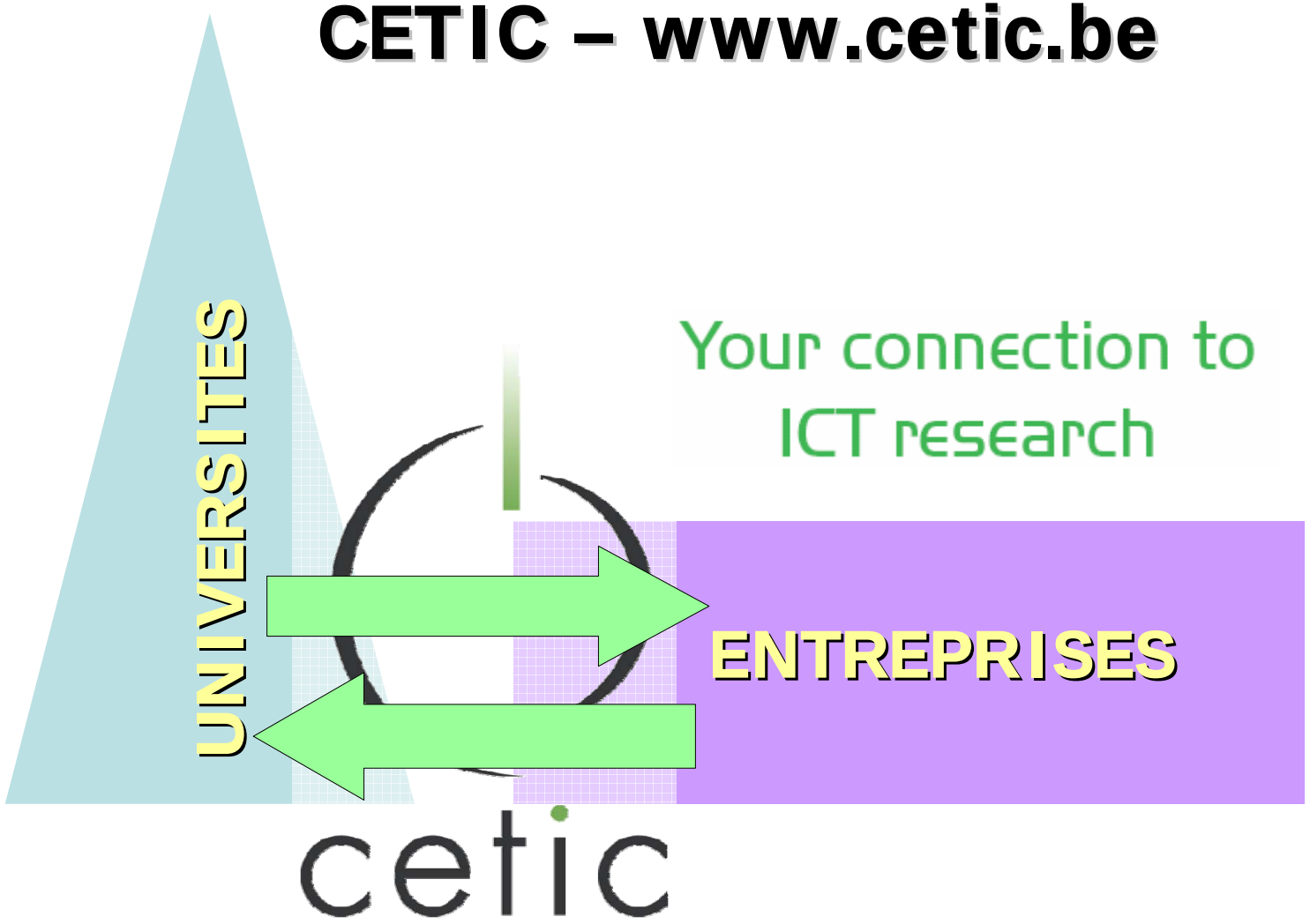
La carte d'identité électronique (eID)
Principes et Applications

UMH -19 Mars 2007

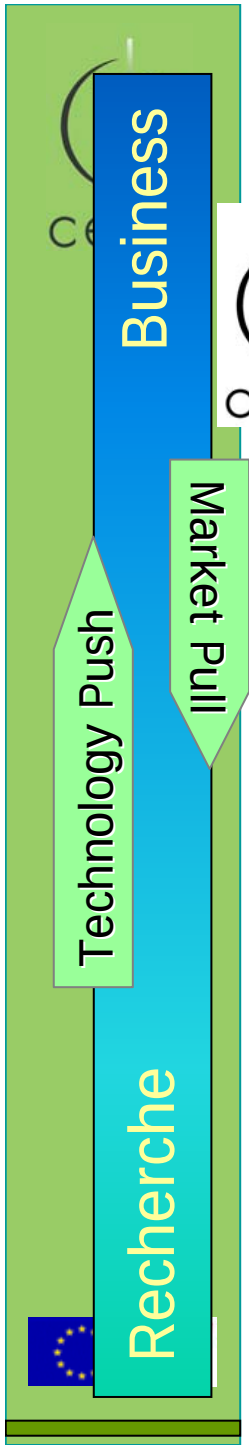
Christophe Ponsard – CETIC

cp@cetic.be

CETIC – www.cetic.be



- Situé dans le Hainaut, sur l'aéropôle de Charleroi
- +/- 25 personnes



cetic

Org. de Recherche

Entreprises (PME)

Entreprises Spin-Off

Grid, Cluster

Temps réel, Logiciel embarqué

Open Source Software Models

Génie Logiciel

Systèmes Distribués

Systèmes Electroniques

Technologies – Méthodologies – Expertise - Equipement

Req. Eng. | Open Source | FPGA | Distributed Syst. | Grid Techn.

Quality | IT Reverse Eng. | SystemC | Mobile Syst.

UCL Université catholique de Louvain

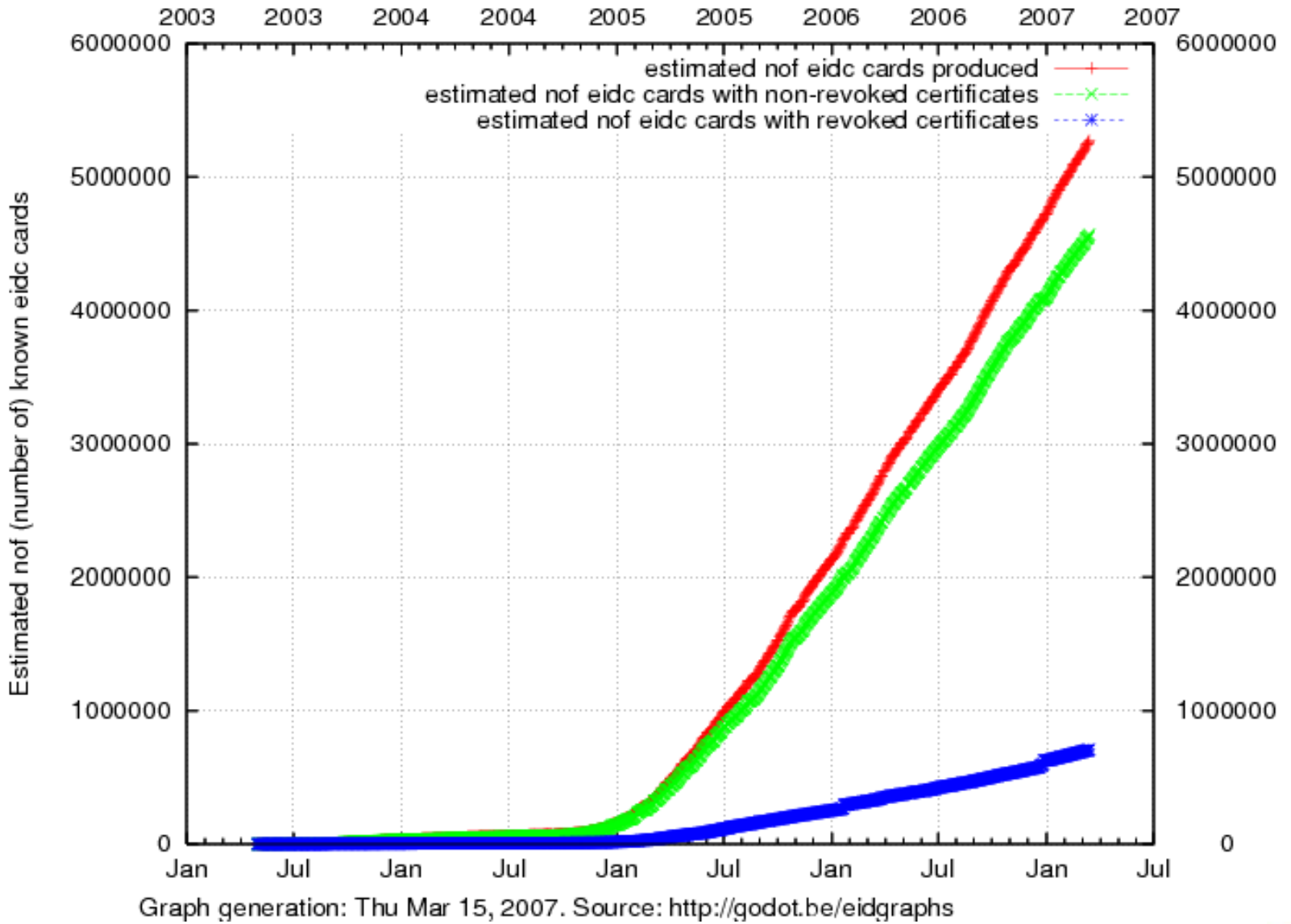
POLY TECH. MONS

Recherche au CETIC - axes

- Génie Logiciel
  - Ingénierie des exigences
    - Sécurité – Modélisation de Systèmes Critiques
    - http://faust.cetic.be
  - Qualité des produits et processus logiciels
    - Métriques, Méthodes éval. Légères
- Systèmes Distribués
  - Technologies Grid, Cluster
  - Web data mining
- Systèmes Electroniques
  - Technologies sans-fil
  - Co-design – FPGA
  - Application E-Health, logistiques

Un petit sondage pour commencer

eID - Qui en a une ?



eID – qu'est-ce qui a changé ?

- Plus petite: format carte de crédit
- Nouveaux éléments visuels: hologrammes...
- Il y a une puce
- Une information a disparut !
- Il y a plein de chiffre derrière
- La durée de validité a changé
- Numéro de registre national
- ...

Qui l'a déjà utilisé ? Pour quel usage ?

- Saisie de données ?
- S'authentifier sur un site web ?
- Application d'une signature numérique ?

- **Où sont les applications ?**

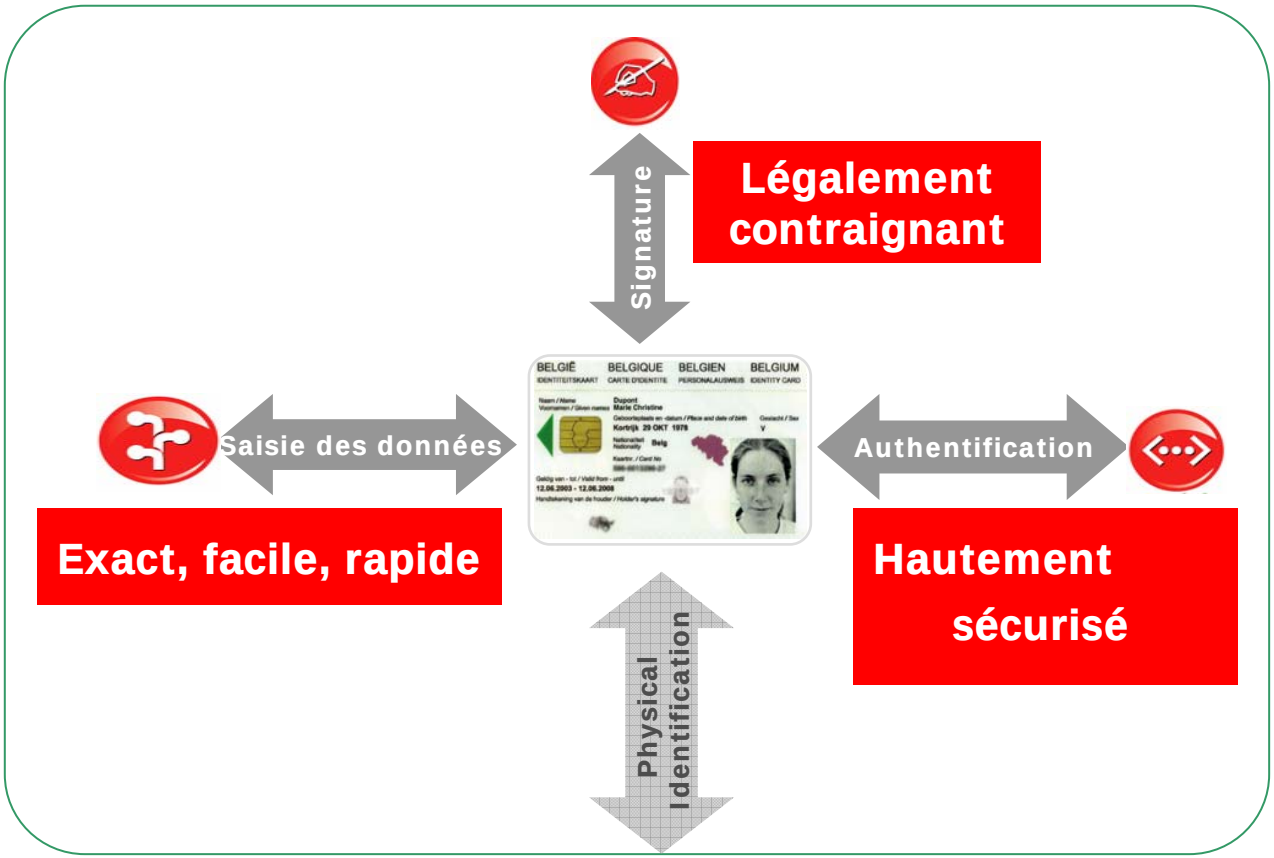
Plan du séminaire

- Présentation générale
  - Fonctions de l'eID
  - Sécurité physique
  - Sécurité électronique
  - Lecteur
  - Types d'eID
  - Processus de distribution de la carte
- Authentification et signature électronique
  - Rappels de crypto
  - Identité vs authentification
  - Signature électronique
  - Mise en oeuvre des certificats: structure, émission, révocation
- Utilisation de l'eID
  - Aperçu des grands types d'applications
  - Quelques exemples: registre national, signature email, guichet électronique
- Bref aperçu de la réalisation d'application eID
  - Outils
  - Mise en oeuvre: un chat citoyen sécurisé
- Conclusions et perspectives
- Quelques références

Présentation de l'eID

crédits à Danny De Cock de la KU Leuven, Zetes
pour une partie du matériel de cette section

Les 4 fonctions de base de la CIE



- Quelle est fonction de sécurité la carte ne supporte-t-elle pas intrinsèquement ?

