

Applications citoyennes de la carte d'identité électronique au niveau communal



eWish

27 Avril 2006

Contexte

BUT = donner, à tous les citoyens belges, un moyen


- de s'authentifier auprès d'applications électroniques
 - c.à.d de prouver son identité
- de placer des signatures digitales sur des documents électroniques
 - avec la même valeur légale que la signature manuscrite

Fait:

- + de 2 millions de cartes électroniques en circulation
- Où sont les applications ?

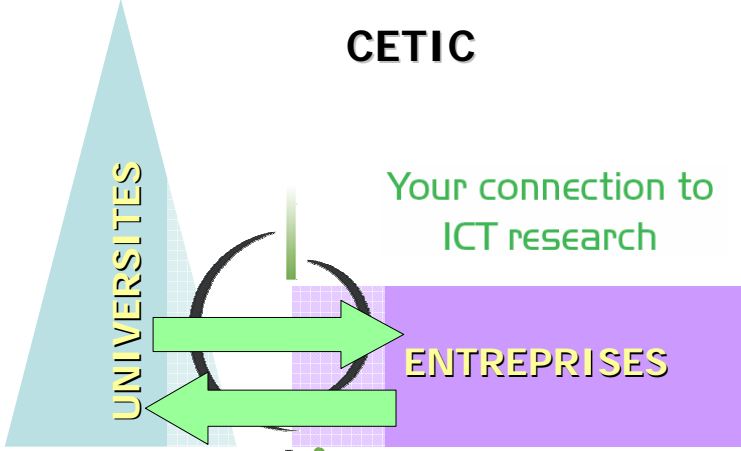
Focus de la présentation

- Niveau applicatif, dans le contexte communal
- Vue critique dans une perspective système et utilisateurs (citoyens et fonctionnaires)



CETIC

Your connection to
ICT research




UNIVERSITES


ENTREPRISES

cetic

- Entreprise = aussi secteur public « eGov »
- Niveau européen, fédéral, provincial (Hainaut) et régional
- Compétences : CdC, sécurité, qualité, systèmes électroniques, systèmes distribués, logiciels libres




3



Aperçu de la présentation

- eID: rappels
- Quelques applications
 - Accès au registre national
 - Contrôle d'accès physique
 - Guichet électronique
 - Forum et chat citoyen
- Conclusions et perspectives
- Quelques références



4

Sécurité

■ Physique

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

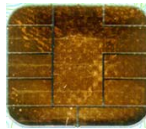


BEL



BELGIQUE
BELGIE
BELGIUM

■ Electronique



- SHA-1
- RSA
- SPA/DPA/... resistant
- EAL5+ certified
- ...

Contenu de la puce

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

Identity Card

Identity | Certificates | Card & PIN | Options | Info

BELGIUM IDENTITY CARD	BELGIQUE CARTE D'IDENTITE	BELGIE IDENTITEITSKAART	BELGIEN PERSONALAUSWEIS
Identity Name: Ponsard Givennames: Christophe Place of Birth: Longier Date of Birth: 21/07/1970 Sex: M Nationality: be Title: National Number: 70.07.21-133.77			
Card Info Chip Number: 534C494E336600296CFF247E3F0E2210 Card Number: 590.0632390.73 Valid From: 31/03/2005 Valid Until: 31/03/2010 Issuing Municipality: Arsenne			
Address Street: Rue de Polvache 18 /A Postal Code: 5336 Municipality: Arsenne Country: be			
Special Status <input type="checkbox"/> White Cane <input type="checkbox"/> Yellow Cane <input type="checkbox"/> Extended Minority			

Contenu de la puce

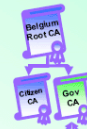
- Identity file (~160 bytes)
 - Chip-specific:
 - Chip number
 - Citizen-specific:
 - Name
 - First 2 names
 - First letter of 3rd first name
 - RRN identification number
 - Nationality
 - Birth location and date
 - Gender
 - Noble condition
 - Special status
 - SHA-1 hash of citizen photo
 - Card-specific:
 - 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



