

Electronic Signature

Internet Security Day

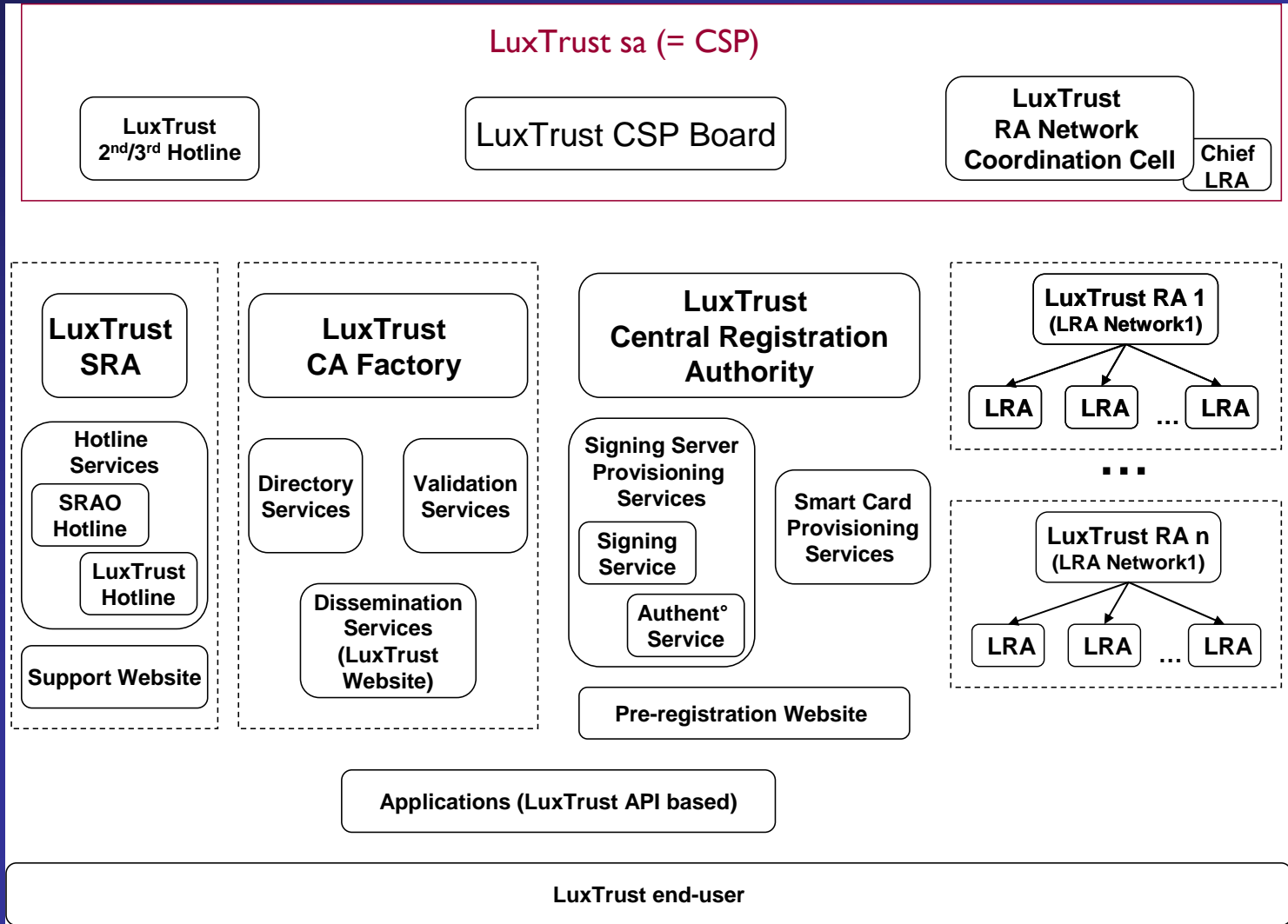
- 1. Questions**
- 2. Trusted Third Parties**
- 3. Certificates**
- 4. Authentication & Privacy**
- 5. Electronic Signature**
- 6. Economic Impact**

In the Internet nobody knows you are a dog

- **Is anonymity what we are seeking for ?**
- **Wouldn't it be helpful if somebody well chosen knows who you really are ?**
- **Is the Electronic Signature THE solution ?**
- **Are you concerned ?**

