

# ***LuxTrust : Cas d'utilisation***

Internet Security Day 2008

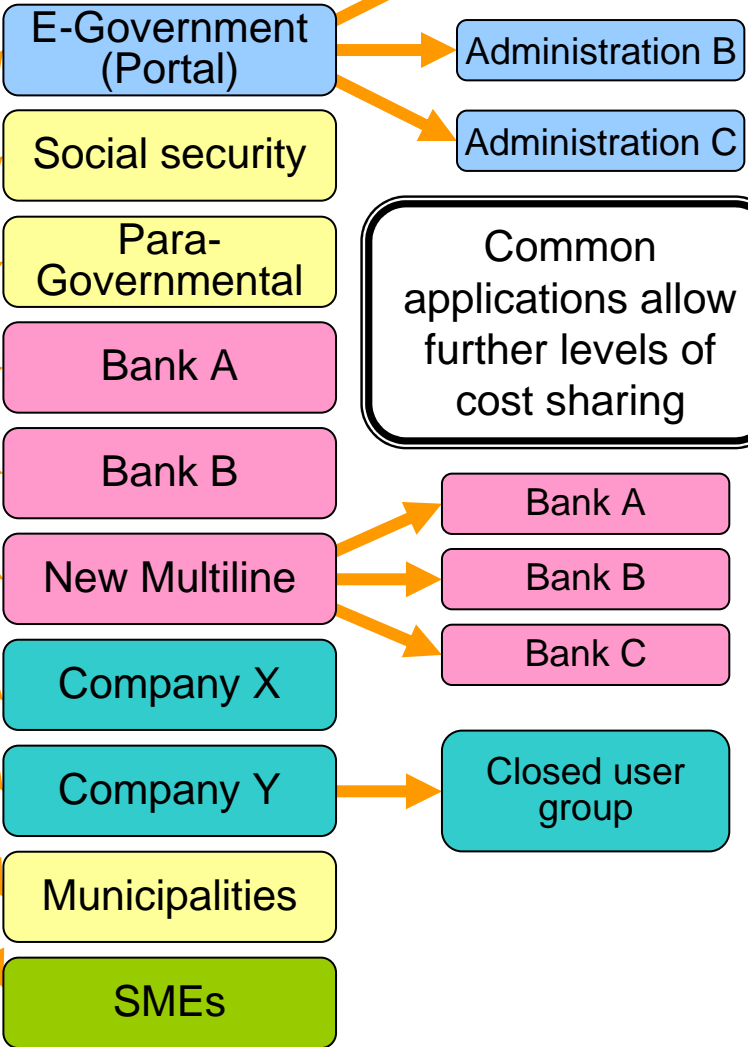
- **Sensitive Data : Image of the individual**
- **Favors new type of communication**
- **Digital divide (cost, complexity)**
- **Protect against new threads : Identity theft**
- **Privacy**

With one LuxTrust Certificate the user can access multiple applications



Each user has 1 LuxTrust ID (PKI)

## Applications (Examples)



Common applications allow further levels of cost sharing

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.

LuxTrust S.A., B.P. 43  
L-2010 Luxembourg  
www.luxtrust.lu  
Fax: + 352 26 68 15 – 789

0000000000002823 000003  
7900 0028 2307 01005

MORPHEUS SPECIMEN 4.01 NEO  
LUXTRUST S.A.  
7, RUE ALCIDE DE GASPERI  
L-2010 LUXEMBOURG

LUXEMBOURG

30101414 000022

---

Chère cliente, cher client,

Nous avons le plaisir de vous remettre votre nouvelle carte à puce LuxTrust. Veuillez lire attentivement les conseils d'utilisation :

- ne vous séparez jamais de votre carte et conservez-la en lieu sûr;
- votre carte est strictement destinée à usage personnel;
- veuillez conserver vos codes secrets séparément de votre carte à puce;
- en cas de perte ou de vol, contactez immédiatement le service de suspension et de révocation LuxTrust au numéro de téléphone **+352 24 550 550** afin de procéder à une suspension de votre carte.

En restant entièrement à votre disposition pour toute information supplémentaire, veuillez agréer, chère cliente, cher client, l'expression de nos sentiments distingués.

---

Dear customer,

Please find enclosed your new LuxTrust smart card. Please find below some proposals for adequate use:

- always keep your card in your possession and in a safe place;
- your card is strictly for personal use;
- do not store your secret codes in the same place as your smartcard;
- in the case of loss or theft, please contact the LuxTrust suspension and revocation desk immediately on **+352 24 550 550** to suspend your card.

Please do not hesitate to contact us for any further information.

---

Sehr geehrte Kundin, sehr geehrter Kunde,

wir freuen uns, Ihnen Ihre neue LuxTrust Chipkarte zukommen zu lassen.

Bitte beachten Sie folgende Benutzungsratschläge:

- bewahren Sie Ihre Karte stets an einem sicheren Ort auf;
- diese Karte ist strikt persönlich, und darf nur von Ihnen angewendet werden;
- bewahren Sie Ihre Karte nie am gleichen Ort wie ihre Geheimzahlen auf;
- falls Sie die Karte verlieren oder Ihre Karte gestohlen wurde, bitten wir Sie unverzüglich die LuxTrust Widerrufsstelle auf der Nummer **+352 24 550 550** anzurufen um ihre Karte einstweilig zu widerrufen.

Für weitere Informationen stehen wir Ihnen gerne zur Verfügung und verbleiben mit freundlichen Grüßen.

LuxTrust S.A.  
B.P. 43  
L-2010 Luxembourg  
www.luxtrust.lu  
Fax: + 352 26 68 15 – 789

30101414 000022

LUXTRUST S.A.  
7, RUE ALCIDE DE GASPERI  
L-1615 LUXEMBOURG  
LUXEMBOURG

000094 000022

Madame, Monsieur,  
Ce pli contient vos codes secrets personnels.

Sehr geehrte(r) Kundin / Kunde,  
dieser Brief enthält Ihre persönlichen Geheimzahlen.

Dear customer,  
please find your personal secret codes underneath.

IMPORTANT

Protégez vos codes secrets!

- Veuillez garder ce bordereau en lieu sûr
- Ne communiquez vos codes secrets à personne, même pas par téléphone ou via courrier électronique
- Veuillez vous assurer que lors de l'utilisation de votre carte, personne ne puisse voir votre code PIN

WICHTIG

Schützen Sie Ihre Geheimzahlen!

