{SIMPLE COMME UN CLIC}

Rencontre internationale sur la simplification et la dématérialisation des formulaires

Signature électronique de la Ville de Luxembourg

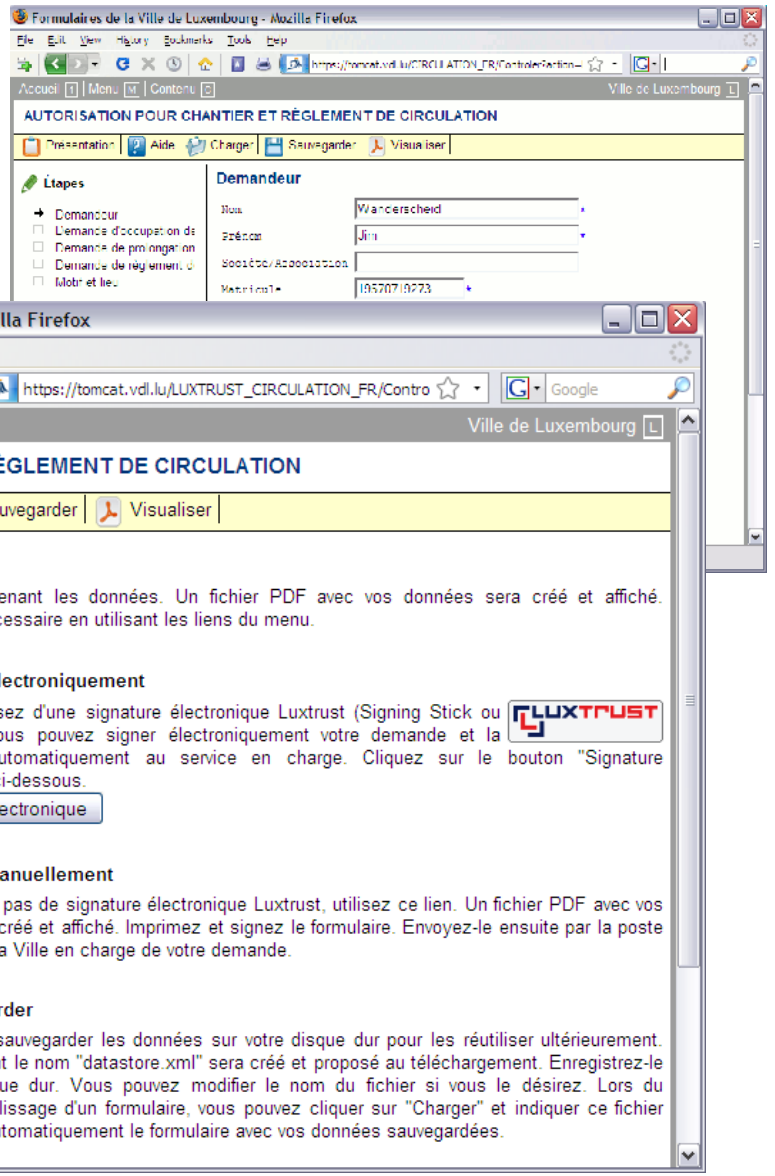
Contexte de la signature électronique

» Base légale
  – Directive 1999/93/CE du 13 décembre 1999 du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques
  – Loi relative au commerce électronique du 14 août 2000

» Infrastructure
  – LuxTrust s.a.
    • État luxembourgeois / SNCI : actionnaire majoritaire, 66 % du capital social
    • Autres : BCEE, Dexia, EPT, Fortis, Chambre de Commerce, HVB, Banque Raiffeisen, Bourse du Luxembourg, Société Nationale de Certification et d'Homologation, Société Nationale de Contrôle Technique, Chambre des Métiers, Nomura Bank
  – Fournit matériel et logiciel
    • Certificats d'authentification et de signature
    • Support : sticks, cartes, générateurs de jetons
    • Serveurs de vérification