Information visible

Front:

- Name
- First two names
- First letter of 3rd name
- Title
- Nationality
- Birth place and date
- Gender
- Card number
- Photo of the holder
- Begin and end validity dates of the card
- Hand written signature of the holder

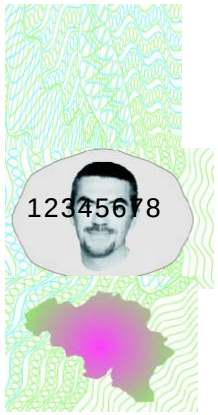
Back side:

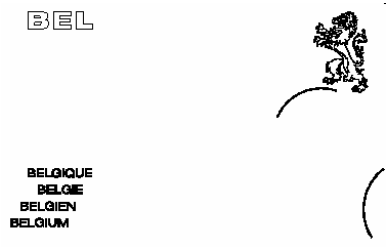
- Place of delivery of the card
- National Register identification number
- Hand written signature of the civil servant
- Main residence of the holder (cards produced before 1/1/2004)
- ICAO (cards produced since 1/1/2005)

- Choix de conception: adresse pas écrite physiquement
  - Évite la réémission d'une carte à chaque changement d'adresse
  - Nécessite la présente d'un lecteur pour tous les contrôles officiels

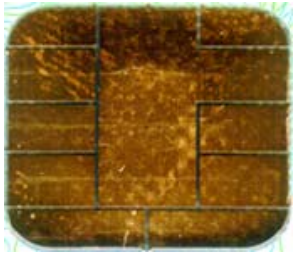
Sécurité

- Physique (cf. ZETES)
  - Rainbow and guilloche printing
  - Changeable Laser Image (CLI)
  - Optical Variable Ink (OVI)
  - Alphagram
  - Relief and UV print
  - Laser engraving

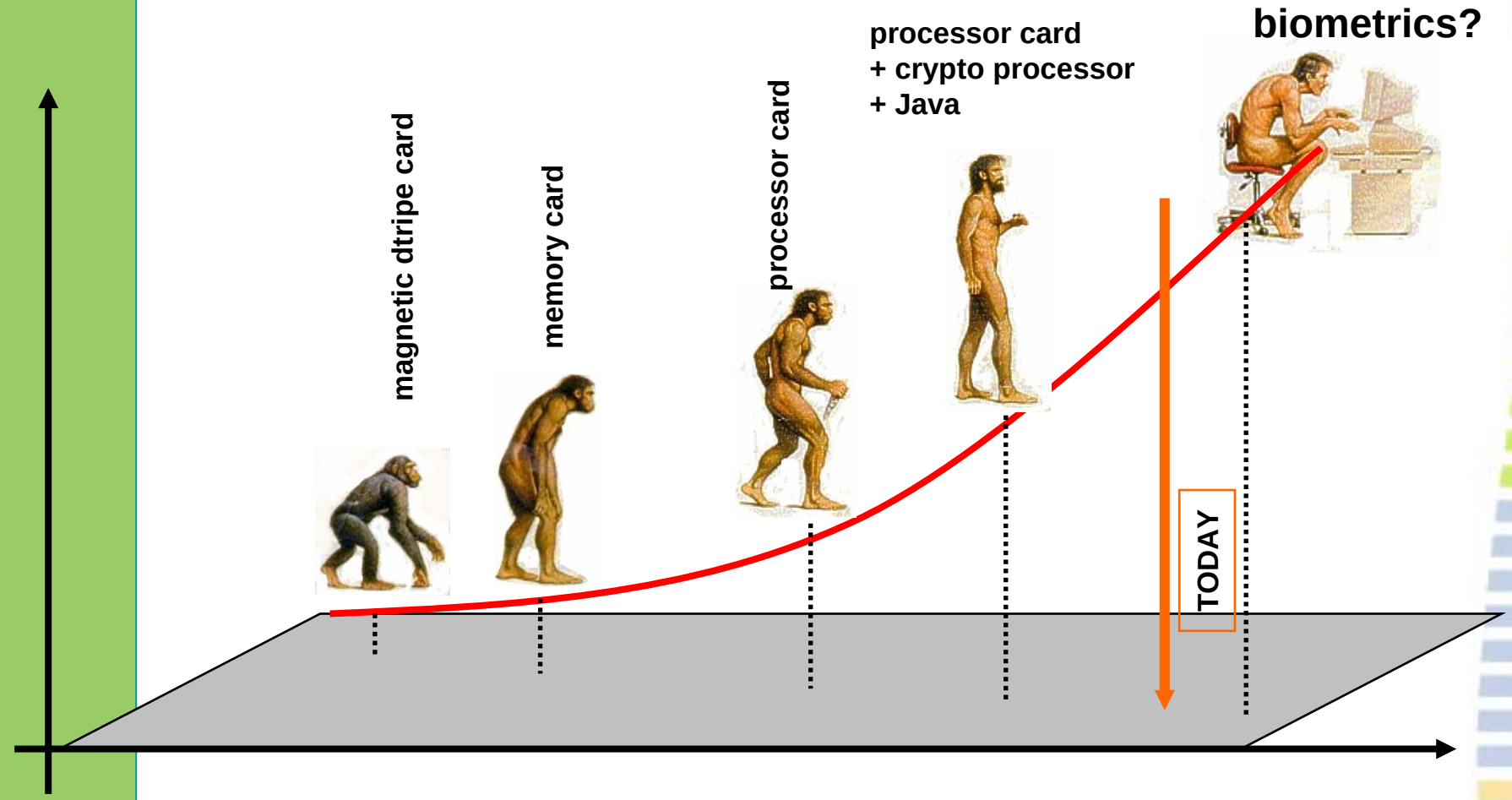




- Electronique



Evolution


magnetic dtripe card
memory card
processor card
processor card
+ crypto processor
+ Java
biometrics?
TODAY

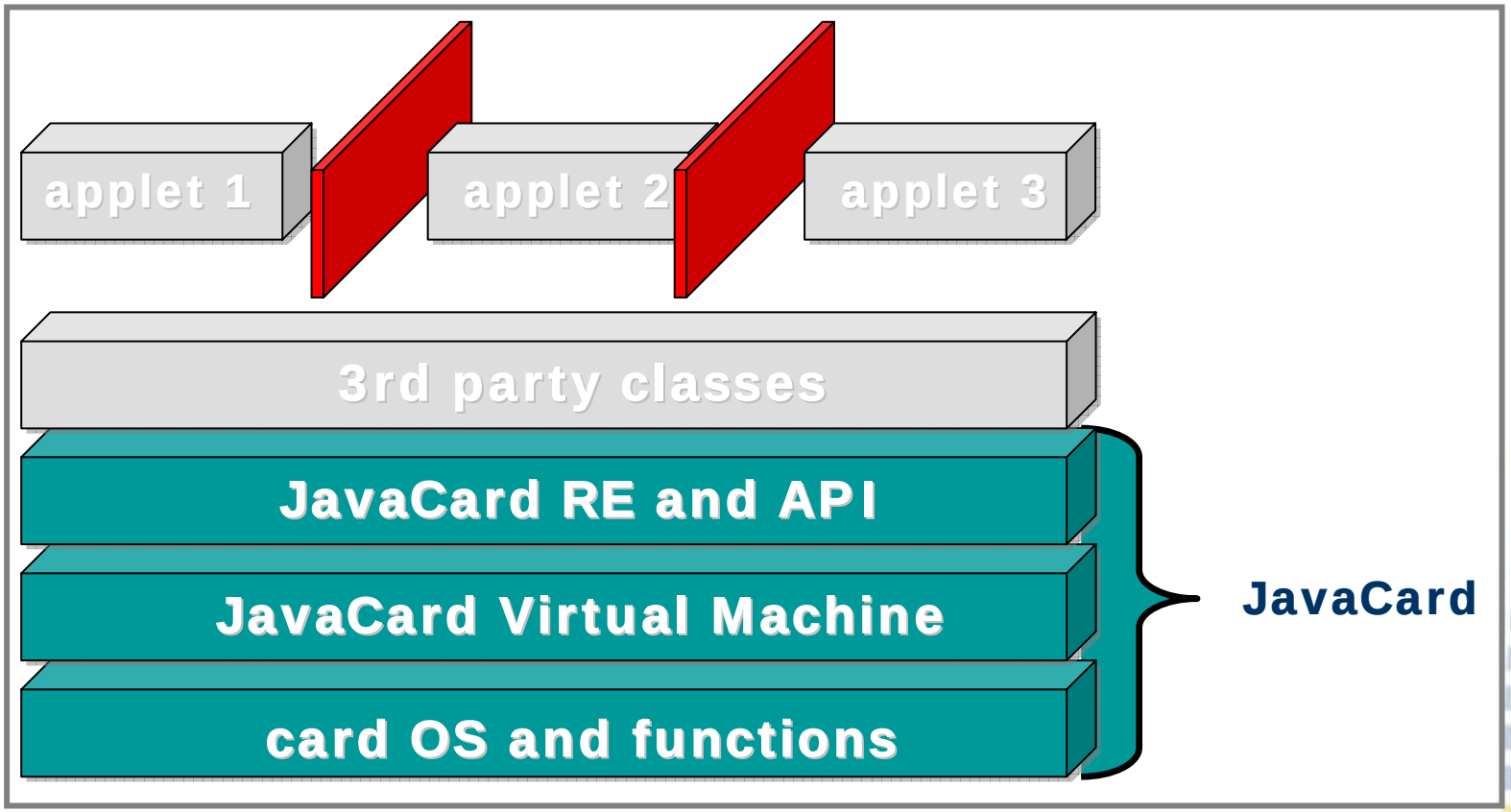
Comparison SIS and eID

- memory card
- nom + RN
- status d'assurance
- -
- -
- -
- Protégée par les apps
- PVC
- Impression standard
- synchrone
- Émise par INAMI

- smart card
- nom + RN
- -
- adresse
- photo
- signature éléctronique
- intrinsèquement sûre
- polycarbonate
- Impression spéciale
- asynchrone
- Émise par RRN

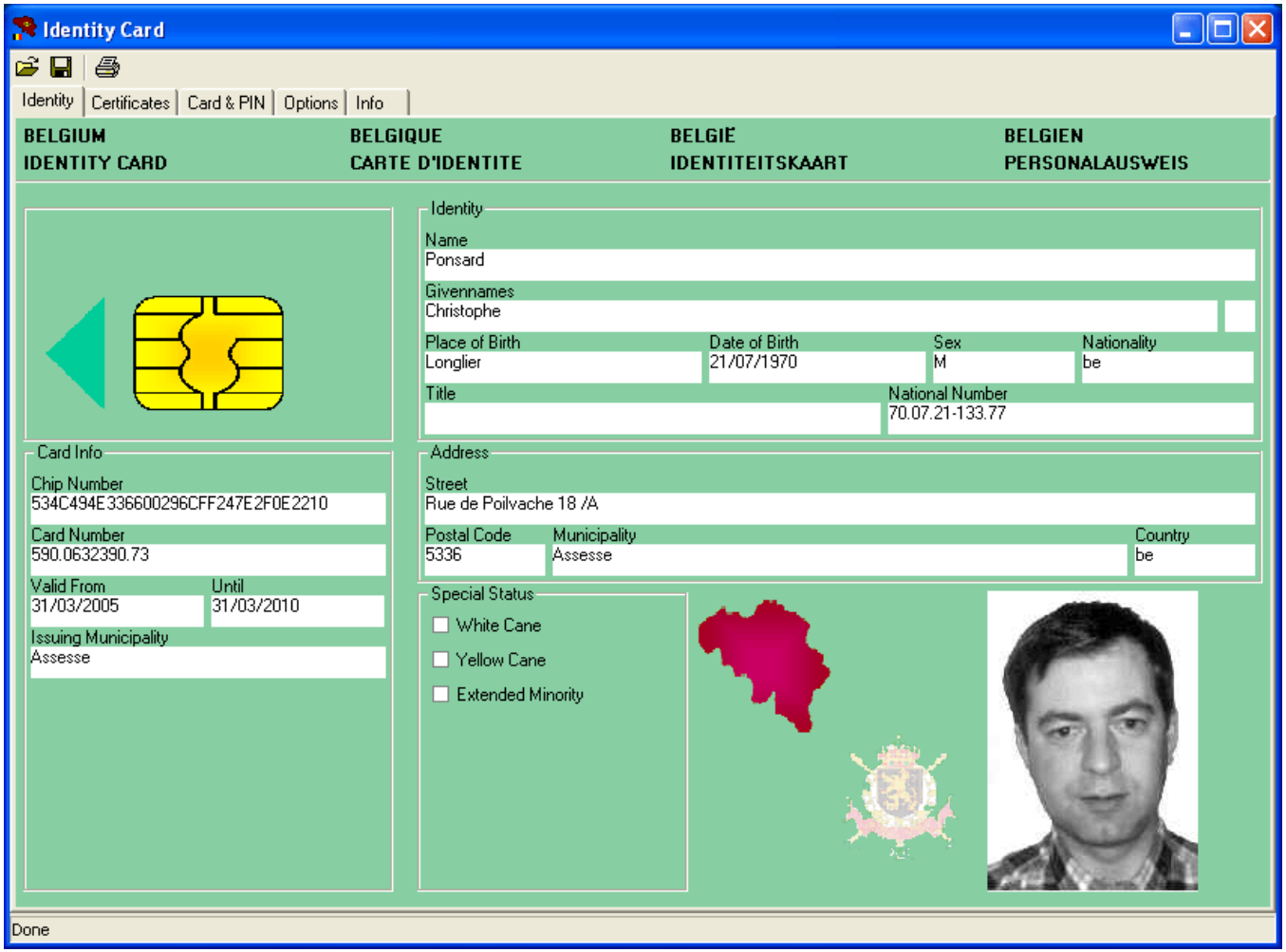
OS et applications sur la carte

Multi-application JavaCard



Contenu de la puce

- Applicatif FEDICT (cf. démo)
- Lecteur: standard PC/SC (USB, PCMCIA...) largement supporté



