Usability is King

How to overcome deficiencies for security deployment

Open Workshop
Beyond IP – Security for the Future Internet

Fachgruppe 5.2.4 "Mobilität in IP basierten Netzen"
Fachgruppe 5.2.2. "Sicherheit in Netzen"

InCharge Systems Inc.
Wilhelm Wimmreuter

28. Nov. 2011

wilhelm@wimmreuter.de

In Cooperation with the

Real-Time Communications Lab
ILLINOIS INSTITUTE OF TECHNOLOGY- School of Applied Technology

Content

- Introduction
- The Users Dilemma
- Two Basic Solutions
- Information Flow and Samples
- Conclusion / what's missing

About this session

- **This session is**
  - a discussion of pains security induces to users
  - discussing things users might need
  - about some ideas to give users confidence & control
  - and what operators can do to make usage painless

- **This session is not**
  - an other indoctrination to change passwords frequently
  - an other idea to bind customers to reduce customer churn
  - how to make security a tool for intercept and spying
  - to find or judge security schemes

Standards are there, but they do not make the user happy

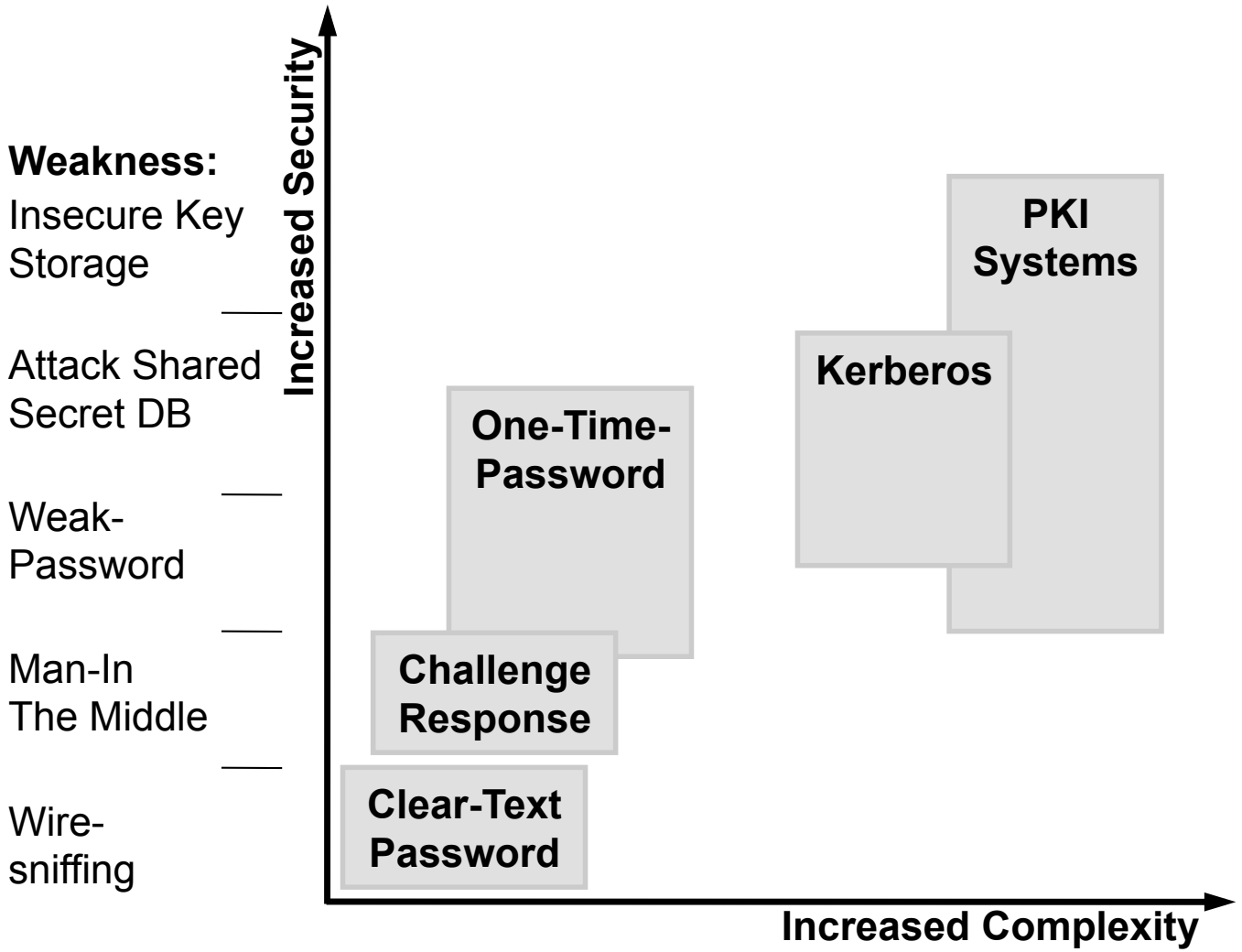
The simple question "Who are You" raised big technology