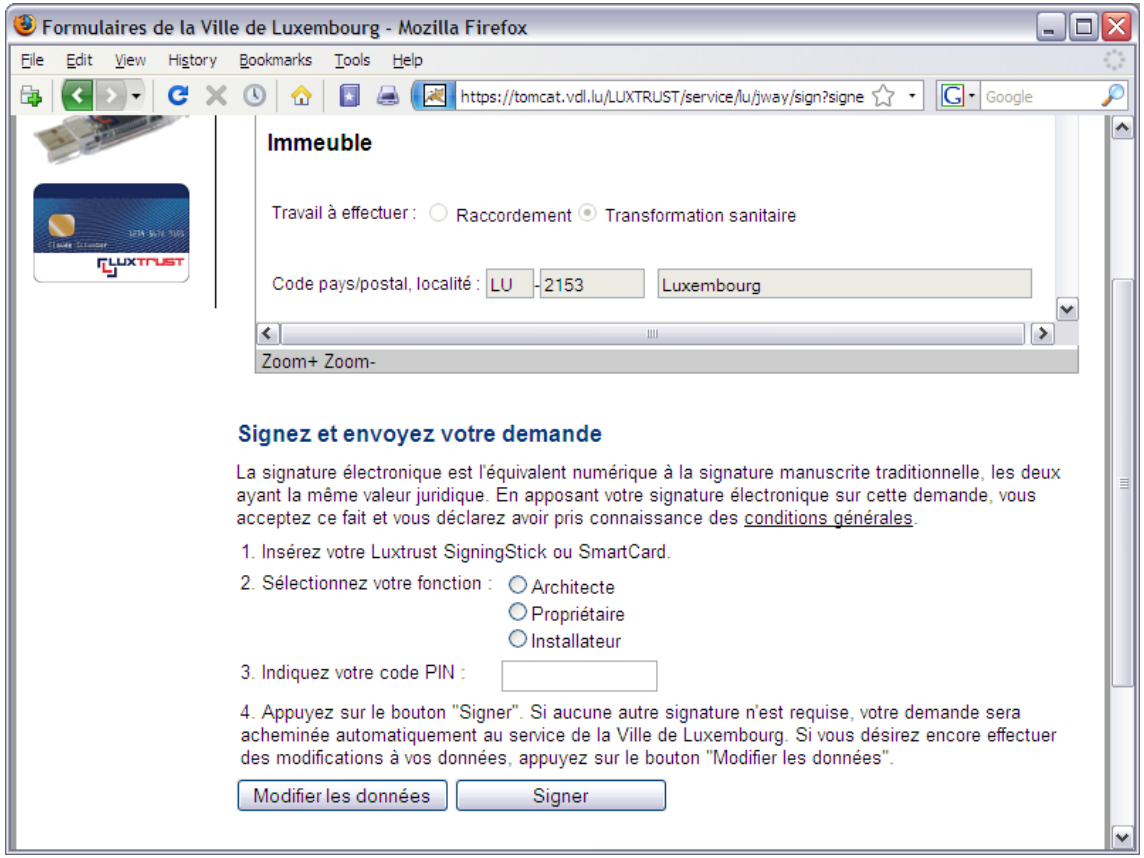
Option Signature à la fin du remplissage en ligne

- Option
  - Signature électronique Luxtrust
- Les autres options sont
  - Vérifier : création et affichage d'un PDF pour contrôler les données
  - Signer manuellement : création et affichage d'un PDF à imprimer, signer et envoyer par fax ou poste
  - Sauvegarder : enregistrement sur le disque dur local des données pour remplir d'autres formulaires