- Bitte diese Angaben an einem sicheren Ort aufbewahren
- Teilen Sie niemandem Ihre persönlichen Geheimzahlen mit, auch nicht über Telefon oder per E-Mail
- Achten Sie bei Gebrauch auf neugierige Blicke, so dass niemand Ihre Geheimzahlen sehen kann

IMPORTANT

Protect your secret codes!

- Keep these codes in safe location
- Don't ever tell anyone what your personal secret codes are and do not communicate them by phone or via e-mail
- Be aware that some people might want to see your PIN code, while you are using your card

**LuxTrust Helpdesk**  
**+352 24 550 550**

**24/7**

Certificate number  
9800 0029 10

En cas de perte / vol de votre carte ou de divulgation de vos codes secrets, prévenez 24h/24h : →

Bei Verlust / Diebstahl Ihrer Karte oder bei Kenntnisnahme Ihrer persönlichen Geheimzahlen durch Dritte, wählen Sie, rund um die Uhr : →

In the case of loss / theft of your card or disclosure of your personal secret codes, call 24 hours a day : →

Veuillez gratter la zone protégée afin de découvrir vos codes secrets

Bitte die Schutzschicht freirubbeln, um Ihre persönlichen Geheimzahlen zu sehen

Please scratch off the protected area to discover your secret codes

**Important:** Notes explicatives voir verso.

**Important:** Read explanation on the back.

**Wichtig:** Bitte Informationen auf der Rückseite lesen.

### **LuxTrust Smartcards, Signing Sticks and Signing Server Certificates will only be 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

### Type of actors:

- Application Providers (i.e. Online-banking)
- Employee / professional person
- Administrators
- Private person

### **Card issuing :**

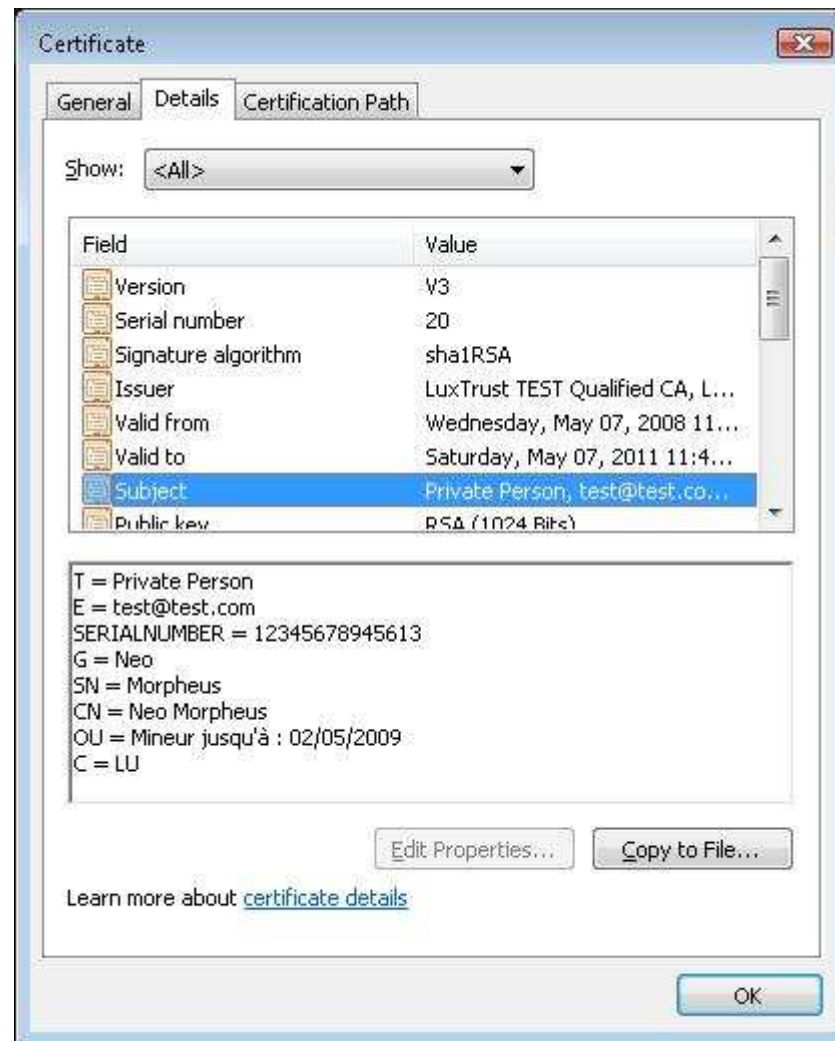
= agreement to issue the card

≠ mandate or specific rights

### **Card usage is regulated by:**

- LuxTrust's General Terms and Conditions
- Contract between company and card holder / Mandate (i.e.: signature rights)
- Contract between company and application provider (i.e.: access rights)

- **Advanced Electronic Signature**
  - Uniquely linked to the signatory
  - Capable of identifying the signatory
  - Created using means that the signatory can maintain under his sole control
  - Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
  
- **Qualified Electronic Signature**
  - Advanced Electronic Signature
  - Based on qualified certificates
  - Created with a secure signature creation device



- **Application Providers**

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

- **Customers**

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

- IT people know WHAT to do,
- But very often don't understand HOW it works
- And even worse ignore WHY certain implementation steps are necessary

**Security is often an illusion**

## **SHA-1 Broken**

“SHA-1 has been broken. Not a reduced-round version. Not a simplified version. The real thing.”

## **RSA Broken**

Branch Prediction Analysis attack

## **Biometrical Passport not secure**

“Adi Shamir was unexpectedly pessimistic about the future, saying that the security of the systems we use worsens as the systems become more complex. He even went so far as to say that we would conclude 30 years down the road, that cryptography had won many battles, but lost the war for greater security.”