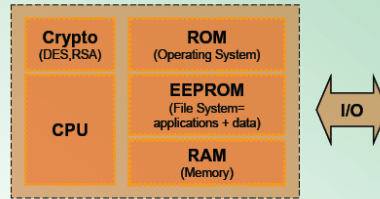
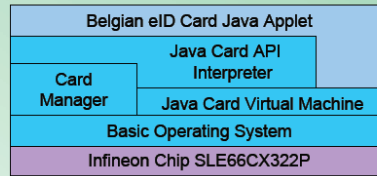
Contenu PKI – clefs & certificats

- 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**

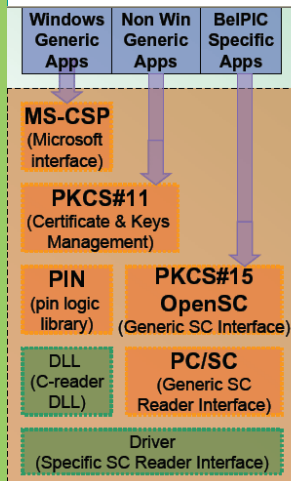


Spécifications de la puce

- 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)



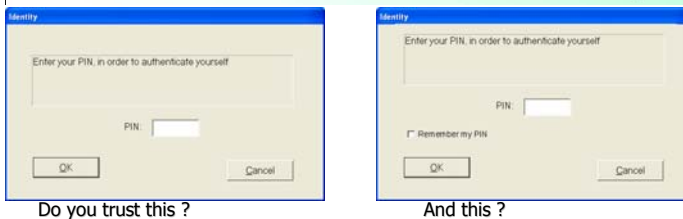
Middleware



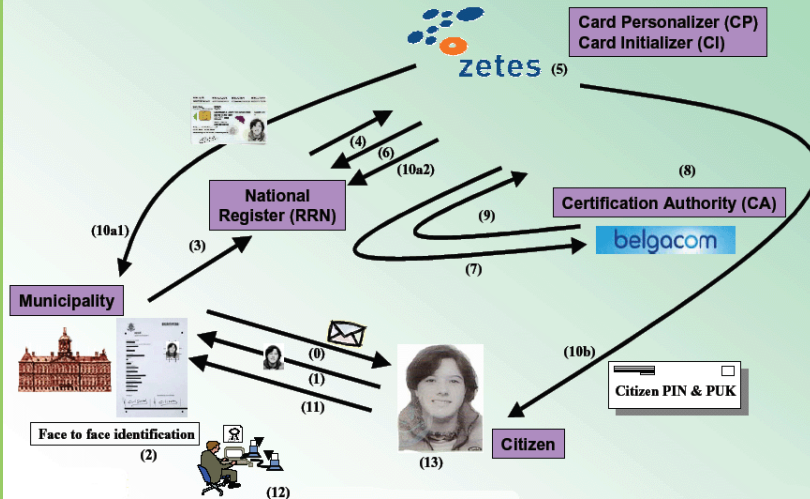
- PKCS#15 file system for ID applications
 - All eID-related data (certificates, photo, address, identity files,...)
 - No key management
- PKCS#11 standard interface to crypto tokens
 - Abstraction of signing functions (authentication, digital signatures)
 - Access to certificates
 - Available for Unix,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

Lecteurs

- 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 !)