- Username & passwords
- Traditional security token formats
  X.509 certificates, and Kerberos tickets, …
- Card-Space, Information-Cards, Open ID, …
- Security Assertion Markup Language SAML, OASIS
- Federations
- …

The Stakeholders

- **Users**
  - have and get identities for various services and even themselves
  - must maintain their Identities
  - must be able to revoke some of their Identities this also includes their name …
  - must have credentials to prove the Identity
- **Service providers / Operators**
  - must be able to validate asserted identities for authorization
  - usually provide identity and authentication silos
  - some of them accept third party authentication
- **Trust Services / Trusted Third Parties**
  - 3rd party services to re-use and outsource authentication

Authentication Methods and Vulnerability … neat discussions we waste our time with?



Content

- Introduction
- The Users Dilemma
- Two Basic Solutions
- Information Flow and Samples
- Conclusion / what's missing

The Users Dilemma

- **More and more services**
  - E-Mail, Web-Pages, Internet Services, Social Networks, IP-TV,
  - Corporate networks, Single Sign-On, Access management
  - Electronic Banking, Government Services, Health-Care
- **Each service has a different identity & lifetime management**
  - Passwords, Software-Tokens, Hardware-tokens, Certificates, Private Keys, One-time-passwords, etc.
  - Users need to maintain / renew these credentials
- **Finally the user looses control and simplifies actions**
  - Same password and username for many services
  - Forget to renew certificates,
  - Give private tokens to other users / representatives
  - …

The Users Dilemma
Responsibilities multiply for each service

A user needs: Email & Social Sites & Web Service & E-Commerce & Public Services & VoIP & even PSTN Voicemail, …

A user gets: Responsibilities

Roughly 4 things to care for each service.

And lifetime management is recurring!

- **Wrong use of a funnel?**
- **Just keep the user busy?**
- **ignorance?**
- **… ?**

Email Address

Email Address
- Password & UID
- Lifetime & PW Management
- Discontinuation

Certificates

Certificates
- Enrollment
- Lifetime & PW Management
- Discontinuation

Tokens HW & SW

Tokens HW & SW
- Renewal
- Lifetime & PW Management
- Discontinuation

User Friendly Solutions
… we have but they still lack acceptance

A user needs: Email & Social Sites & Web Service & E-Commerce & Public Services & VoIP & even PSTN Voicemail, …

1.) The user subscribes to:
- Trusted third Party Authentication
- Gets Credentials (PKI, Info-Cards, …)

Token HW & SW
- Renewal / Revocation
- Lifetime & PW Management

2.) subscribes to:
- each service and presents his credential for further authentication and authorization

TTP
Validation Service

n.) Service Providers:
- Authenticate the asserted Identity of the user.
- Save Investment for own lifetime management.
- Outsource cost positions

Content

- Introduction
- The Users Dilemma
- Two Basic Solutions
- Information Flow and Samples
- Conclusion / what's missing

