Les applications pratiques de la signature électronique

Olivier Delos, Sylvie Lacroix
Partners SEALED

Message de l'exposé

- "Signer ou ne pas signer (électroniquement) ?"
  - Plus aucune barrière technique ou juridique …
  - mais cas d'implémentation inadéquats dus à des approches différentes et manque de rigueur dans l'implémentation technico-business
    - e-Invoicing
    - e-Contracting
- Nombre d'applications en croissance grâce à l'eID … mais combien d'implémentations « correctes » du processus complet de signature électronique?
- Besoin criant de lignes de conduites claires pour une implémentation correcte de la signature électronique et de référence en la matière
  - Standards existants, QuEST,

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

“Signer ou ne pas signer ?”

- Aujourd’hui: plus de barrières juridiques à la dématérialisation
- En particulier pour l’utilisation de la Signature Électronique (S.E.)
- Mais il reste quelques cas “étranges”, dus
  - à des approches juridique et technique différentes
  - à un manque d’information / de connaissance quant à l’implémentation “correcte” de la S.E.

  Illustration sur deux cas:
  - e-Invoicing
  - e-Contracting

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Quelle signature pour quel outil ?

"Signer ou ne pas signer ?"

- S.E. Avancée
- Certificat Qualifié
- SSCD

Aussi longtemps qu'elle est liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable

Signature Qualifiée
≡ Signature manuscrite

- S.E. Avancée
- Certificat d'Authentification
- (SSCD)

Citizen CA décline toute responsabilité !?

S.E. Avancée
≡ Signature à laquelle on ne peut nier un effet juridique

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

e-Invoicing

"Signer ou ne pas signer ?"

- Directive 2001/115/EC
- Emetteur peut envoyer une facture électronique si le destinataire accepte et si solution garantit:
  - Authentification de l'origine de l'e-facture
  - Intégrité de celle-ci
- Signature Electronique basée sur une S.E.A. ou une S.E.Q. remplit ces conditions …
- Signer ou ne pas signer ?
- Une signature « légale » sur une facture a aussi stricto senso une autre signification à savoir **la reconnaissance du paiement !!!**

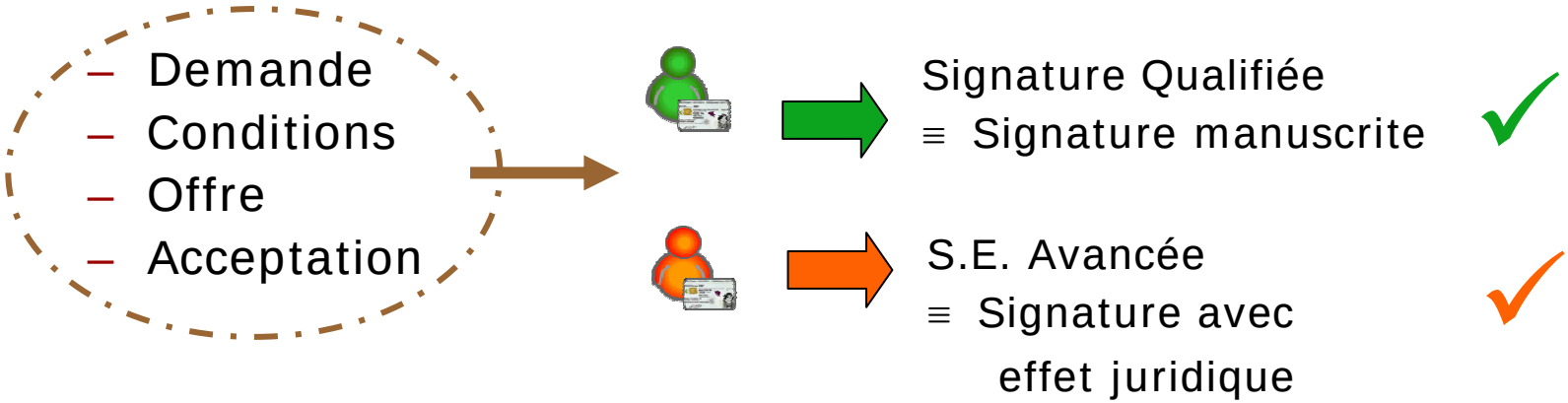
Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

e-Contracting

"Signer ou ne pas signer ?"

e-Contracting



Peut importe que le certificat supportant la signature soit destiné à l' "authentification" ou à la "signature", l'effet juridique de la signature électronique réalisée ne peut être nié par l'une ou par l'autre partie

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Approche Technique

Technologie PKI ou cryptographie à clé publique:

Aucune différence entre la formule de

	Acte	**Vérification**
– "Signature digitale"	Clé privée	Clé publique
– Authentification	Clé privée	Clé publique
– Chiffrement	Clé publique	Clé privée

S'il s'agit de la même formule mathématique

alors comment fait-on techniquement la différence ?