Vérification, conditions générales, fonction

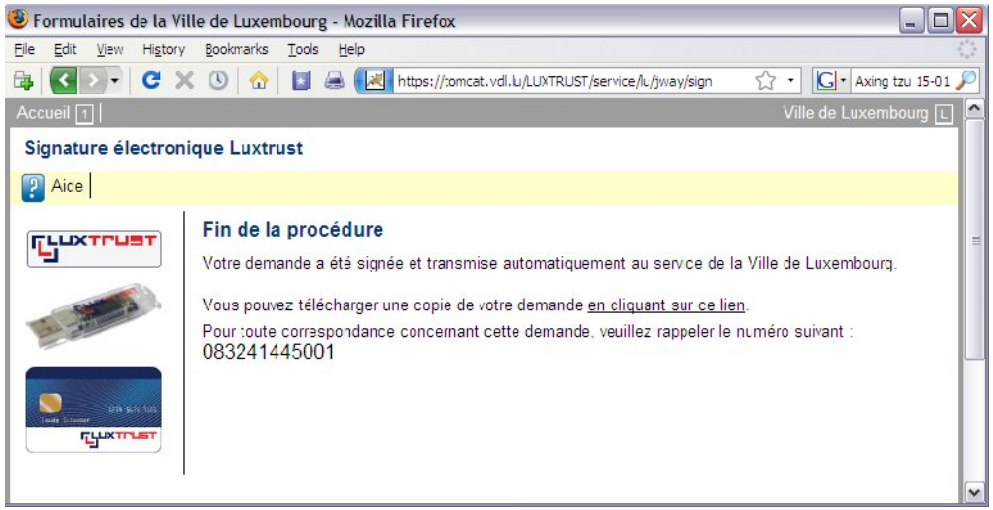
- Fichier à signer
  - Fichier au format Html des intitulés des questions et des réponses données
- Vérification
  - Affichage du fichier à signer dans un « Iframe »
- Conditions générales
  - Lien vers le texte des conditions
- Choix de la fonction
  - Un seul signataire
    = Une possibilité
  - Plusieurs signataires
    = Sélectionner sa fonction
- Contact avec Luxtrust
  - En arrière-fond
