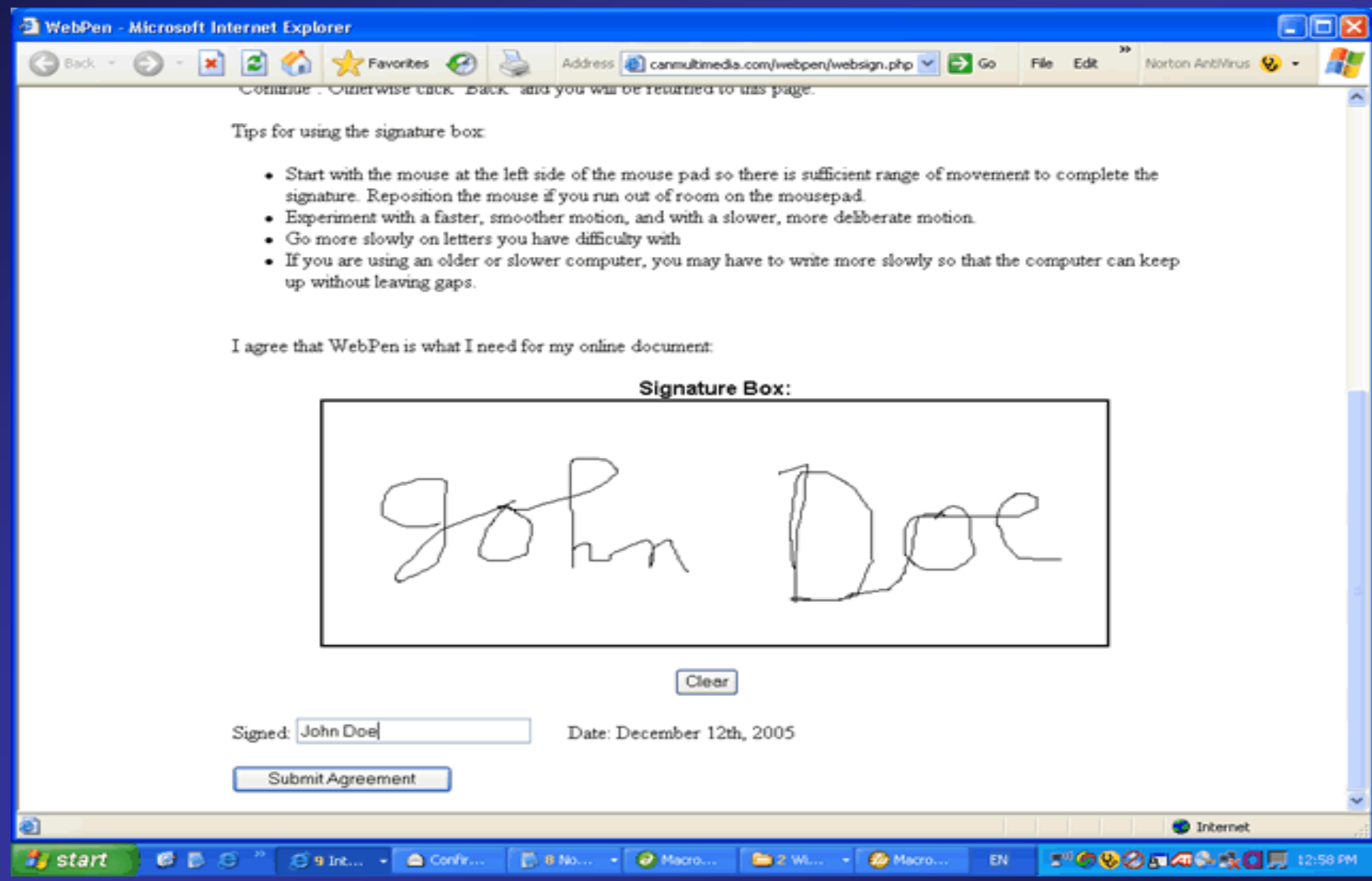


# ***LuxTrust SA***

***a national centre of excellence in  
trust business***





WebPen - Microsoft Internet Explorer

Address: canmultimedia.com/webpen/websign.php

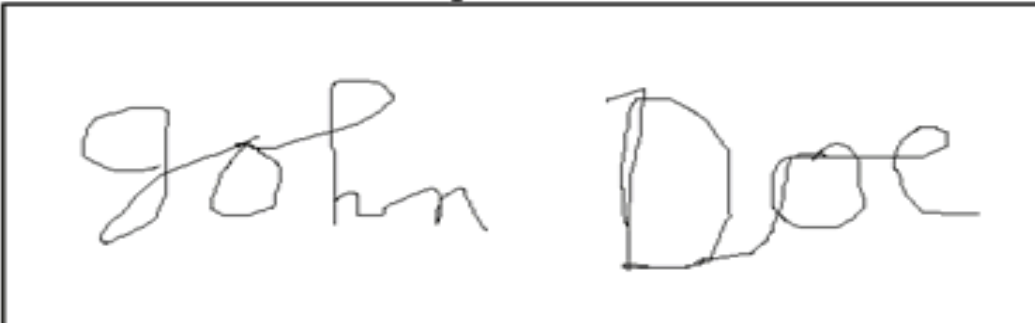
Continue - Otherwise click "back" and you will be returned to this page.