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Approche Technique

"Signer ou ne pas signer ?"

	Acte	Vérification
– "Signature digitale"	Clé privée	Clé publique
– Authentification	Clé privée	Clé publique

L'utilisation de la clé privée sur un message ou des données électroniques permet à la partie vérifiante de s'assurer de:

- L'authentification de l'origine des données
- L'intégrité de ces données
- Le caractère non-réfutable de l'opération

si

- La clé publique correspondante est certifiée par un tiers de confiance comme appartenant à une entité déterminée
- Le certificat est toujours valide

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Approche Technique

"Signer ou ne pas signer ?"

	Acte	Vérification
– "Signature digitale"	Clé privée	Clé publique
– Authentification	Clé privée	Clé publique

La différence peut être aussi infime qu'un simple "bit" dans le certificat digital certifiant la clé publique de "signature" ou d' "authentification" dans le champs "Key Usage":

- Digital Signature "bit" renvoie à l' "authentification"
- Non Repudiation "bit" renvoie à la "signature"

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Signature vs Authentification

"Signer ou ne pas signer ?"

Dans le champs "Key Usage":

- **Digital Signature "bit"** signifie que « la clé publique est utilisée dans un mécanisme de signature digitale pour supporter des services de sécurité autre que la non-répudiation, la signature de certificat ou de CRLs, et est souvent utilisé pour
  - L'authentification d'une entité (détenteur de la clé privée)
  - L'authentification de l'origine de données avec intégrité »
- **Non Repudiation "bit"** signifie que « la clé publique est utilisée dans un mécanisme de vérification de signature digitale protégeant de la négation par le signataire de l'acte de signature »

Problèmes:

- Définitions peu claires, confusion totale même pour initiés
- Le mot signature ne devrait pas être utilisé dans ce contexte technique (UNICITRAL)
- Pure vocation d'automatisation sans plus

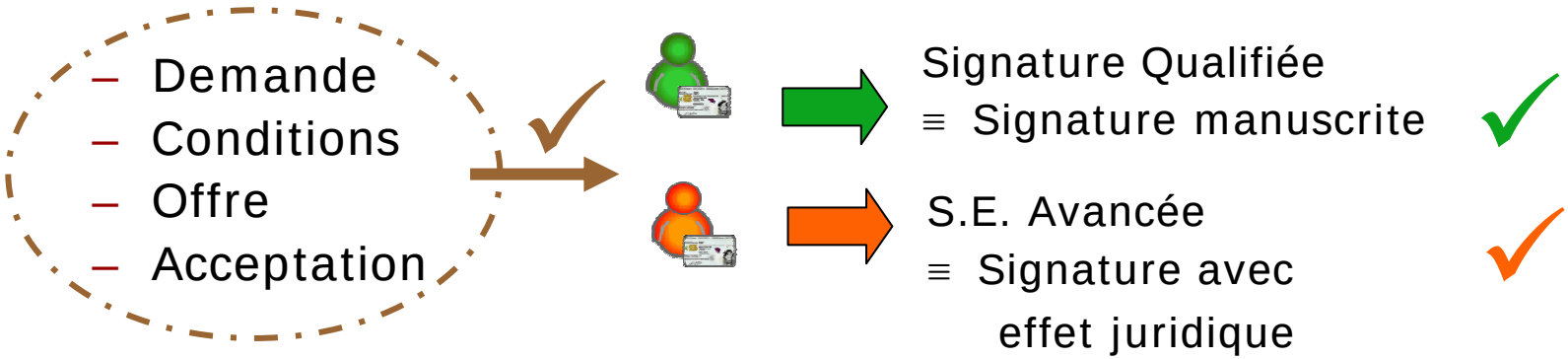
Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Approche juridique

"Signer ou ne pas signer ?"