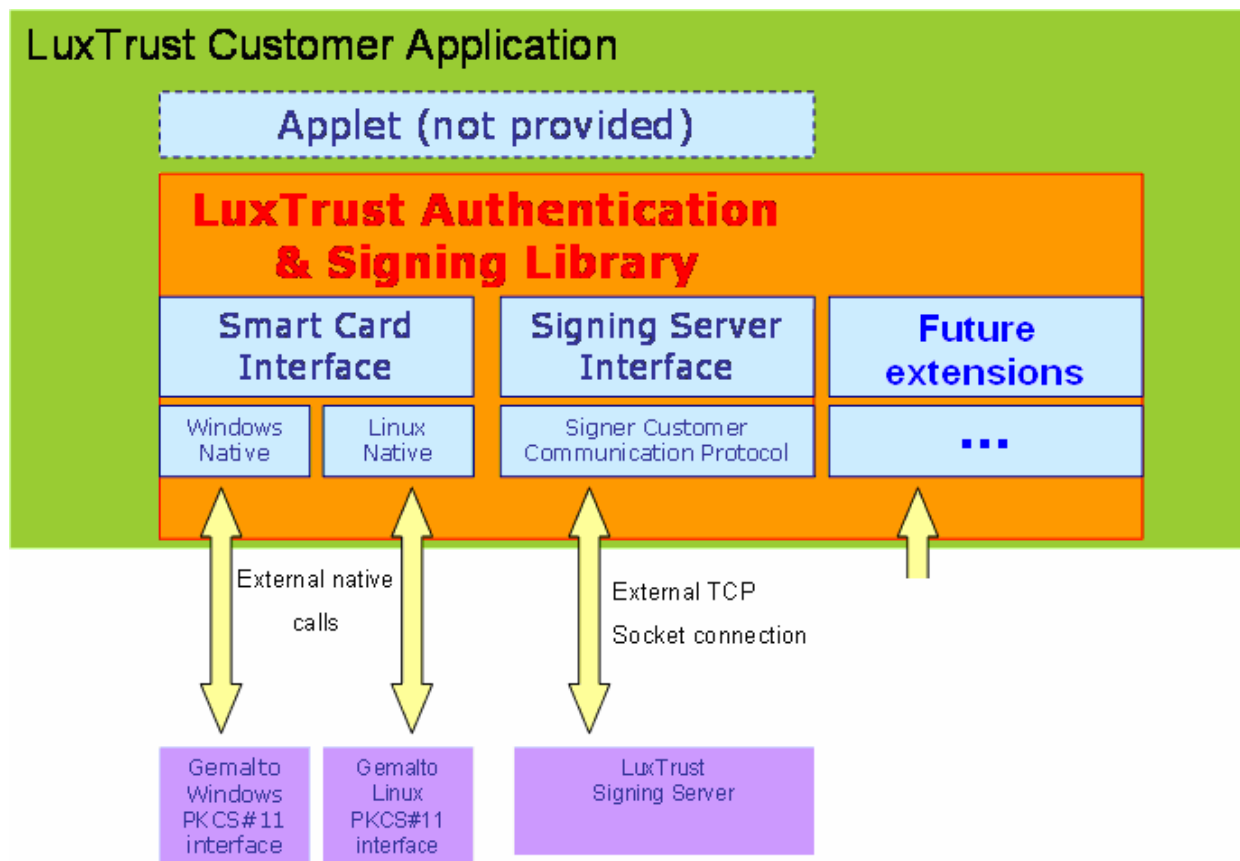
- Doubts due to real or sensational press releases
- Provided applications not really helpful to give confidence
- Technology not understandable
- Acceptance by flexibility : anywhere, anytime

**People need Control Possibilities**

## **No intelligence on PC ?**

There is, but it **was** not our business.

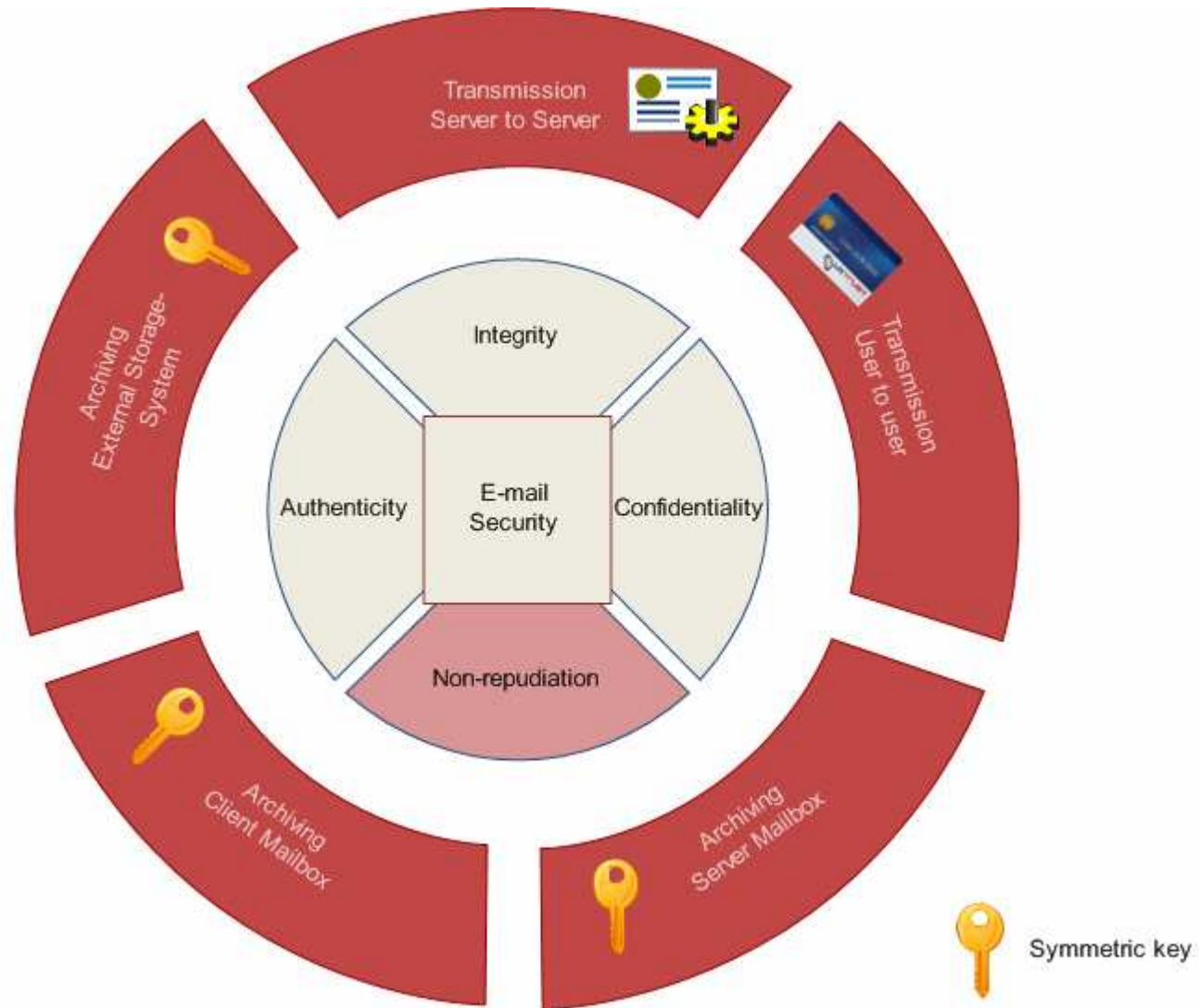
Securing a by design un-secure environment.

