## Security Policies (23. November 2006)

# Security challenges in role-based identity management

Josef Noll,
Prof. stip., UniK
Senior Advisor, Movation AS
josef@unik.no

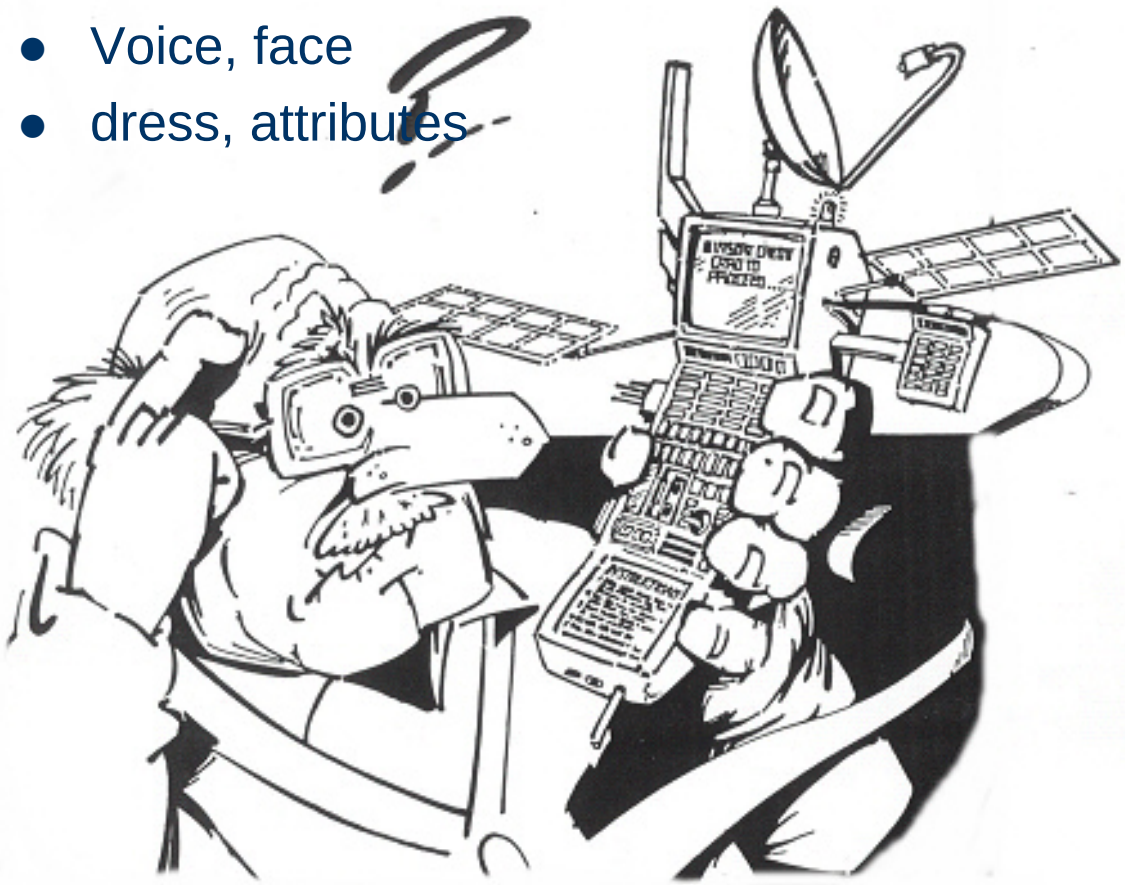
# Introduction

- Identity is attributes of your persona
  - Social, Corporate and Private IDs
- Internet was built without an identity layer
  - Identity 2.0 stems from Web 2.0
  - People, information and software
  - More user-oriented (wikis, comments, tags)
  - More seamless web services (AJAX)
- Service related security
  - Provide just the information which is necessary
- Mobile challenges