  - Vérification si certificat révoqué (perte, vol, etc...)



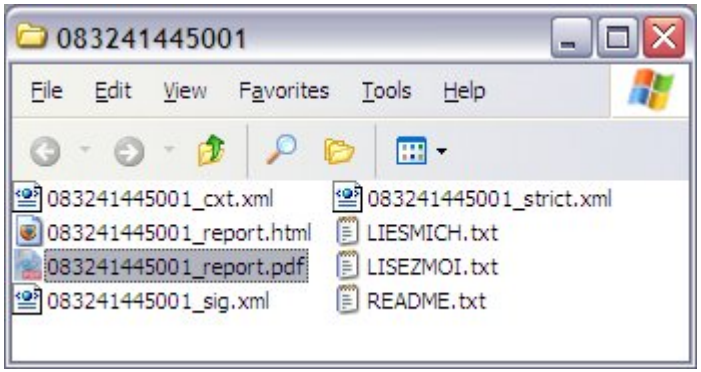
Insertion d'un certificat de signature

Fin de la procédure

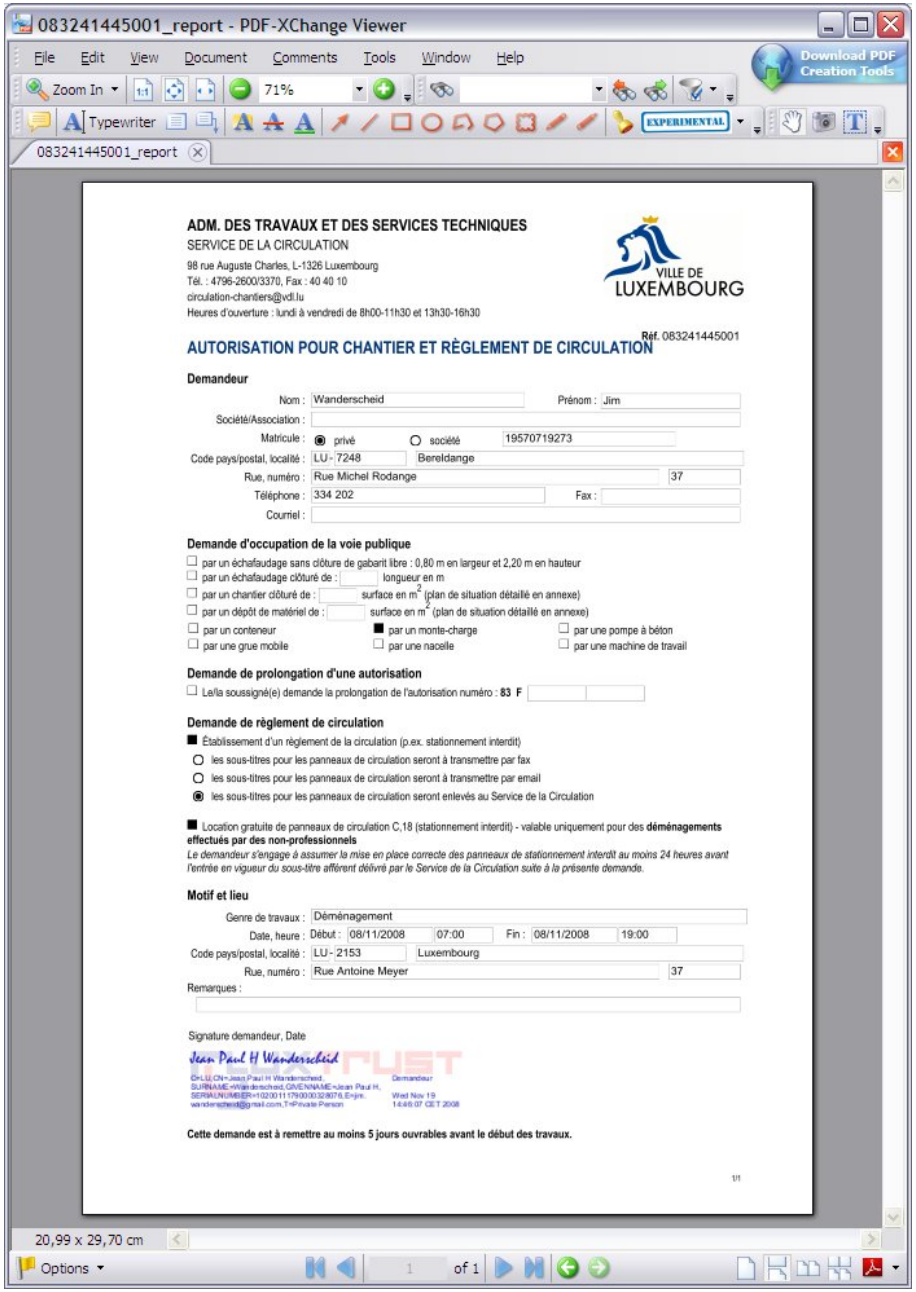
- Envoi automatique au service en charge de la demande
  - Serveur prépare le dossier
  - Achemine le dossier par email au service de la Ville
- Affectation d'un n° de dossier à rappeler dans les communications
- Affichage des annexes papier à fournir
  - Février 09