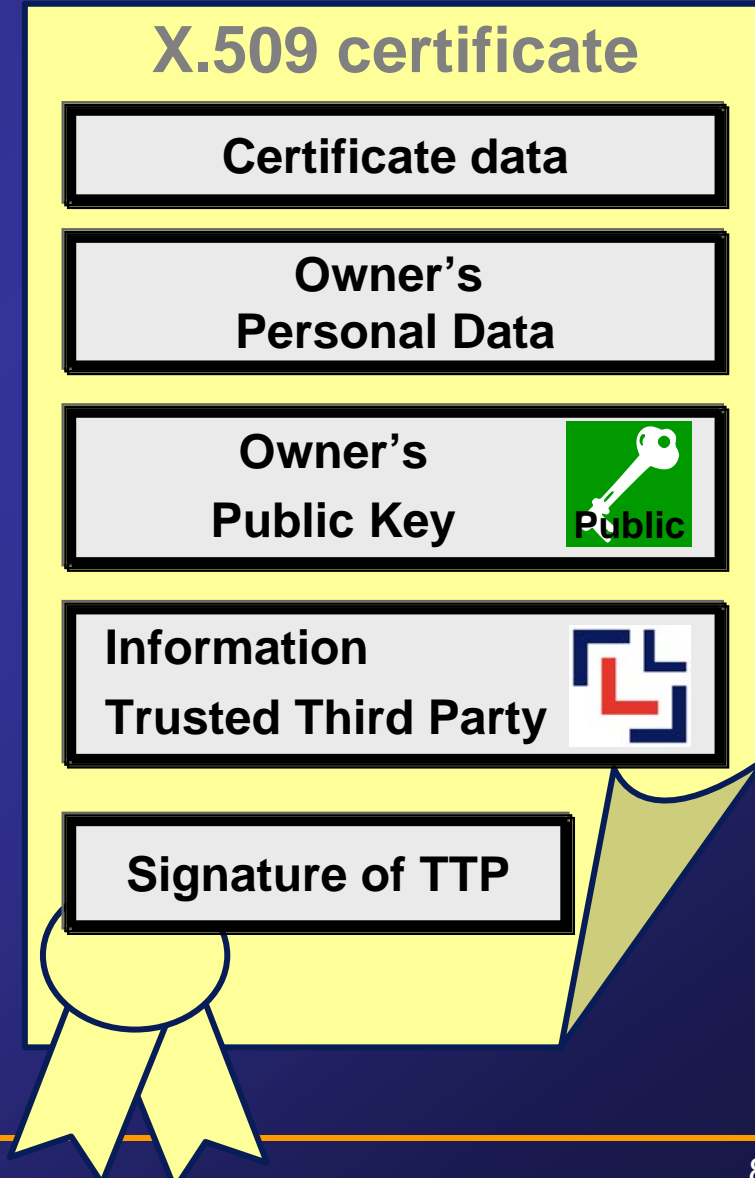
1. Questions
- 2. Trusted Third Parties**
3. Certificates
4. Authentication & Privacy
5. Electronic Signature
6. Economic Impact

- Manages the physical infrastructure called Public Key Infrastructure (PKI)
- Guarantees the identity of the holder of the certificate by enforcing strong registration procedures
- Provides online validation / revocation services



1. Questions
2. Trusted Third Parties
3. **Certificates**
4. Authentication & Privacy
5. Electronic Signature
6. Economic Impact

- A Digital Certificate is the digital identity of the holder of a private key
- Personal Data:
 - First Name
 - Last Name
 - E-Mail
 - ...
- Signature by TTP



