



Prime issues



Phishing



Identification



Manipulation

The Internet identity crisis



Mutual identification



Mutual identification



Mutual identification



The basis of legal value

Following **Directive 1999/93/EC** of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

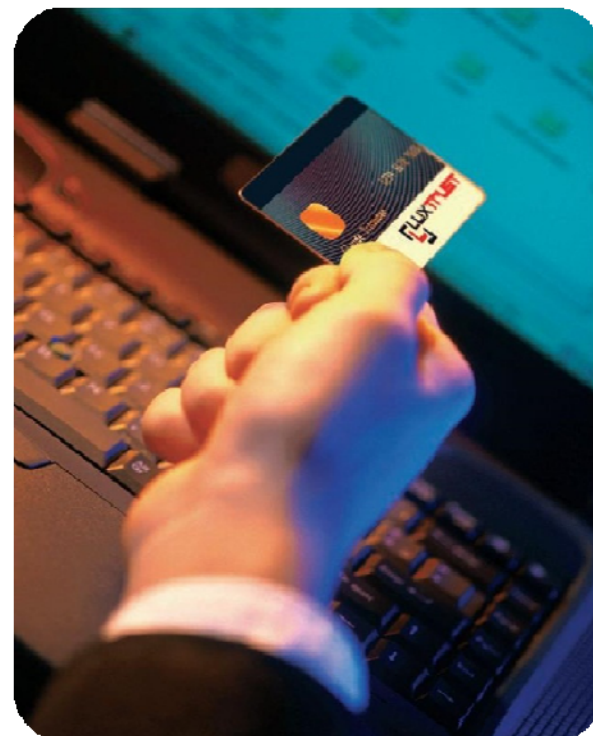
Qualified Electronic Signature:

- ▶ EU lays down **criteria** for legal recognition of **electronic signatures**
- ▶ Defines requirements for certification authorities:
 - ▶ Common **obligations** for CSPs
 - ▶ Common rules for **liability** – helps to build confidence and trust for subjects and relying parties

For issuance of a token containing Qualified Certificates:

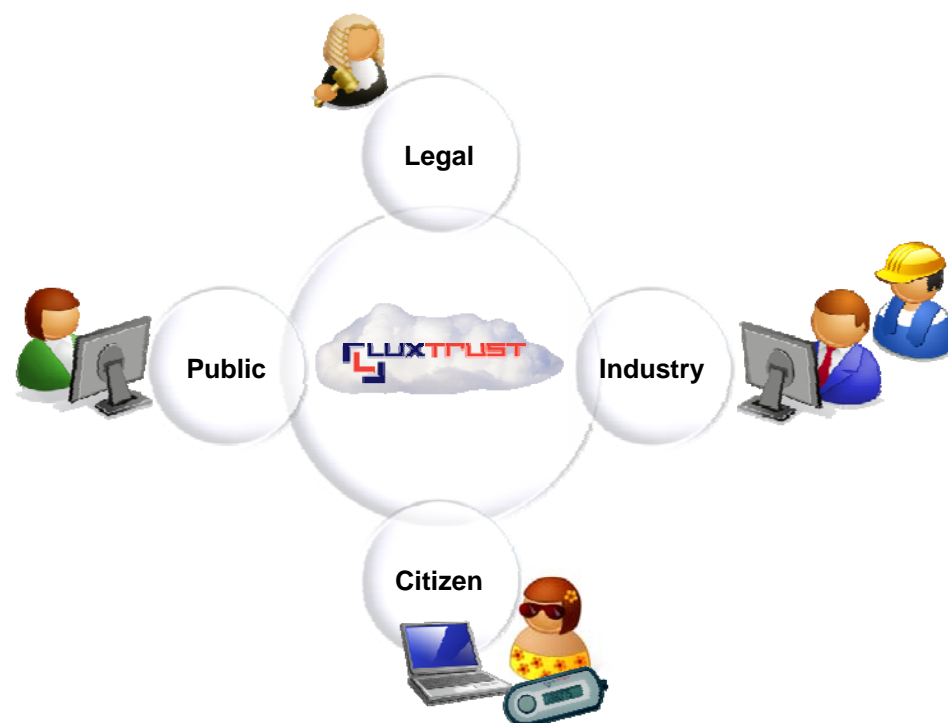
must in particular include:

- ▶ Enrollment process with:
 - ▶ Strong identification (face to face) of the subscriber
 - ▶ Assessment of its identification documents
- ▶ Request the creation of a card to the personalization env.
- ▶ On card generation of subject keys
- ▶ Certification of the keys by the CA
- ▶ Provisioning of the token and activation data to the subject



Trusted Third Party

- Management of physical PKI for **various** applications
 - **Strong** registration procedures, compliant with **EU** and **governmental** requirements
 - Provides e-Identity for physical & moral persons
 - 24x7 revocation
 - 24x7 validation
 - **International center of excellence**
 - Trusted Time Stamping
-
- Mutualized services
 - Large exploitation, mature technology
 - Cross Platform support
 - Joined user groups
 - High scalability
 - Fast time to market





User devices

Signing Server Certificate

- with Token-OTP* or SMS-OTP for advanced PKI-based authentication, signature and encryption.



