

Virtual Crypto SmartCard, which security system to implement



CARTES & IDentification congress

6 November 2008

Planning

Background

User Case (Authentication and Digital signature)

Solutions

- ▶ Software Certificate
- ▶ Crypto SmartCard
- ▶ Virtual Crypto SmartCard

Comparison

Testimony user

Conclusions



Background

Importance of authentication and signature

- ▶ Online taxes statement (7,4 millions declaration in 2008)
- ▶ Bank online
- ▶ 3D Secure
- ▶ BtC : bank loan

Focus on solutions using electronic certificates (PKI)



User CASE (BtC) : 3DSecure

Needs:

an authentication and digital signature solution

Problems:

many solutions for authentication, but not both authentication and digital signature

Solutions :

« Digital Certificates »

- ▶ S1 : Software certificates
- ▶ S2 : Crypto SmartCard
- ▶ S3 : Virtual Crypto SmartCard



SI: Software Certificate

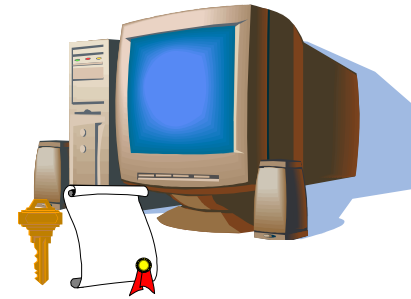
Digital certificate confined to the PC

Advantage :

Easy to deploy (and install?)

Disadvantage:

Requires a not amateur user to manipulate the certificate



Main safety features :

User **MUST HAVE FULL CONFIDENCE** in the use environment

- ▶ **One-factor authentication** (What you have)



S2 : Crypto SmartCard

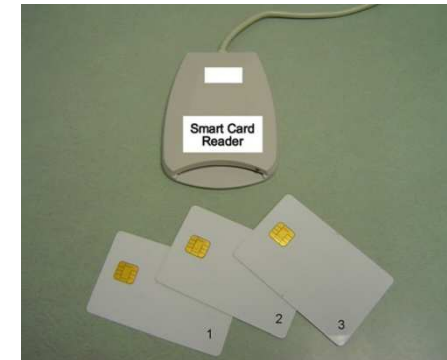
Digital certificate confined in a Crypto SmartCard

Advantage :

- ▶ Mobility (device)

Disadvantages :

- ▶ Heavy deployment (reader, installation, etc.)
- ▶ Management devices



Main safety features :

User **DO NOT NEED TO HAVE CONFIDENCE** in the use environment

▶ Two-factor authentication :

- ▶ What you know (your PIN, password, etc.)
- ▶ What you have (a Crypto SmartCard)



S3 :Virtual Crypto SmartCard

Digital certificate confined in a device

Advantages :

- ▶ Easy to deploy (in different devices :
CD, DVD, USB generic key, etc.)
- ▶ Mobility (device)
- ▶ Ease of use

Disadvantages :

- ▶ Management devices (depending on the device)

Main safety features :