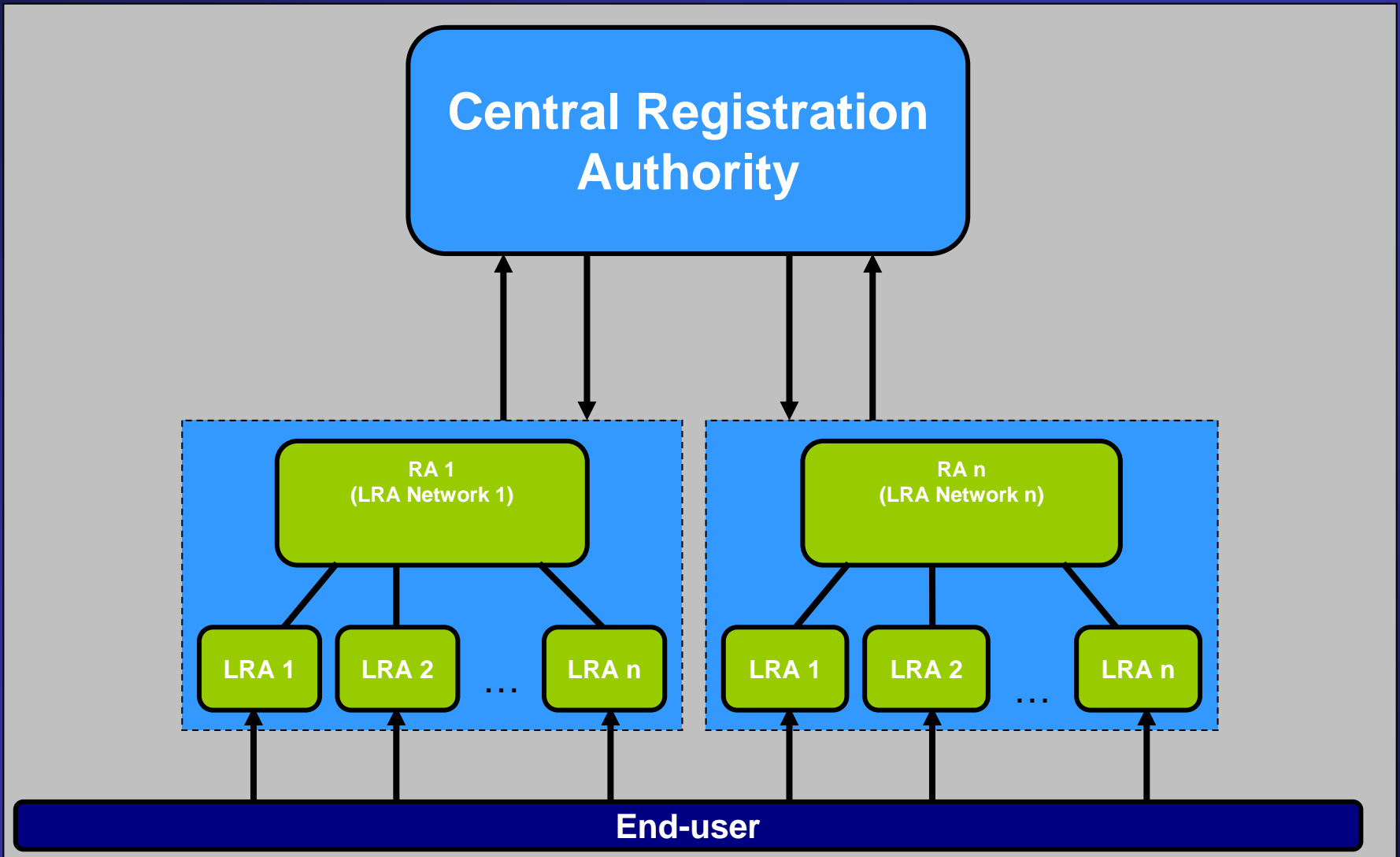
- **SSL/TLS certificates** to identify an entity in an electronic communication and to set up an encrypted information flow
- **Object Certificates** to sign application code

