RegioPKI®

Complete National / Regional PKI system enabling

Electronic secured transactions
based on Trust, Security & Digital Signatures

for

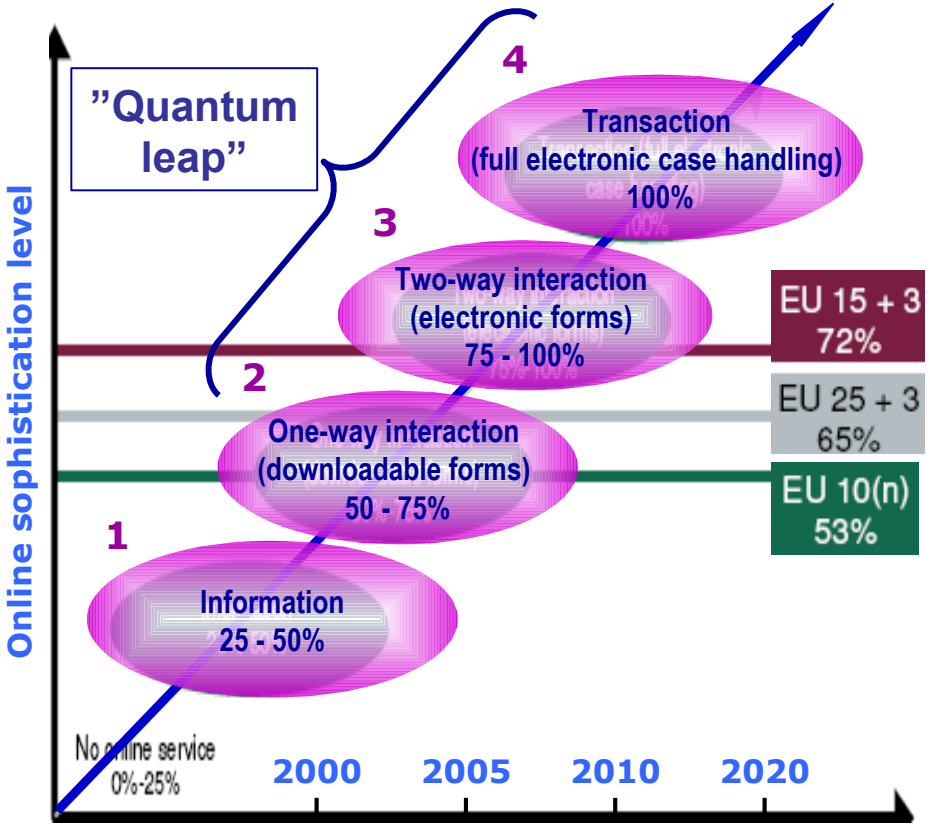
eServices & eBusinesses

Tapio Rissanen
Conseils Oy SimplySecure
EuroConseils sprl

2006

"Online Availability of Public Services: How is Europe Progressing?"