User **SHOULD HAVE CONFIDENCE** in the use environment

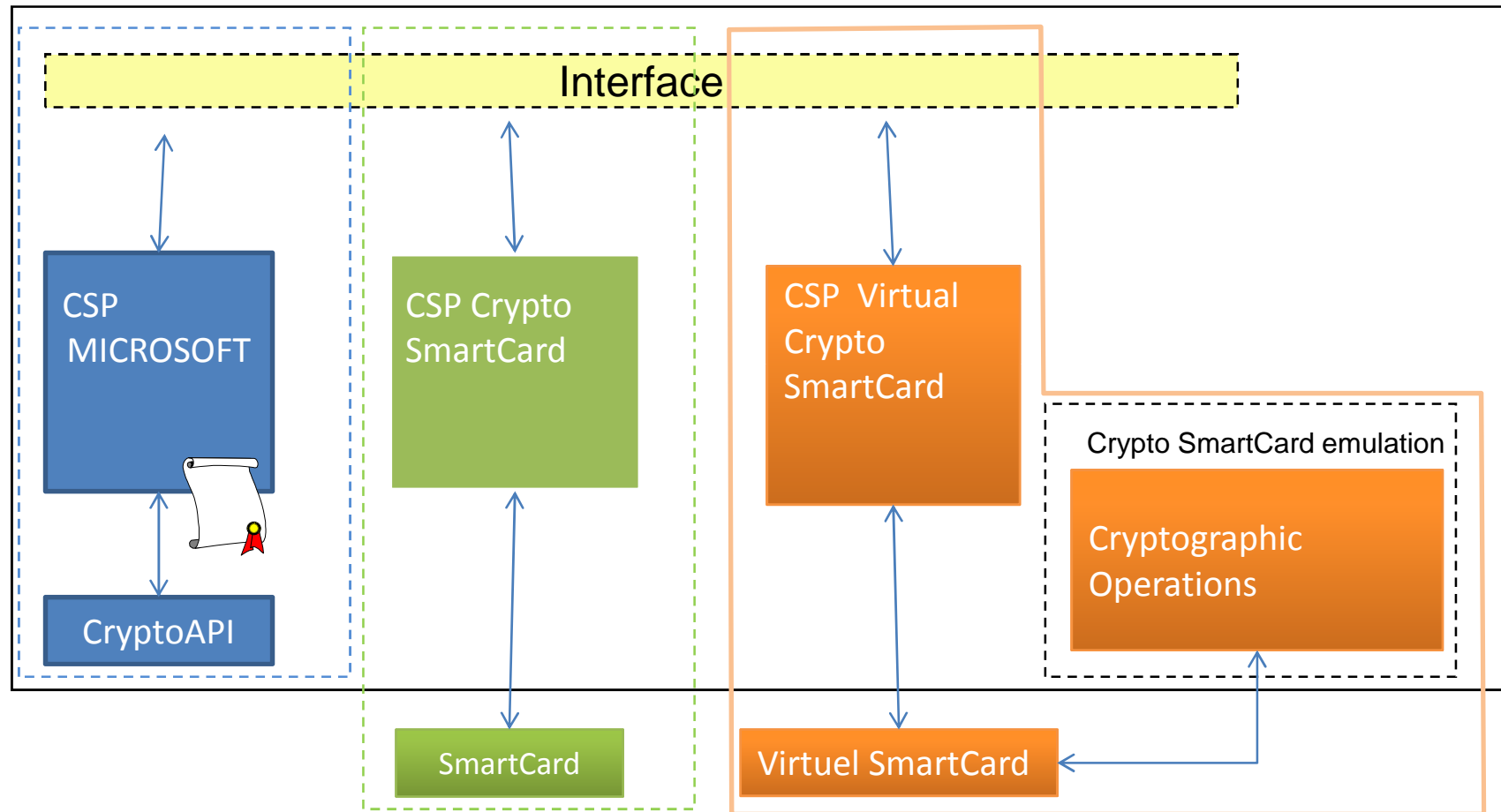
▶ Two-factor authentication :

- ▶ What you know (your PIN, password, etc.)
- ▶ What you have (a device)



Trust environnements

SO (Microsoft Windows Vista)



Risques assessment

Threat	S1 : Software Certificate	S2 : Crypto Smartcard	S3 : Virtual Crypto Smartcard
T.MASQUERADE_USER	1	4	3
T.PRIV_KEY_DISCLOSURE	2	5	4
T.KEYS_MODIF	3	5	4
T.COMM_EAVESDROP	1	4	3
T.MASQUERADE_TOE	2	4	3
T.MASQUERADE_ADMIN		4	3
T.PUBLIC_KEY_MODIF	4	4	4



Security Features

Security	S1 : Software Certificate	S2 : Crypto Smartcard	S3 : Virtual Crypto Smartcard
Privacy	1	4	3
Integrity	2	4	3
Availability	1	5	4