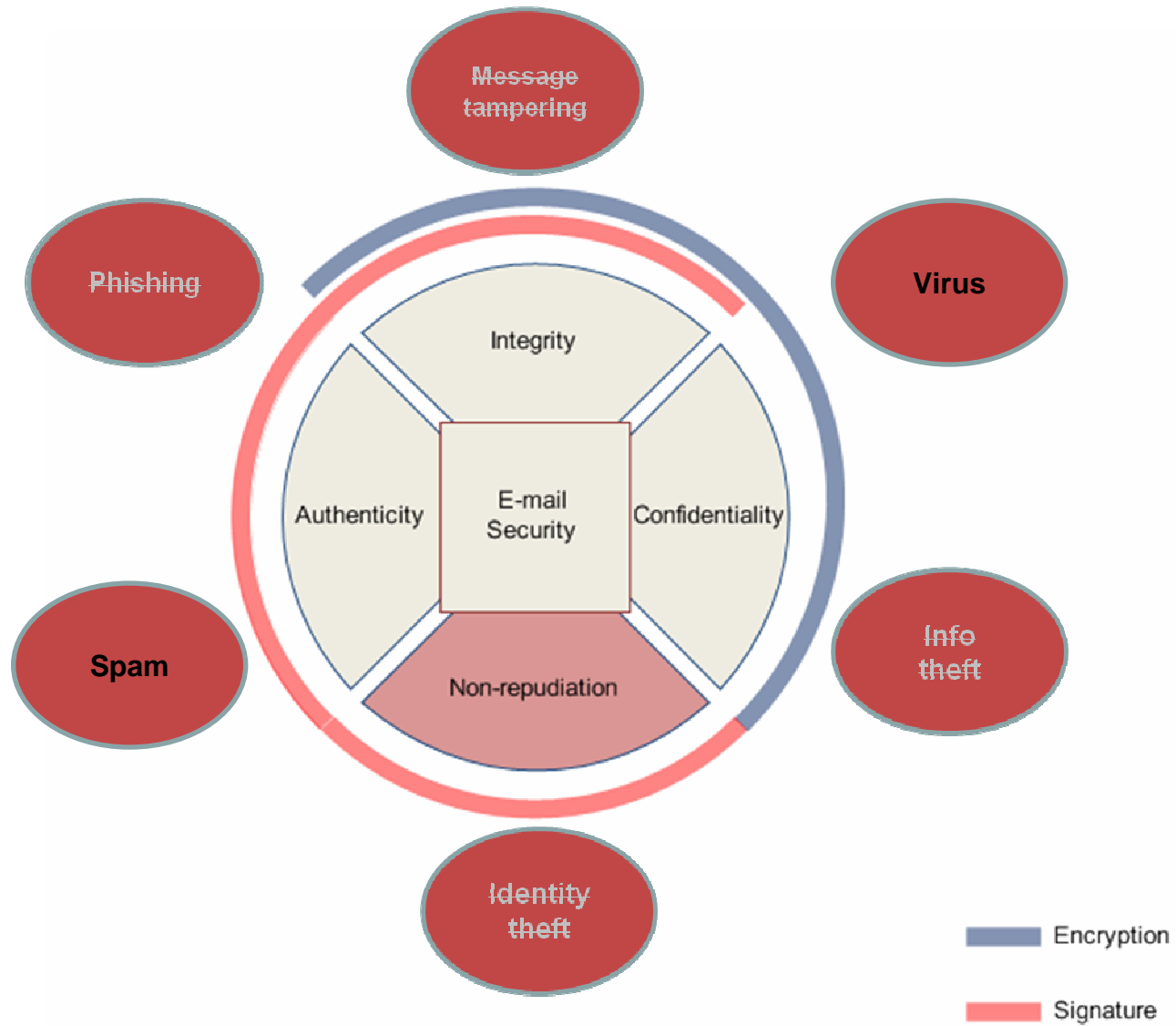


Abstraction of smartcard and Signing Server communication  
Plain Java Objects for easy integration into applications

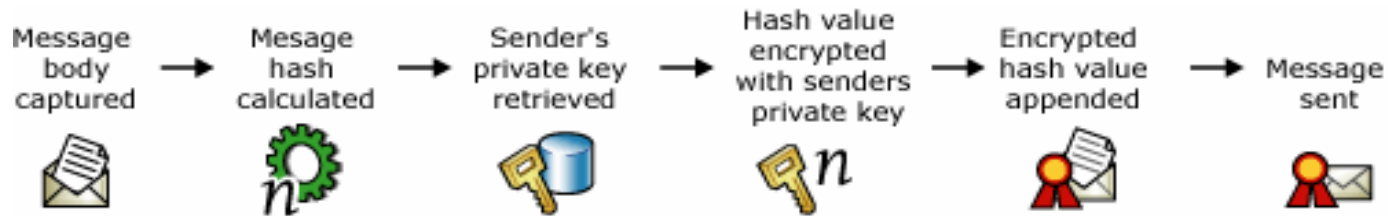
- **Big Bang Migration**
- **Protection against all threads**
- **Loose control of security** : Application providers
- **Privacy** : one id-number for everybody ?