Overall Results



Source: DG-Information and Media Study 4 March 2005

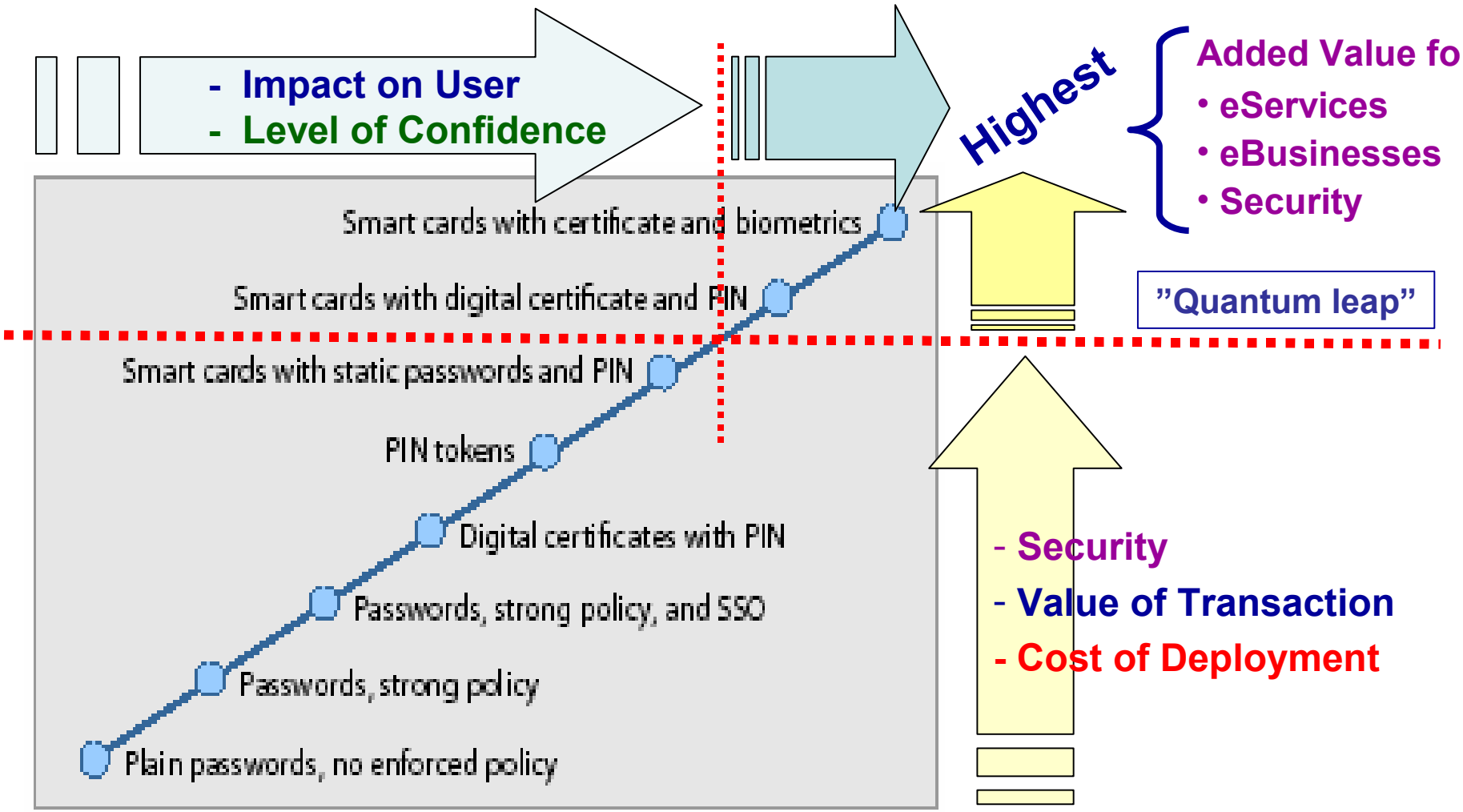
Problems

- Requirement for service sophistication is progressive
- Lack of Interoperability & compatibility between actual systems
- **Change from phase 2 to 3 and 4 requires Quantum leap in trust, security and privacy protection levels for interactive e-Services**

Solutions

- Adequate authentication of users to eServices (is happening)
- **Trustable Digital Signature – PKI infrastructure**
- **Cross Certification and Bridging of Digital Certificates, CA hierarchies**

Evaluation of Authentication types



(Source: Forrester Research Inc., USA)