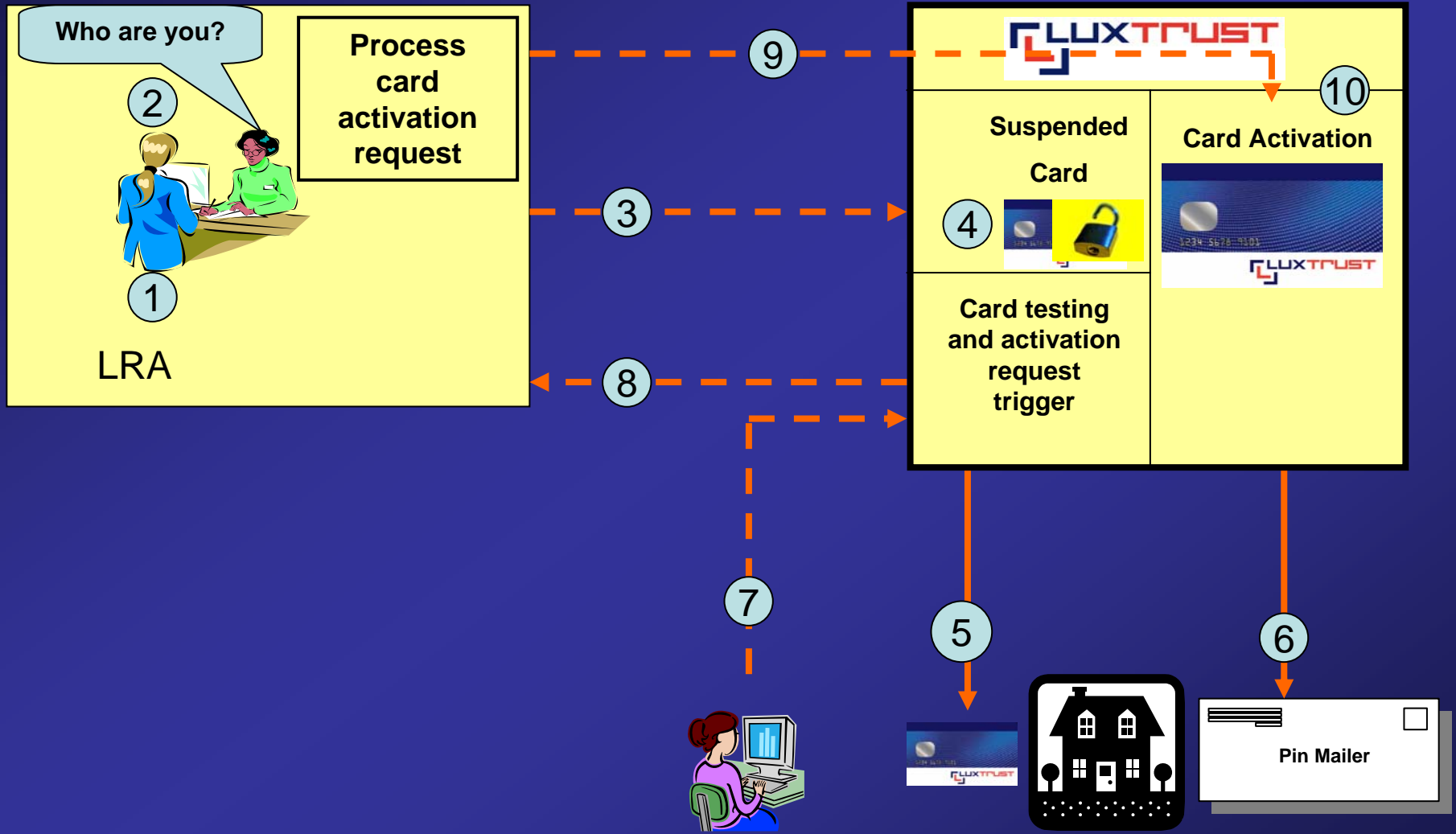
Give your customer the possibility to check the origin of the data

User Certificates are issued to :

- **Physical persons** as **private individuals**
 - Signatures and other operations are made as a private person
- **Physical persons** as **employees** or representatives of a company / institution
 - Signatures and other operations are made as a representative of a company or institution

- The customer needs to be identified through a face-to-face procedure prior to receiving a normalized personal certificate.
- The LRA – Local Registration Authority - is where this face-to-face identification is done and where the certificate request of the client is then encoded.





- **Smartcards** holding two certificates (one for authentication and encryption and a second one dedicated to advanced digital signatures)



- **Signature Server** certificate with OTP-Token or SMS-OTP that allows advanced PKI-based authentication, signature

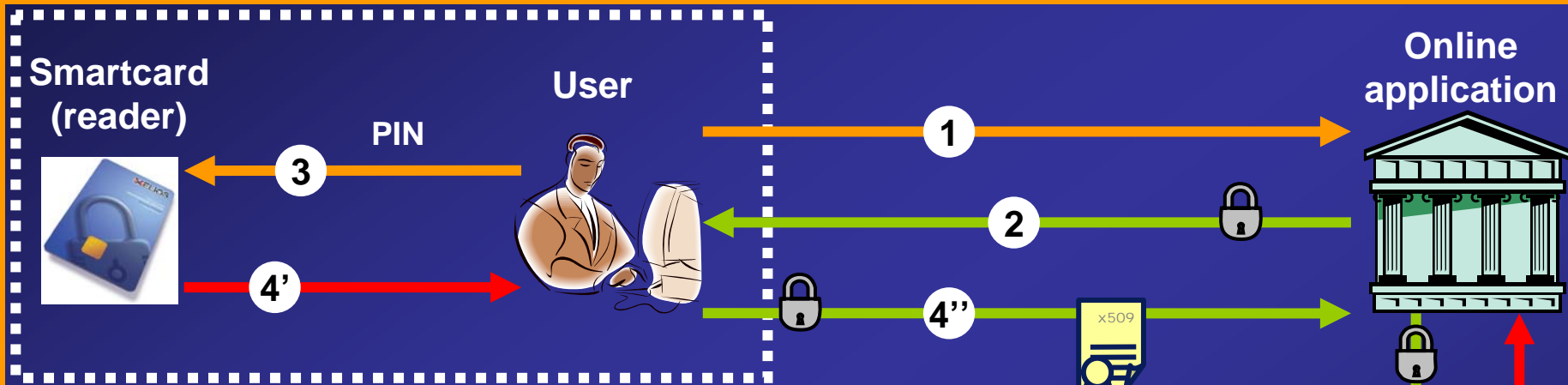


1. Questions
2. Trusted Third Parties
3. Certificates
- 4. Authentication & Privacy**
5. Electronic Signature
6. Economic Impact