- A « l'opposé » de l'approche technique
- Le contexte prime sur l'outil
- Du point de vue du juriste, l'utilisation du bit dS ou nR est seulement un élément additionnel, non déterminant quelle que soit sa qualité
- Le plus important pour décider s'il y a eu relation contractuelle entre les parties réside dans le contexte dans lequel ils ont évolué



Sylvie Lacroix
sylvie.lacroix@sealed.be
Olivier Delos
olivier.delos@sealed.be

Approche juridique

"Signer ou ne pas signer ?"

- L'utilisation d'un simple "bit" ne suffit pas pour assurer la non-répudiation
- La vérification d'une signature digitale sur la seule base du certificat supportant celle-ci ne permet pas d'établir que le signataire a consenti au contenu d'un contrat
- Cette vérification prouve que la clé privée correspondant à la clé publique certifiée a été utilisée pour signer ces données (authentification de l'origine avec intégrité, et non-répudiation de signature si certificat de confiance et valide)
- Processus technique de vérification de la signature:
  - Est un processus post-signature
  - Ne correspond pas au mécanisme de "trusted witnessing" existant dans le monde papier
- Le prestataire de services de certification (émettant les certificats) n'intervient en rien dans le processus de signature

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Approche juridique

Possibilité de limitations de l'utilisation d'un certificat permises par la Directive 1999/93/EC, et exonération de la responsabilité du PSC sur les **certificats qualifiés:**

- Limitation quant à la valeur maximum d'une transaction
- Limites fixées à son utilisation à condition que ces limites soient discernables par les tiers
  - Key Usage bit (ds, nR) ne peut suffire
  - Champs standards pour certificat qualifiés seulement, mais
    - taille très réduite et
    - problème d'interprétation/lisibilité par les applications courantes
  - Autres champs ont aussi une taille limitée
  - Par référence vers CP, CPS ou GTC mais souvent ardu et incompréhensible pour les tiers, et difficile à en prouver l'acceptation
  - Message doit être discernable par les tiers (usage permis **et** non)

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Réconcilier juridique et technique

"Signer ou ne pas signer ?"

- **Profil de Certificat**: Essentiel que l'utilisation autorisée et ses interdits soient indiqués clairement et de façon discernable par les tiers au sein même du contenu du certificat par le PSC.

  Le certificat n'est pas le seul outil pour cela dans le contexte de la S.E.

- **Processus et format de signature** doivent être privilégiés pour fournir cette information et faire partie intégrante du format de la signature:
  - Utilisation d'attributs signés indiquant le contexte de la signature
    - **Commitment Type**: indication de la portée de la signature (par le signataire)
    - Référence vers une **Politique de** (Validation de) **Signature**
  - Politique de (Validation de) Signature
    - Indication des règles relatives à la création et la validation de signature digitale y faisant référence, y compris la portée et l'engagement pris par signature

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Réconcilier juridique et technique

- Encore faut-il avoir des **Applications** « à la hauteur »:
  - Interprétation et visualisation correcte du profil/contenu du Certificat
  - Processus et format de signature
    - Conforme à l'état de l'art (legal, policy, design, technologie) et aux besoins « business »
    - Compréhensible et gérable par le signataire et le vérificateur
    - De confiance

La grande majorité des applications actuelles ne remplissent pas tous ces critères …

Le concept de pérennité est souvent sous-estimé et peu intégré (archivage, vérification à postériori, timestamping…)

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Réconcilier juridique et technique

"Signer ou ne pas signer ?"

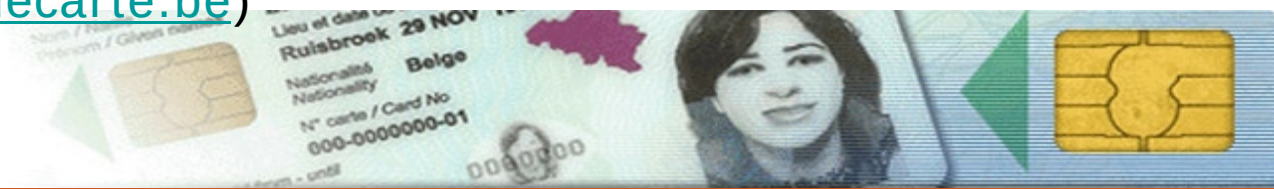
- Améliorations au point de vue de la législation:
  - La Directive risque de très peu changer ...
  - Au point de vue national (État Membre), quelques pistes de réflexion:
    - Clarification de la notion et du processus d'authentification
    - Clarification et explicitation des obligations des parties tierces vérifiantes
  - Clarification des dispositions relatives aux prestations de services connexes (e.g. timestamping, archivage sécurisé, ...)