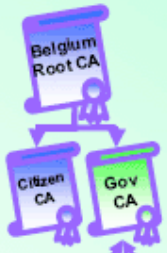
Contenu de la puce

- Identity file (~160 bytes)
  - Chip-specific:
    - Chip number
  - Citizen-specific:
    - Name
    - First 2 names
    - First letter of 3rd first name
    - RRN identification number
    - Nationality
    - Birth location and date
    - Gender
    - Noble condition
    - Special status
    - SHA-1 hash of citizen photo
  - Card-specific:
    - Card number
    - Validity's begin and end date
    - Card delivery municipality
    - Document type
- Digital signature on identity file issued by the RRN
- Citizen's main address file (~120 bytes)
  - Street + number
  - Zip code
  - Municipality
- Digital signature on main address and the identity file issued by the RRN
- Citizen's JPEG photo ~3 Kbytes

King, Prince, Count, Earl, Baron,…

No status, white cane (blind people), yellow cane (partially sighted people), extended minority, any combination

Belgian citizen, European community citizen, non-European community citizen, bootstrap card, habilitation/machtigings card

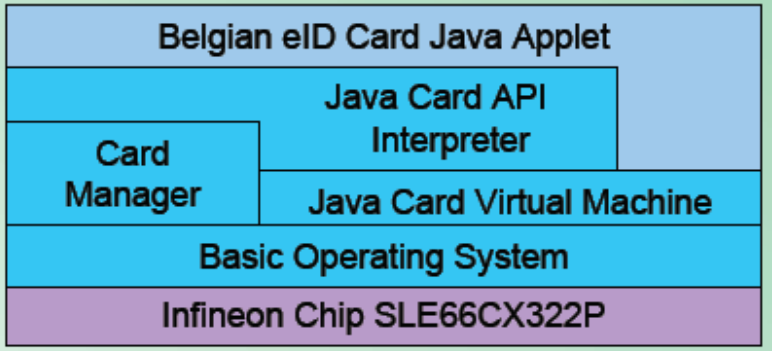


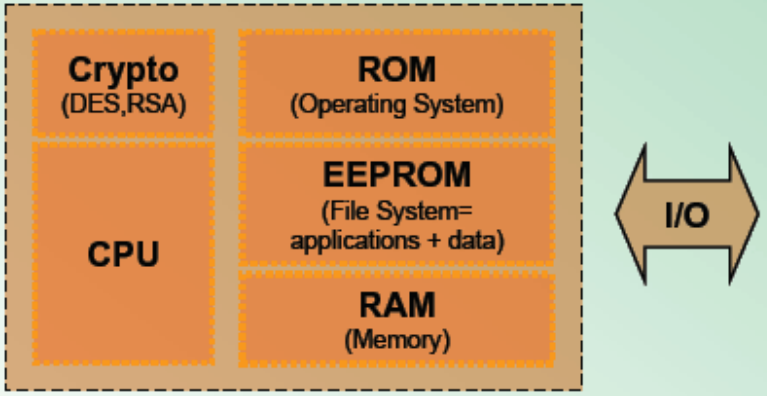
Contenu PKI – clefs & certificats

- 2 key pairs for the citizen:
  - Citizen-authentication
    - X.509v3 authentication certificate
  - Advanced electronic (non-repudiation) signature
    - X.509v3 qualified certificate
    - Can be used to produce digital signatures equivalent to handwritten signatures, cfr. European Directive 1999/93/EC
- 1 key pair for the card:
  - eID card authentication (basic key pair)
    - No corresponding certificate: RRN (Rijksregister/Registre National) knows which public key corresponds to which eID card
- There is NO decryption key
  - No encryption certificate

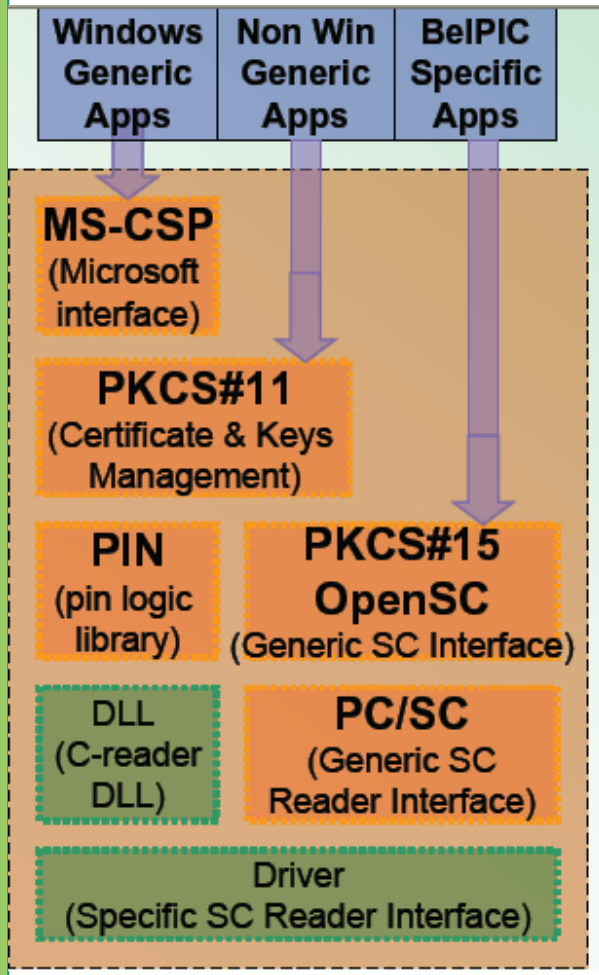
Spécifications de la puce

- Cryptoflex JavaCard 32K
  - CPU (processor): 16 bit Microcontroller
  - Crypto-processor:
    - 1100 bit Crypto-Engine (RSA computation)
    - 112 bit Crypto-Accelerator (DES computation)
  - ROM (OS): 136 kB (GEOS Java Virtual Machine)
  - EEPROM (Application + Data): 32 KB (Cristal Applet)
  - RAM (memory): 5 KB
- Standard - ISO/IEC 7816
  - Format & Physical Characteristics ⇔ Bank Card (ID1)
  - Standard Contacts & Signals ⇔ RST, GND, CLK, Vpp, Vcc, I/O
  - Standard Commands & Query Language (APDU)





Middleware



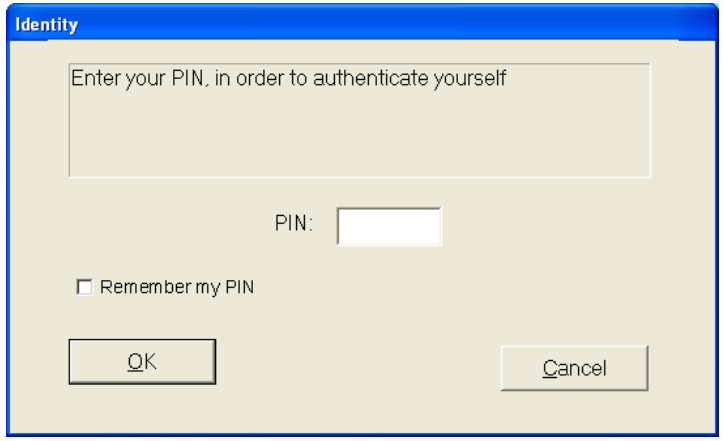
- PKCS#15 file system for ID applications
  - All eID-related data (certificates, photo, address, identity files,…)
  - No key management
- PKCS#11 standard interface to crypto tokens
  - Abstraction of signing functions (authentication, digital signatures)
  - Access to certificates
  - Available for Unix, Windows, MacOSX,…
- CSP for Microsoft Platforms
  - Only keys & certificates available via MSCrypto API
  - Allows authentication (& signature)
  - For Microsoft Explorer, Outlook,…

Lecteurs de cartes eID

Lecteurs de cartes

- Standard PC/SC, largement disponible et supportés par les OS
- Interfaces: USB, PCMCIA
- A présent coût très raisonnable
- Avec/sans pavé intégré (sécurité !)
- Avec/sans authentification du lecteur (sécurité !)

Do you trust this ?



And this ?

Classification des lecteurs

	Class 1	Class 2	Class 3	Class 4	Class 5
Connection	unconnected	connected PC/SC	connected PC/SC	Connected (PC/SC)	Connected (PC/SC)
PIN entry	key pad	-	key pad	key pad	key pad
UI	LCD display	(LED)	LED (buzzer)	LCD display buzzer	LCD display buzzer
Embedded Crypto Device	X	-	-	-	X
Embedded software	Firmware	firmware	firmware	firmware progr/downl	progr/downl
Example	Classic Vasco C/R tokens	"ISABEL" reader	SPR532 Cherry keyb.	Xiring XiPass ACS ACR80	FINREAD

Simple card readers (class 2)

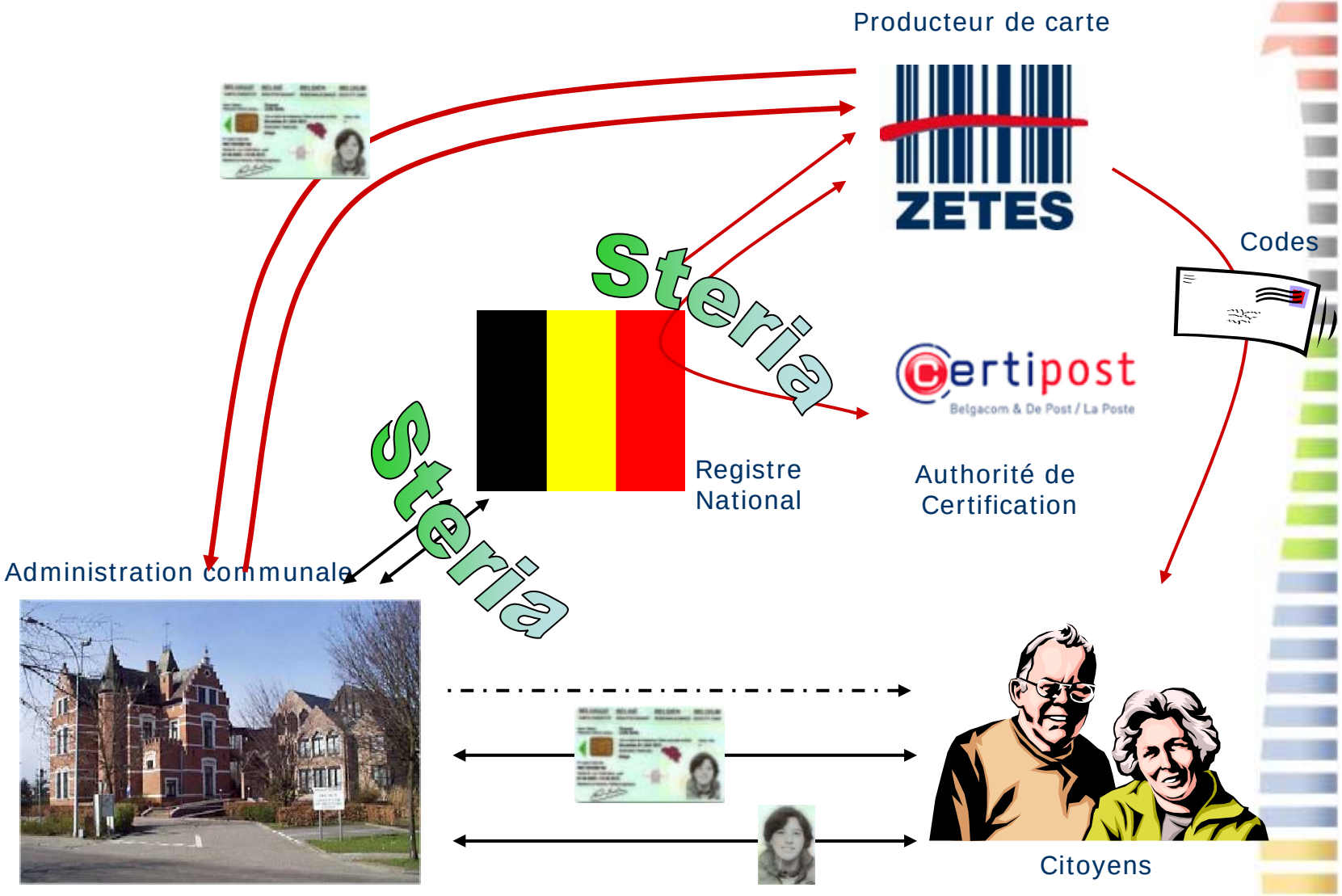
PIN-pad readers Class 3

PIN-pad readers Class 4

Types de cartes

- 0-6 ans: carte enfant sans certificat
- 6-12 ans: carte enfant avec uniquement le certificat authentification
- 12-18 ans: carte eID avec uniquement le certificat authentification
  - Signature activée à la majorité
- 18+ ans: carte eID complète
  - Signature désactivable (définitivement)
- Étrangers: carte d'étranger