- Internal Usage : VPN, SSO
- Secure electronic exchange (Sofie, e-File)
- Reduce administrative burdens and costs
- International Interoperability
- Multi-application cards
- Paperless Legal Archives

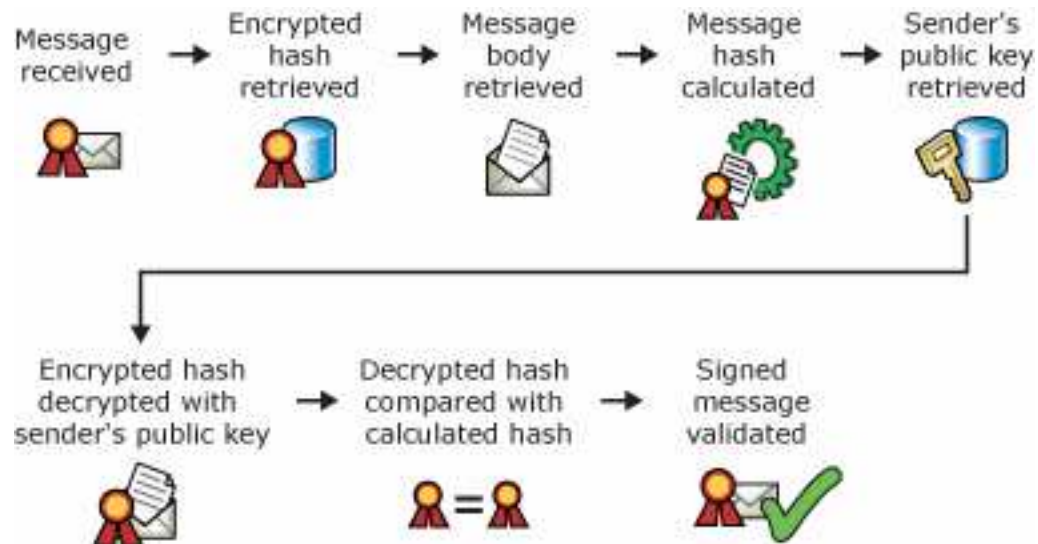




## Sender

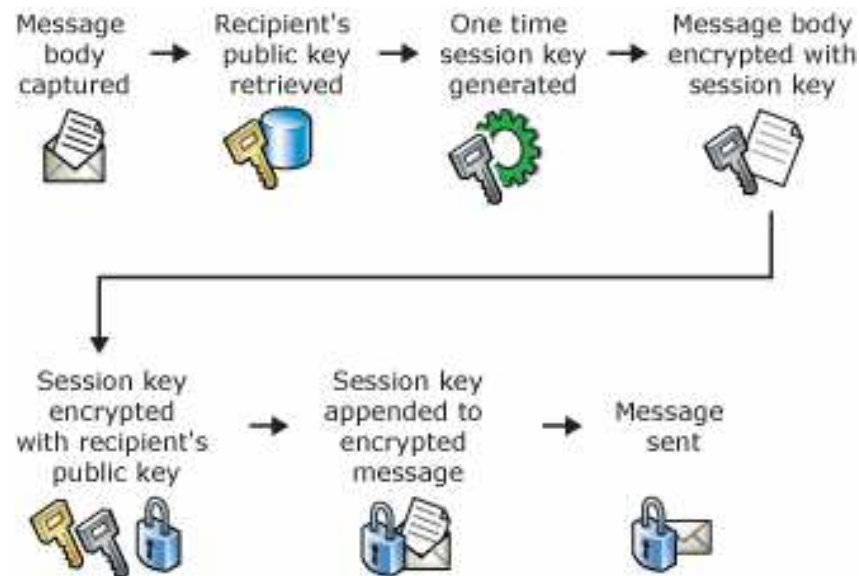


## Receiver

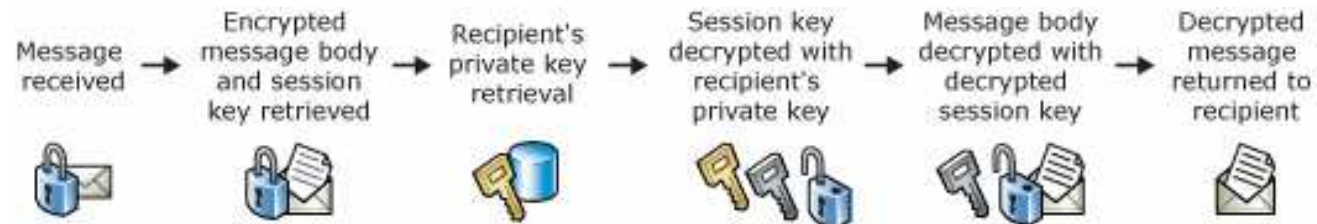


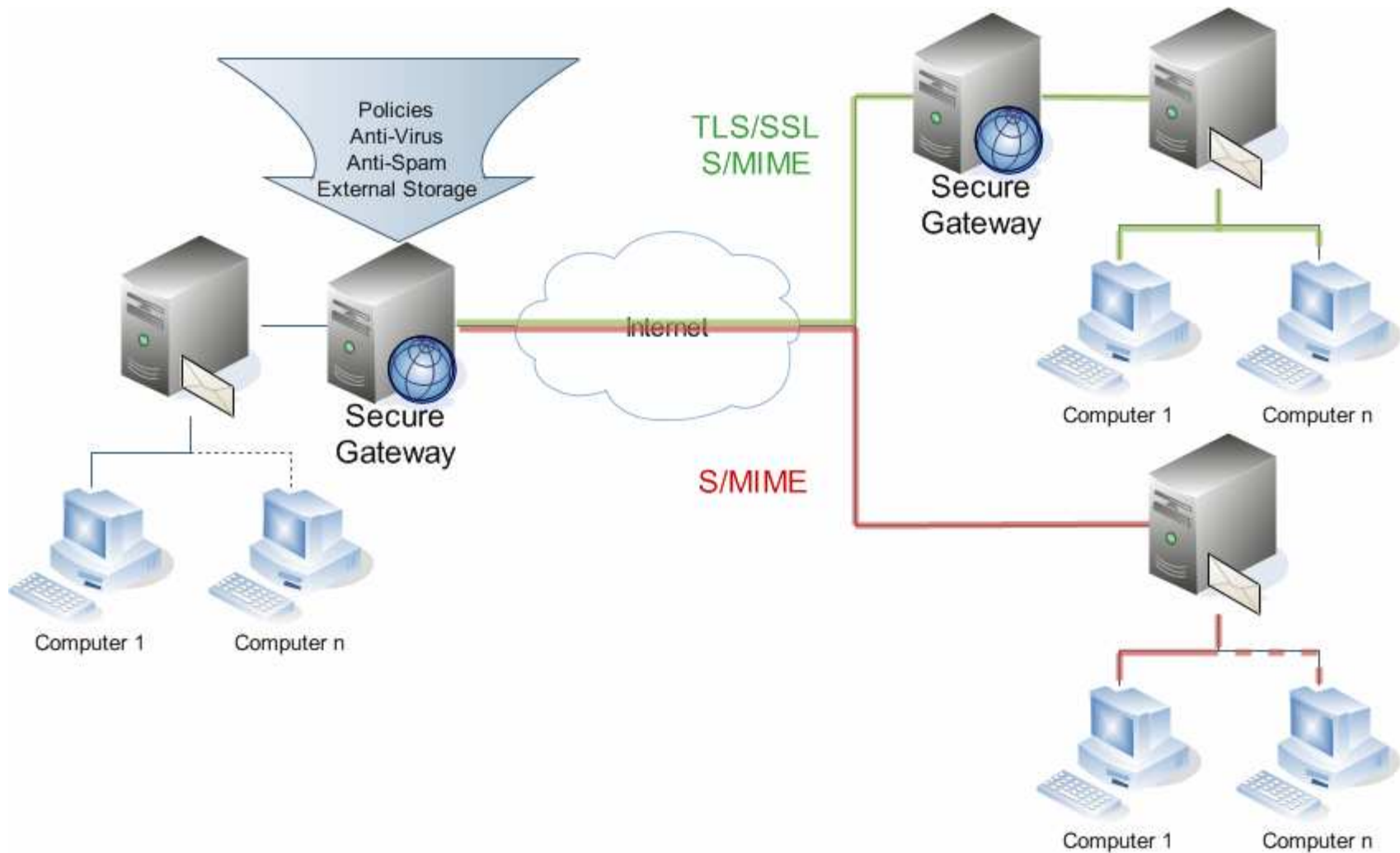
# S/MIME Encryption: Message Confidentiality