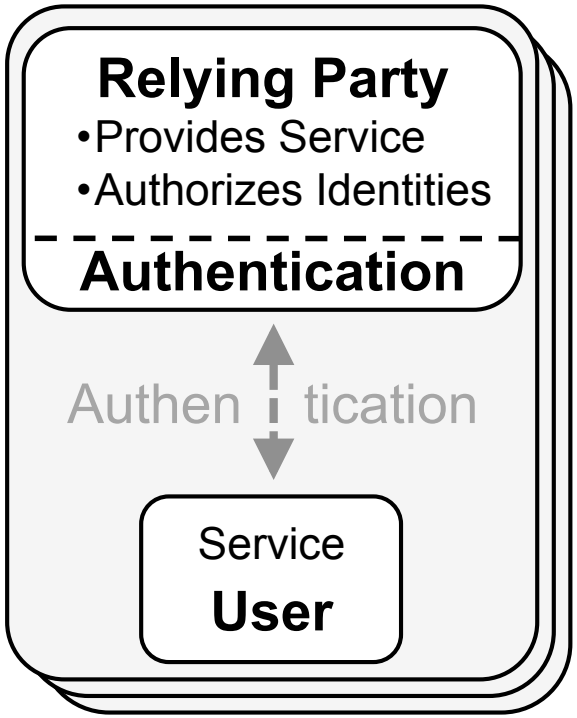
Two Basic Aproaches

- **Operator Centric Authentication limited Re-use**
  - User gets Identity & Credentials from Operator
    Radom-Number/identity or any Name, Phone number, Email, …
  - User subscribes this service and performs initial validation
  - User then re-uses this identity for services that accept

  Problem: Other service Providers hardly accept trust from Competitors providing other services as well.
- **User Centric Authentication full Re-use**
  - User Subscribes Identity to Independent Trust Service for Re-Use
    Typically his real name, Phone number, E-Mail, Domain-Name, …
  - Service Providers Countersign and issue Attribute-Certificates for their authorization needs.
  - Service providers and users can revoke the business relation without revoking the “Master Certificate” / Identity

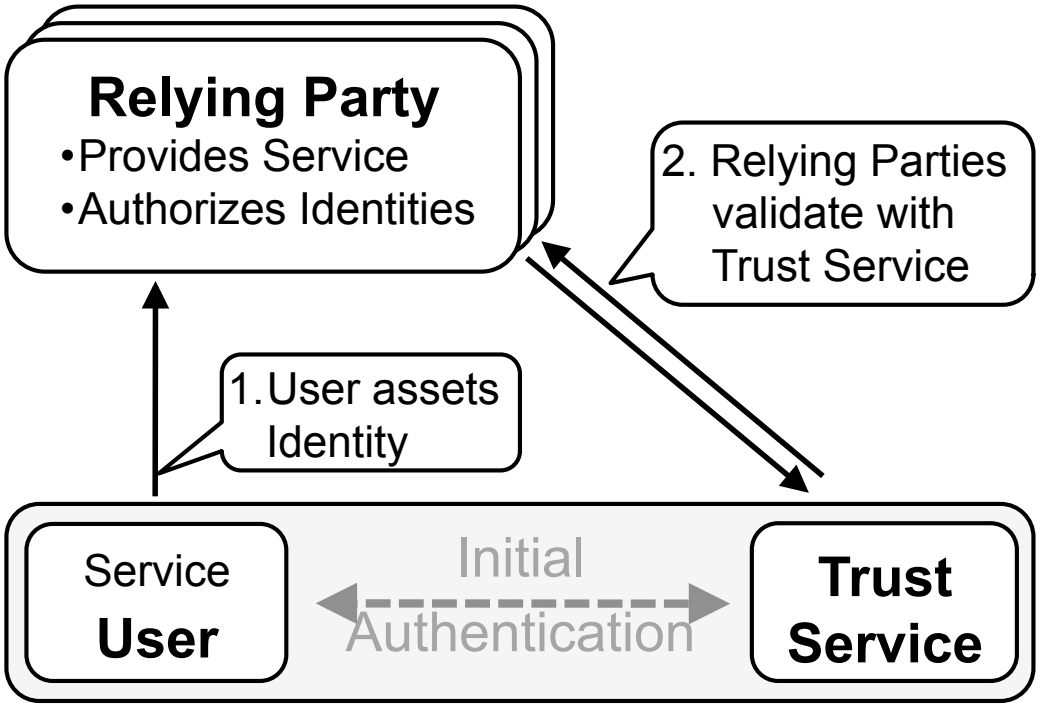
Migration and Re-use of Identities
Outsourcing for Users and Relying Parties