PKI infrastructure

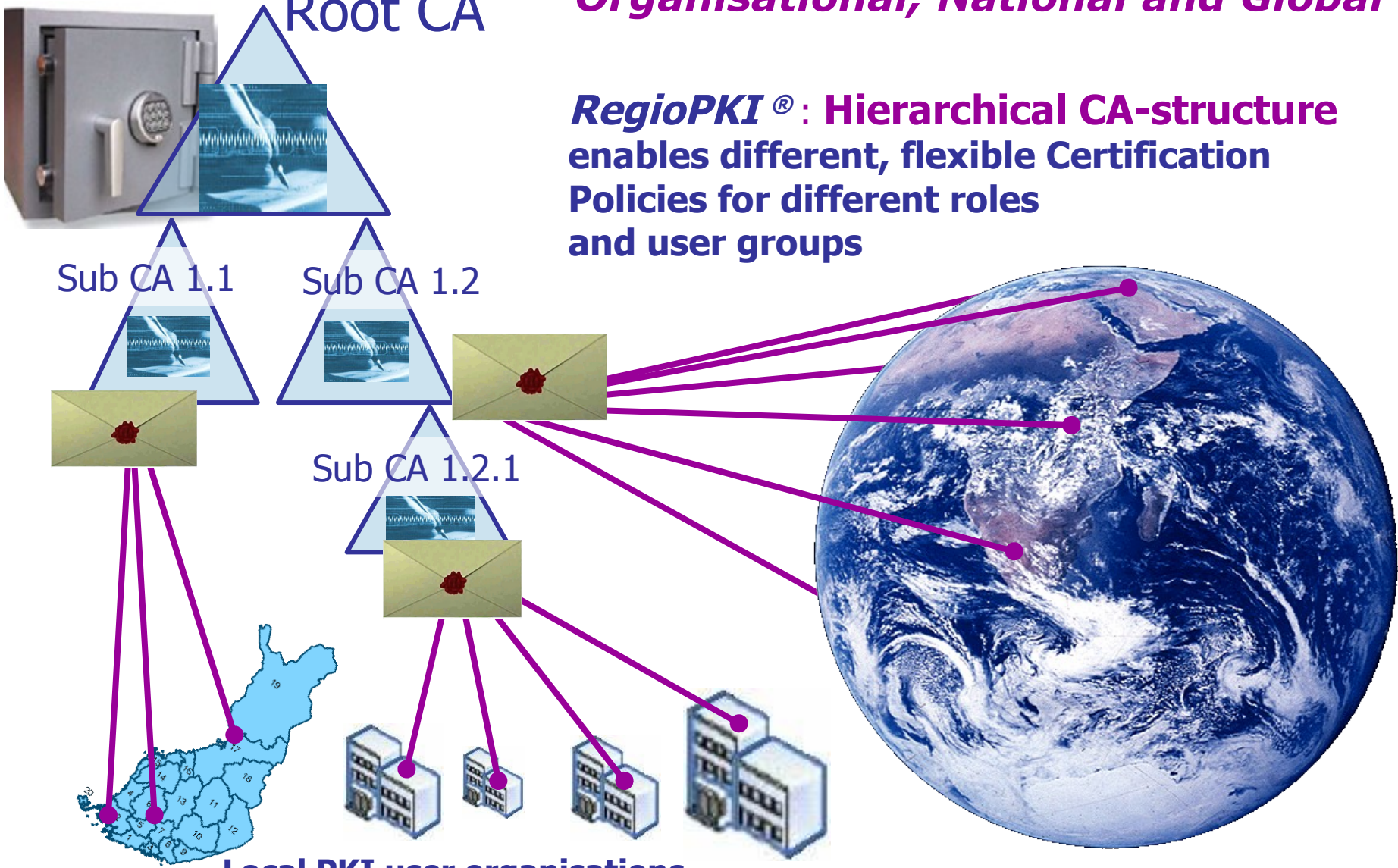
- **PKI is the only generally accepted technology, that fulfils the trust and security requirements of electronic data and information management within ICT systems**
- According to various studies, **Strong authentication with Single Sign On (SSO) offers remarkable opportunities for efficiency improvements and savings within the organisation, its value chains and processes.** (Source: Forrester Research Inc., USA)
- **Digital signatures are needed to certify the non-repudiation of legally binding electronic transactions, data, information or documents in open digital world.**