Characteristics of implementation

FONCTIONALITE	S1 : Software Certificate	S2 : Smartcard	S3 : Virtual Crypto Smartcard
Mobility	1	4	5
Deployment	4	2	5
Costs	1	5	2



User CASE : Testimony user : 3D Secure payment

Authentication device with two-factor

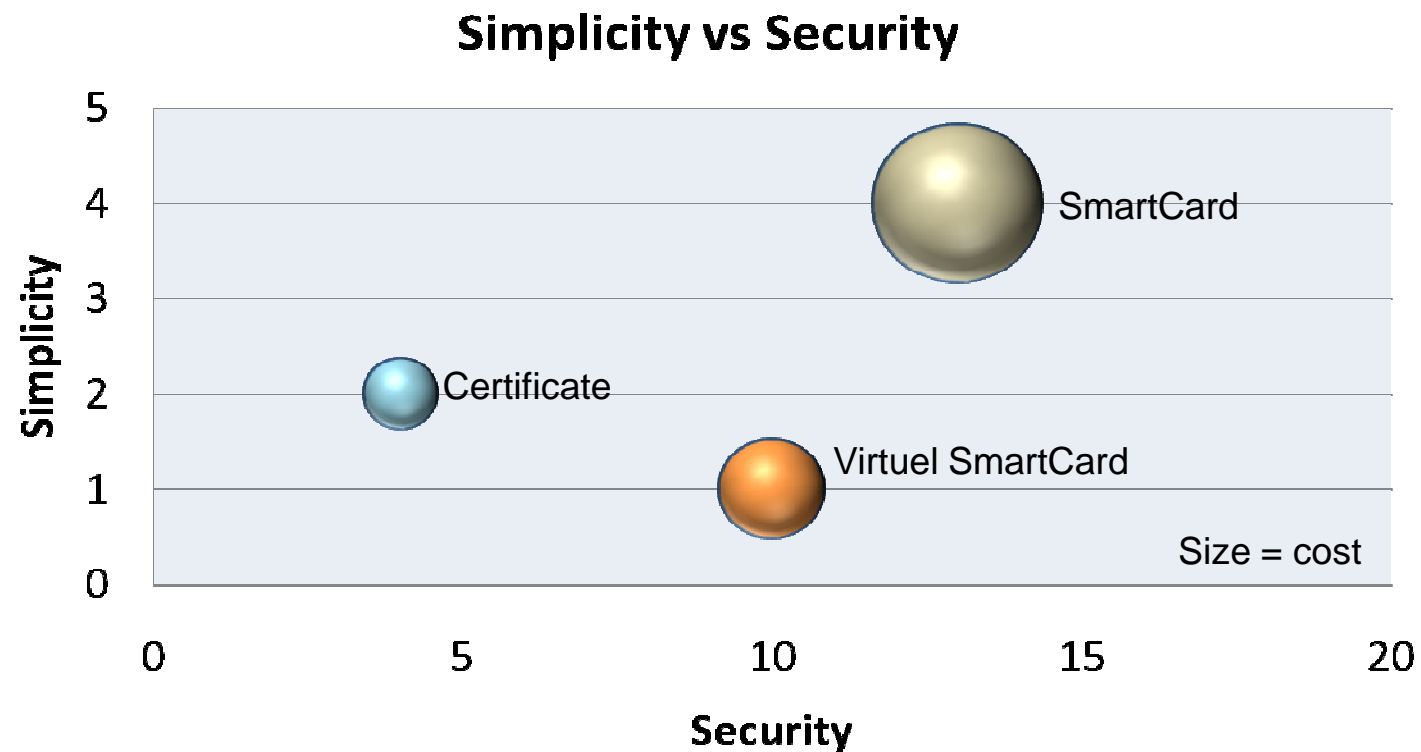


Easy to deploy : 99% of users have a CD reader or a USB port in their PC.