Centralized Authentication



Cost of centralized service:
+Replication for each service
+Password reset
+Lifetime Management
+Backup Risk

User Centric Authentication

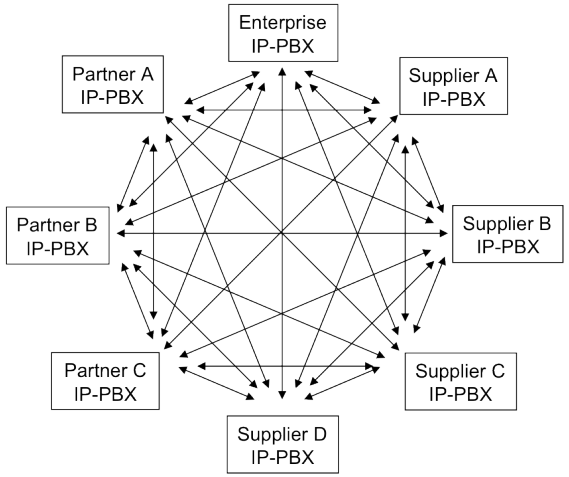


Cost of user centric service:
−Shared by many Relying Parties
−User manages one Identity only
−Lifetime Management re-usable
−Backup risk covered once for many

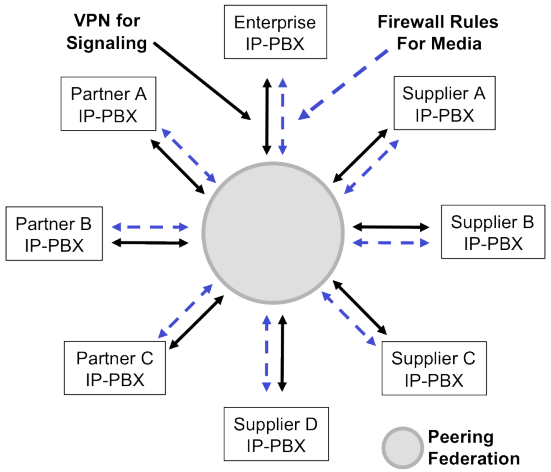
Re-Use has Issues we Shall Care for

from **Pre arranged (n^2)** to **Federated** to **End-2-End** Trust

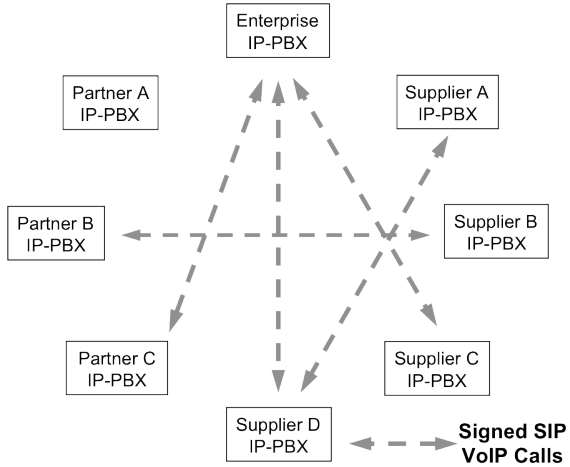
The number of pre-arranged trust relations increases with number of peers squared = n^2-n the "n^2 Problem"



The intermediary solution uses trust federations to reduce administration of trust