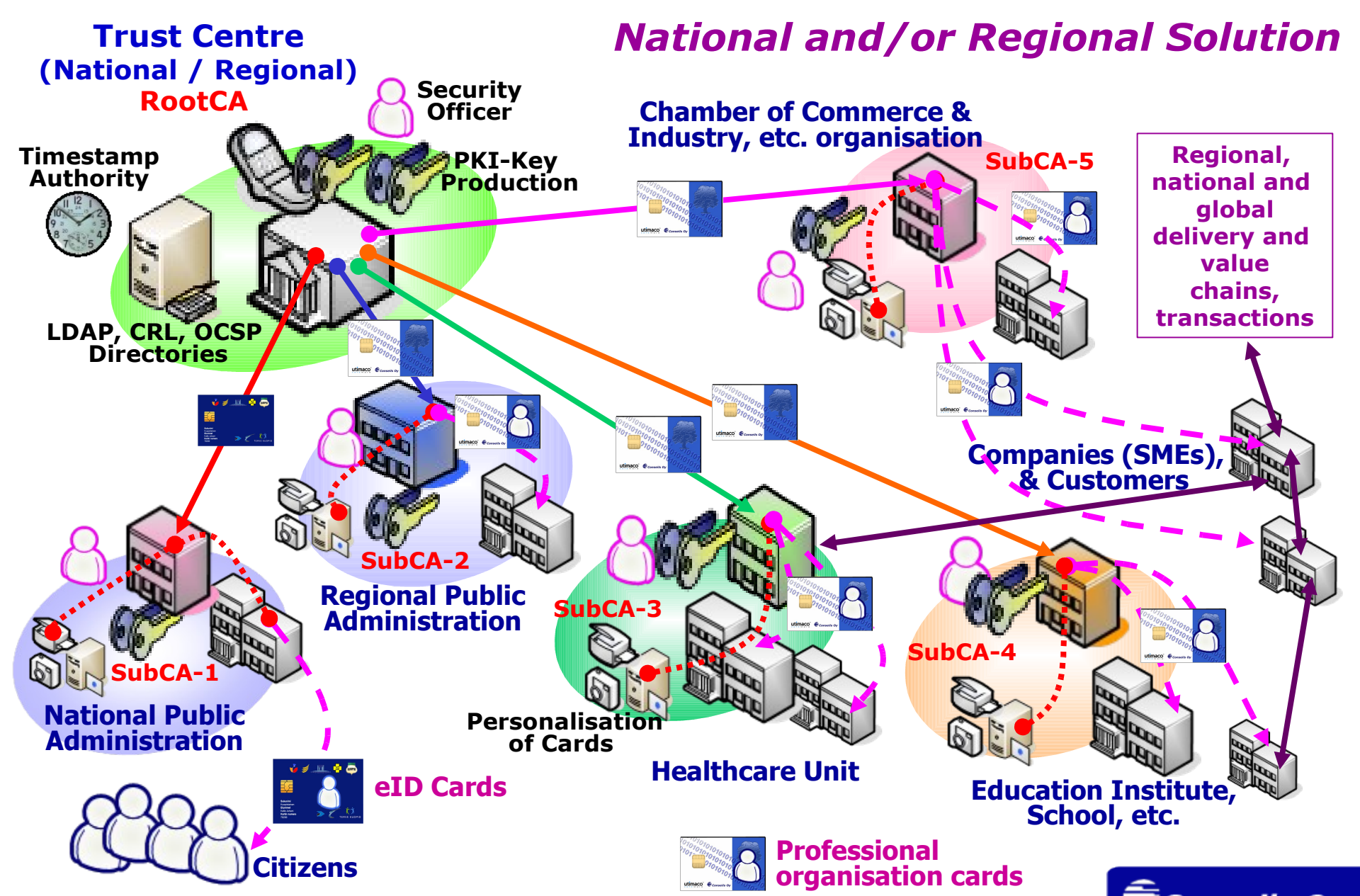
N.B.:

Digital transactions carried out within systems based on other than PKI authentication procedures (e.g. passwords), do not replace digital signatures, as the validity of these actions is limited only to the system itself (= documents are neither legally binding nor auditable if archived electronically outside the same system)

