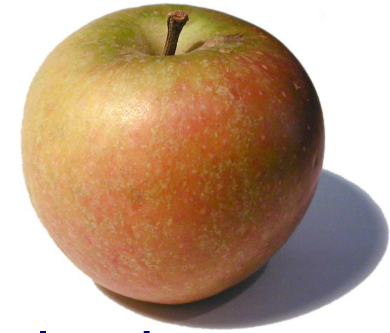


# Technical standards on electronic signatures vs. regulations: Finland

Teemu Rissanen  
Managing Director  
Conseils Oy

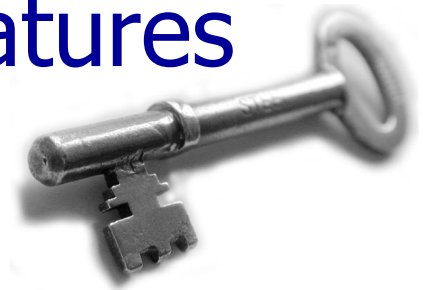


# Agenda



- Setting the stage
  - Legal background for e-signatures in Finland
  - Service background
- E-signature technology & requirements
  - Finnish legal specificities
  - Signature / authentication
    - Scoreboard
  - Where are the business incentives?
  - A solution?
- Conclusions

# Legal background for e-signatures



- The Act on Electronic Signatures
  - Since the 1<sup>st</sup> of February 2003
  - Defines Qualified Certificates in compliance with the European directive on electronic signatures (1999/93/EC)
- Identity Card Act
  - Since 1<sup>st</sup> of December 1999
- Act on Electronic Communications with the Authorities
  - Since the 1<sup>st</sup> of January 2000
  - Mandates public authorities to fund technical and other measures for providing e-services
  - Regulates the use of electronic signatures in the public administration
- Section 23 of the Population Information Act
  - Since 1<sup>st</sup> of December 1999
  - Lays down provisions on certification authority services (eID)
  - Defines e.g. the data content and tasks of a citizen certificate of the State granted by the Population Register Centre to a natural person.

## The service background



- The Finnish Communications Regulatory Authority (FICORA) supervises the CA's.
- The Population Register Centre is the Government's CA and also the only CA to issue Qualified Certificates in Finland (since 1999)
- FINEID and FINUID
  - The Finnish identification and signature application ([www.fineid.fi](http://www.fineid.fi)) is compliant with requirements on trusted signature application
  - FINUID: Finnish Unique Identification Number (DN), which is derived from the SSN. It is included in the FINEID application of the citizen eID

# Technology & requirements



## Technology:

- FINEID certificates : ~100 000 issued since 1999
  - Authentication (PIN1), Signature (PIN2) and S/MIME (PIN1)
  - eID, Organization certificates, SSL certificates
  - PKCS#15 structure, PKCS#11 interface, Setec SetCOS, now JAVA
  - Biometric data (probably MOC) under study (bio-passports)
- Bank TUPAS OTP system: >3 mil. users since beginning of 1990's
  - 2-factor authentication based on PW, username, OTP (+checklist)
  - Bank, insurance, public e-services, e-commerce, etc.

## Requirements:

- No legislation related to authentication (new legislation on biometric authentication is under preparation, though)
- No domain specific legal requirements for Qualified Certificate usage (e.g. e-invoicing)

# Finnish legal specificities



- Qualified Certificate (QC) usage is not mandatory:
  - A qualified certificate is mandatory only when deliberating on an official decision
  - Security oriented organizations can use QC (e.g. "power" ministries, health care professionals)
- QC offer no added value *per se*:
  - A qualified certificate does not diminish the value of other types of electronic signatures
  - Finnish law is based on free evaluation of evidence: in case of repudiation of signature, all evidence is reviewed