## Sender



## Receiver





## RFC 3850 S/MIME 3.1 Certificate Handling Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as ....

Using Distinguished Names for Internet Mail End-entity certificates MAY contain an Internet mail address....

The email address SHOULD be in the subjectAltName extension, and SHOULD NOT be in the subject distinguished name.

Receiving agents MUST recognize and accept certificates that contain no email address.

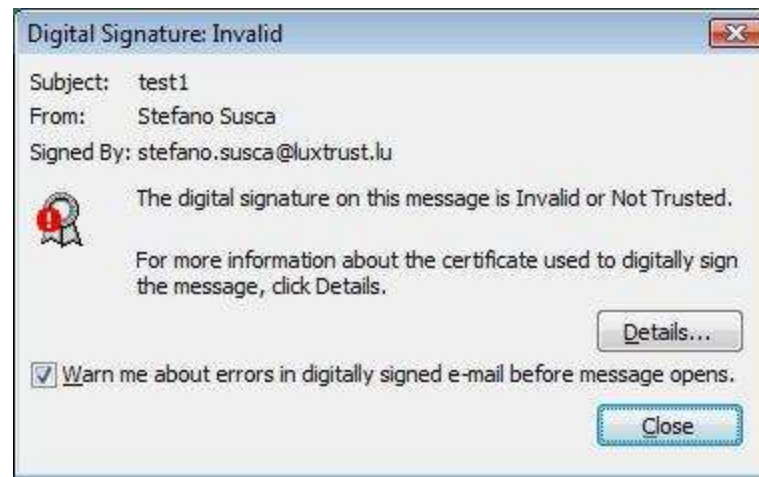
Receiving agents MUST recognize email addresses in the subjectAltName field. Receiving agents MUST recognize email addresses in the Distinguished Name field .

Sending agents SHOULD make the address in the From or Sender header in a mail message match an Internet mail address in the signer's certificate. Receiving agents MUST check that the address in the From or Sender header of a mail message matches an Internet mail address.....

A receiving agent SHOULD provide some explicit alternate processing of the message if this comparison fails, which may be to display a message that shows the recipient the addresses in the certificate or other certificate details.


# Mail Client Behaviours

1st e-mail address	2nd e-mail address	sending e-mail address	Outlook Express	Outlook 2003/2007	Thunderbird
1@domain.lu	-	1@domain.lu	✓	✓	✓
-	1@domain.lu	1@domain.lu	✓	✓	✓
1@domain.lu	-	2@domain.lu	✗	✗	✓
1@domain.lu	2@domain.lu	1@domain.lu	✓	✓	✓
1@domain.lu	2@domain.lu	2@domain.lu	✗	✗	✓
-	-	1@domain.lu	✗	✗	✓





Lorem Ipsum Inc.  
24, rue Sit Amet  
L-1212 Consectetuer

  
**Néo**  
**Morpheus**  
**Spécimen 4.01**

Digitally signed by Néo Morpheus  
Spécimen 4.01  
DN: c=LU, cn=Néo Morpheus  
Spécimen 4.01, sn=Morpheus  
Spécimen 4.01, givenName=Néo,  
serialNumber=101005837900002  
82307, title=Private Person  
Date: 2008.01.09 09:36:31 +01'00'

**Ipsum Lorem Inc.**  
**42, rue Amet Sit**  
**L-2121 Adipsicing**

**Objet** : Lorem ipsum dolor

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed non risus. Suspendisse lectus tortor, dignissim sit amet, adipiscing nec, ultricies sed, dolor. Cras elementum ultrices diam. Maecenas ligula massa, varius a, semper congue, euismod non, mi. Proin porttitor, orci nec nonummy molestie, enim est eleifend mi, non fermentum diam nisl sit amet erat. Duis semper. Duis arcu massa, scelerisque vitae, consequat in, pretium a,

Signature Properties

Signature is VALID, signed by Néó Morpheus Spécimen.




Summary Document Signer Date/Time Legal

Signed by: Néó Morpheus Spécimen [Show Certificate...](#)

Reason: Not available

Date: 2008/04/28 15:22:26 +02'00' Location: Not available

Validity Summary

-  The Document has not been modified since this signature was applied.
-  The signer's identity is valid.
-  Signature date/time are from the clock on the signer's computer.


Signature was created using Adobe Acrobat 8.1.0.

[Validate Signature](#) [Close](#)


Signature Properties

Signature is VALID, signed by Néó Morpheus Spécimen.