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Applications en forte croissance

- Plus grande maturité dans le monde business
  - quant aux technologies sous-jacentes (qui elles sont matures depuis bien longtemps)
  - quant au processus inévitable de dématérialisation
    - ROI direct ou indirect
    - Démarque par rapport à la concurrence
  - Quant à la perception de l'absence de barrières juridiques
- La carte eID comme booster incontestable
  - 2.5 à 3 millions de cartes déjà en service
  - Offre en lecteurs de plus en plus accessible (www.lecteursdecarte.be)



Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Applications eID existantes

- e-Gouvernement
  - Déclaration d'impôts (taxonweb)
  - Mondossier.be (RRN)
  - Immatriculations de véhicules
  - etc.
- eRecruitment
  - Selor
- eJustice
  - Sousmission électronique de conclusions
- eMunicipality
  - Data Capture
  - e-Guichet: Certificats de mariage, de naissance, etc.
  - Accès physique aux parcs à conteneurs, bibliothèques, piscine, etc.
  - Collège en ligne
- e-Commerce
  - Ouverture en ligne de services
  - Digital Rights Management
  - Contract signing
  - Authentification de clients sur des sites/services web
- eBanking
  - Online mortgage request
  - Ouverture en ligne de compte en banque (keytrade)
  - Data capture
- eOffice
  - Signed e-mails
  - Registered mail (X)
  - Signed documents (Adobe pdf, MS Office)
- Accès en ligne
  - ONEM Consultation de dossiers
  - Accès web restreint
- Guichet Unique
  - Acerta
- Systèmes de pointage
  - Acerta
- Hotels Check-in
  - Planet-Winner
- Accès physique
  - Locaux
  - Parcs à container

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Blocs de base supportant la signature

Liste non exhaustive (à titre d'exemple):

- Grand public:
  - Microsoft Office, Infopath …
  - Adobe PDF
  - Internet Explorer, Mozzilla, …
- Spécifiques
  - D-Soft , Avain Technologies, Ar, Aladdin, etc.
  - Isabel
  - Open Limit
  - SDKs: IAIK, Utimaco, Cryptolog, RSA, OpenSSL, etc.
- Sur mesure

Sur base de ces blocs, comment construire correctement une application avec flux complexe (ex: e-bidding)?

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Guidelines et standard d'implémentation

- Initiatives existantes « d'aides » aux organisations désirant développer des applications de signature électronique:
  - Standards existants
    - ETSI TS 101 733 (CAdES), ETSI TS 101 903 (XAdES) et associés
    - CEN Workshop Agreements (CWA) 14170-14171 contenant des guidelines pour le développement d'application de création et de vérification de signature électronique
    - …
  - Initiative QuEST (Qualified Electronic Signature Tutorial) de Microsoft et experts indépendants
  - Consultance spécialisée
- Nouvelle initiative autour de l'utilisation de la carte eID:
  - Digital Identity Standard Institute

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

- Initiative visant
  - à uniformiser l'aide aux organisations désirant développer des applications autour de la carte eID
    - signature électronique,
    - authentification forte des détenteurs de cartes et
    - saisie de données d'identité
  - à augmenter le niveau de confiance des utilisateurs envers les applications des fournisseurs de services business et e-gouvernementaux
- Organisme d'accréditation d'applications vis-à-vis d'un standard d'implémentation de la carte eID (E.S., Auth°, saisie de données)

Sylvie Lacroix
sylvie.lacroix@sealed.be
Olivier Delos
olivier.delos@sealed.be

Digital Identity Standards - eID

Applications ou Services basés sur l'implémentation de la carte eID devraient satisfaire des