Dossier transmis



- 083241445001.zip
  - _report.pdf : représentation PDF du formulaire rempli et de la signature
  - _report.html : le fichier qui a été signé
  - _sig.xml : le fichier qui contient les informations concernant la signature
  - _cxt.xml : le contexte de la signature
  - _strict.xml : les données exploitables électroniquement
  - Fichiers « LisezMoi » en français, allemand et anglais : explication du contenu de l'archive et mises en garde

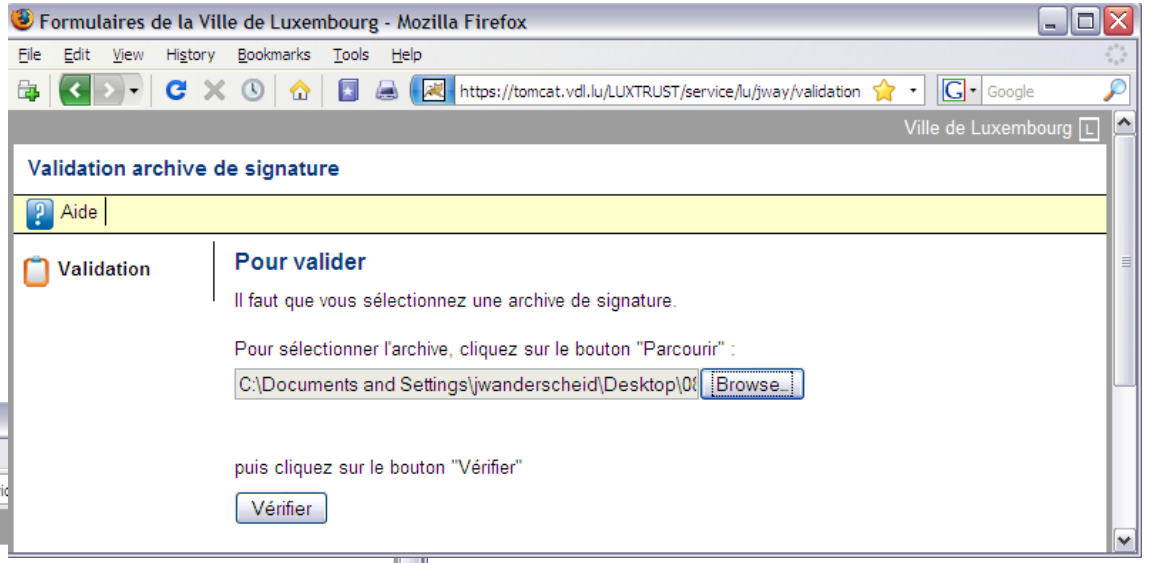


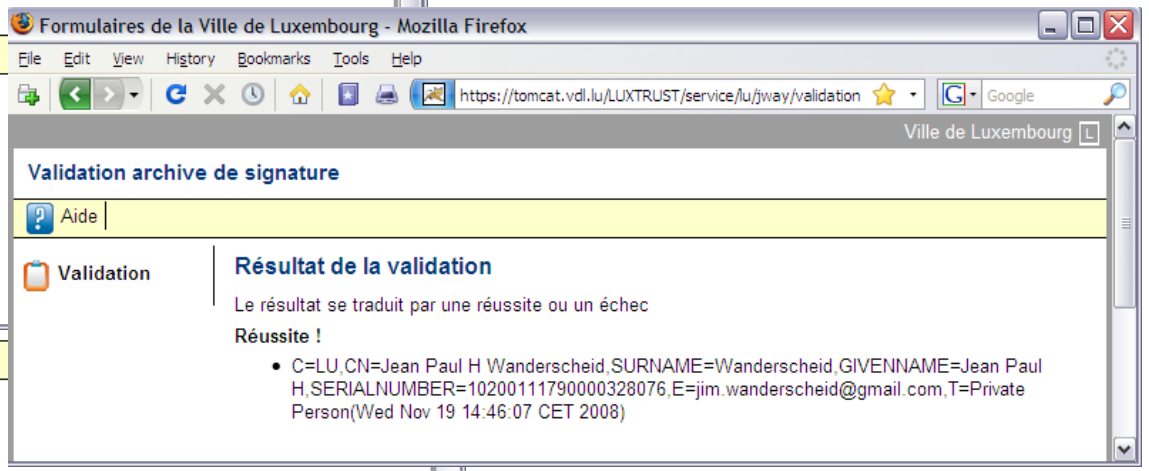
Procédure interne

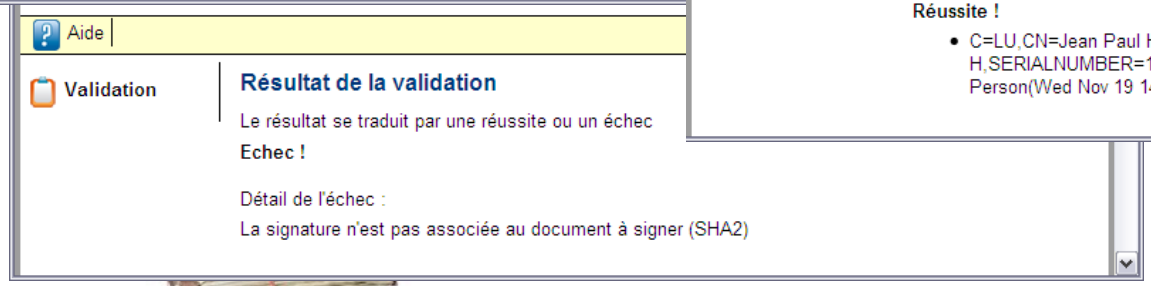
- Réunions d'information des services de la Ville
  - Présentation, démonstration live, réponses aux questions
- Travail effectué par le service en charge
  - Ouvre l'archive ZIP de l'email
  - Lit et/ou imprime le fichier PDF
  - À l'endroit prévu pour la signature doit se trouver le « tampon »
  - En cas de doute, validation avec l'outil de la Ville
- Archivage
  - Chaque service est responsable de sauvegarder l'archive ZIP pendant 10 ans
  - Le Service Informatique sauvegarde aussi les archives ZIP sur disques
  - Après 10 ans, la responsabilité est transmise au Service des Archives
    - Décide ou non de garder les archives ZIP

Validation d'une signature

- Télécharger l'archive ZIP sur le service de validation de la Ville
- Réussite
  - Affichage du signataire
- Échec
  - avec indication du problème







XML de signature

<SignatureMethodAlgorithm>SHA2.SignerID</SignatureMethodAlgorithm>

<ContentInfo>b63298cd297b700e550e8b2b13ae45eb6107bce3016a3528ddbabd6d8eafadf4.083251049001</ContentInfo>