Processus de délivrance



- Disponible sur demande !
- Processus normal: 3 semaines. Il existe deux procédures “express” plus coûteuses
- En cas de perte: STOP CARD => désactivation, réactivation possible dans la semaine

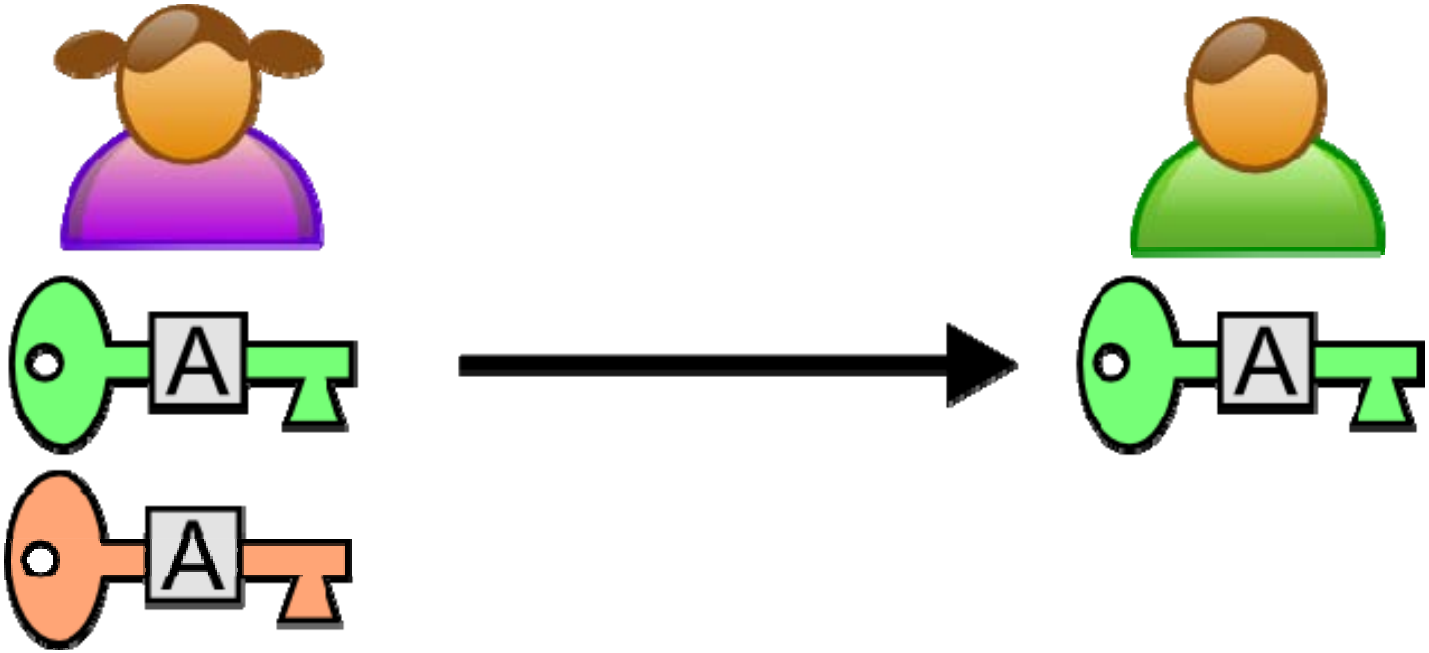
Introduction / Rappel de sécurité informatique

Sécurité informatique

- La sécurité informatique vise généralement cinq principaux objectifs :
  - L'**authentification**, consistant à vérifier l'identité des partenaires.
    - pas de fausse identité
  - La **confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
    - rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction (>< tierce partie espionne)
  - L'**intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
    - pas d'altération accidentelle ou intentionnelle
  - La **disponibilité**, permettant de maintenir le bon fonctionnement du système d'information ;
    - garantir l'accès à un service ou à des ressources (>< DoS)
  - La **non répudiation**, permettant de garantir qu'une transaction ne peut être niée ;
    - aspect contractuel

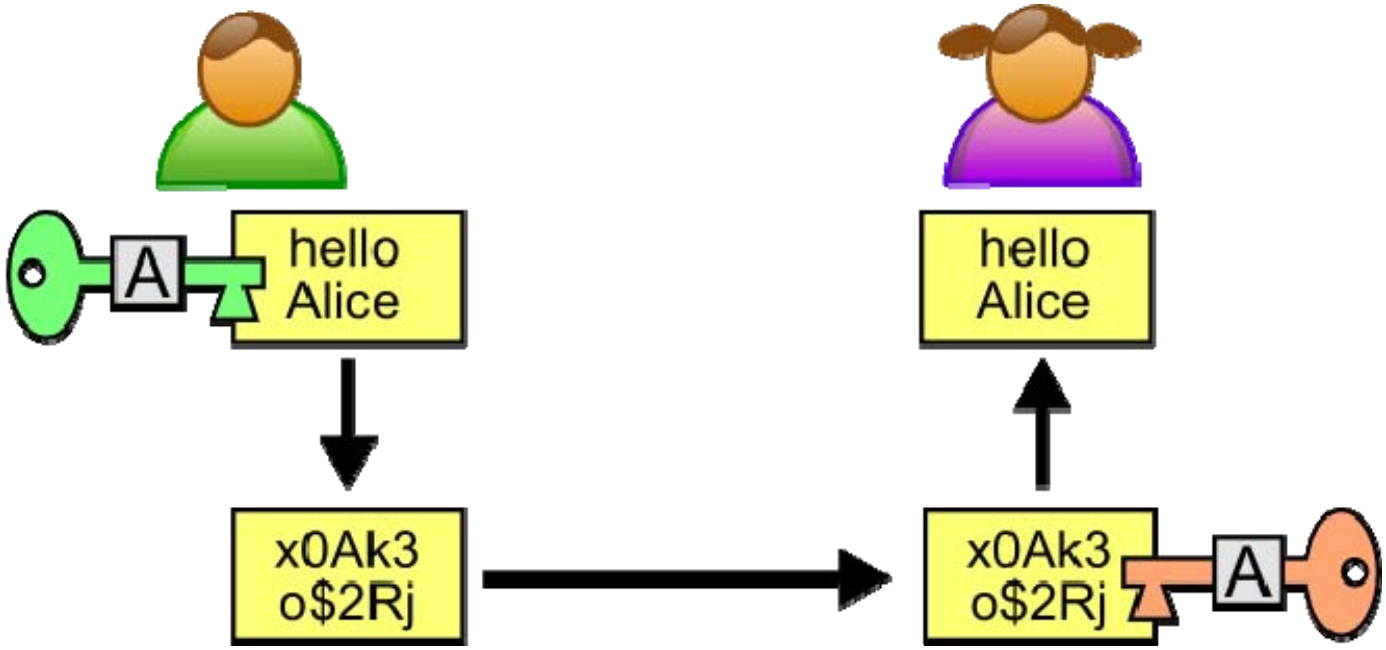
Principe PKI: crypto asymétrique

- 1° étape : Alice génère deux clés. La clé publique (verte) qu'elle envoie à Bob et la clé privée (rouge) qu'elle conserve **précieusement** sans la divulguer à quiconque.



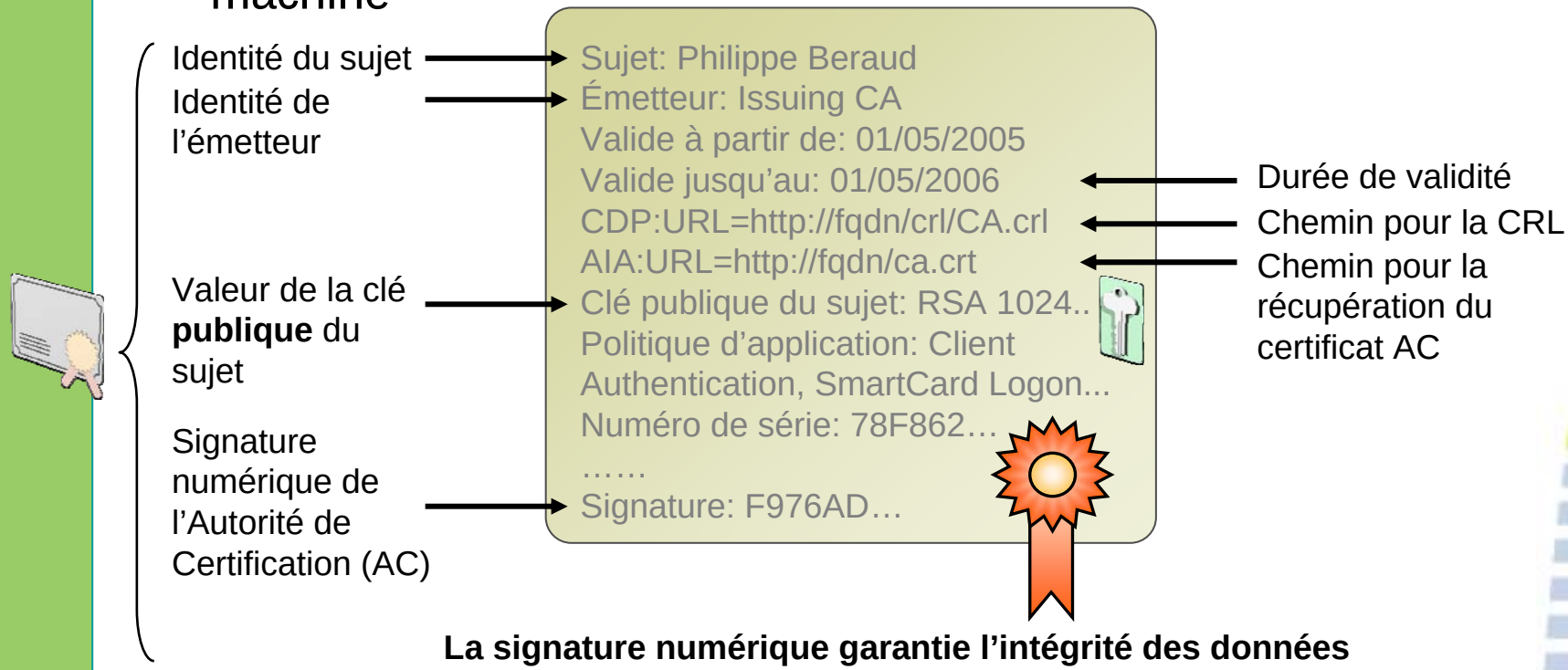
Utilisation des paires de clefs

- 2e et 3e étapes : Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.



Certificats numériques

- Certificats X509 v3
- Équivalent d'une pièce d'identité pour un utilisateur ou une machine

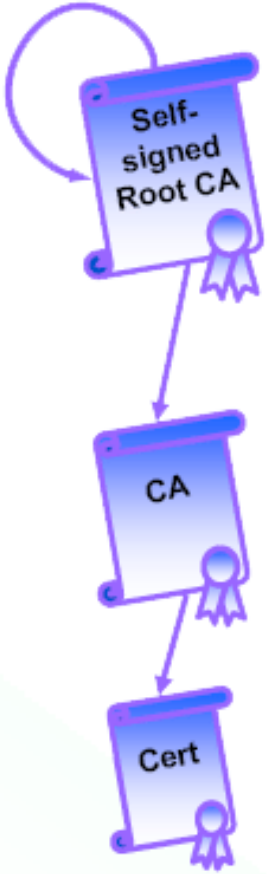


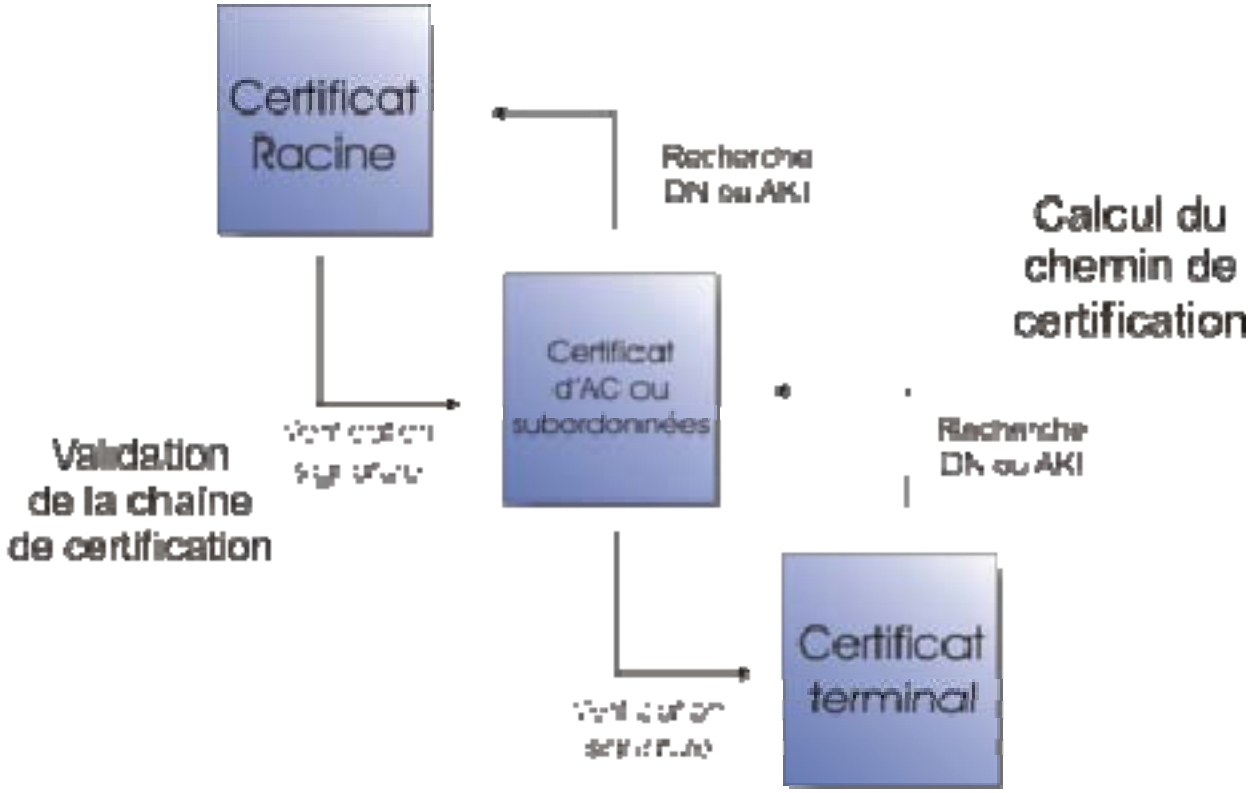
La signature numérique garantie l'intégrité des données