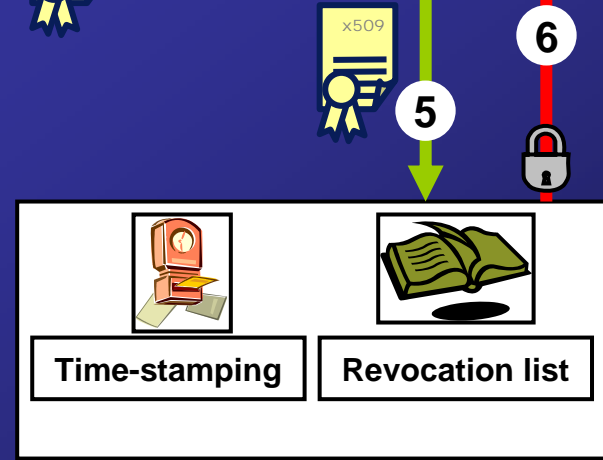
- The Smartcard holds **2 certificates** on its chip :
 - 1 **Authentication / Encryption Certificate**
 - 1 **Signing Certificate**

- This kind of product is mainly dedicated for **B2B usage**, but not exclusively
 - The Smartcard is used together with a **Card Reader**



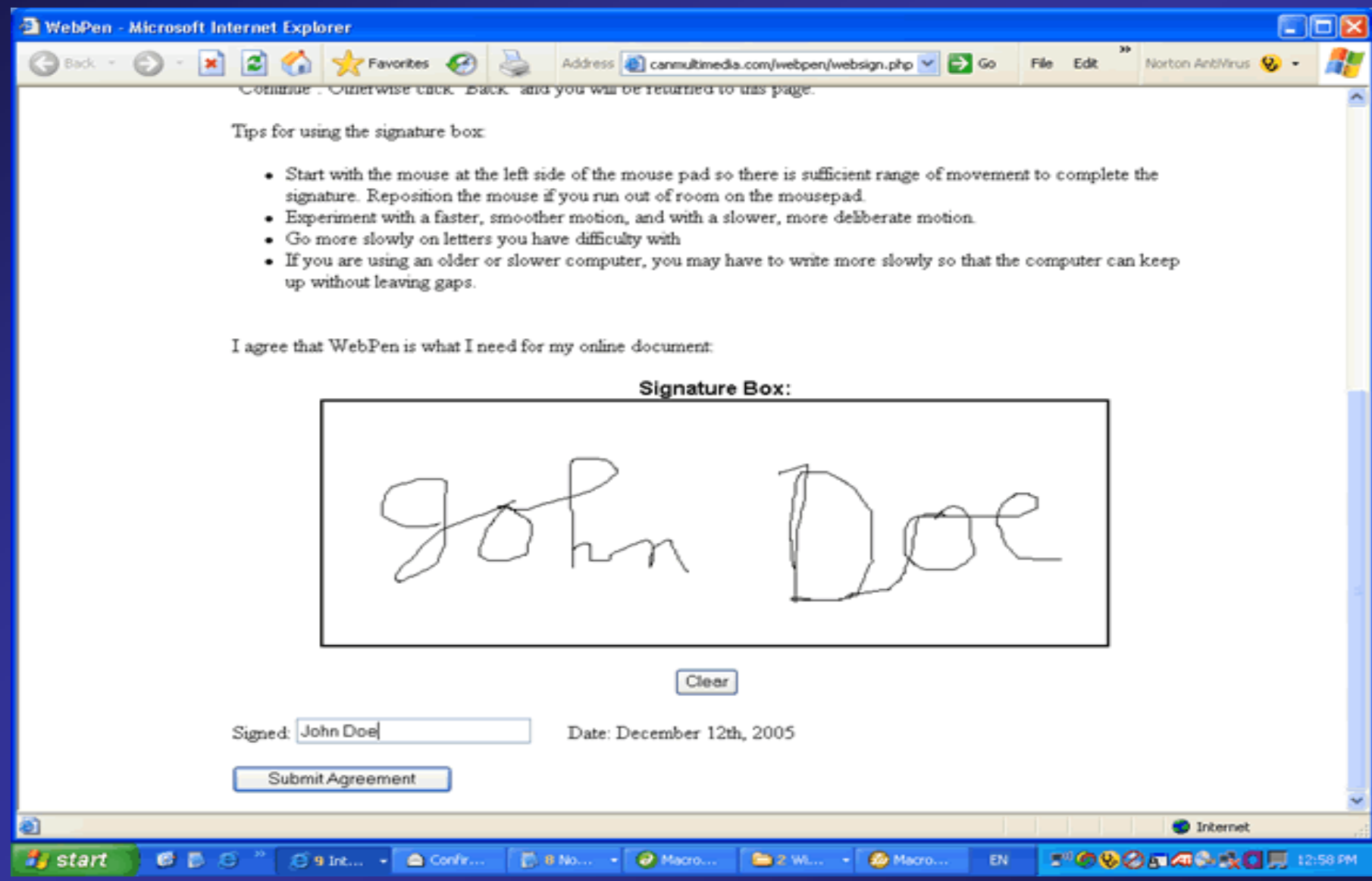


1. The user connects to the online application site (www...)
2. The application opens a **secure connection** and sends a “**challenge**” (i.e. random session ID) to be signed by the users (If required, the client side applet/servlet is send to the user)
3. The user enters his **PIN** in order to get access to the private key
- 4'. The « challenge » from the bank is “**hashed**” and the hash is signed with the **authentication certificate** on the Smartcard.
- 4'’. The signed hash is send to the application with the authentication certificate.
5. The application **validates the hash** and **checks the validity of the certificate** with LuxTrust.
6. TTP reports **OK or NOK** and, if required, a time stamp.