Added value : Digital signature



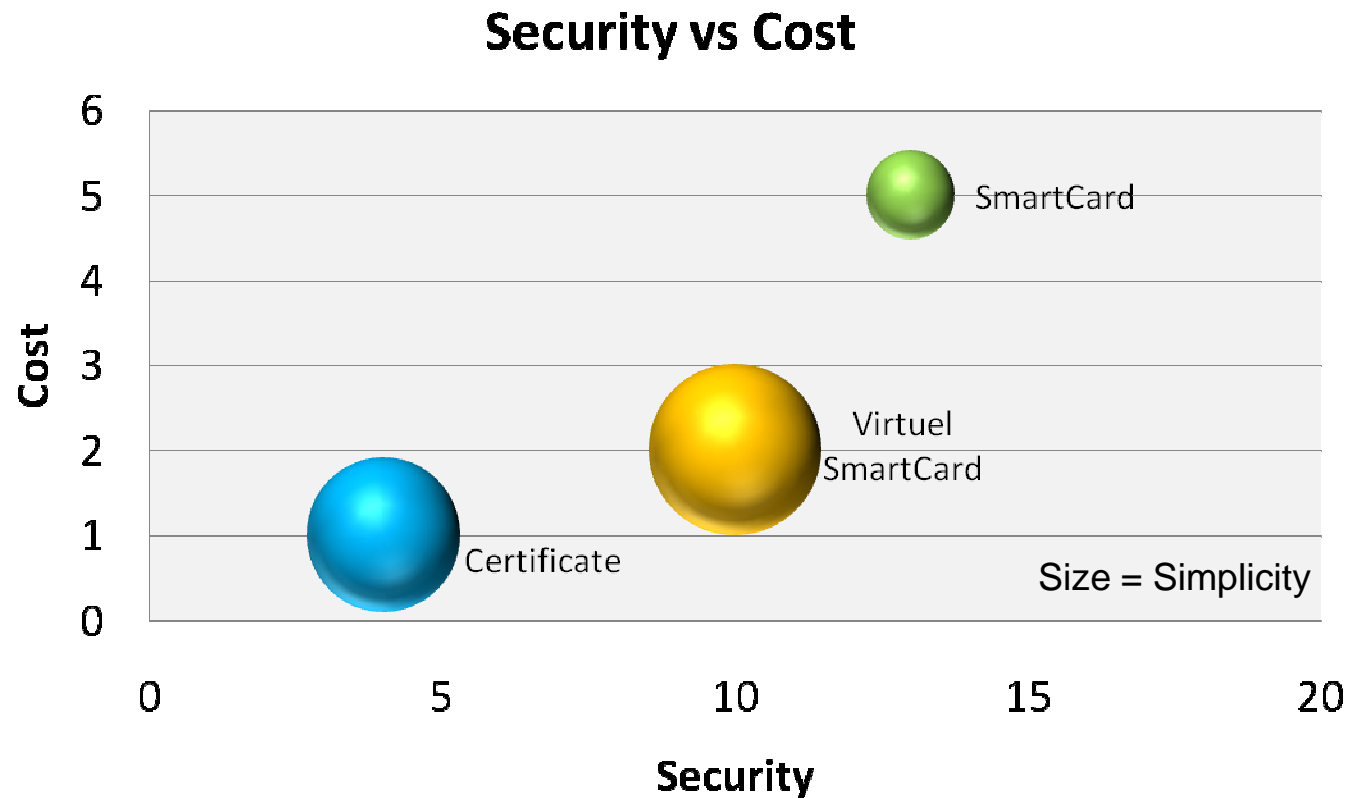
Conclusion



- ▶ “An ideal Concept must combine two priorities : **Security** and **simplicity**, in an economical way optimizing the cost”



Conclusion



- ▶ “An ideal Concept must combine two priorities : **Security** and **simplicity**, in an economical way optimizing the cost”



Thank you for your attention

Paul FRAUSTO (MEDISCS)
and
Nicolas REIMEN (VIALINK)

**We invite you to come and visit us
on our stand : 4P092**