- De plus en plus intégrés avec les services et applications
  - Ouverture de session par carte à puce, messagerie sécurisée, applications de signature électronique, VPN, WiFi, etc.

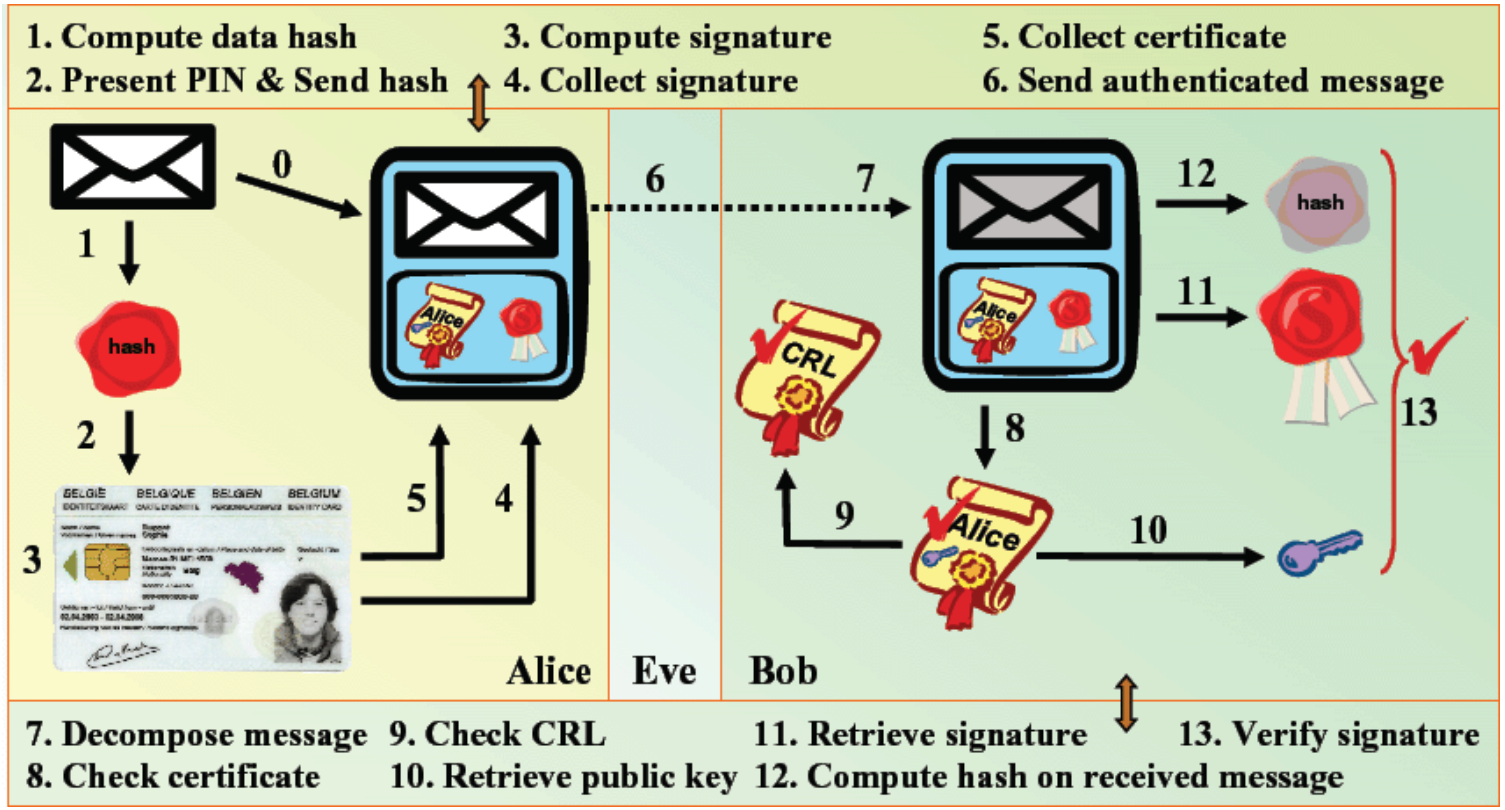
Hiérarchie de certificats

- Certificat signé par une autorité => à vérifier !
- La validation « remonte » la hiérarchie jusqu'à une racine « auto-signée »
- Il faut faire confiance à la racine





Signature électronique



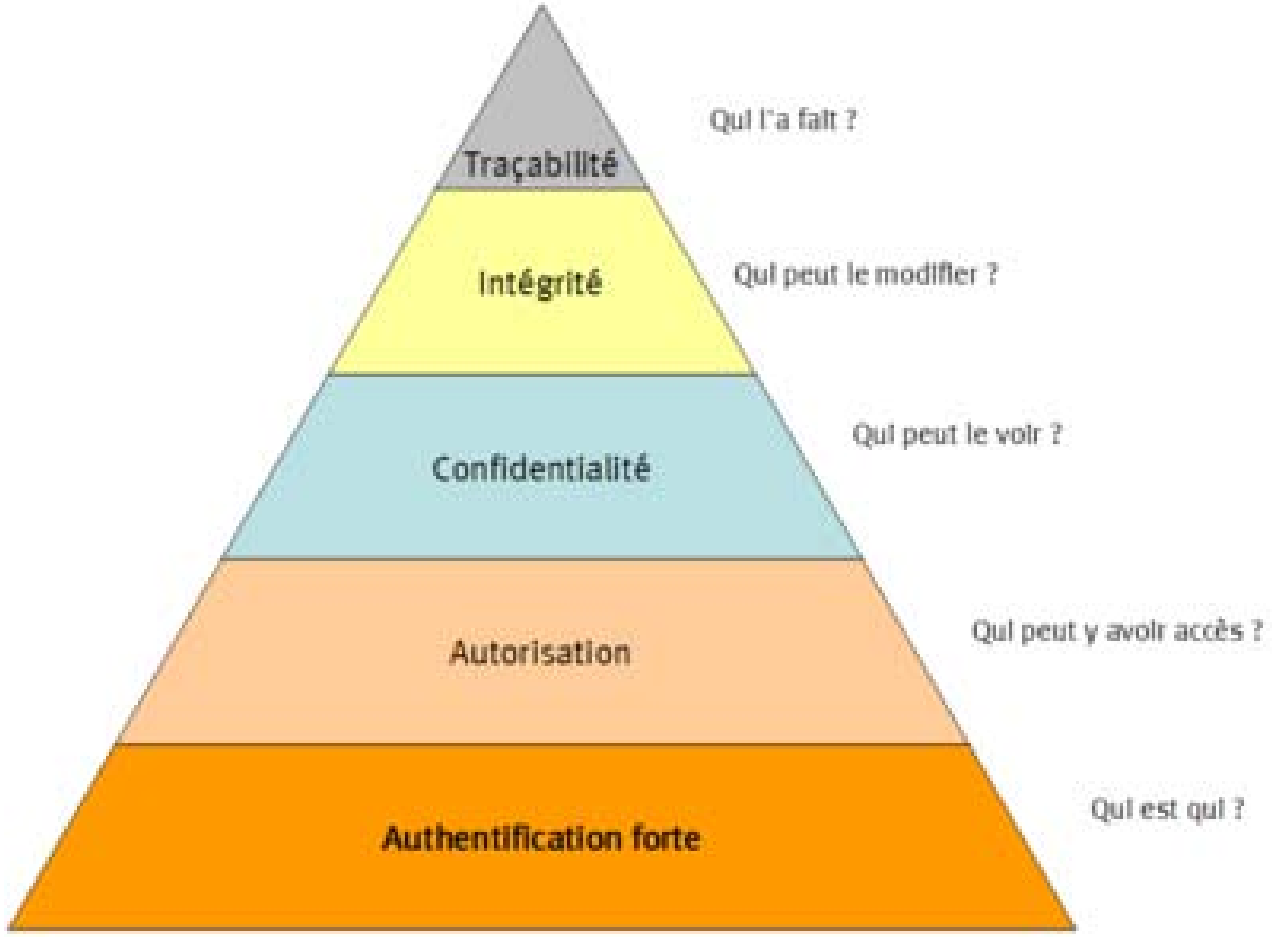
- Résultats:
  - OK: Bob knows that
    - the eID of Alice was used to produce digital signature
    - the message integrity is preserved
  - KO because message was compromised
  - KO because key revoked (using CRL)
- ! message is not encrypted and could be read by “Eve”
  (encryption can be implemented using by exchanging signed key session)

Propriétés de la signature

- La signature électronique
  - Authentifie son auteur
  - Ne peut être contestée
  - Garanti l'intégrité du document signé (contrairement à la signature manuscrite)
  - Ne garanti pas la confidentialité du document signé
- Restent valides **éternellement**, même si le certificat est révoqué, à condition de conserver:
  - le document signé et sa signature
  - le certificat du signataire
  - la preuve de la validité du certificat
  - un horodatage de la signature
- Validité légale équivalente à la signature manuscrite

Authentification

- A la base d'une pyramide de sécurité



Techniques d'authentification

- Dans le cas d'un individu, l'authentification consiste, en général, à vérifier que celui-ci possède une preuve de son identité ou de son statut via:
  - Ce qu'il sait: mot de passe, PIN
  - Ce qu'il possède: carte à puce, certificat, token, GSM,...).
  - Ce qu'il est: biométrie
  - Ce qu'il sait faire: geste, signature

- eID: 2 mécanismes
  - authentifier l'utilisateur par rapport à la carte: PIN
  - la carte par rapport au système: certificat

Authentification par certificats

- Étapes pour que A s ’authentifie auprès de B :
  - A envoie son certificat à B
  - B en vérifie la validité en utilisant la clé publique du CA
  - B envoie un challenge à A
  - A chiffre le challenge avec sa clé privée et répond à B
  - B déchiffre avec la clé publique de A
- Démarrage de la session
  - B envoie une clé de session (chiffrée) à A
- Authentification mutuelle
  - B s ’authentifie de la même manière auprès de A

Applications de l'eID

Aperçu des applications

- Contrôle d'accès physique: parc à conteneurs, bibliothèque, police,...
- Authentification électronique: login sur une station de travail, SSH, SFT
- Signatures digitales: emails, fichiers PDF,...