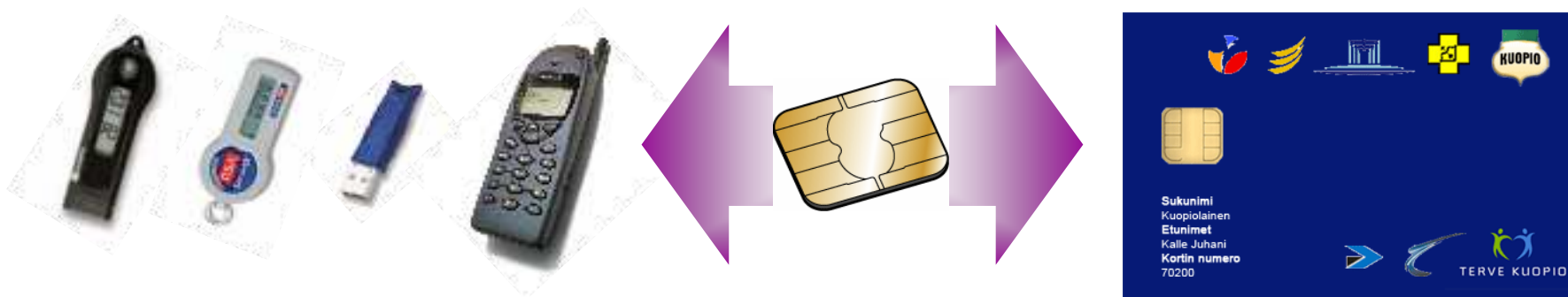
# Signature, or Authentication?

## ■ Authentication



- QC is secure, but...
  - ...tokens offer flexibility...
  - and OTP's are cheap
- > business & service needs are well served

## ■ Signature

- QC is the only option
  - Un-flexible policies
  - Enables paperless processes
- > is there a real need?



# Scoreboard

	Security	Usability	Availability	Functions	Price
Tokens 	0	+	+	0	+
QC 	+	-	-	0	-

- Several proven methods exist for authentication
- Qualified Certificates have less "good" qualities for general purpose use than token-solutions