# Identity 2.0

Real world: see and/or talk

- Voice, face
- dress, attributes



Virtual world: email, web

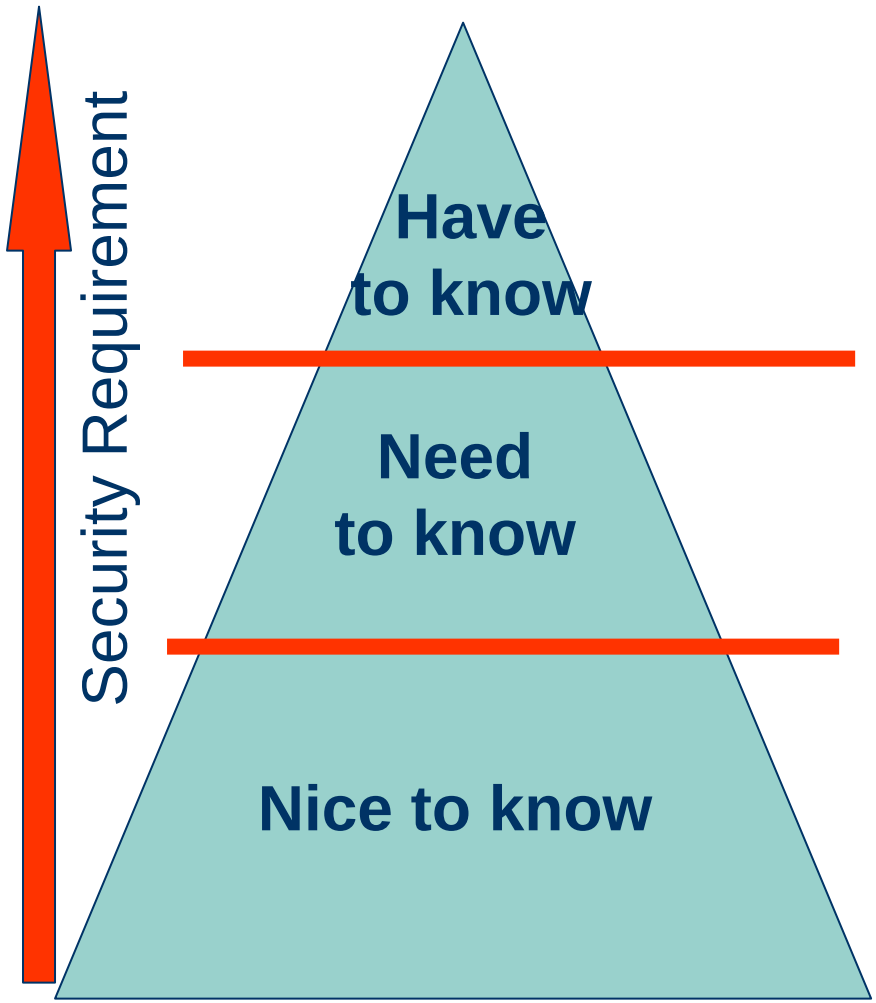
- Username, passwd
- SIM, PKI
- Security, privacy

Service world (between providers)

- Identity management
- Service level agreement (SLA)
- Trust relation

Security requirements:

# Application specific security




Examples:

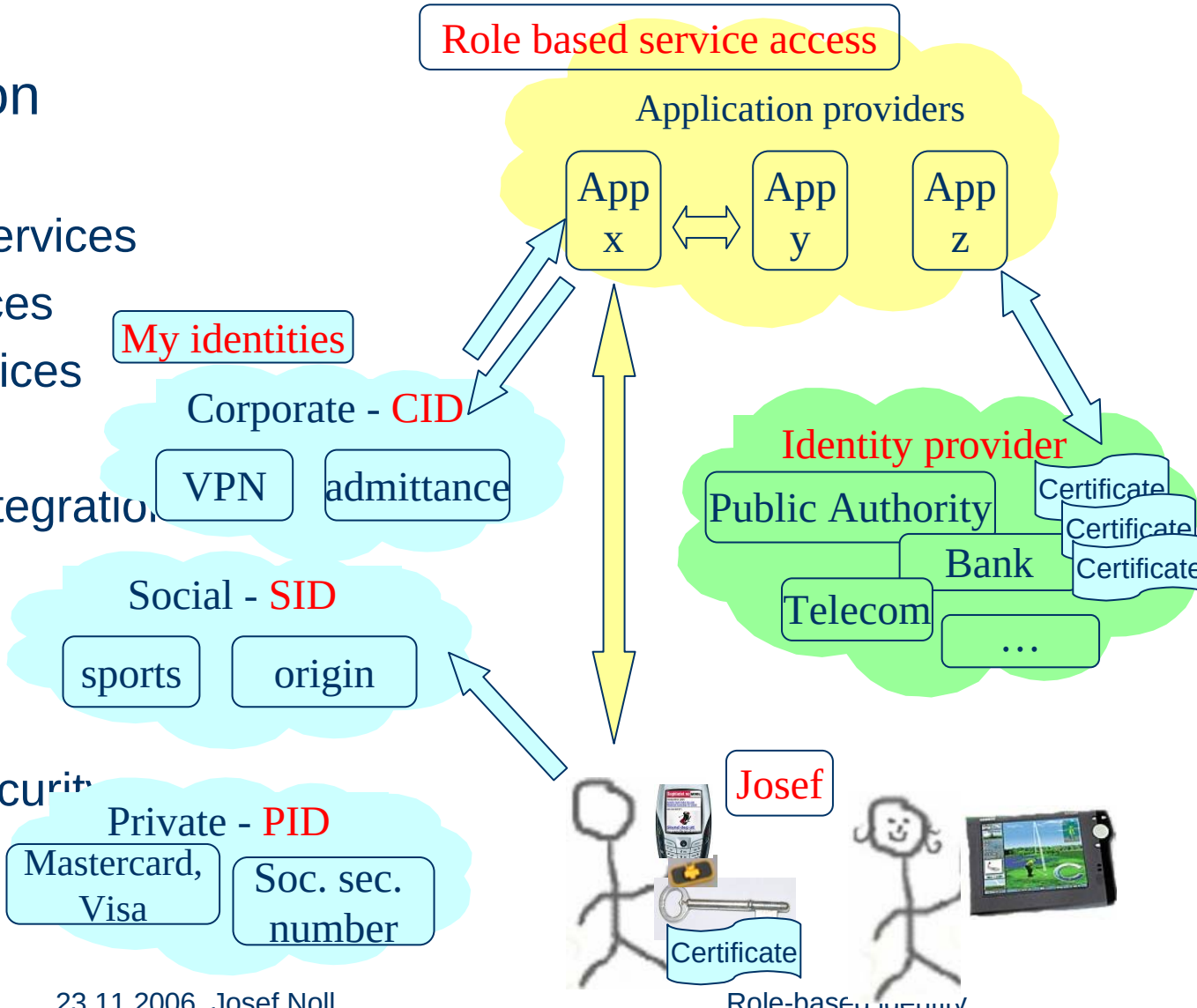
mHandel,
VPN

Intranet, email,
Admittance

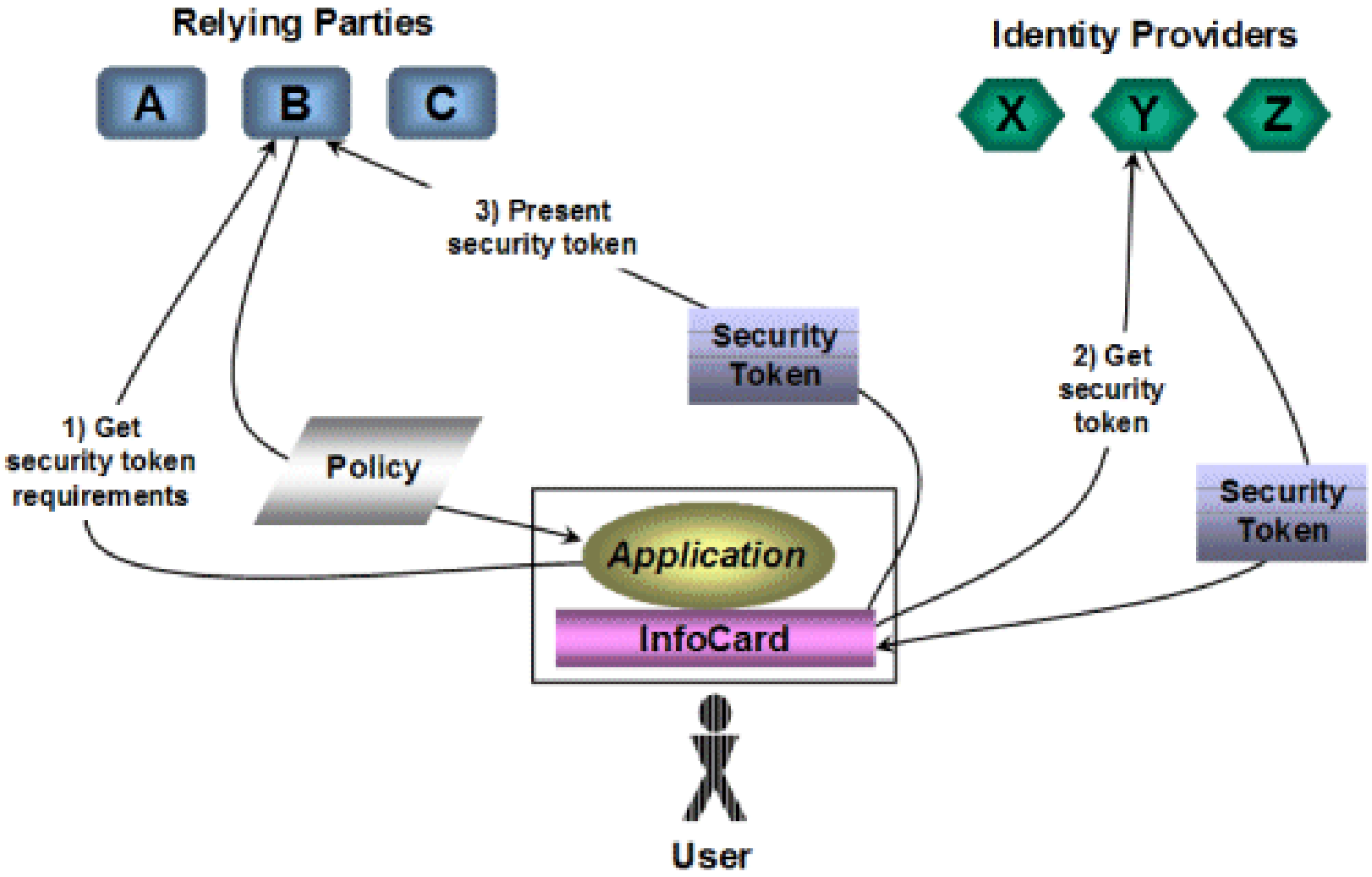
Network access

# Challenge: Role based service access

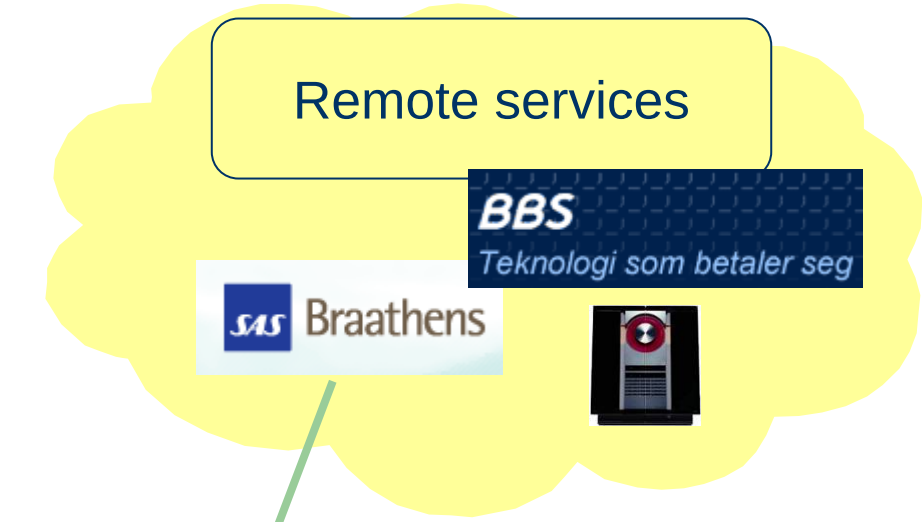
- Next Generation Applications:
  - Customized services
  - Remote services
  - Proximity services
  - High flexibility
  - Telecom-IT integration
- Challenges
  - Privacy
  - Trust
  - Application security