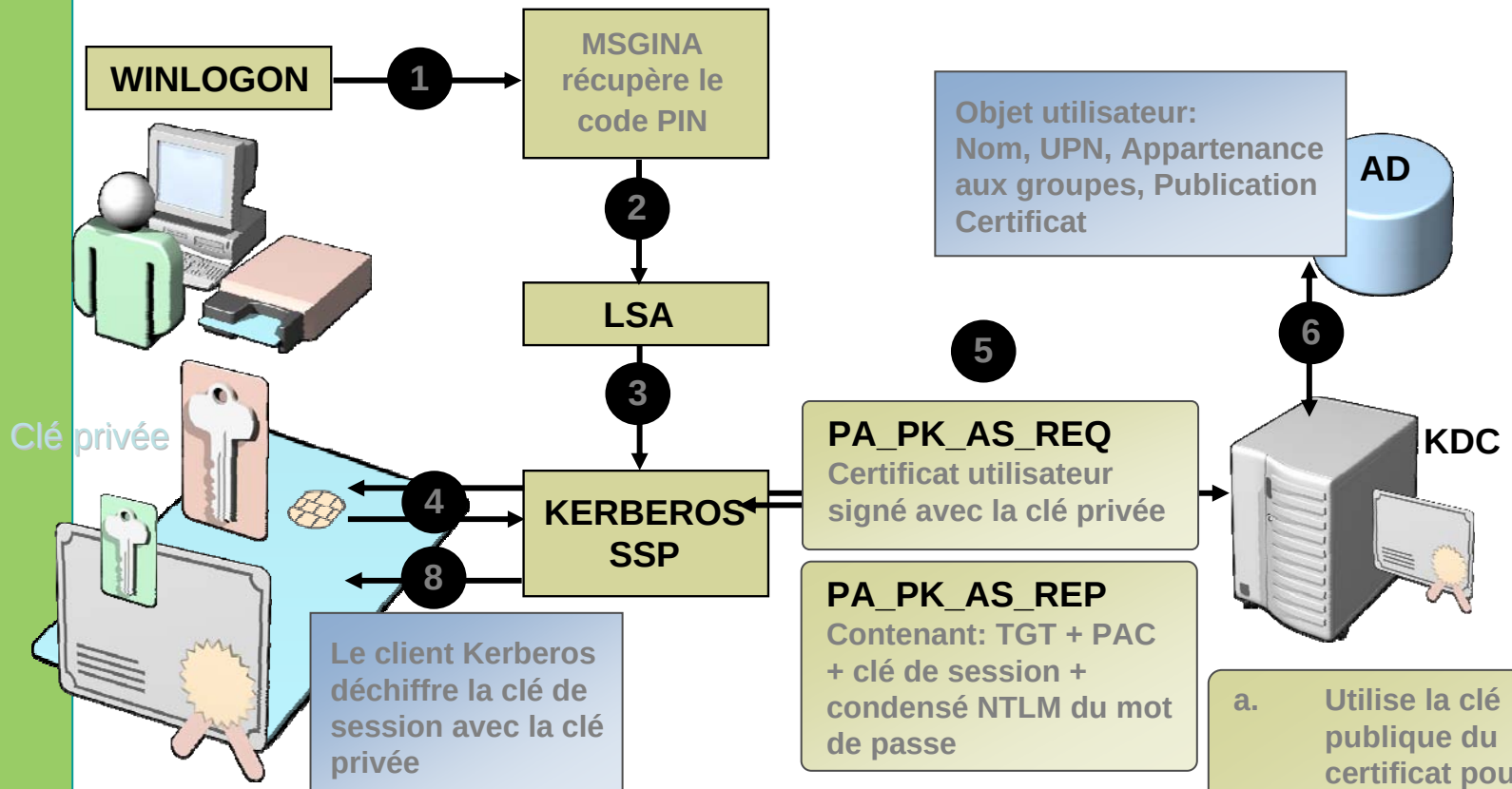
- Application eGov:
  - accès web au registre national
  - déclarations : tax-on-web, TVA
  - commande de documents,
  - E-vote ?
- Chat sécurisé sur Internet
  - Kids:
    - http://www.chat.be
    - http://www.skynet.be via www.kidcity.be
    - http://www.telenet.be
    - http://place.to.be
    - http://www.krey.net/saferchat/
  - Seniors !
    - https://www.seniorennet.be/Pages/Vrije_tijd/chatbox.php
  - Chat « communal »

internet pour tous

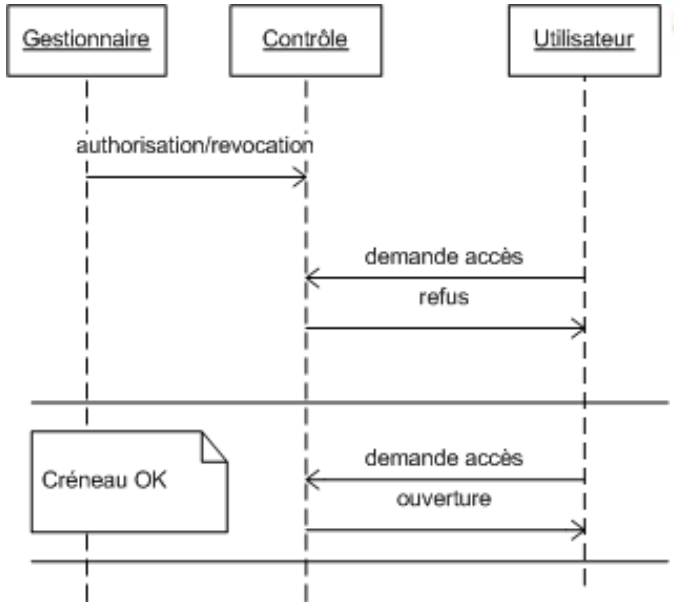
- eCommerce: eTicketing, transactions commerciales, signature de contrats, ...

Ouverture de session par carte à puce

- Windows - Extension Kerberos PKINIT



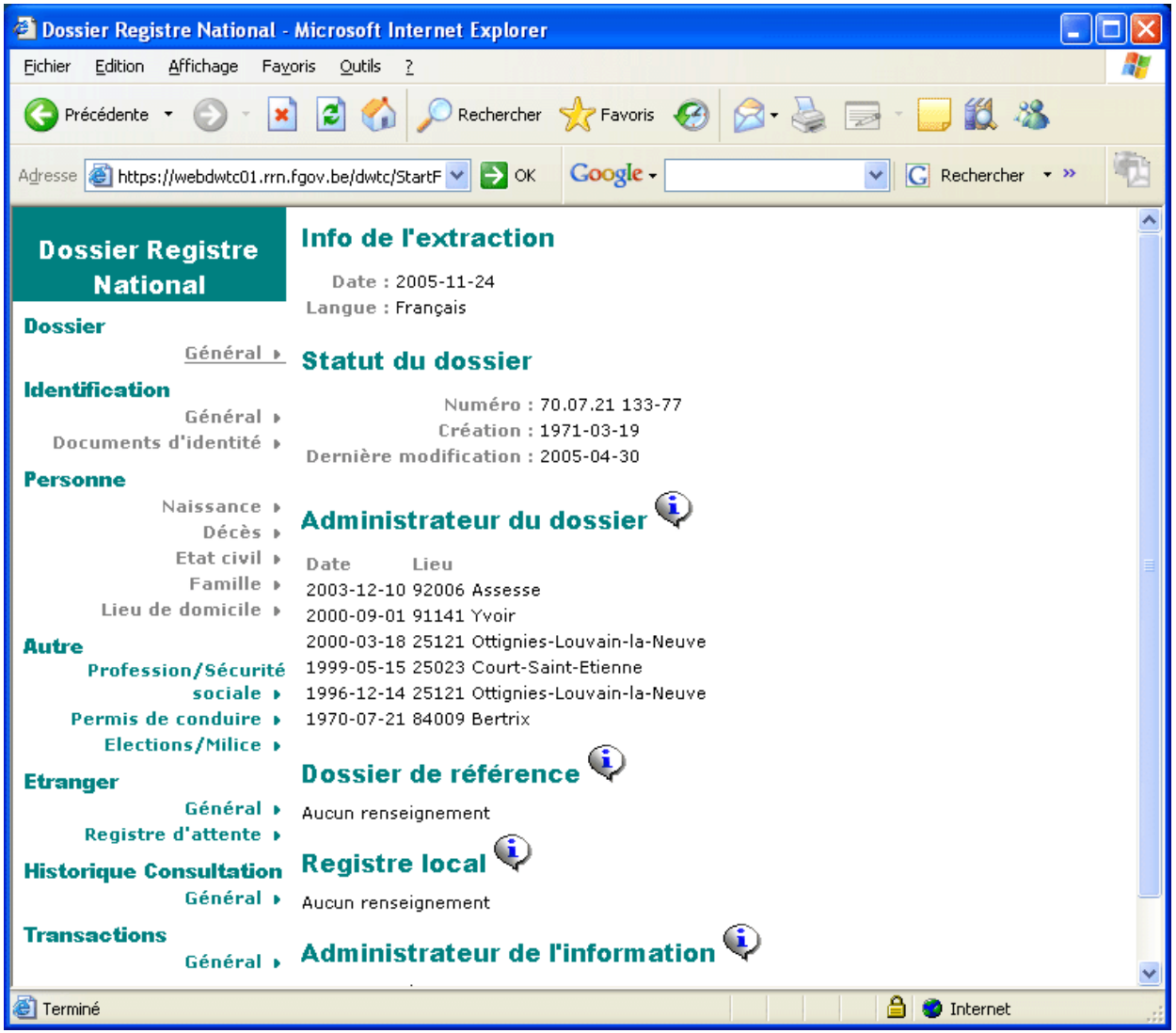
Contrôle d'accès physique à une infrastructure communale



- Exemples:
  - Parc à container
  - Salle de réunion communale
  - ...
- Avantages
  - Contrôle fin: telle personne dans tel créneau horaire
  - Plus de facilité: plus de clef à transmettre
  - Accès plus étendu (ex. pour le soir)
  - Informatisation de la planification
- Dangers
  - Complexification: introduction de matériel et logiciel
  - Déresponsabilisation => dégradation
    - Système mixte
    - Personne autorisée = responsable

Consultation du Registre National

https://mondossier.rrn.fgov.be/



Accès au dossier personnel + historique de consultation !

Guichet électronique

- Commande de formulaires
  - Population: ménage, domicile, nationalité
  - État civil: extraits d'actes de naissance, mariage, divorce,...

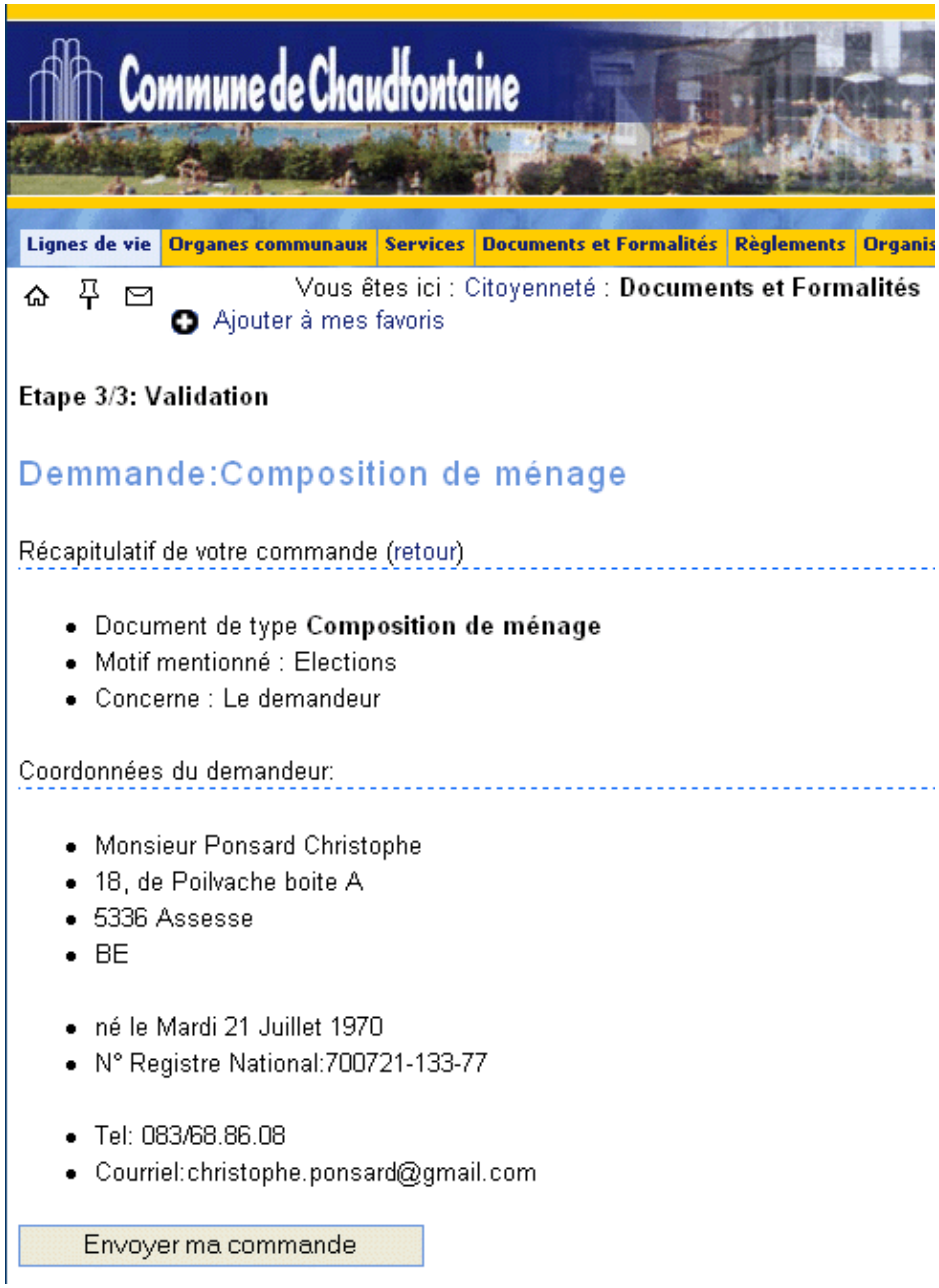
  (note: pas mal de ces infos sont sur la carte...)