Summary Document Signer Date/Time Legal

 The signer's identity is valid.

Signed by: Néó Morpheus Spécimen [Show Certificate...](#)

 Click Show Certificate for more information about the signer's certificate and its validity details, or to change the trust settings for the certificate or an issuer certificate.

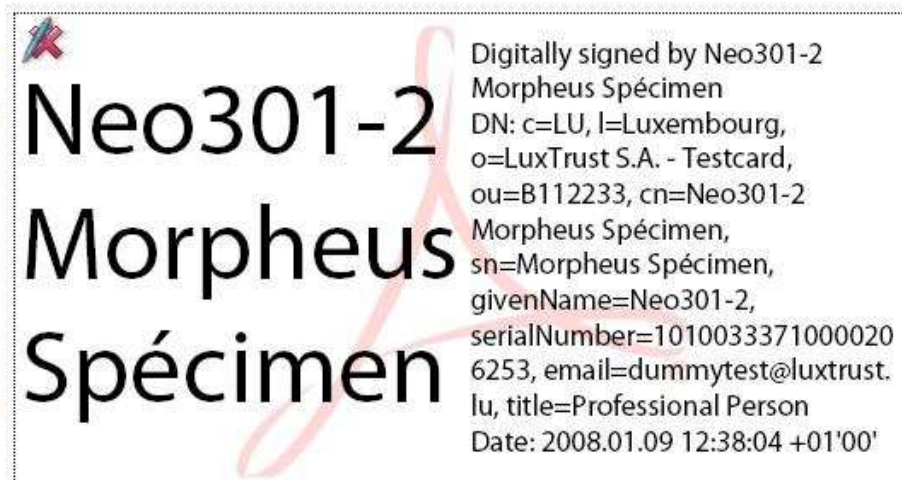
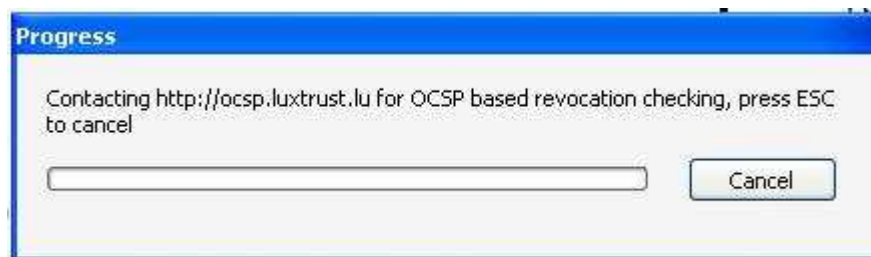
Validity Details

-  The signer's certificate has been issued by a certificate authority that you have trusted to issue certificates for the purpose of signing.
-  The path from the signer's certificate to an issuer's certificate was successfully built.
-  The signer's certificate is valid and has not been revoked.

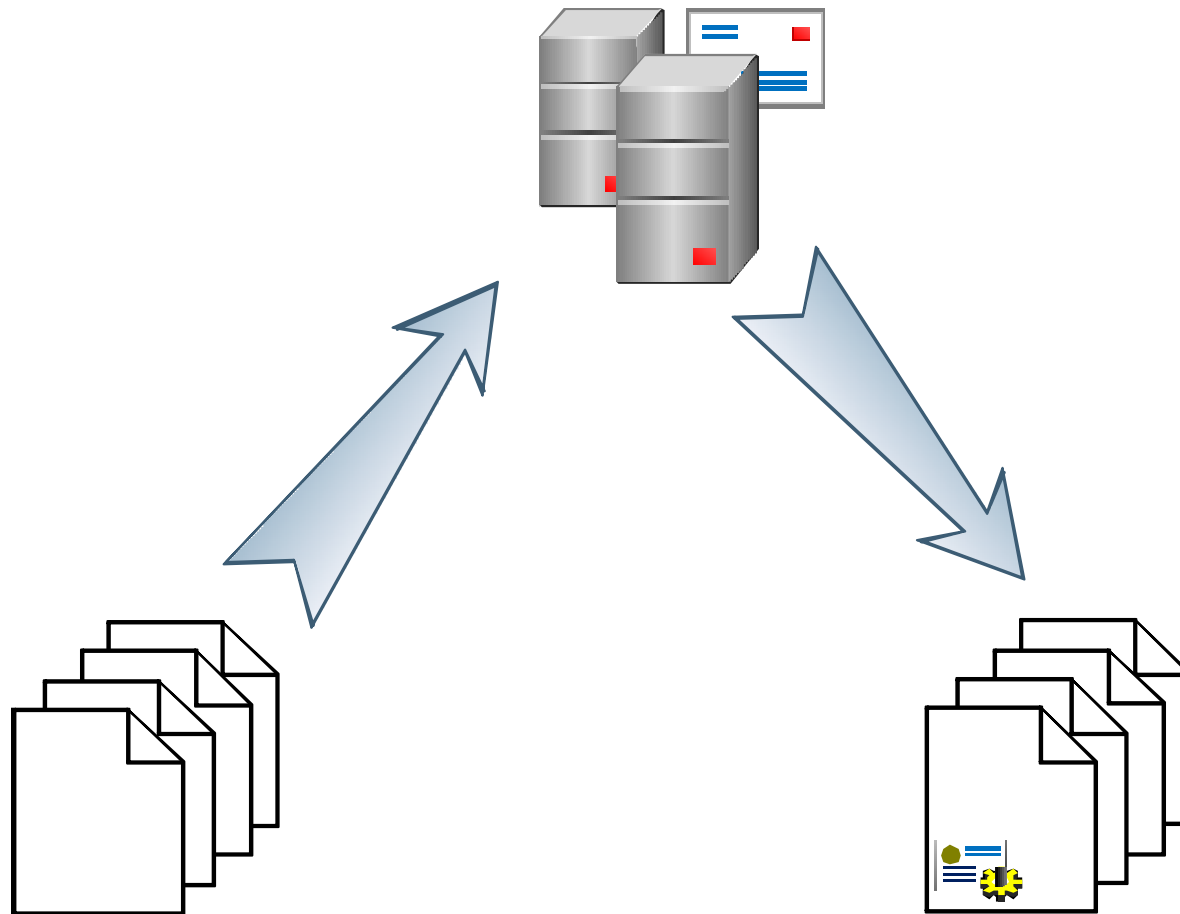
Signer's Contact Information: Not available