# Internet Identity Architecture
## [Microsoft / SXIP]

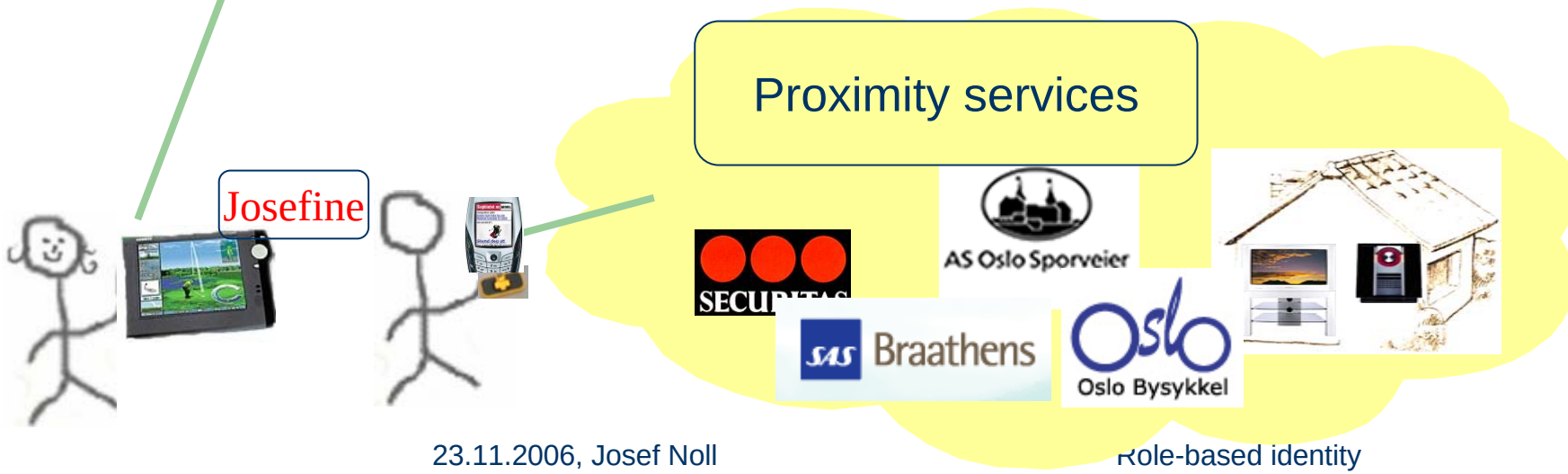


# New role:
# Identity provider





- Who provides?
  - ID provider
- Where to store?
  - Network
  - Phone
- How to store/backup?
  - long term, short term



# Proximity Services:
# NFC – Near field communication

- Based on RFID technology at 13.56 MHz
- Typical operating distance 10 cm
- Compatible with RFID
- Data rate today up to 424 kbit/s
- Philips and Sony

- ECMA-340, ISO/IEC 18092 & ECMA-352, …standards
- Powered and non-self powered devices

# Identity 2.0
# Goals and Suggestions

- User centric
  - More like real life ID's (passport, license)
  - Multiple ID's
  - Choose attributes ~more privacy
- ID providers
  - Multiple providers
  - Self providing
- Mobile, and de-centralized

SID
-low/medium security
-origin, history
-social network

Identity provider

Certificate

Certificate

CID
-medium/high security
-user preferences, colleagues
-VPN, access

PID
-medium/high security
-medium: DRM
-high: user get known when used
-need user confirmation
-stored in mobile?

# MyBank example:
# Banking from the mobile phone

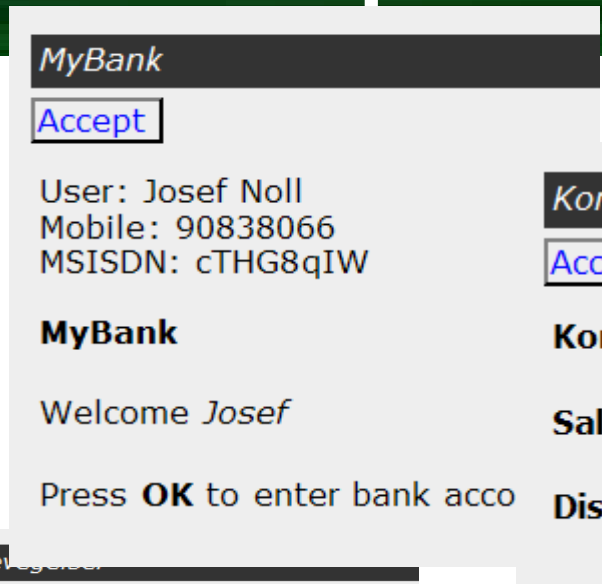
BBS
Teknologi som betaler seg

User incentive:

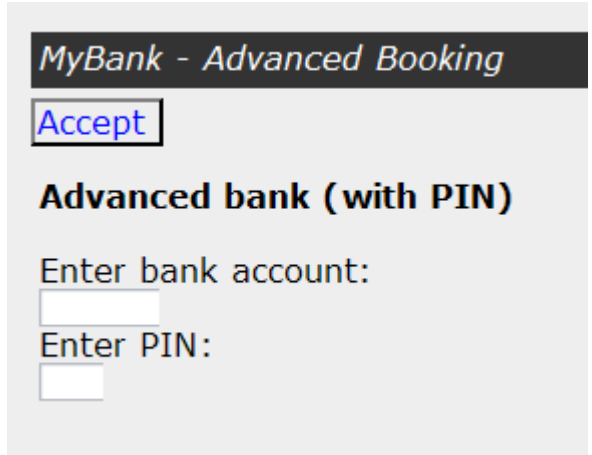
- "My account is just one click away"
- "enhanced security for transactions"

→Phone (SIM) authentication

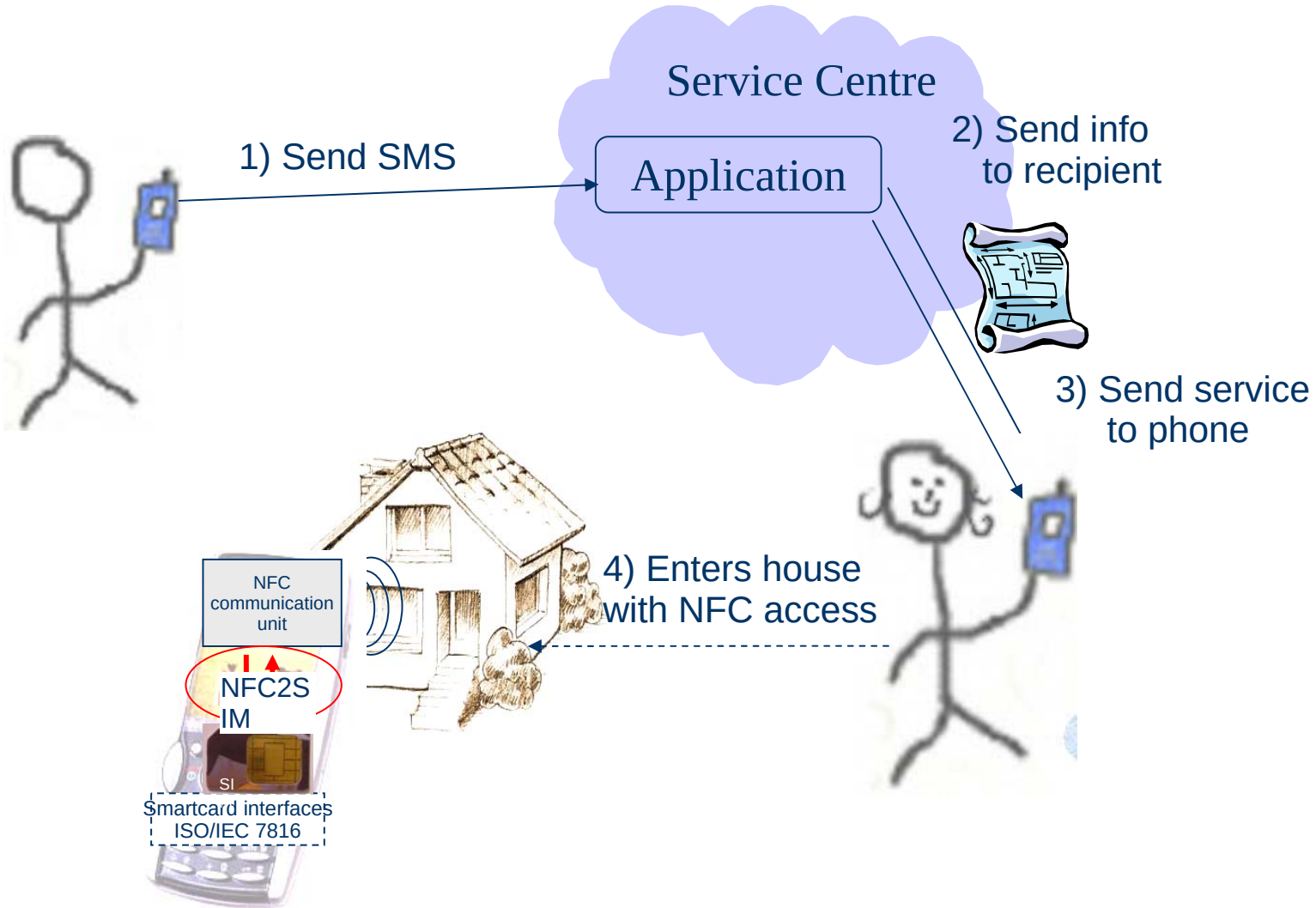
→Level 2 security through PKI/BankID/PIN?