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... | Confr... | 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
```

- A Digital Certificate is the digital identity of the holder of a private key
- Personal Data:
  - Name
  - eMail
  - ...
- Trusted Third Party: LuxTrust S.A.

## X.509 Certificate

Certificate Data

Owner's  
Personal Data

Owner's Public Key

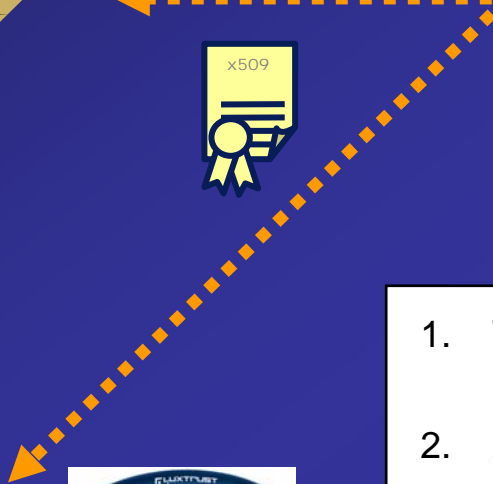
Information  
Trusted Third Party



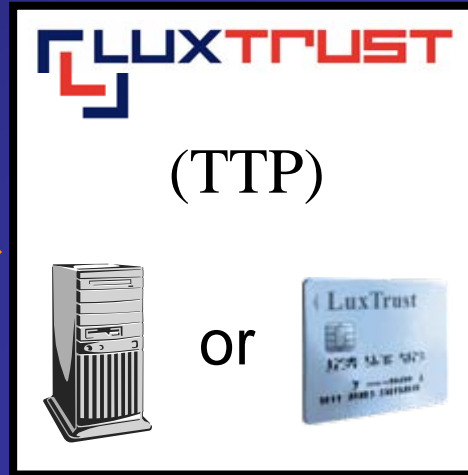
Signature of TTP



## Local Registration Authority



or



1. The client goes to a local registration authority with the documents required for this procedure (ID card, ...).
2. At the registration desk, the registration agent executes the necessary procedures in order to issue a certificate.
3. The local registration authority sends the data required for the issuing of a certificate to the TTP.
4. The TTP creates the certificate on a Smartcard or signing-server.
5. The Smartcard is sent to the ordering client or to the local registration authority (depending on the client's choice).

LuxTrust Certificates will be issued to either:

- Physical persons as private individuals
- Physical persons as employees or representatives of a company / institution

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

## **Manage Legal Risks**

- Ensure Data Privacy (CNPD)**
- Create legal proof, compliant to (inter)national regulations**
- Secure official documents : ePass, eHealth , driving licence...**
- Improve legal value of electronic archives**



- **User-friendly method of authentication and signing**
  - **Mobility:** Match with basic requirements for roaming
  - High level of **security** and **confidentiality**
- Only one LuxTrust ID for multiple applications
- Trust in a nationwide & cross-border non-proprietary solution
- Secure Access to and control of personal data

- An Electronic signature is a mathematical operation on a document using the private key of the signer.
- The signature allows the recipient to:
  - Verify the integrity of the document
  - Authenticate/identify the signer
- The trusted timestamp provided by LuxTrust supports non-repudiation

## Digital Signature

### Original document



(any electronic format:  
text, graphic, code, ...)

### Trusted Timestamp



### Signer's Certificate





### Signed Hash Code

## Certification Services

- Signature Server certificate with OTP-Token or SMS-OTP that allows advanced PKI-based authentication, signature and encryption.
- Smartcards holding two certificates (one for authentication and encryption and a second one dedicated to advanced digital signatures). The solution is designed to evolve towards a “qualified” solution when required.
- SSL-server certificates
- Object certificates
- ICAO certificates for Luxembourg’s e-Passports
- Customised solutions (Smartcards for internal use)



	2006						2007														
	Trim 3			Trim 4			Trim 1			Trim 2			Trim 3			Trim 4					
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12			
<b>Biometrical Passports</b>	Test			Production																	
<b>Website certificates</b>				Test			Production														
<b>Smartcards</b> 	Test						Production														
<b>Signing Server Certificates</b> 							Test						Production								

A common Strategy & Business Development

**LUXTRUST**  
 Centre of excellence in Trust Business with international reach

### The Regulators

### Sub-contractor: u-trust

### Technology Provider

### The Shareholders

# ***LuxTrust SA***

***a national centre of excellence in  
trust business***