Trust relation on demand without "n2" and without peering-federations

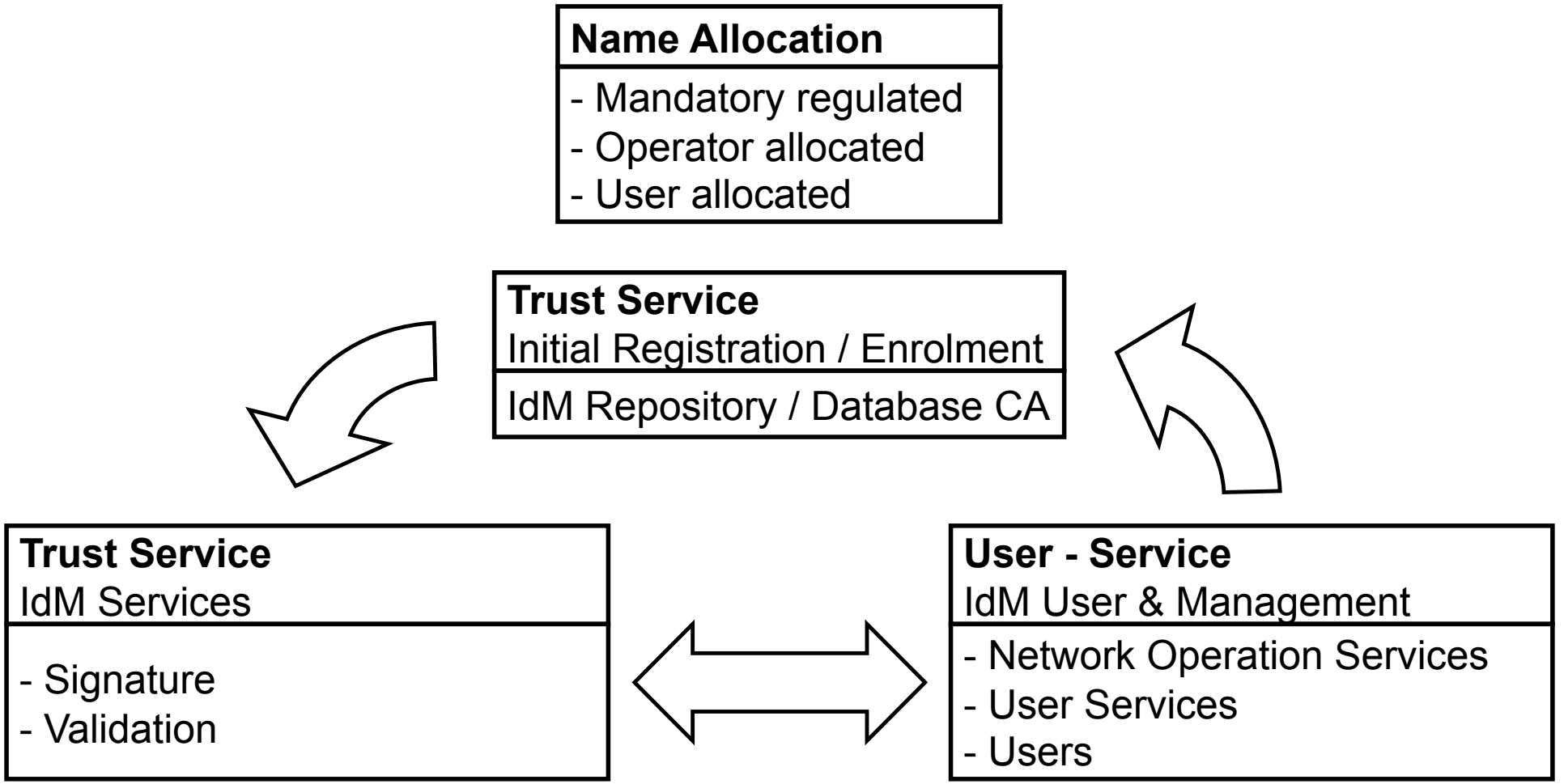


- **Avoid to replicate physical constraints from network layer for trust**
- **Identity is a endpoint property and can save operational expenses**

Content

- Introduction
- The Users Dilemma
- Two Basic Solutions
- Information Flow and Samples
- Conclusion / what's missing

IdM Components: Information Repository Functions and Information Flow



Enhance information flow with better HW
e.g.: OTP token that acts as a keyboard

- **Before USB and Plug & Play**
  - User had to read the OPT from token
  - and enter it on the Keyboard