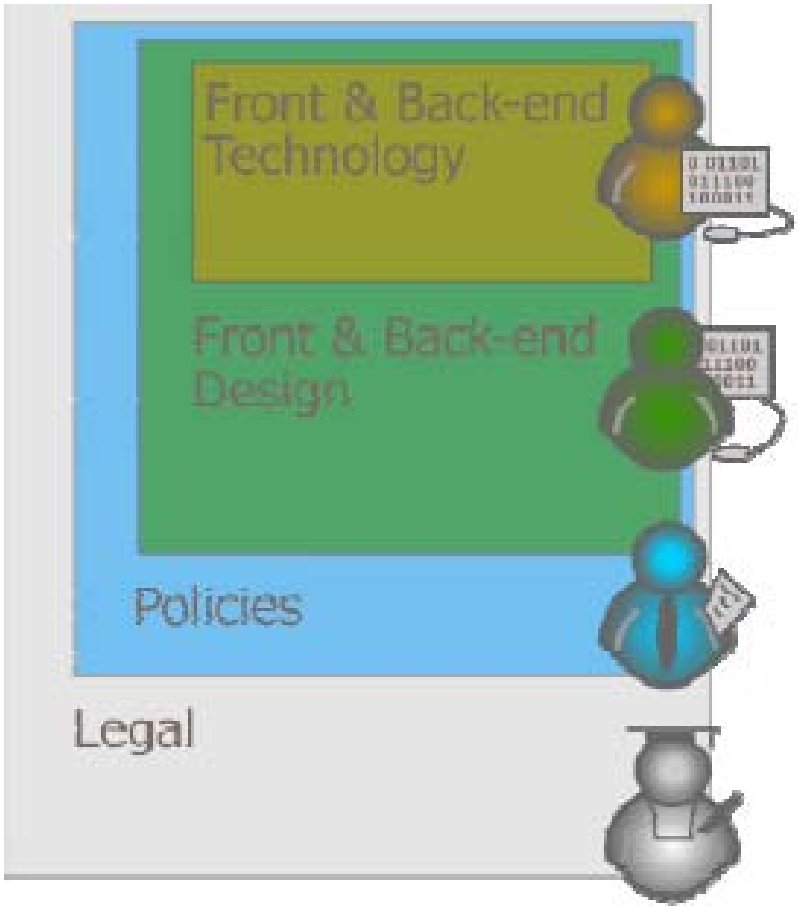
- **Exigences statiques (As-Is)** en termes de:
  1. Aspects légaux
  2. Policies
  3. Design
  4. Technologie
- **Exigences dynamiques (durables)** en termes de:
  1. Environnement sains en matière de politiques et juridique
  2. Processus sains en termes de développement, d'opérations, et de gestion de la sécurité

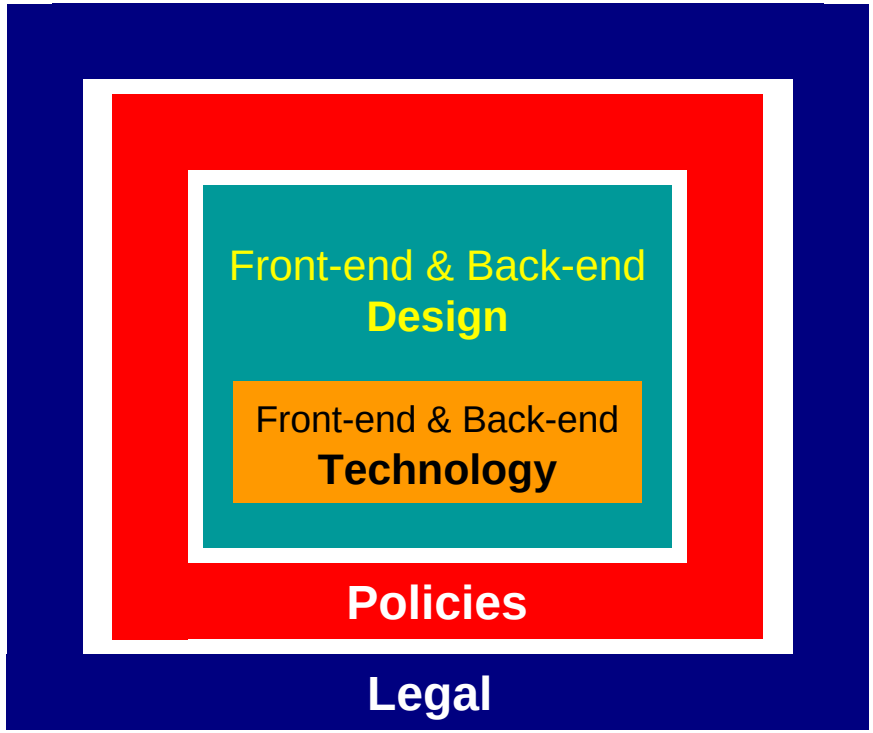
que le focus de l'application soit la S.E., l'authentification, la saisie des données d'identité ou une combinaison