Organisational, National and Global

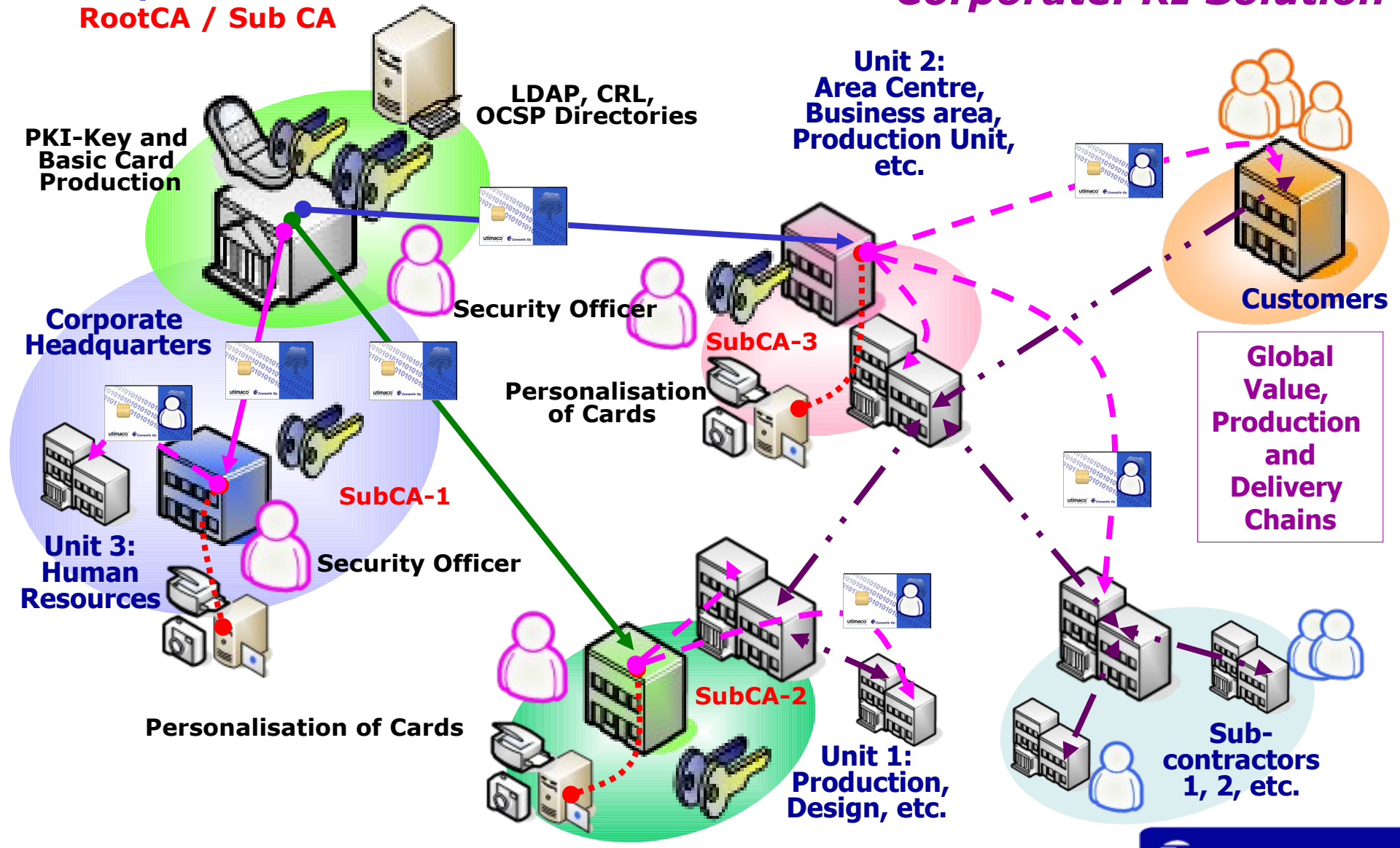
RegioPKI ®: Hierarchical CA-structure
enables different, flexible Certification Policies for different roles and user groups



