-set, the mobile itself etc.

# WPKI Project – Deliverables

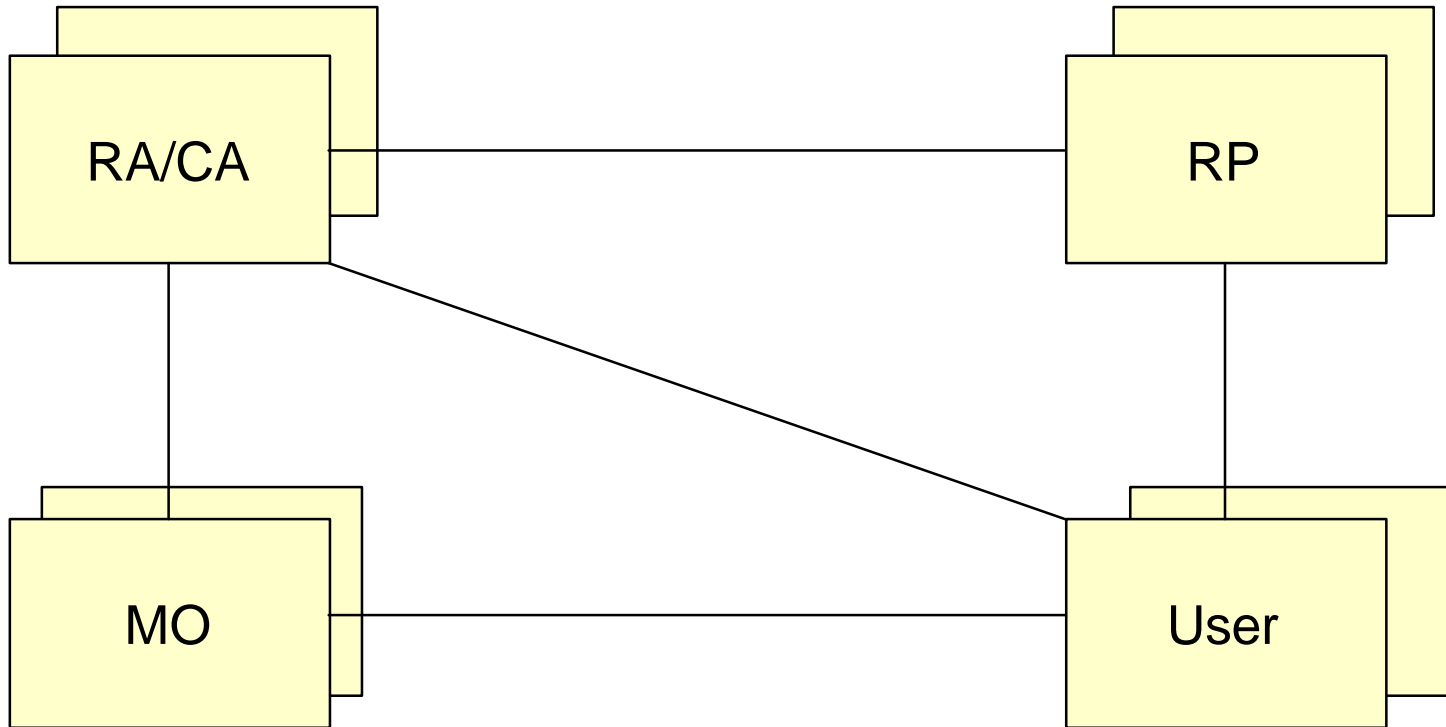
Agreements, standards, demonstrator, "maintaining body"....



# WPKI Infrastructure – When?

- The WPKI-specs 1.0 were delivered from the WPKI project on Dec 21, 2004
  - The WPKI specs 1.0 were published on [www.wpki.net](http://www.wpki.net) March 23, 2005
  - The WPKI Non-Profit Association was founded March 30, 2005
- ⇒ Anyone can start implementing their part of the infrastructure and products&services building upon the specs
- ⇒ Pilots likely during 2005 in smaller scale:  
Corporate services  
Trials with well-defined user groups