  Problem: Errors in typing

Error prone
Reading &
Typing

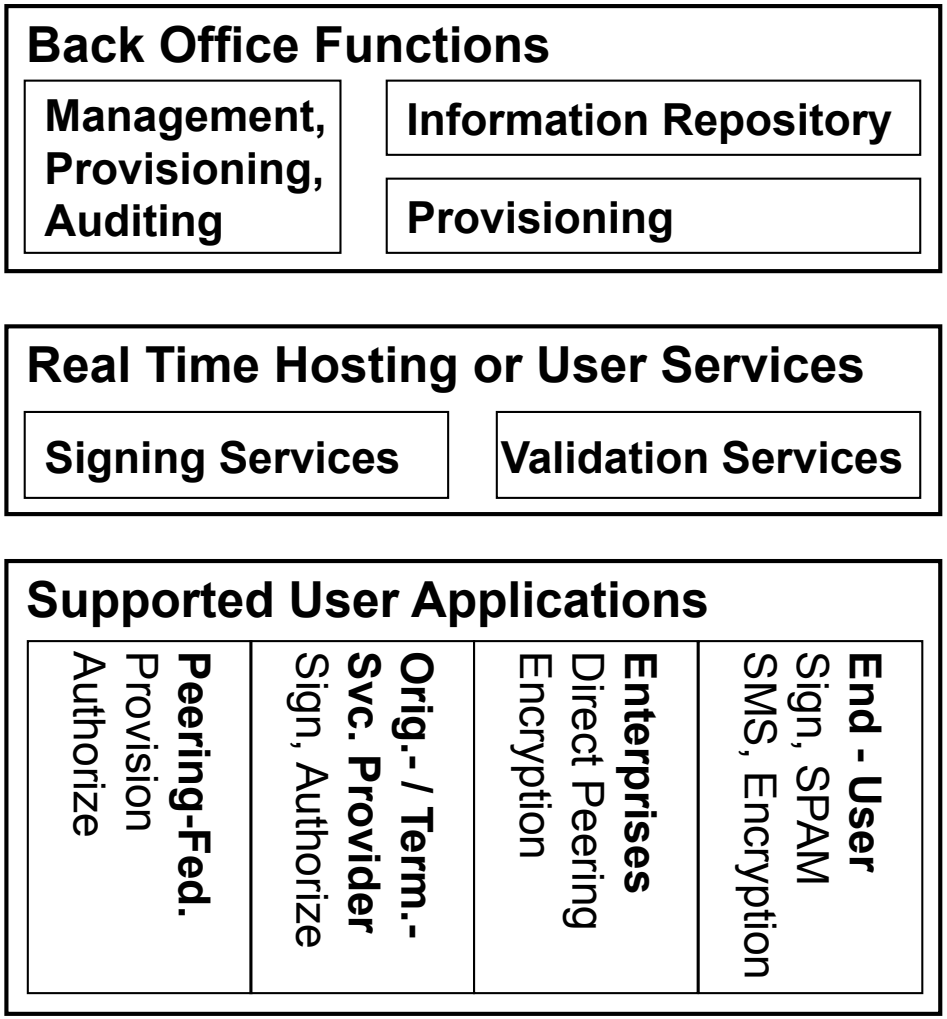
- **With USB and Plug & Play**
  - User jus plugs the token in to USB
  - acts like a one button keyboard