Signing Stick

- two certificates for advanced PKI-based authentication, signature and encryption; no additional reader needed.



Smartcard

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



(*One Time Password)

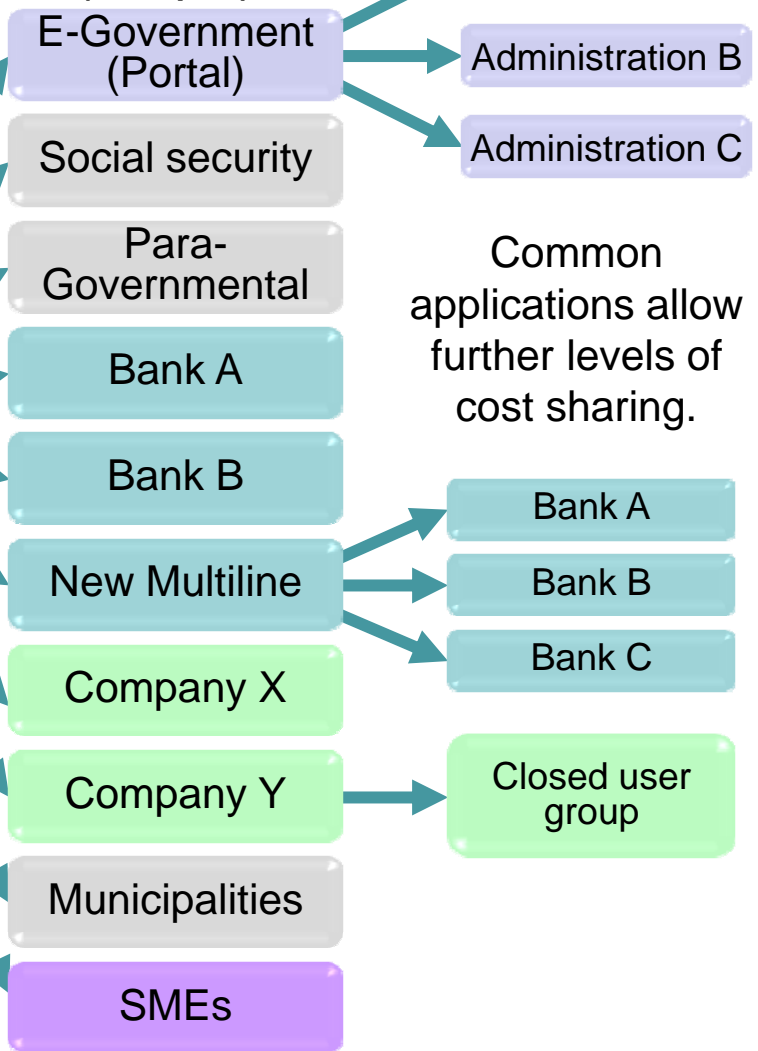
Mutualisation Effect

With one LuxTrust Certificate the user can access multiple applications.