[Validate Signature](#) [Close](#)

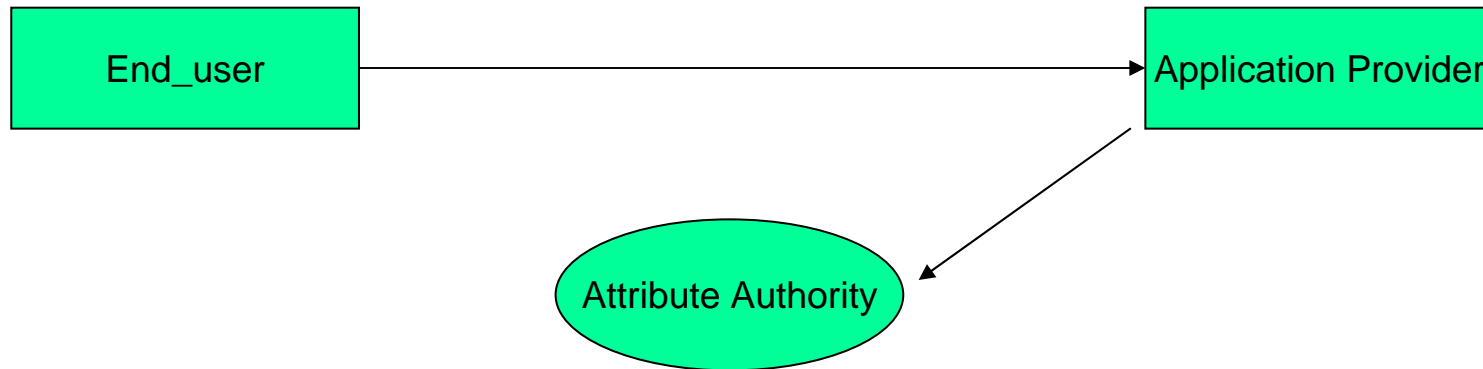
# Adobe : Revoked Certificate



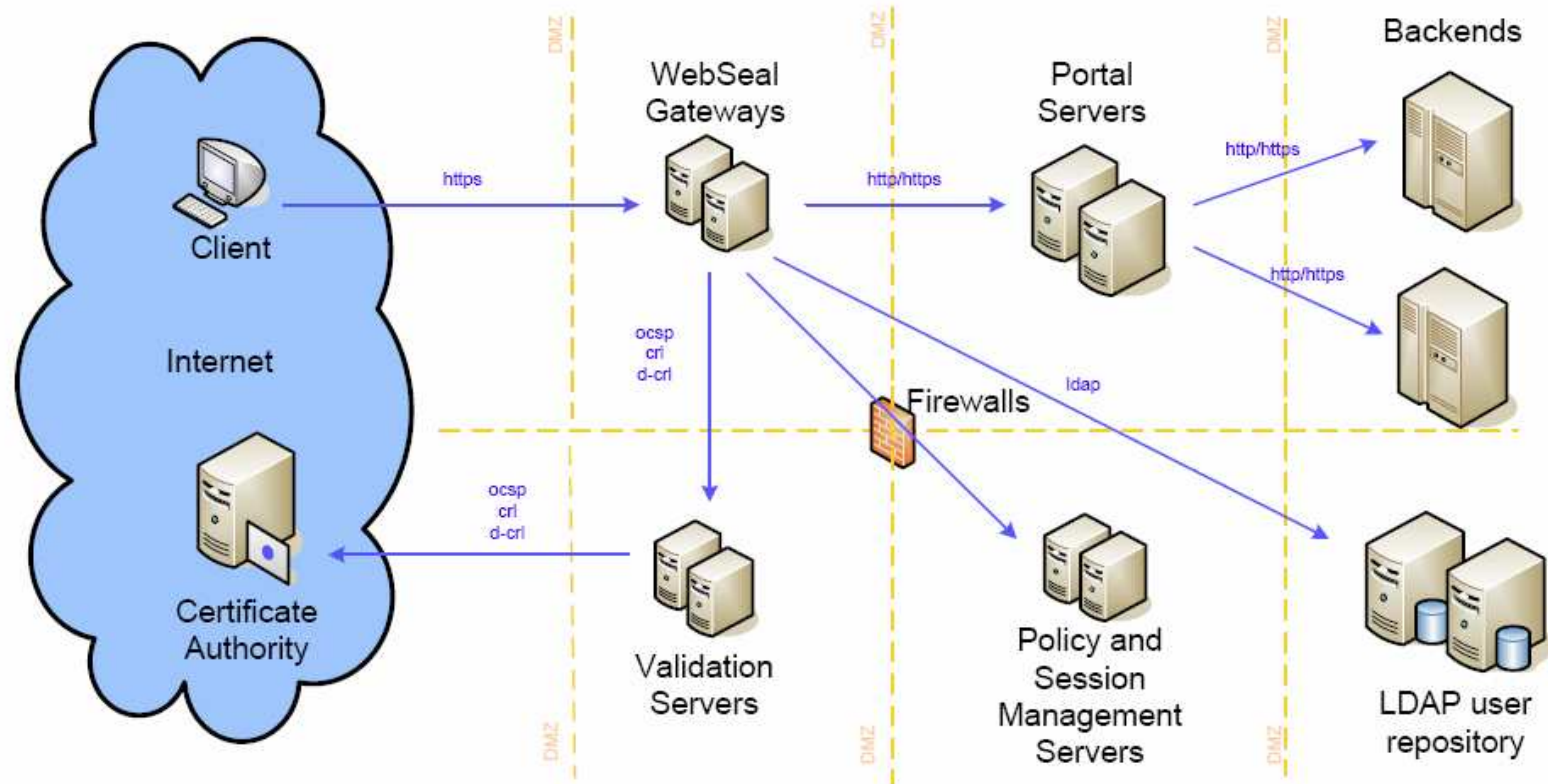
# *Mass signature & Timestamping*



- Authorization
- Rights on certain objects
- Role based
- Attribute certificates
- Acceptance by the market ?



- Information, not only privileges
- Information holder has control over his data
- Information delivered on an 'as needed' base
- Multiple pseudonyms, sector specific
- Anonymize user towards application provider
- Accountable transactions by TTP proofs
- Traceable by authorities



- One card, multiple usages
- Higher security level
- Secure Remote Access
- Monitored access