  Problem Solved: no mistyping

A Yubikey eliminates
manual transfer
and allows larger key-size

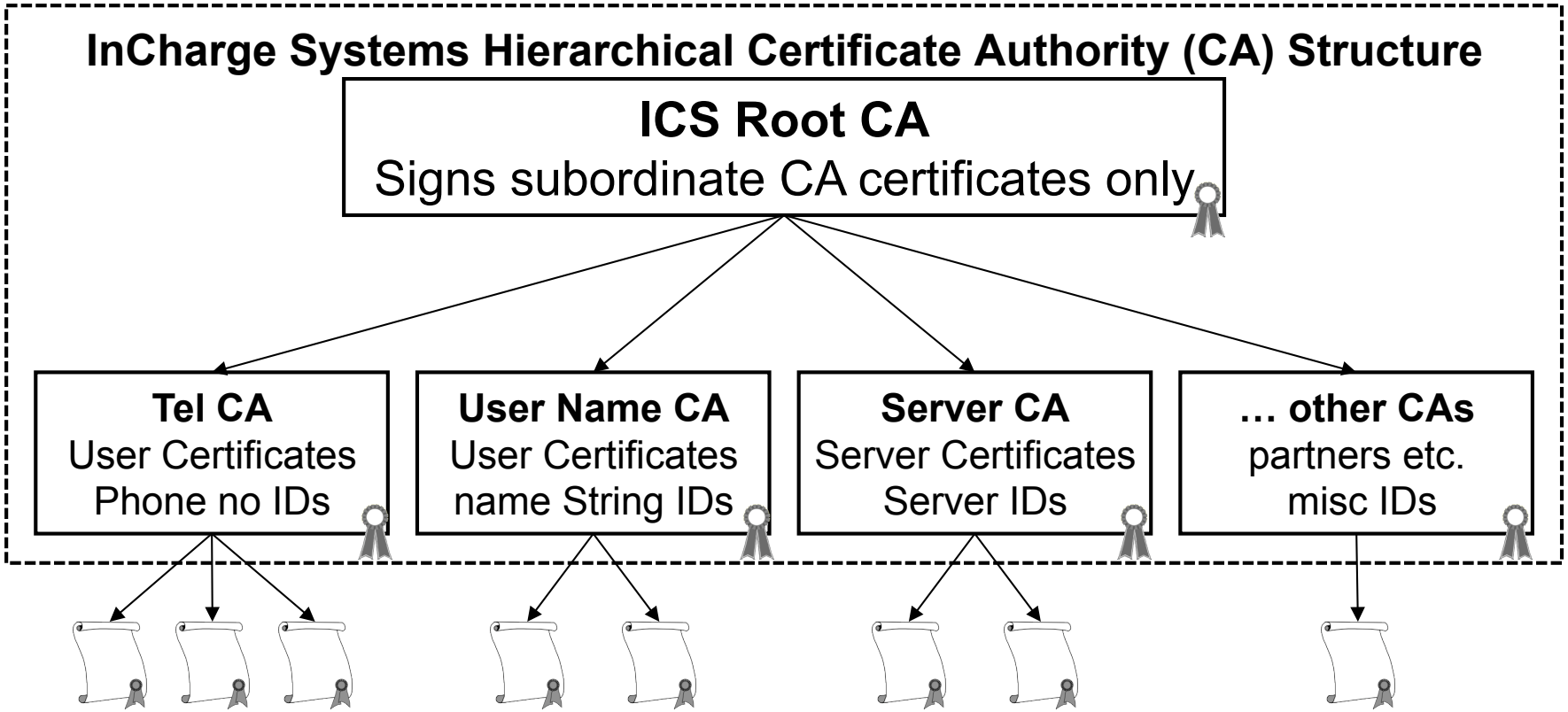
These RFC 4474 based Services need Interoperable PKI Infrastructures

- **Provisioning, Management**
  - Enrollment / DN-Assignment
  - Auth.:2 Channel, Multi-Factor
  - Generate Account, Key-Pairs
  - Manage Public Repository
- **Real Time Services**
  - Code Stubs or Proxy Function
- **Customer Application Support**
  - Authenticate (sign invites)
  - Trust Replaces Provisioning
  - SPIT, SMS, Encryption, Community Services, Collaboration, …