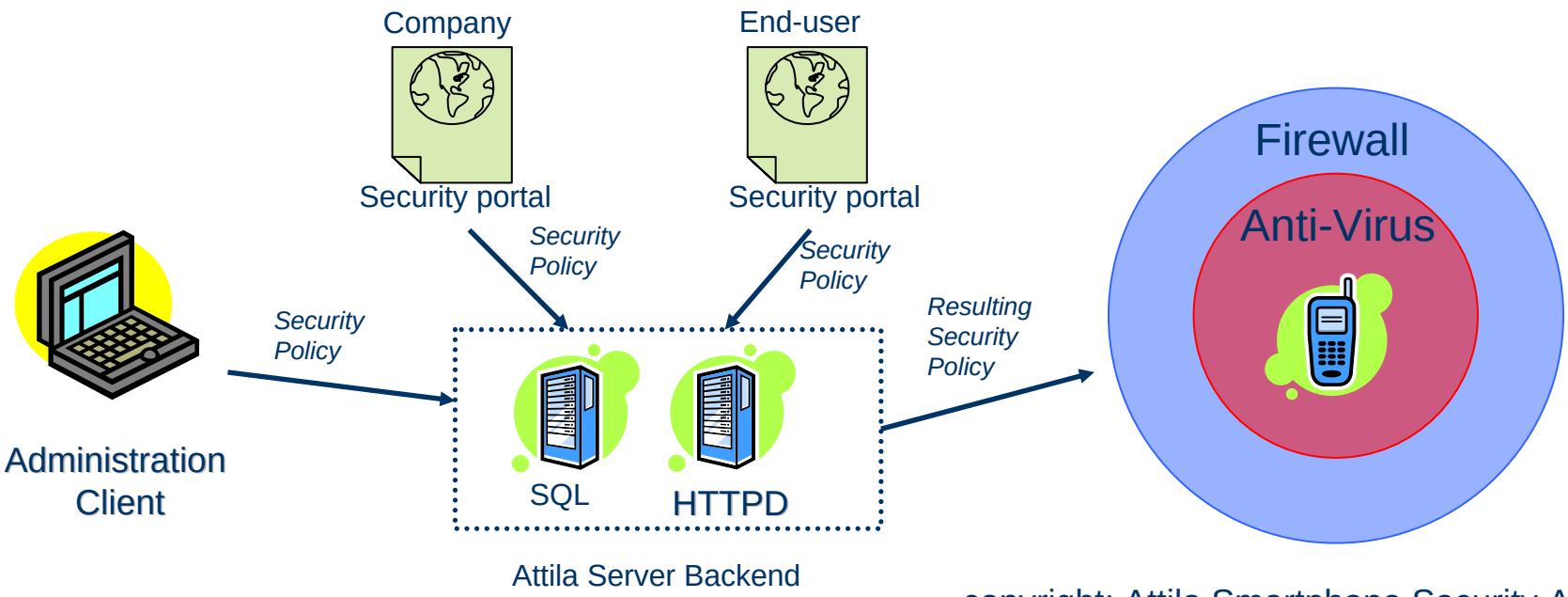



# Proximity Service Example:
# SMS key access



# Security Policy, example:
# Attila Smartphone Security

- Turnkey solution to administrate the firewall and 3rd Party anti-virus configuration on thousands of phones.
- Different management possibilities for Operators, companies and end-user.



# Conclusions

- The user is always connected to services using multiple networks
- Service related information
  - privacy (just what is needed)
  - application security
- Identity is attributes of your persona
  - Social, Corporate and Private IDs
- Identity provision
  - from public authorities, banks, mobile operators, …
  - using preferences, keys and certificates
  - distributed in network and SIM