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Aperçu des exigences statiques

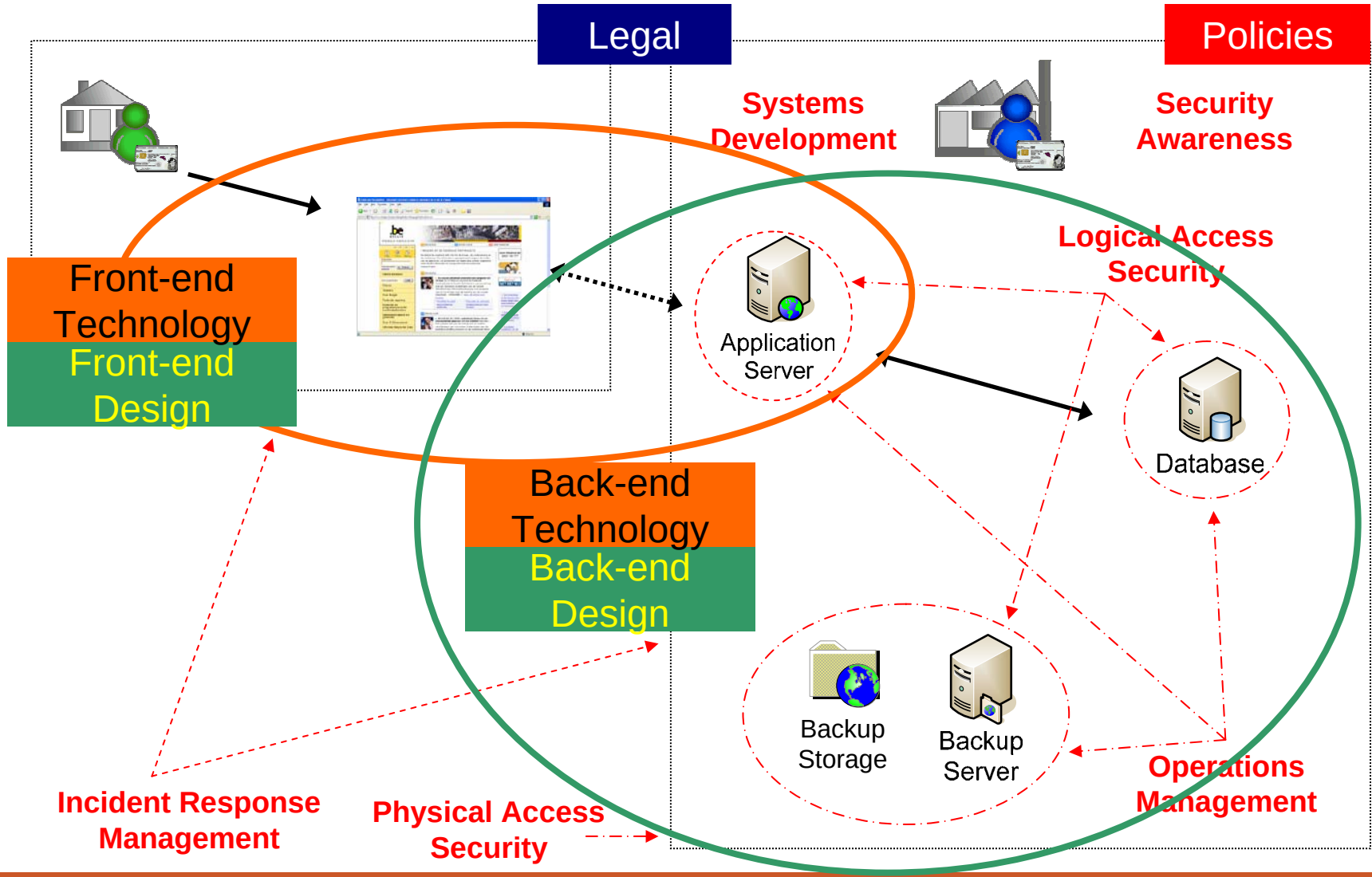




Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Exigence statiques – Aperçu détaillé



Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Contenu du standard DIS eID

Legal

- Vie privée
- Utilisation du numéro de registre national
- Communication avec les utilisateurs, signature électronique et conclusion de contrat
- Fair trade practices et protection du consommateur
- Cyber-criminalité
- Continuité et responsabilité

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Contenu du standard DIS eID

Policies

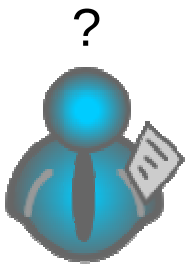
- Assurer une conformité durable avec les exigences juridiques, technologiques et en matière de design liées à la carte eID
- Assurer la conformité avec les politiques obligatoires de gestion des systèmes eID en particulier avec :
  - Développement de systèmes
  - Sensibilisation à la sécurité
  - Gestion des opérations
  - Sécurité des accès logiques
  - Sécurité des accès physiques
  - Gestion des incidents

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Contenu du standard DIS eID: signature

Design



Facile d'implémenter une signature électronique ?

Quelle Signature Electronique ?

- E-mail footer
- Signature Electron. Avancée
- Signature Electron. Qualifiée
- Autre ?

- Signatures multiples
- Co-signatures
- En série / en parallèle
- etc.

Dans quel contexte Business, Juridique et/ou Policy ?

- e-Mail
- e-Contracting
- e-Invoicing
- e-Tendering
- e-Government
- etc.

Avec quelle portée ou engagement ?

- Authentification de l'origine des données avec integrité
- Approbation ou accord
- Auteur ou possession
- ...

Que vérifier et comment ?

Avec quelle preuve et pour quelle durée ?

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Contenu du standard DIS eID

Design

Design (Front-end & Back-end)

- Méthode de développement sécurisé & sécurité des applications
- Signatures électroniques
  - Création de Signature (Front-end)
    - Qualified ES versus Advanced ES
    - Viewer sécurisé (WYSIWYS)
    - Attributs signés
    - Recommandations & Information envers les signataires
  - Signature (Validation) Policy (Front & Back-end)
  - Vérification de Signature (Back-end)
  - Preuves à long terme
- Authentification (Forte) (Front & Back-end)
  - Incluant les processus d'authentification et de vérification
- Saisie des données d'identité (Front & Back-end)

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Contenu du standard DIS eID

Technology

- Secure Development Methods
- Front-end technology
  - Configuration
  - Card versions
  - Card conditions
  - Card personalisations
  - Card behaviour
  - Card access (now : crypto)
- Back-end technology
  - Network (access) security
  - Data transmission
  - Data storage (Front & Back)
  - State-of-the-art security measures
  - Audit trail (i.e. Logging)

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Conclusions

- Réconcilier les approches techniques et juridiques
  - Contenu discernable du certificat quant aux limitations / usages
  - Contenu discernable des contextes de signatures au sein de celles-ci
- Pistes d'améliorations juridiques (e.g.):
  - Obligations des parties vérifiantes
  - Aspects d'authentification (vs signature)
  - Niveau non-qualifié mais assimilable (ETSI Niveau Normalisé)
- Sensibilisation autour d'initiatives visant à l'augmentation de la confiance en ces applications
  - Standards existants, QuEST,

Sylvie Lacroix
sylvie.lacroix@sealed.be
Olivier Delos
olivier.delos@sealed.be

Conclusions

Observations en faveur de l'e-signature:

- Nombre d'applications en croissance grâce à l'eID (au niveau Belge et Européen) mais éducation nécessaire sur l'avant, pendant et après signature
- Intérêt tant des constructeurs que des utilisateurs dès qu'ils sont « rassurés » quant à:
  - Conformité légale
  - Facilité d'utilisation
  - Coûts (ROI)
  - Niveau de confiance (e.g., accréditation DIS-Institute)
- Interopérabilité supportée par l'Europe

Sylvie Lacroix
sylvie.lacroix@sealed.be

Olivier Delos
olivier.delos@sealed.be

Questions ?

Information de contact:

www.sealed.be

- *Sylvie Lacroix*
  sylvie.lacroix@sealed.be
- *Olivier Delos*
  olivier.delos@sealed.be