If OK, the authentication of the user has been successful



- **Transparency : information access**
- **Protect against Identity Theft**
- **Information delivered on an 'as needed' base**
- **Authentication/Identification**

1. Questions
2. Trusted Third Parties
3. Certificates
4. Authentication & Privacy
- 5. Electronic Signature**
6. Economic Impact



WebPen - Microsoft Internet Explorer

Address: canmultimedia.com/webpen/websign.php

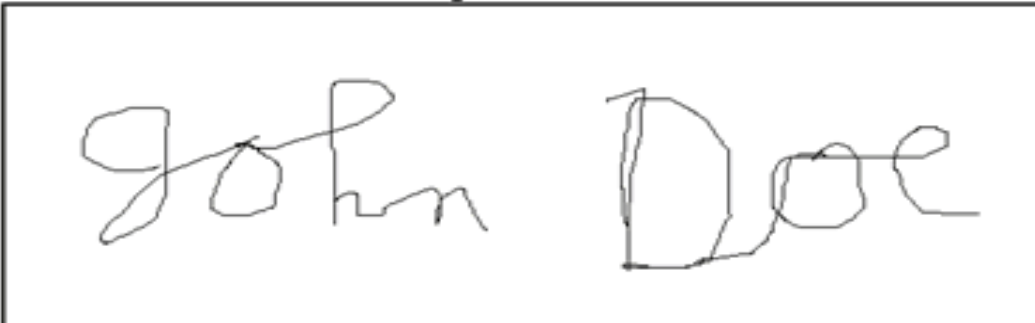
Continue - Otherwise click "back" and you will be returned to this page.

Tips for using the signature box:

- Start with the mouse at the left side of the mouse pad so there is sufficient range of movement to complete the signature. Reposition the mouse if you run out of room on the mousepad.
- Experiment with a faster, smoother motion, and with a slower, more deliberate motion.
- Go more slowly on letters you have difficulty with
- If you are using an older or slower computer, you may have to write more slowly so that the computer can keep up without leaving gaps.

I agree that WebPen is what I need for my online document.

Signature Box:



Clear

Signed: Date: December 12th, 2005

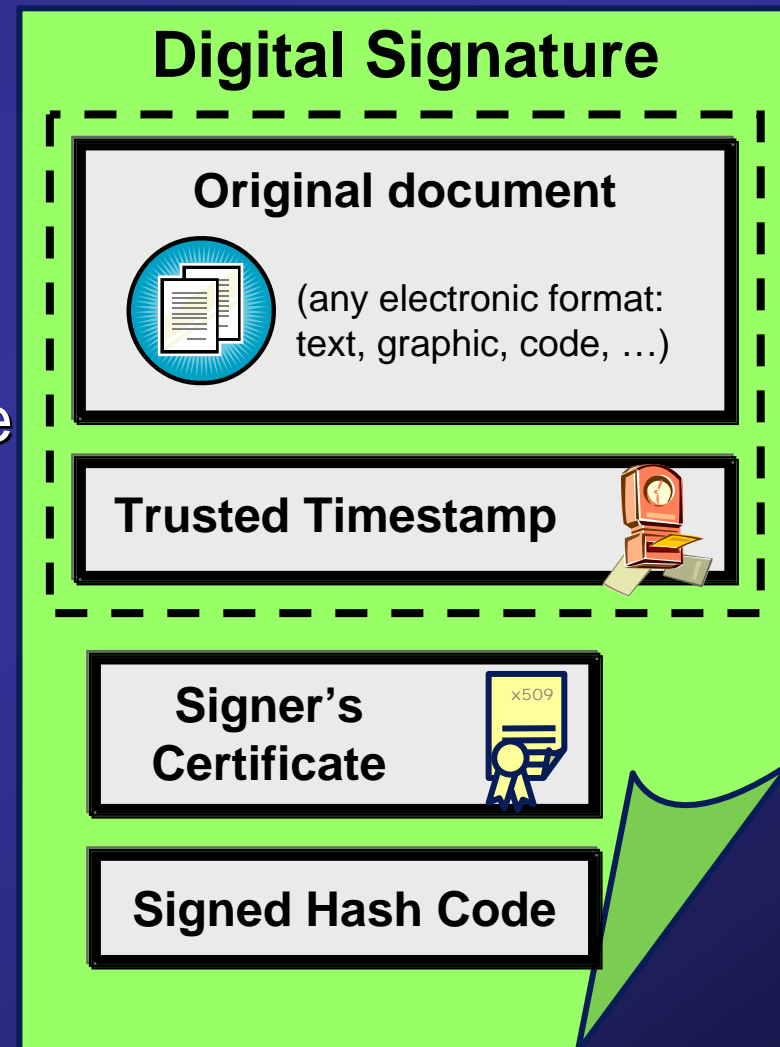
Submit Agreement

start | 9 Int... | Confir... | 8 No... | Macro... | 2 Wl... | Macro... | EN | 12:58 PM

THIS is a digital signature

```
ae aa 9f fc b7 d2 cb 1f 5f 39 29 28 18 9e 34 c9
6c 4f 6f 1a f0 64 a2 70 4a 4f 13 86 9b 60 28 9e
e8 81 49 98 7d 0a bb e5 b0 9d 3d 36 db 8f 05 51
ff 09 31 2a 1f dd 89 77 9e 0f 2e 6c 95 04 ed 86
cb b4 00 3f 84 02 4d 80 6a 2a 2d 78 0b ae 6f 2b
a2 83 44 83 1f cd 50 82 4c 24 af bd f7 a5 b4 c8
5a 0f f4 e7 47 5e 49 8e 37 96 fe 9a 88 05 3a d9
c0 db 29 87 e6 19 96 47 a7 3a a6 8c 8b 3c 77 fe
46 63 a7 53 da 21 d1 ac 7e 49 a2 4b e6 c3 67 59
2f b3 8a 0e bb 2c bd a9 aa 42 7c 35 c1 d8 7f d5
a7 31 3a 4e 63 43 39 af 08 b0 61 34 8c d3 98 a9
43 34 f6 0f 87 29 3b 9d c2 56 58 98 77 c3 f7 1b
ac f6 9d f8 3e aa a7 54 45 f0 f5 f9 d5 31 65 fe
6b 58 9c 71 b3 1e d7 52 ea 32 17 fc 40 60 1d c9
79 24 b2 f6 6c fd a8 66 0e 82 dd 98 cb da c2 44
4f 2e a0 7b f2 f7 6b 2c 76 11 84 46 8a 78 a3 e3
```

- An Electronic signature is a mathematical operation on a document using the private key of the signer
- The signature can be made visible graphically and verified automatically in the customer environment
- The trusted time-stamp provided by LuxTrust supports non-repudiation



- **Authentication:** Validate the online identity of a correspondent
- **Advanced electronic signature:** Give online agreement, with **legal value**, to the contents of an electronic document
- **Data integrity:** Ensure that an online document has not been altered since it has been signed
- **Non-repudiation:** A correspondent cannot deny being at the origin of a signature or authentication