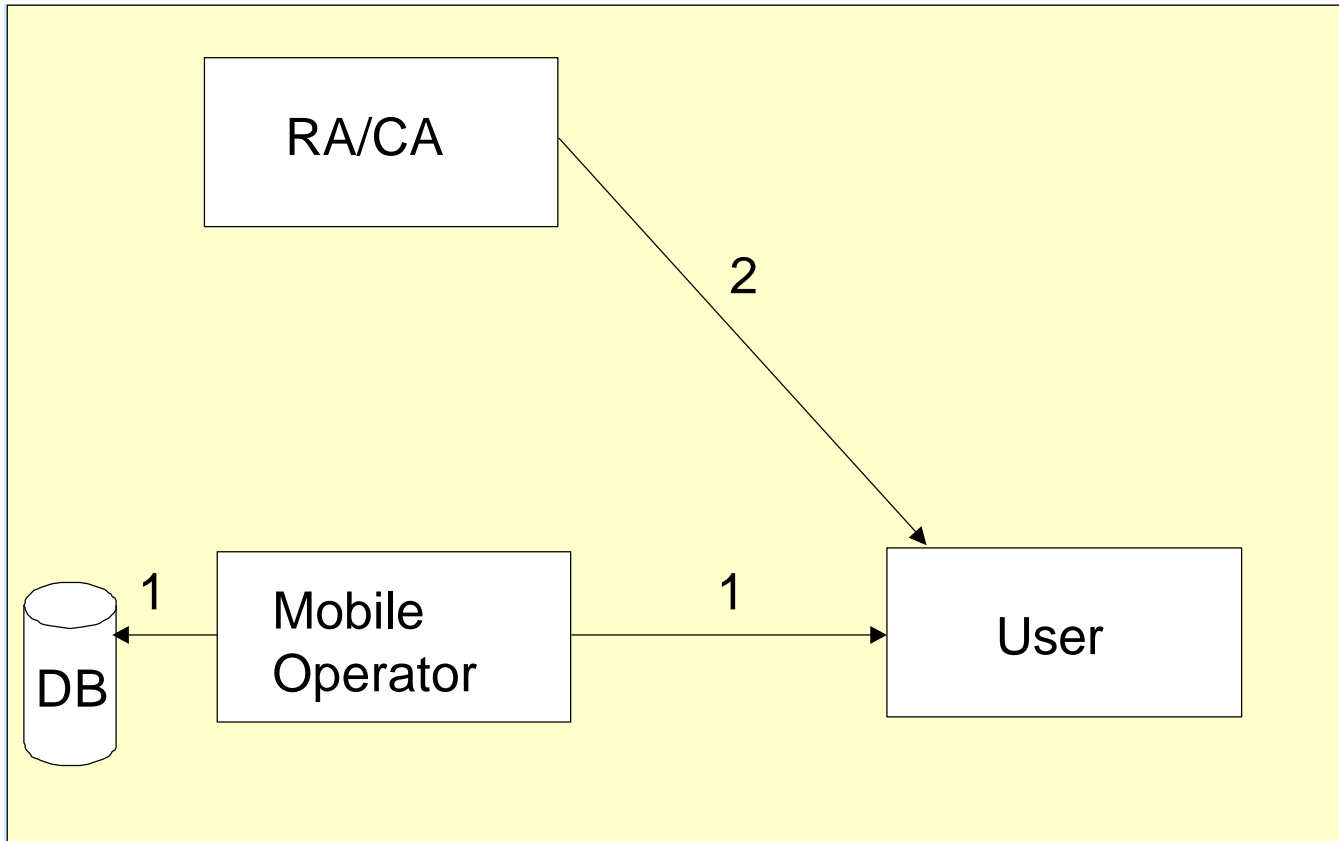
# WPKI Infrastructure - Roles



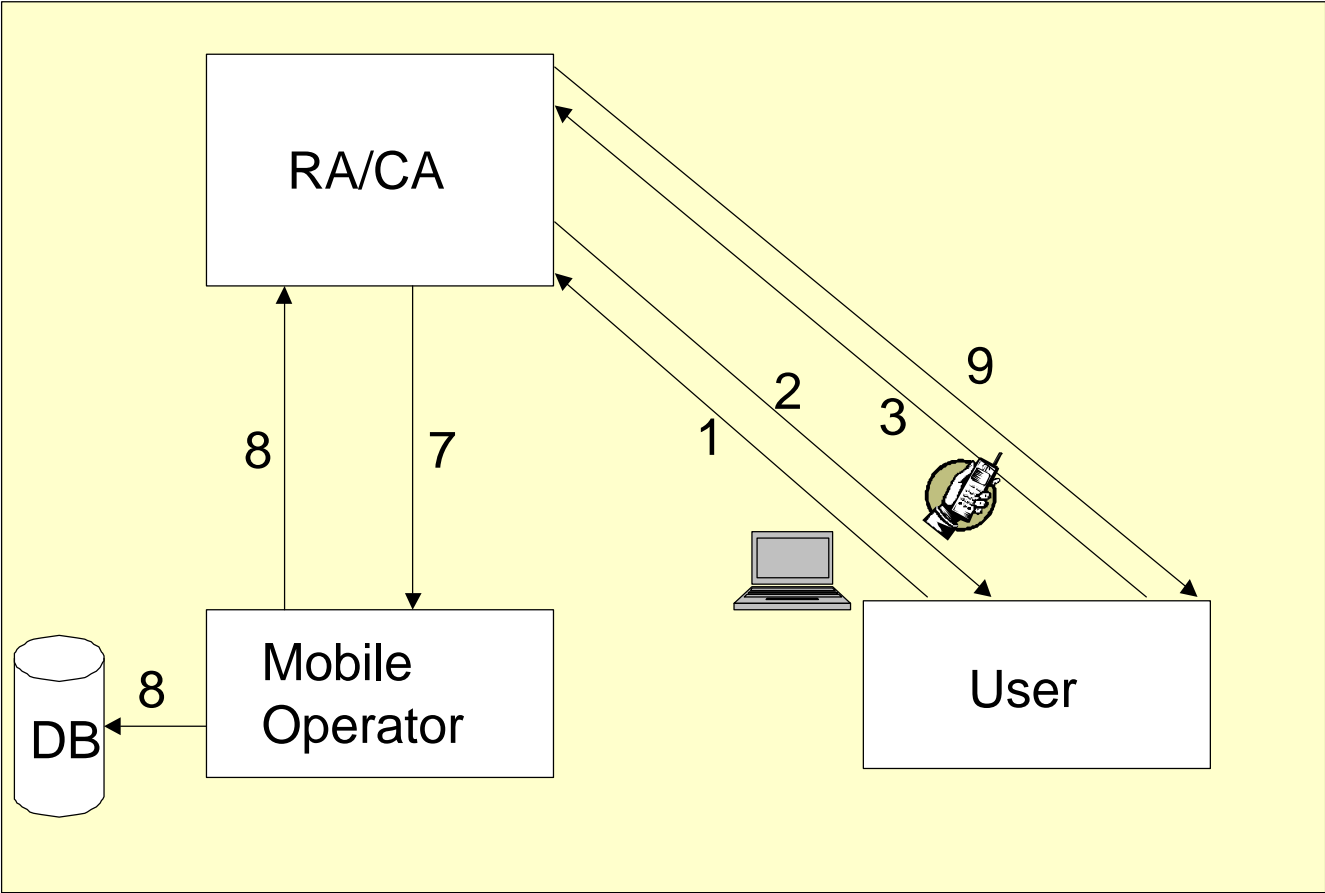
# WPKI Infrastructure – Roles cont.

- MO – Mobile Operator
  - Offer Mobile Internet access
  - Issue SIM-cards with WPKI functionality, i.e with private keypair and a URL pointing out the device certificate
  - Keep a database with device certificates (incl public keys)
- RA/CA – Certificate issuer
  - Perform Original Identification
  - Issue mobile e-ID/user certificate
  - Store user certificate
- RP – Relying Party
  - Offer the service that uses the WPKI infrastructure
  - Integrate WPKI in the service dialogue
- User – End User
  - User of services and holder of mobile e-ID