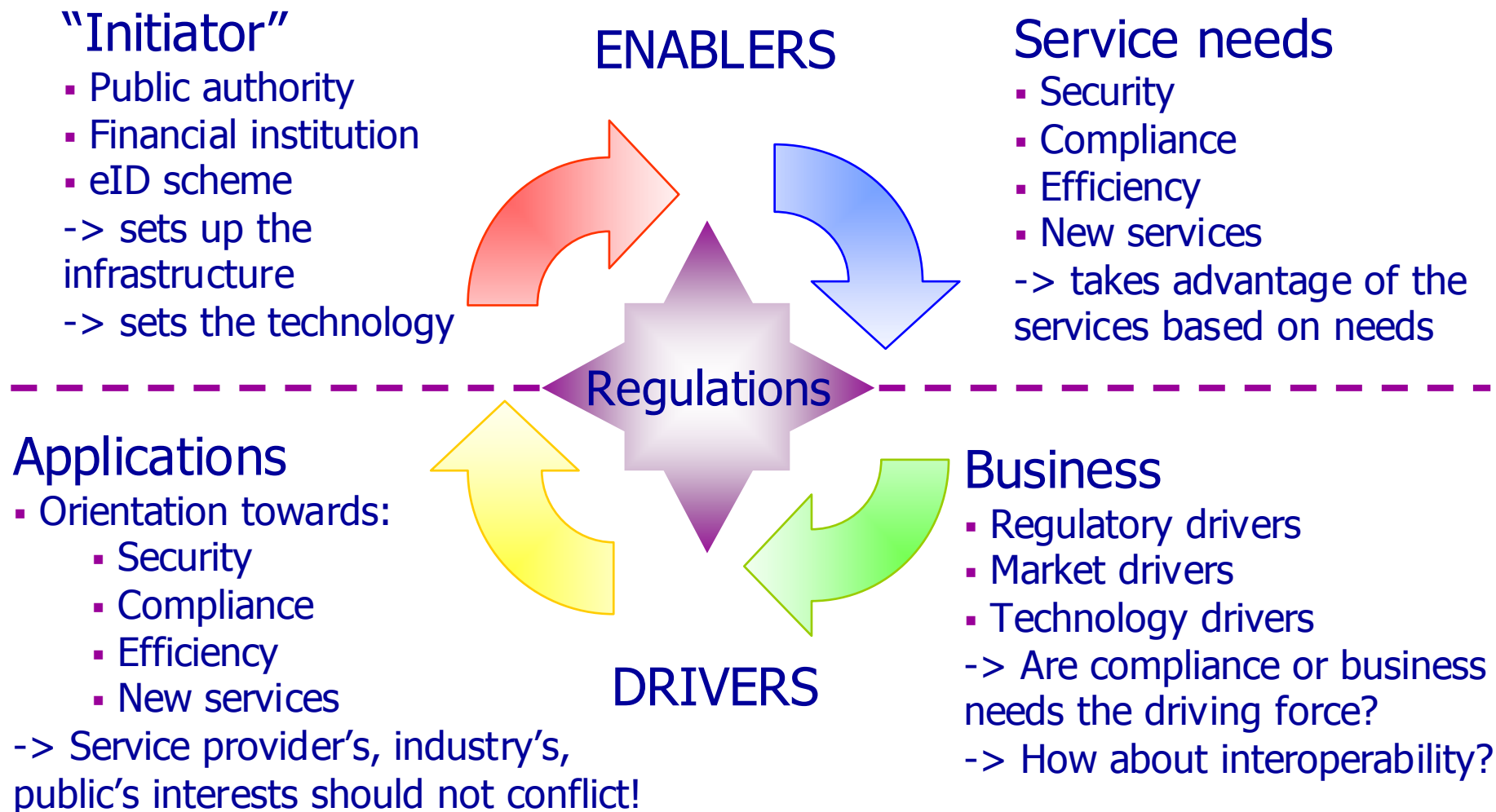
## Legend

+ Good/strong/interesting

0 Dependent on implementation

- Less good/difficult/rare/not interesting

# Where are the business incentives?

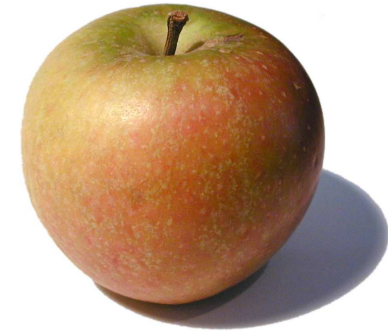


# A solution?

- European eID schemes
  - Availability increases with citizen eID's
  - All interoperability issues should be addressed
    - > How about setting up a common RootCA?
- Multi-purpose, multi-functional smartcards
  - PKI enabled solutions for authentication + signature
  - Merging of different technologies (PKI, biometrics, Java&Multos and RFID applications, Identity management & federation, business solutions)
    - > More flexibility to QC standards: EU Commission is preparing new recommendations; so is Finland, how about others?
- A need to de-regulate, while maintaining strong standards
  - Integration of local, organizational, regional, national, European and global entities



# Conclusions



- Finland has a long experience in:
  - Qualified CA services (first eID in 1999)
  - Internet banking & e-invoicing (>10%)
  - Public sector ICT and e-services
- Finnish regulatory environment is liberal
  - No mandatory compliance requirements for any generic service area
  - No jurisprudence on e-signatures or authentication (very few phishing cases)
- Use of electronic signatures is very rare
  - Few e-signature enabled services; focus is set on authentication
  - Difficulty to communicate advantages of e-signatures into real business needs
- The needs are out there, the perfect solution is still missing!



# Thank You!

More information:

[teemu.rissanen@conseils.fi](mailto:teemu.rissanen@conseils.fi)

[www.conseils.fi](http://www.conseils.fi)

[www.simplysecure.biz](http://www.simplysecure.biz)

+358(0)50 379 5343