- Avantages
  - Évite les files aux guichets
  - Plus grande réactivité
  - Garde la disponibilité des employés pour les démarches plus complexe nécessitant un contact direct
  - Meilleure sécurité par rapport aux formulaires actuels, basés sur la confiance ou la vérification a posteriori

- Dangers
  - Perte de contact de proximité
    => pas pour toutes les démarches
  - « Fracture numérique »

    => garder le guichet physique bien sûr
    => mettre des bornes « eID-enabled » dans la commune

Exemple: Chaudfontaine



Le projet Commune-Plone

- Mutualisation des développements eGov pour les communes
- Soutenu par Union des Villes et Communes de Wallonie
- Choix de la plateforme Plone (basé sur zope)
- Comporte un module eID
- URL:
  - http://www.communesplone.org/
  - http://demo.communesplone.org/

Guichet électronique: conception

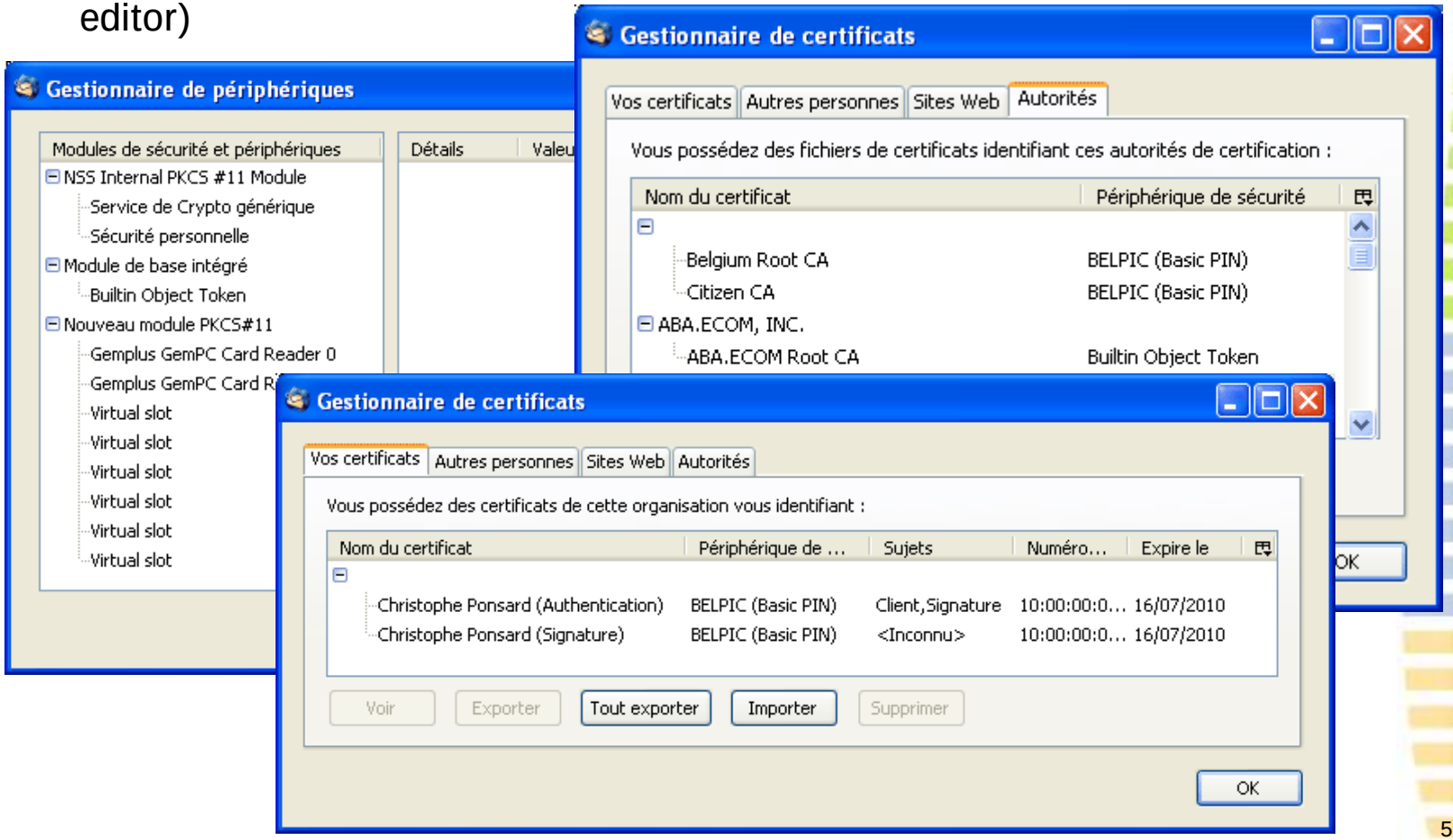
- Formulaire Internet simple: possible mais étape de vérification nécessaire
  - lors du retrait physique (1 déplacement au lieu de 2)
  - via une transaction financière (envoi postal possible). Exemple: Mons
- Avec eID:
  - remplissage « automatique » possible
  - authentification dès le début de la démarche
- Authentification du fonctionnaire:
  - Exemple: processus d'émission de la carte elle-même
  - Problèmes: identité ≠ fonction, usage privé vs. professionnel
  - « Token fonctionnaire » plus approprié
- Sécurité: éviter le « fishing »
  - Espace des noms communaux non standard !
  - SSL avec certificat authentifiant la commune

Évolution

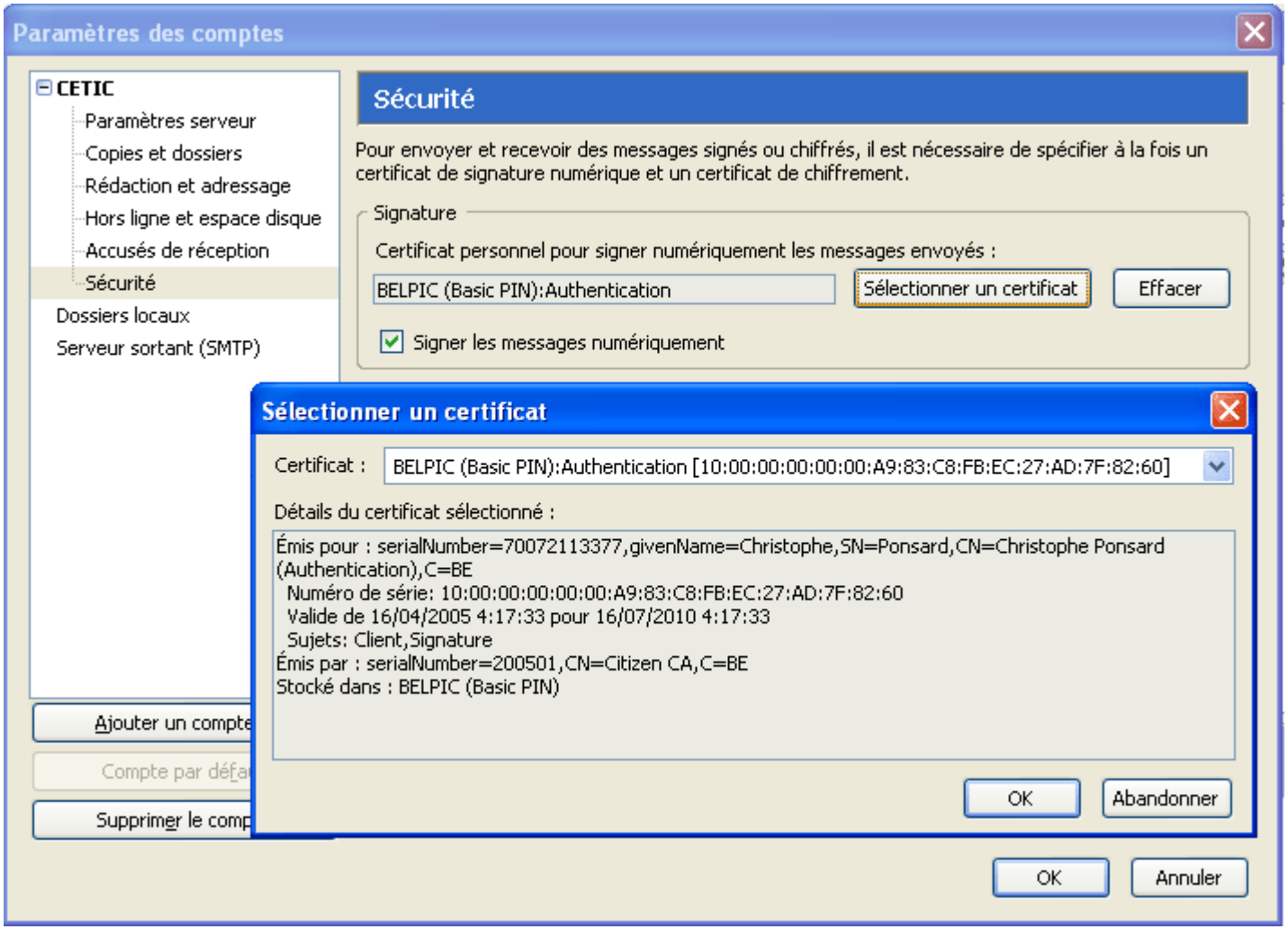
- Profil communal:
  - Suivi de dossiers: demande de permis,...
  - État des pesées de la poubelle à puce
  - ...
- Guichet « unique »
  - Interopérabilité des données gérées à différents niveaux de pouvoir: commune – province – région - fédéral
  - Point d'accès unique
  - Intégration des données
    - Portail unifié et consistant, intégrant des données gérées à différents niveaux de pouvoir
    - Projet « Co-marquage »
  - Intégration des procédures
    - Moins de démarche pour le citoyen
    - Automatisation de certains traitements
    - Interconnexion (+ simplification) administrative
    - Projet « Interop » (primes soltherm & réhabilitation)

Signature d'emails avec Thunderbird (1)

- Installer le module PKCS#11 (dll: \WINDOWS\SYSTEM32\beidpkcs11.dll)
- Importer les certificats et les authorités de certificats (CA) via PKCS#11
- Note: CA aussi disponible sur http://repository.eid.belgium.be
  (pour les clients sans eID)
- On doit faire **confiance** à Citizen CA pour les email (aussi: web site, application editor)