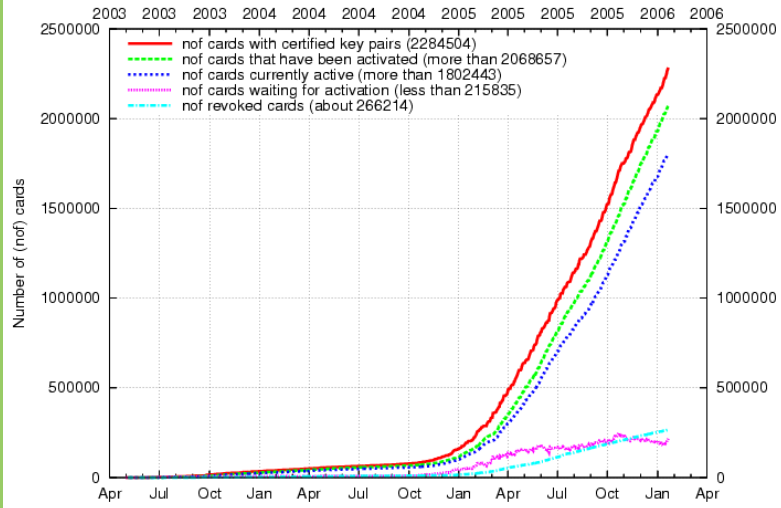
Processus de délivrance



- 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

Diffusion

Overview of all eID cards in the field



Graph generation: Sun Jan 22 22:00:40 2006. Source: <http://godot.be/eidgraphs>



Applications citoyennes



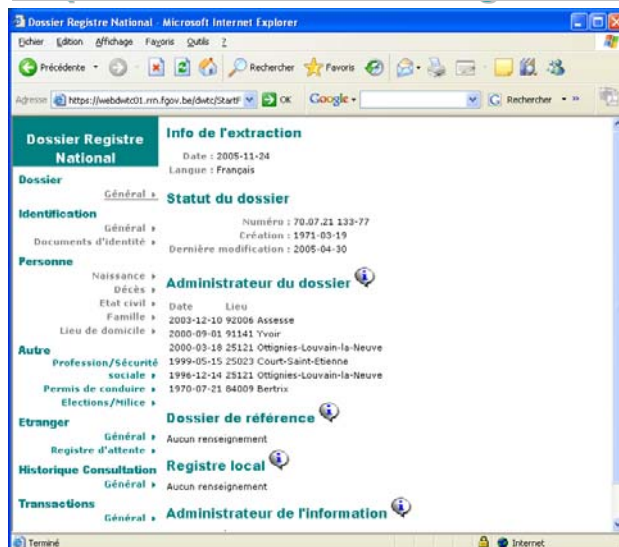
Aperçu des applications

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



Consultation du Registre National

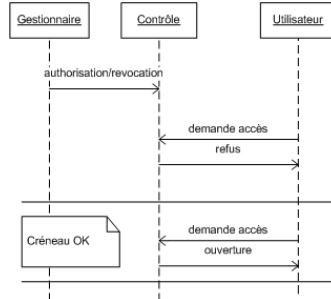
<https://mondossier.rn.fgov.be/>



Accès au dossier personnel + historique de consultation !

Contrôle d'accès physique à une infrastructure communale


- Exemples:
 - Parc à conteneur
 - 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



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: Mons



Page d'accueil

Rechercher: OK

Sommaire Vos élus E-Mail Abonnement Documents Agenda Liens Recherche Aide

Documents administratifs



- [Commande](#)
- [Mode d'emploi](#)

Commande


Commande de documents administratifs en ligne

Sélectionnez dans la liste ci-dessous le document que vous souhaitez commander :

<p>Documents "population"</p> <ul style="list-style-type: none"> • Composition de ménage • Certificat de domicile (extrait du registre de population ou des étrangers) • Certificat de nationalité 	<p>Important:</p> <p>La personne concernée par ces documents doit obligatoirement être inscrite dans les registres de la population ou des étrangers de Mons</p>
<p>Documents "Etat-civil"</p> <ul style="list-style-type: none"> • Copie ou extrait d'acte de naissance • Copie ou extrait d'acte de mariage • Copie ou extrait d'acte de divorce • Copie ou extrait d'acte de décès 	<p>Important:</p> <p>La personne concernée par ces documents doit obligatoirement être née, mariée ou décédée dans l'entité montoise.</p>



21

Exemple: Chaudfontaine



Commune de Chaudfontaine

Lignes de vie Organes communaux Services Documents et Formalités Règlements Organismes

Vous êtes ici : Citoyenneté : **Documents et Formalités**

Ajouter à mes favoris

Etape 3/3: Validation

Demande: [Composition de ménage](#)



Récapitulatif de votre commande (retour)

- Document de type **Composition de ménage**
- Motif mentionné : Elections
- Concerne : Le demandeur

Coordonnées du demandeur:

- Monsieur Ponsard Christophe
- 18, de Poilvache boîte A
- 5336 Assesse
- BE
- né le Mardi 21 Juillet 1970
- N° Registre National:700721-133-77
- Tel: 083/68 86.08
- Courriel: christophe.ponsard@gmail.com