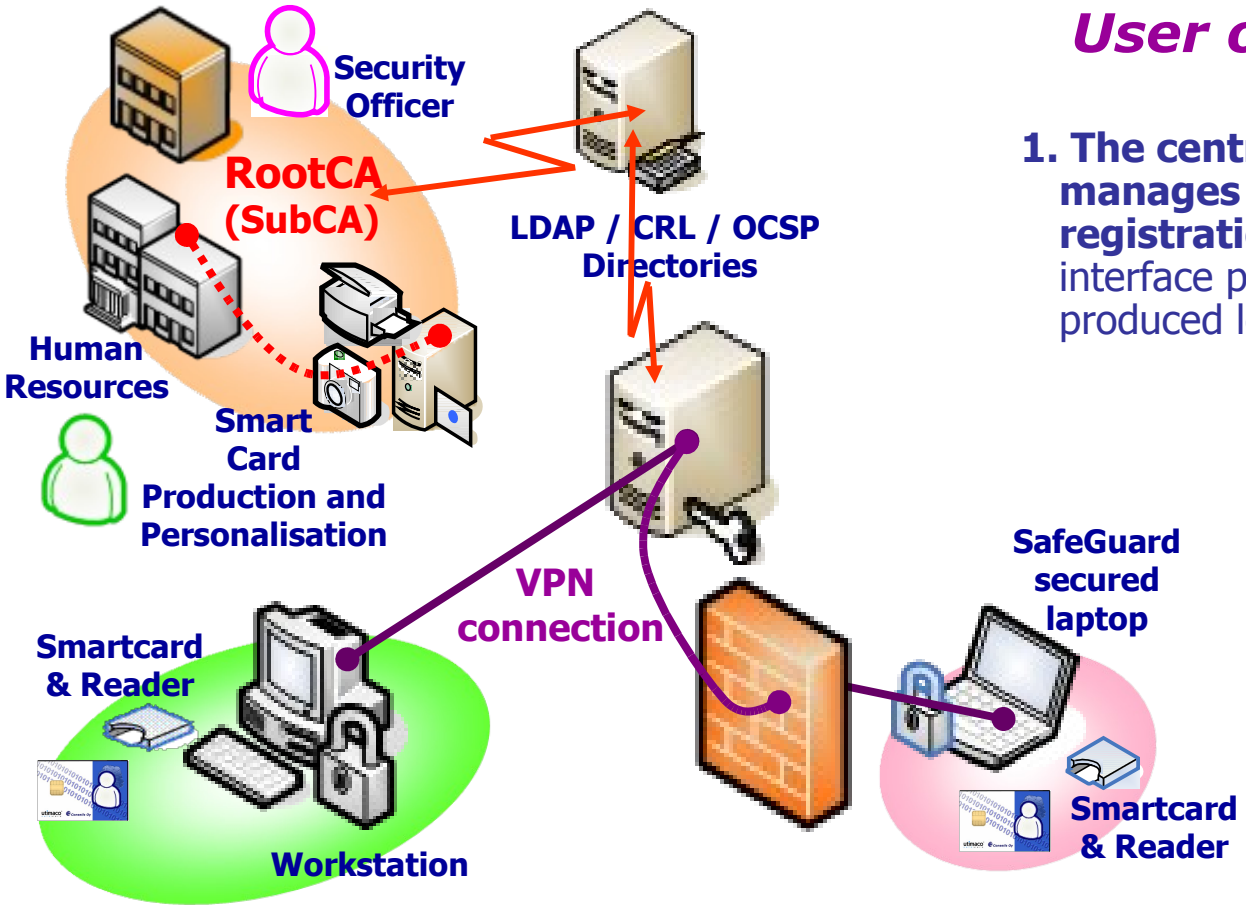


Corporate Trust Centre
RootCA / Sub CA

CorporatePKI Solution



User organisation system



1. **The central PKI service provides and manages all certificates based on registration requests.** All, including dual interface professional smart cards can be produced locally, close to the users.

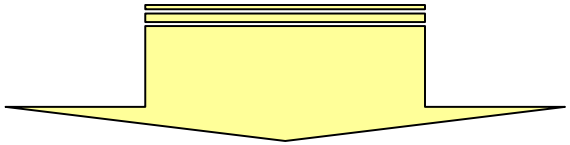
2. **PKI certificates are used for strong user authentication, data encryption and digital signatures.** Data is encrypted, hence data and information on servers and databases are secured and are accessible only to users with appropriate permissions, even as a subcontractor or customer.

3. **Remote and extranet connections for the entire organisation and / or value chain are provided by means of a VPN** (Virtual Private Network). The same strong authentication and encryption methods are used in remote working places as in the Intranet, hence the whole networking organisation is secured equally. For example somebody teleworking from home does not have any difference in user rights between his / her work office and home office.

Certification levels - total flexibility

RegioPKI® supports all certificate models:

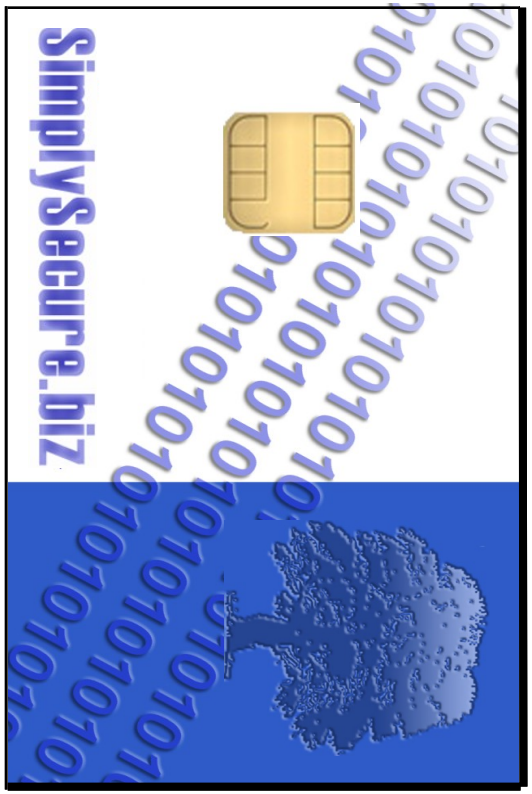
- **Qualified Certificates** require audited certification of the Trust Centre
  - » expensive and do not offer the best flexibility for the organisation
- **Advanced certificates** offer flexibility for organisational use
  - » sufficient for eBusinesses and daily routines