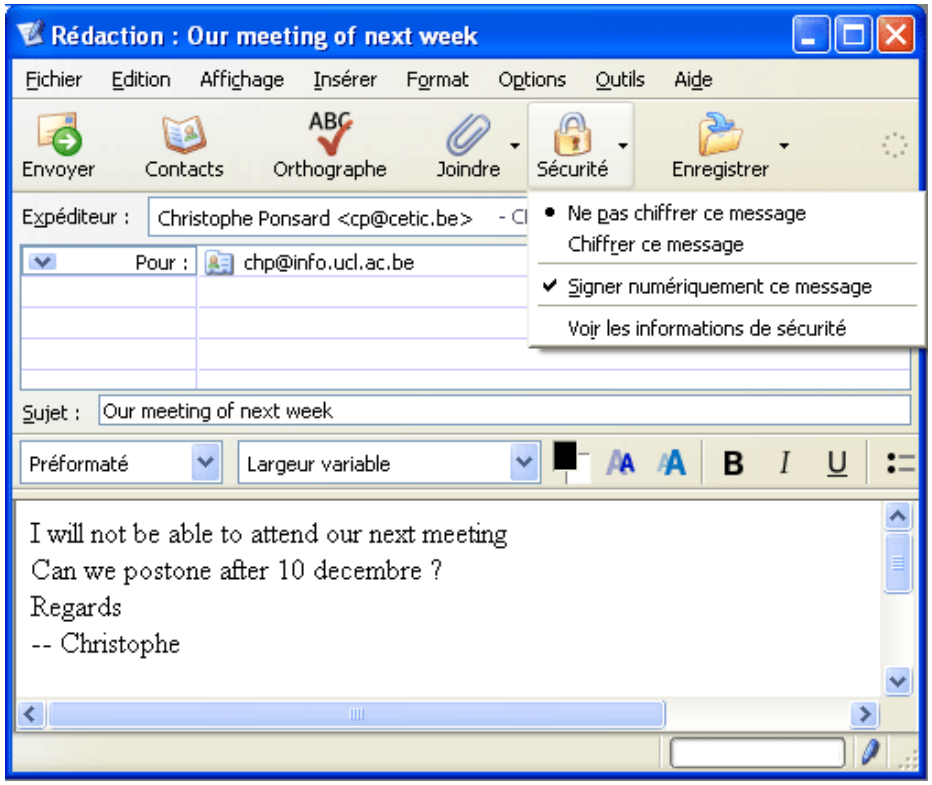


Signature (2) sélection du certificat



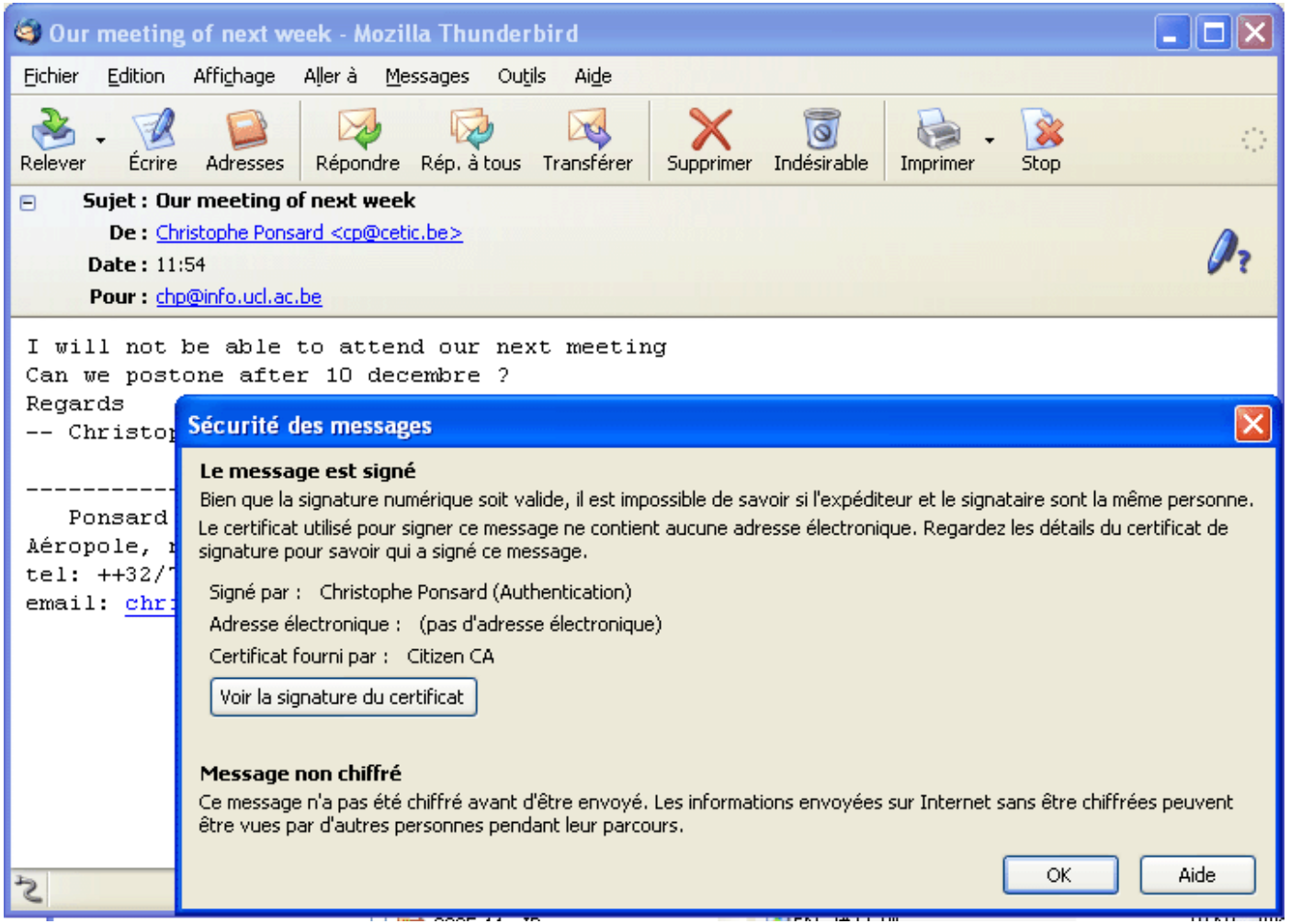
Signature (3) – Envoi de l'email

- Rédiger l'email



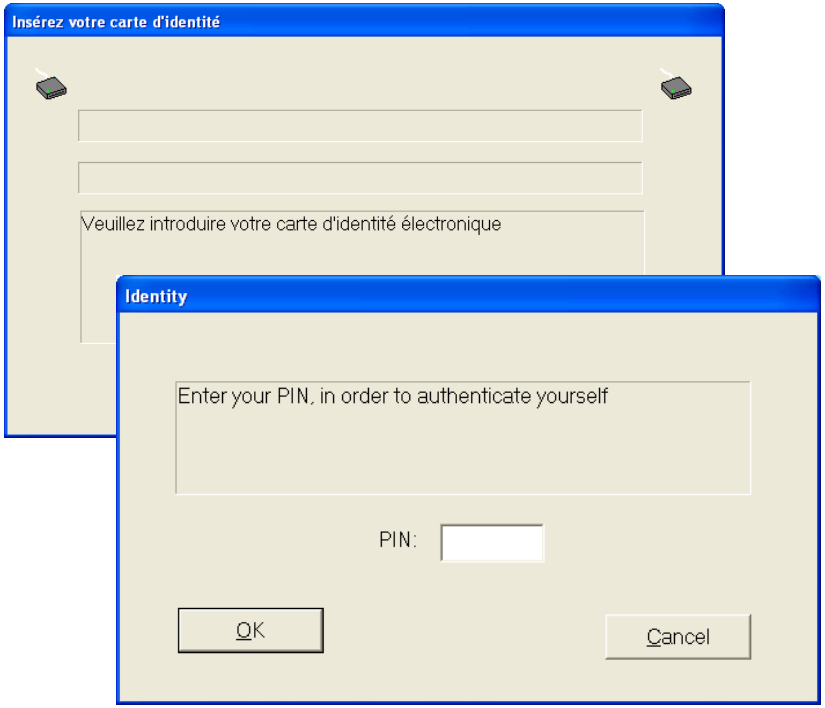
- Authentification PIN: lien personne physique

Signature (4) – validation de la signature



- Test: altérer le contenu du mail
- Aussi: gestion de la révocation (CLR, OCSP)

Chat avec authentification



Développer avec l'eID

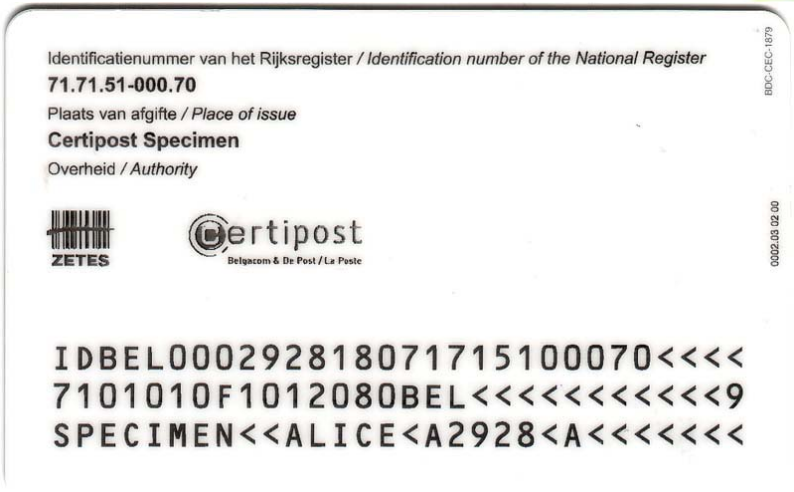
Quelques Outils de base

- Middleware et SDK eID
  - API Java de l'eID
  - Accès aux fonctions de la carte en JAVA
  - Wrapping possible: javascript, VB...
- Authentification web: reverse proxy apache
  - Serveur web modifié
- [Un peu de code s'il reste du temps]

Et payant: eID Shop

Test – carte de test

- Signée par CA de test !
- Certificats avec plusieurs statuts: Suspendu, Expiré et Révoqué



Réalisation d'un chat « eID »

- Lieu thématique permettant de débattre de la vie de la commune en temps réel (chat) ou différé (forum)

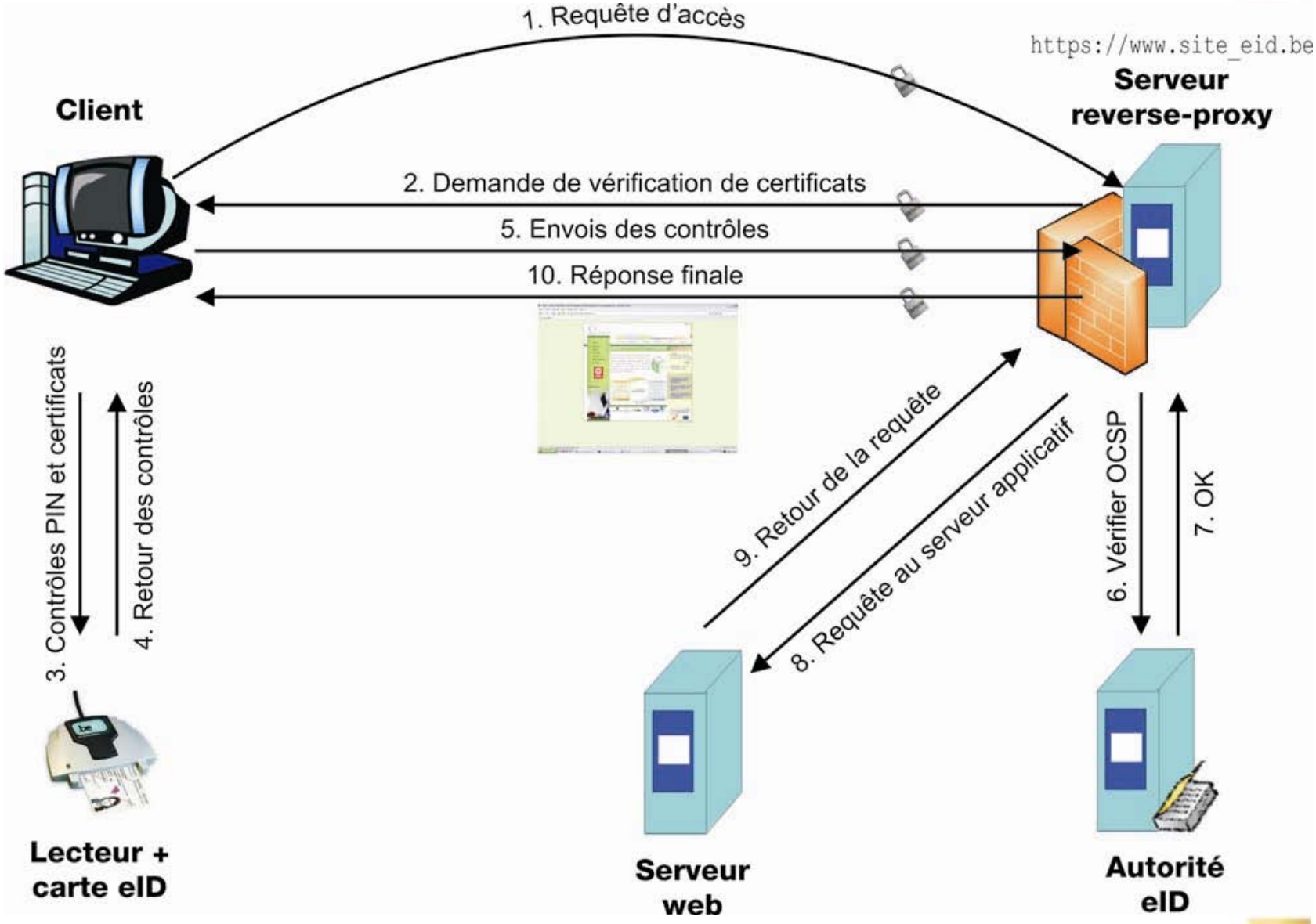
- Avantages:
  - Restriction d'accès suivant divers critères (âge, sexe, lieu de résidence...)
  - Authenticité: pas de fausse identité

- Dangers:
  - Être trop restrictifs

    => mécanisme supplémentaire d'autorisation (invitation)
  - Violation de la vie privée

    => permettre de garder le contrôle de certaines information et confiance associée en conséquence

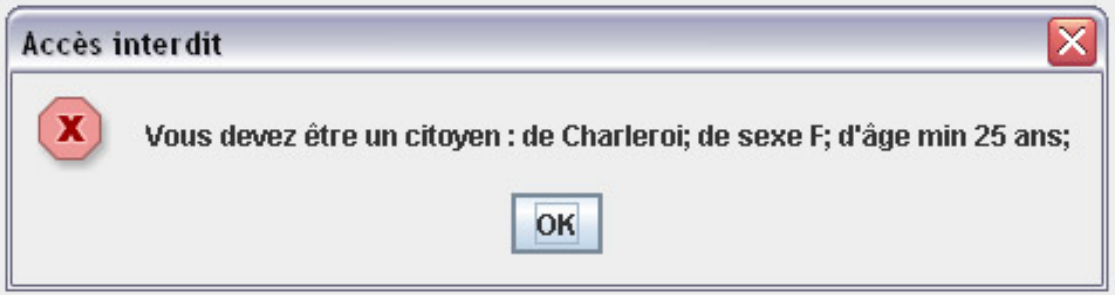
Architecture d'un système eID on-line



Utilisation de SSL

- Transport Layer Security (TLS), anciennement nommé Secure Socket Layer (SSL)
- Mode client-serveur avec 4 objectifs de sécurité :
  - l'authentification du serveur ;
  - la confidentialité des données échangées (ou session chiffrée) ;
  - l'intégrité des données échangées ;
  - de manière optionnelle, l'authentification ou l'authentification forte du client avec l'utilisation d'un certificat numérique.
- Outils: openSSL – apache (modssl+modif eID)

Chat eID - login



Chat-eID

jj est entré(e) sur le chat
jj : Salut tout le monde
cp est entré(e) sur le chat
cp : Salut

Nickname : jj
Nom : Jonckers
Prenom : Jérôme
Sexe : M
Age : 22 ans

Message : Envoyer

Sortir | Qui est qui?

Transparence des participants (et considérations de vie privée)

Nickname	N° National	Nom	Prénom	Age	Sexe	Photo
jj	84041916983	Jonckers	Jérôme	22 ans	M	

retour au chat

Conclusions, perspectives et références

Conclusions et perspectives

- Apport de l'eID
  - Ne remplace rien
  - Facilite et sécurise les applications
  - Ouvre de nouvelles perspectives
- Dangers à prendre en compte
  - Plus de sécurité mais également de nouvelles menaces
  - Fracture numérique pour les citoyens
  - mais aussi pour les communes, pas toutes égales
- Directions à prendre
  - Mutualiser: regrouper les expériences et les réalisations !
  - Pistes: UVCW, RIC, communes ayant de l'expérience, commune-plone,...
  - Projets pilotes: en cours

Références générales sur l'eID

- Introduction:
  - http://eid.belgium.be/
  - http://www.registrenational.fgov.be/cie/cdocu.htm
  - http://www.certipost.be/fr/article.php3?id_article=110
  - http://www.microsoft.com/belux/fr/eid/
- Développement:
  - eID shop: http://www.eid-shop.be
  - GODOT's site: http://www.godot.be/
  - Dossier UVCW: http://www.uvcw.be/articles/33,90,39,39,1393.htm
- Contrôle: certificats, valeur légale
  - http://repository.eid.belgium.be/FR/index.html
  - http://www.stethonet.org/informatic/signature.htm
- Site concours eID: http://www.elidcard.be
- Newsletter eID (n°4 disponible) sur http://eid.belgium.be