<PKCS7content>MAAGCSqGSIb3DQEHAqCAMIIGawIBATEJMAcGBSsOAwIaMFwGCSqGSIb3DQEHAaBPBE03ZTgwZmE3MzI2YmVhM
TE5NGJlZDU1MTgyNzllMGEyOTE2OGY4OWYwOGVkYjY1YTg1ZDhjNGE1YjVkY2YwZTkxLjA4MzI1MTQwOTAwMaCCBQwwggUIMIID8K
ADAgECAgIVyjANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQGEwJMVTEVMBMGA1UEChMMTHV4VHJ1c3Qgcy5hMR8wHQYDVQQDE
xZMdXhUcnVzdCBOb3JtYWxpc2VkIENBMB4XDTA4MDIwMTEzMzUwN1oXDTExMDIwMTEzMzUwN1owgcAxCzAJBgNVBAYTAkxVMSEw
HwYDVQQDExhKZWFuIFBhdWwgSCBXYW5kZXJzY2hlaWQxFTATBgNVBAQTDFdhbmRlcnNjaGVpZDEUMBIGA1UEKhMLSmVhbiBQY
XVsIEgxHTAbBgNVBAUTFDEwMjAwMTExNzkwMDAwMzI4MDc2MSkwJwYJKoZIhvcNAQkBFhpqaW0ud2FuZGVyc2NoZWlkQGdtYWIsL
mNvbTEXMBUGA1UEDBMOUHJpdmF0ZSBQZXJzb24wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALI9CnWtfPHf9uQDQ2+Dywxj
2RxdDeICX4v45TJgIhrXDYzVodkPxK7rkjHxRvFX2ffMM9GA8LJTHcYhM7KO3aZQwBEpAjrssaStW2j2R/XhfCYxc9YmuNlDNkyEk1uzp6Hm
9ZDlkrTjjbRIs+EWqi98xeZefsWfm8+WmqpU5+TlAgMBAAGjggIIMIICBDAMBgNVHRMBAf8EAjAAMGAGCCsGAQUFBwEBBFQwUjAjBggr
BgEFBQcwAYYXaHR0cDovL29jc3AubHV4dHJ1c3QubHUwKwYIKwYBBQUHMAKGH2h0dHA6Ly9jYS5sdXh0cnVzdC5sdS9MVE5DQS5jcn
QwggEQBgNVHSAEggEHMIIBAzAIBgYEAI96AQIwgfYGCCuBKwEBAgEDMIHpMIG7BggrBgEFBQcCAjCBrhqBq0x1eFRydXN0IE5vcm1hb
GlzZWQgQ2VydGlmaWNhdGUgb24gU1NDRC4gVXNhZ2U6IEVsZWN0cm9uaWMgU2lnbmF0dXJlIChPSUQgMS4zLjE3MS4xLjEuMi4xLjM
pIEF1dGhlbnRpY2F0aW9uICBhbmQgRW5jcnlwdGlvbiAoT0lEMS4zLjE3MS4xLjEuMi4xLjQpLiBLZXkgR2VuZXJhdGlvbiBieSBDU1AuIDApB
ggrBgEFBQcCARYdaHR0cDovL3JlcG9zaXRvcnkubHV4dHJ1c3QubHUwCwYDVR0PBAQDAgSwMB8GA1UdIwQYMBaAFM7+Rp1jL4n98j
gWJdjxbN5H+M7BMDEGA1UdHwQqMCgwJqAkoCKGIGh0dHA6Ly9jcmwubHV4dHJ1c3QubHUvTFROQ0EuY3JsMB0GA1UdDgQWBBR6
Amc26oxhOs1sg+j0XDR5ZV8b1jANBgkqhkiG9w0BAQUFAAOCAQEAHvzy0N1UI4rDtw6dnR6tqXNT0tKJ4JMxIWf72yWTgUD+RXAQEkN
WUsYNDefdp78UVvIYO0aLAOrTi4vbhesciKAA==</PKCS7content>