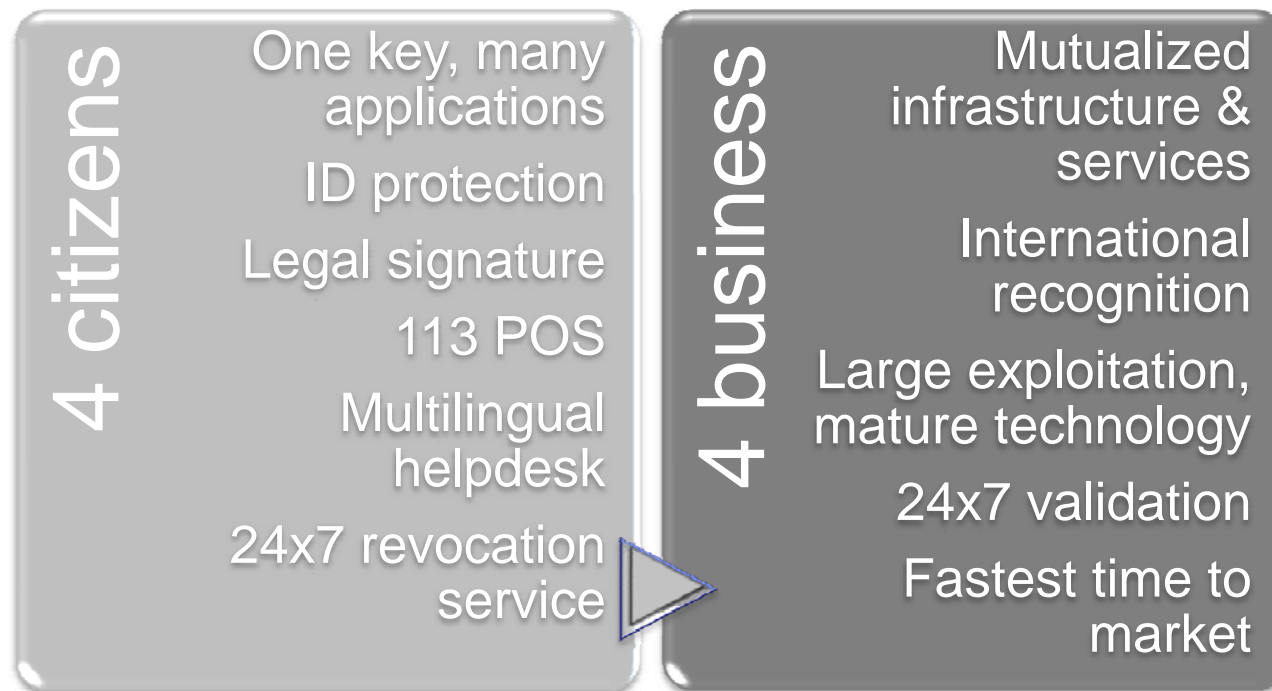


The costs for the certificate can be **shared among the multiple application providers** allowing them to get PKI technology at a fraction of the price of an own solution.

Applications (Examples)

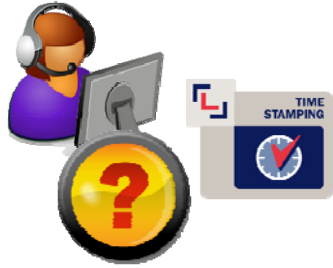


Customer benefits

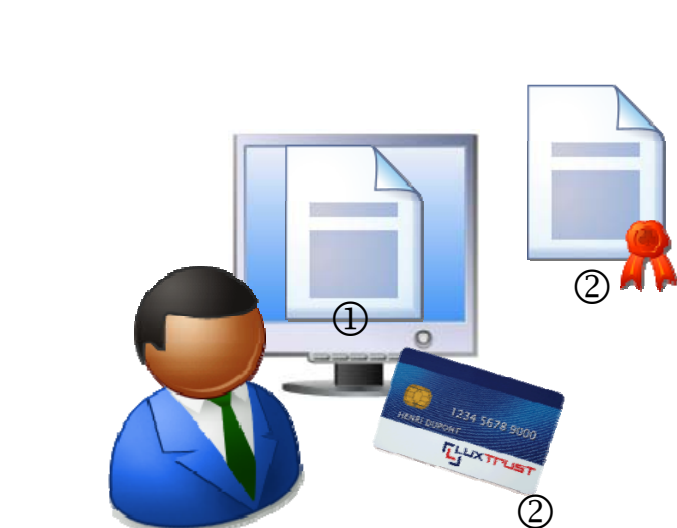
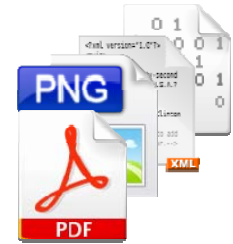


24x7 validation & timestamping services

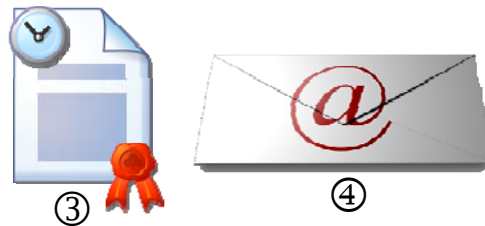
Contract signature (legal value)



1. Edit contract.
2. Sign contract with Smartcard;
3. Timestamp contract;
4. Send contract to customer (FTP server, e-mail...).



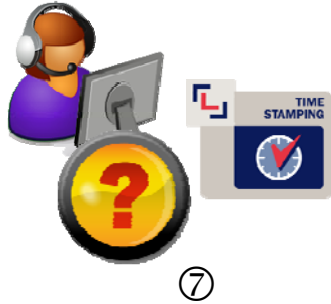
Seller



Buyer

24x7 validation & timestamping services

Contract signature (legal value)



4. Receive contract from insurance agent;
5. Verify data integrity;
6. Verify author ID;
7. Validate certificate;
8. Verify Timestamp;
9. Accept/refuse contract;
10. Settle commercial matters, countersign contract.



Seller



Buyer



Thank you!