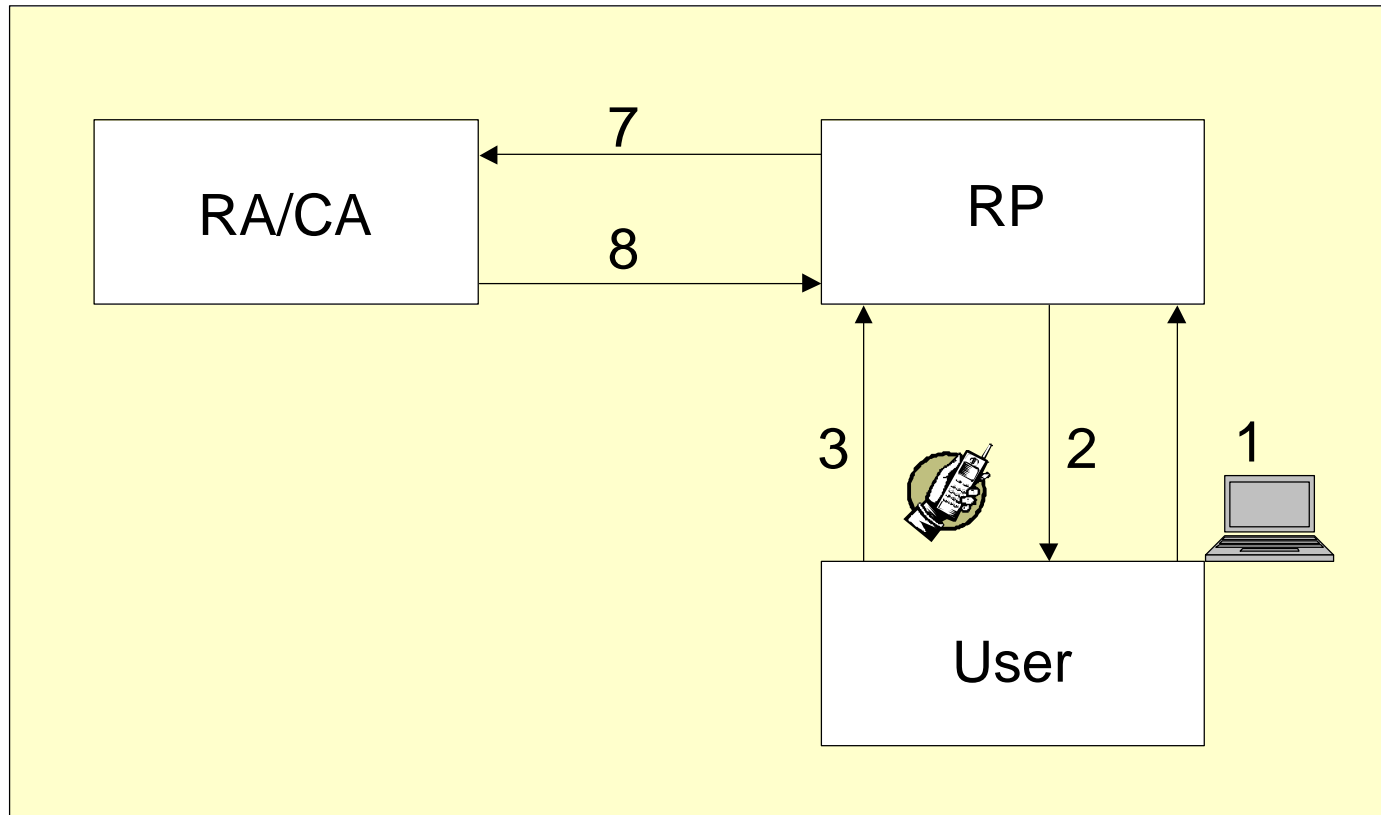
# WPKI Infrastructure - Pre-enrolment



# WPKI Infrastructure – Enrolment



# WPKI Infrastructure – Usage



# WPKI Infrastructure – Critical Success Factors

- Market growth over time
  - steadily increasing penetration of WPKI-enabled mobile telephones
  - smooth upgrade to SIM-cards with WPKI functionality
  - stimulating new types of services requiring secure identification
- Usability
  - quick to get started, learn and remember
  - easily portable between different information channels
  - easily portable between different mobile telephones
  - recognisable elements in the security dialogue (steps, terminology, buttons etc) between different services
- Cost
  - price/cost competitive with current alternatives for all involved parties
- Security
  - offering a higher security level than current alternatives when needed