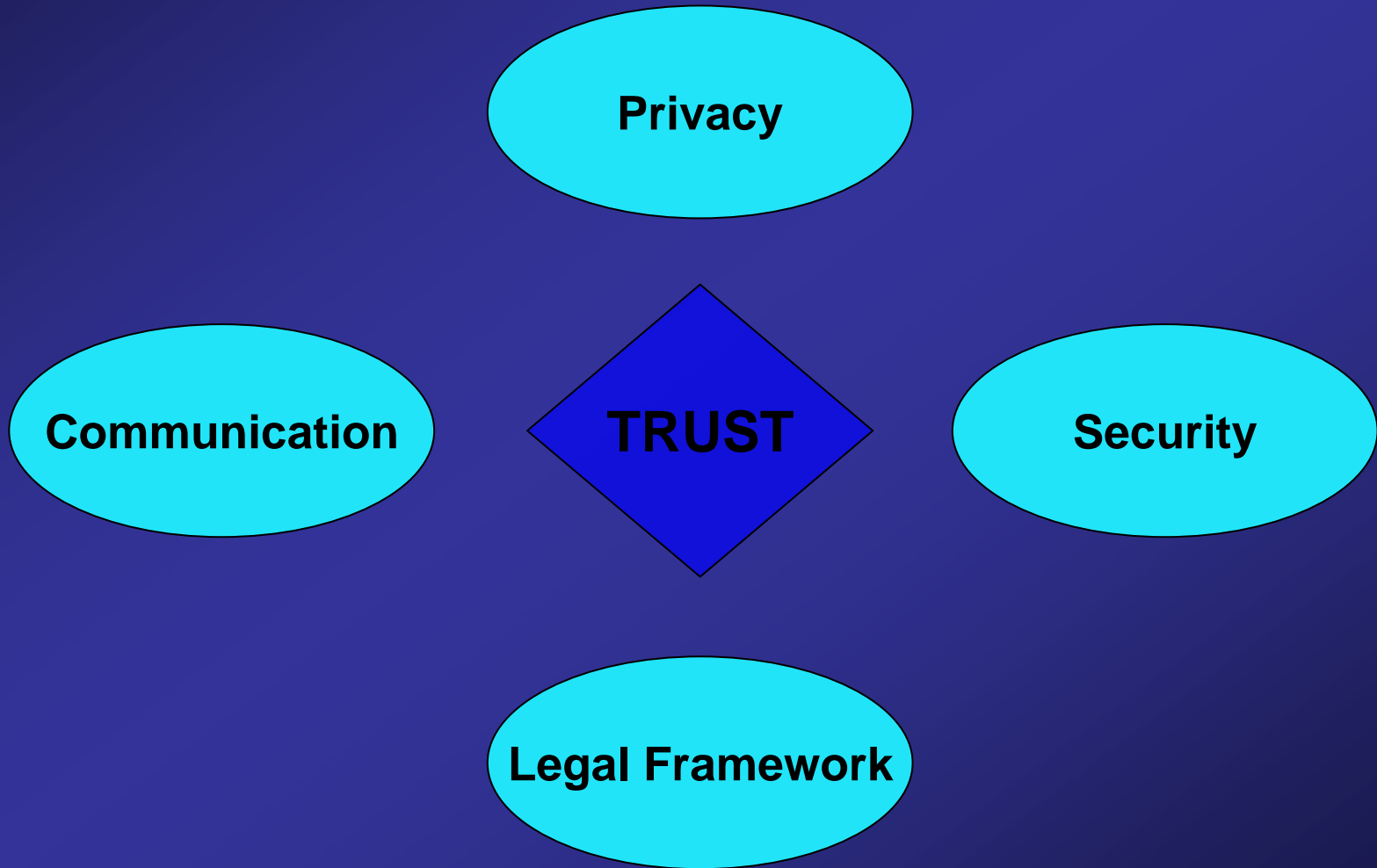
- **Application Providers**
 - Elements of proof
 - Cost reduction by mutualisation of resources
 - Keep control of authorisation and internal security
 - Facilitate compliancy
 - Solution against new type of attacks

- **Customers**
 - Sole control of security credentials
 - Elements of proof
 - Control of personal data

- **Expensive** : Critical Mass
- **Complex** : Customers/Application providers
- **Level of Security**
- **Loose control of security** : Application providers
- **Digital divide**
- **Privacy** : one id-number for everybody ?

1. Questions
2. Trusted Third Parties
3. Certificates
4. Authentication & Privacy
5. Electronic Signature
6. **Economic Impact**

- Spin-offs in security business
- New applications : e-Archiving, e-Invoicing, Health Care
- Reduce administrative burdens
- Cost cutting by common IDM infrastructure
- Prerequisite for international business



By 2010 all European citizens, businesses and administrations shall benefit from secure means of electronic identification that maximize user convenience while respecting data protection regulations.

Goal presented by the European eGovernment Signpost Paper