<X509PublicKey>30819f300d06092a864886f70d010101050003818d0030818902818100b23d0a75ad7cf1dff6e403436f83cb0c63d91c5d0de
2025f8bf8e53260221ad70d8cd5a1d90fc4aeeb9231f146f157d9f7cc33d180f0b2531dc62133b28edda650c01129023aecb1a4ad5b68f647f5e1
7c263173d626b8d943364c84935bb3a7a1e6f590e592b4e38db448b3e116aa2f7cc5e65e7ec59f9bcf969aaa54e7e4e50203010001</X509Pu
blicKey>

<OCSPanswer>308205480a0100a08205413082053d06092b06010505073001010482052e3082052a3081a9a216041435b22b1426abb6636
3c8b93652be1bb6d438c3be180f323030383131323030393434355a30653063303b300906052b0e03021a0500041403b4fcffd21c3177b72
91fbb5277900e90c9d72b0414cefe469d632f89fdf2381625d8f16cde47f8cec1020215ca8000180f323030383131323030393030323 75aa0111
80f323030383131323331333333032375aa1173015301306092b06010505073001020406011db94e22fc300d06092a864886f70d0101050500
038181007b9d79109e9d1e1cf5255d2cbf50578aabf964c84a4a8c27d3f86a4714538ac321ac65e97925dfa84e38d79ef3e0ded72a15f809333f
be936c74e6f167597db0ae1f94f3eef0667027a7379a5c47d403a561591d32c8ca80eb7e49bb9d8c3fb237b57e870a5f4baffea350996a730990
c95abe3ed21607b7cf33e03526b4c2c1a08203e7308203e3308203df308202c7a00302010202022e1b</OCSPanswer>

Validation

» Contrôle en cas de contestation
  – Hashcode
    • Hacher le fichier HTML avec l'algorithme SHA/2
    • Obtention de ContentInfo : b63298cd297b700e550e8b2b13ae45eb6107bce3...
    • Si pareil que le hashcode dans le XML = Personne n'a modifié le fichier HTML
  – Décryptage
    • Décrypter le contenu de PKCS7 avec la clé publique X509PublicKey
    • Obtention de ContentInfo : b63298cd297b700e550e8b2b13ae45eb6107bce3..
    • Si pareil que le hashcode dans le XML = Ce certificat a crypté le hashcode.
  – Donc, si on obtient la même valeur
    • Le fichier HTML n'a pas été modifié
    • Il a été signé avec la carte qui contenait le certificat
  – Vérification de la réponse OCSP
    • Effectué par Luxtrust

Comparaison Ville de Luxembourg – Signature manuelle

	VdL / Luxtrust	Signature manuelle
Vérification de l'identité du signataire	✔	✘
Signatures multiples	✔	✔
Réutilisation de données sauvegardées	✔	✘
Document signé verrouillé	✘ hashcode modifié	✘
Copie non modifiée disponible	✔ serveur VdL	✘
Données exploitables automatiquement	✔ lecture du XML	✘
Annexes intégrées	✘ courrier postal (fév 09)	✔
Archivage	Archives ZIP	Papier

Comparaison Ville de Luxembourg – Gouvernement

	VdL / Luxtrust	De Guichet / Luxtrust
Technologie de signature	Applette Java	Adobe Acrobat
Logiciels nécessaires	Navigateur	Navigateur + Acrobat 9
Configuration standard Navigateur	✔	✘installation plugin Acrobat
Configuration standard Acrobat	-	✘installation certificat Luxtrust
Technologies du Navigateur	Cookie + Javascript + Java	Cookie + Javascript
Format interne des données	XML	XML
Document signé	HTML généré à partir du XML	PDF généré à partir du XML
Signatures multiples simultanées	✔	✔
Signatures multiples dissociées	✔	✘
Acheminement automatique au service	✔ Smtp	✔ Soap
Accès authentifié	✘via De Guichet	✔
Sauvegarde des données	✔ ordinateur	✔ serveur
Annexes intégrées	✘	✘
Document signé verrouillé	✘	✘
Validation signature	✔ application Java	✘
Copie non modifiée disponible	✔ serveur VdL	✔ serveur CIE
Données exploitables automatiquement	✔ lecture XML	✔ lecture XML

Merci pour votre attention

Jim WANDERSCHEID

Chef de projet
Technologies Internet et Systèmes Mobiles
Ville de Luxembourg / e-City

Téléphone : +352 47 96 33 36
Mobile : +352 691 98 33 36
Courriel : jwanderscheid@vdl.lu

FIN