e.g. InCharge Systems ACerted Trust Infrastructure

Re-useable Certificate authorities need open access to the certificate authority

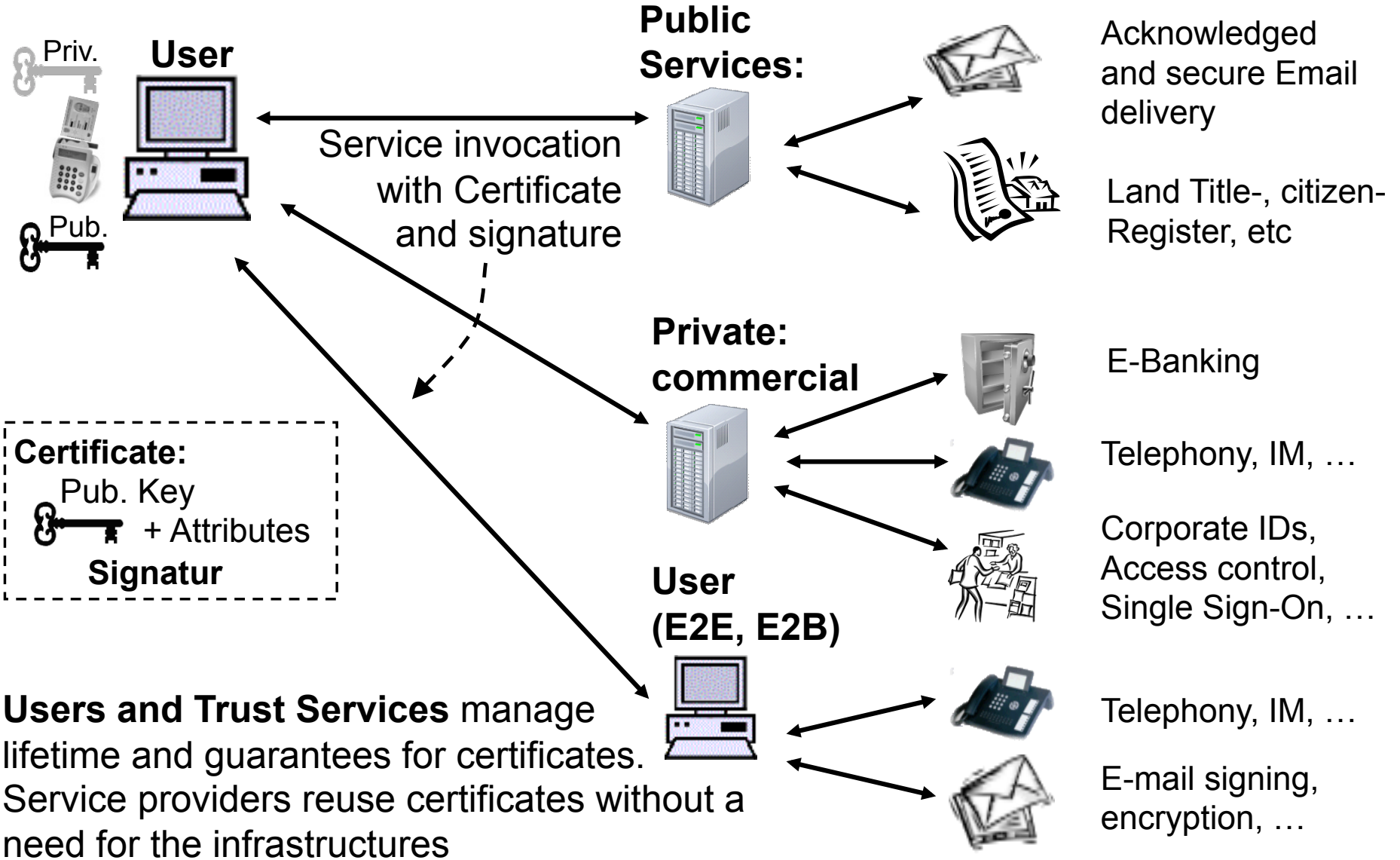


Notes:

- **The Root-CA is offline (used only to manage underlying Issuing CA certificates)**
- **Issuing CAs governed by optional different CP and CPS commitments**
- **Issuing CAs may be added or removed as required and allowed by policies**
- **Issuing CAs are responsible for publishing client certificates**

e.g.: Inchargesys.com

Migration and Re-use of Identities
Outsourcing for Users and Relying Parties



Users and Trust Services manage lifetime and guarantees for certificates. Service providers reuse certificates without a need for the infrastructures

Content

- Introduction
- The Users Dilemma
- Two Basic Solutions
- Information Flow and Samples
- Conclusion / what's missing

Conclusion
What's missing

- **There is no One Shoot User Enrollment Registration**
  - Users must enroll initially
  - Users must present credentials to service providers
  - Some companies piggy-pack on existing services to re-use Grown trust (e.g. InCharge Systems with phone numbers)

  Problem: Other service Providers hardly accept trust from Competitors providing other services as well.
- **Providers still believe that they can bind customers**
  - By locking them in to their IDM and authentication system
  - using their name space for authentication as well

  Problem: Each of them ends up with their own authentication silo and thus can not save cost on re-use.