- **Hybrid solution** offers flexibility and non-repudiation on the same card:
  - » Qualified certificates for legally valid signatures and
  - » Advanced Certificates for eBusiness & organisation's purposes (authentication, encryption)

***RegioPKI*® enables Qualified Certificates, if required**

Applications of a dual interface, multipurpose smart card



PKI Management

- **Key Management**
  ***RegioPKI®* system key management** is based on FIPS 140-2 Level 3 certified **Hardware Security Modules** (HSM), guaranteeing highest security level of key management security
- **Card and Token Management**
  ***RegioPKI®* system supports best-of-breed card and token management systems**, enabling effective and wide-ranging use of different card- and token-based applications and services (PKI, Java, MULTOS, RFID, HID, Legic, etc.)
- **Identity Management and Federation**
  With its PKI-based identification and authentication, ***RegioPKI®* system supports and strengthens built-in or third party Identity Management systems and Identity Federation solutions and schemes, enabling secure and trustworthy communication of user rights and credentials across organisations.**
  - *Identity Federation plays a key role in securing user access rights management in the extended organisation - PKI based identification is one of the strongest links in the trust chain.*

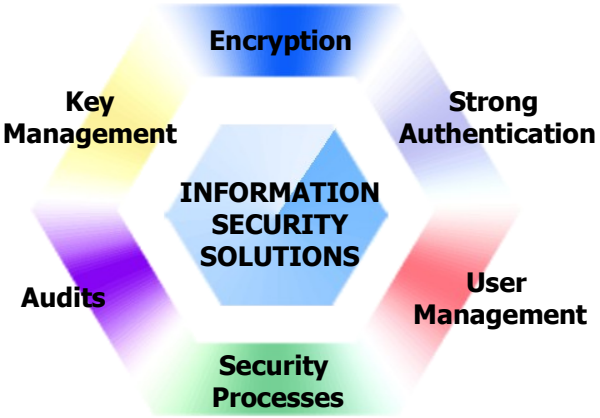
Project Proposal for harmonizing global PKI services

- **In order to maximise user trust and to harmonise existing and future PKI infrastructures, the most feasible solutions are:**
  - Cross Certification
  - Bridging of Digital Certificates
  - Setting up of hierarchical CA services
- **The most promising solution is the setting up of a hierarchical Root CA / Sub-CA TREE structure, which guarantees strong level of trust within the same "family-tree",** with high level of interoperability, flexibility and service availability between different CA services
- **I propose to set up a two layer Consortium open to any Certification Authority fulfilling legal and other conditions of the Consortium**
  - Core Consortium consisting of the most advanced European Certification Authorities (CAs) in charge of PKI infrastructure
  - Second layer consisting of CAs from any country (Europe and outside) willing to join the consortium (also at later stage)
- **First phase and European funding from the EU Commission's Competitiveness, Innovation Programme (CIP), starting 1/1/2007**

Trust and Security Solutions for ICT processes

Conseils Oy SimplySecure & EuroConseils

Support and advice for public & private organisations
- to create trust and security strategies and solutions,
- for the conversion to trust and security systems



- ***Consultancy***
  - strategic planning
  - creation of certification policies
  - other project-based consultancy
  - EU-and other funding opportunities
- ***Training***
  - trust and security basics
  - preparation against risks
  - take-up of trust and security systems
- ***Products***
  - ***RegioPKI*** **-** national/regional PKI system solutions
  - ***BusinessPKI and CorporatePKI*** – turn-key PKI system solutions for public and private organisations
  - Other ICT related security products

Conseils Oy SimplySecure
Teemu Rissanen*, Managing Director*
Hämeentie 153 B, FIN-00560 HELSINKI
mobile: +358(0)50 379 5343
e-mail: teemu.rissanen@SimplySecure.biz

EuroConseils sprl - EU*project****ACADEMY***
Tapio Rissanen*, Principal Consultant*
Av. Colonel Daumerie 5, B-1150 BRUSSELS
tel: +32 2 779 0503
GSM (BE): +32 485 330 102
e-mail: tapio.rissanen@SimplySecure.biz

Web shop (FI): www.conseils.fi/shop/

Website & shop (European, opening soon): www.simplysecure.biz

RegioPKI® - a Complete PKI System

Thank you

for your attention