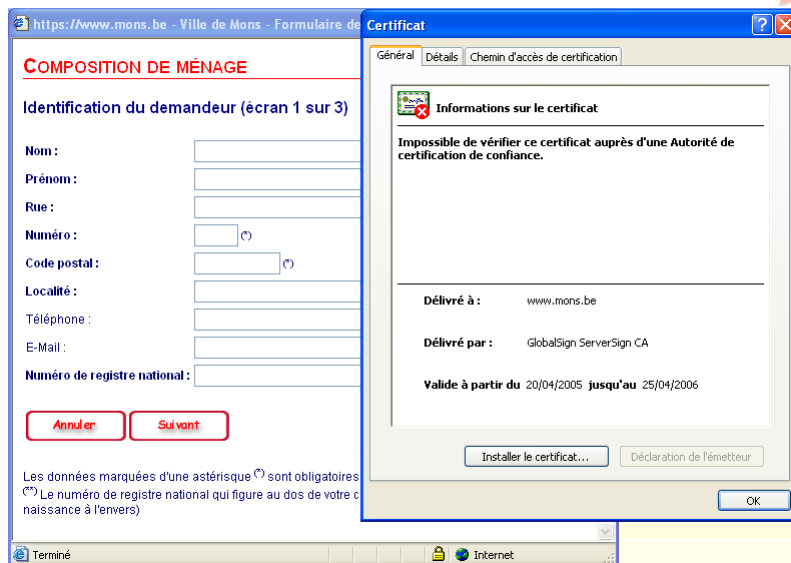
Envoyer ma commande



22

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

Authenticité du site communal





The screenshot shows a web browser window with the URL <https://www.mons.be>. The page title is "Ville de Mons - Formulaire de Certificat". The main content is a form titled "COMPOSITION DE MÉNAGE" with the sub-heading "Identification du demandeur (écran 1 sur 3)". The form contains several input fields: "Nom", "Prénom", "Rue", "Numéro", "Code postal", "Localité", "Téléphone", "E-Mail", and "Numéro de registre national". There are "Annuler" and "Suivant" buttons at the bottom of the form. Below the form, there is a note: "Les données marquées d'une astérisque * sont obligatoires" and "Le numéro de registre national qui figure au dos de votre carte de naissance à l'envers".

Overlaid on the browser window is a dialog box titled "Informations sur le certificat". It contains the following text: "Impossible de vérifier ce certificat auprès d'une Autorité de certification de confiance." Below this, it lists: "Délivré à : www.mons.be", "Délivré par : GlobalSign ServerSign CA", and "Valide à partir du 20/04/2005 jusqu'au 25/04/2006". At the bottom of the dialog box, there are buttons for "Installer le certificat...", "Déclaration de l'émetteur", and "OK".




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)






25



Application de « forum/chat » communal

- Forum thématique permettant de débattre de la vie de la commune en temps réel (chat) ou différé (forum)
- Avantages:
 - Restriction d'accès aux intéressés (membre de la commune) en écriture ou aussi en lecture
 - Authenticité: pas de fausse identité
 - Moyen supplémentaire de proximité
 - Permet de débattre de problèmes particuliers (PASH, travaux dans tel quartier,...)
 - Contact avec la « diaspora » communale
- Dangers:
 - Être trop restrictifs
=> mécanisme supplémentaire d'autorisation
 - Escalade des discussions à distance
=> modérateur, à coupler avec des réunions physiques

26

Chat avec authentification

The image displays the SaferChat website interface in a Mozilla Firefox browser. The main window shows the chat site with a sidebar menu and a central chat area. Overlaid on this are two windows: one for entering an eID card and another for entering a PIN to authenticate the user. A separate window shows the chat log with a welcome message and system notifications.

27

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

28

Quelques communes actives

- www.bornem.be
- www.borsbeek.be
- www.chaufontaine.be
- www.gent.be
- www.geraardsbergen.be
- www.jabbeke.be
- www.lasne.be
- www.leuven.be
- www.oln.be (Ottignies - Louvain-la-Neuve)
- www.oudenaarde.be
- www.seraing.be
- www.vilvoorde.be
- www.woluwe.be

Références générales sur l'eID

- Matériel:
 - <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/>
(microsoft « awareness »)
- Développement:
 - eID shop: <http://www.eid-shop.be>
 - GODOT's site: <http://www.godot.be/>
- Contrôle: certificats, valeur légale
 - <http://repository.eid.belgium.be/FR/index.html>
 - <http://www.stethonet.org/informatic/signature.htm>