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

eWish

27 Avril 2006

1

## 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:

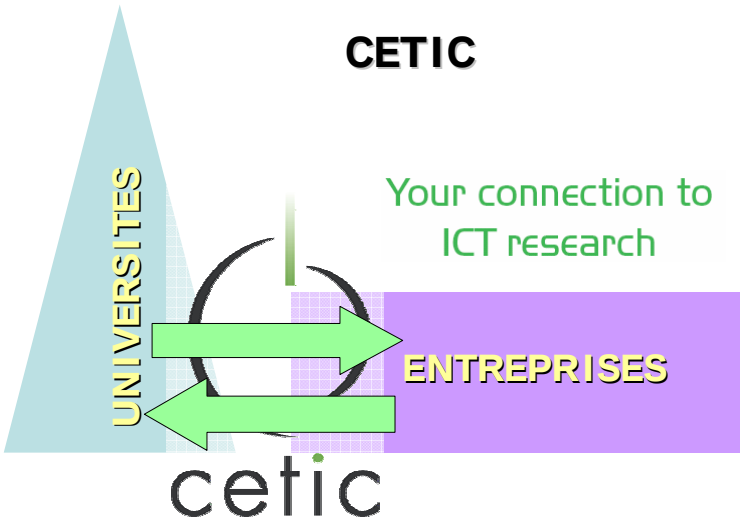
- + de 2 millions de cartes électroniques en circulation
- Où sont les applications ?

Focus de la présentation

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

2

## 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

# Présentation de l'eID (rappels)

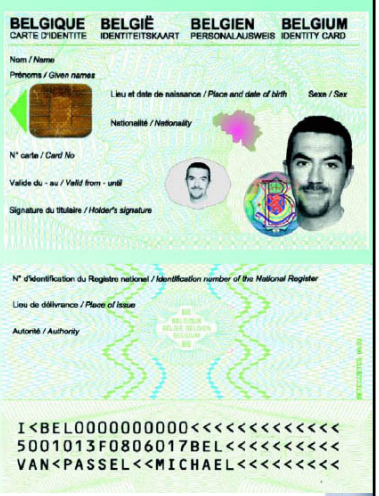
crédits à Danny De Cock de la KU Leuven
pour une large partie du matériel de cette section

5

# 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)

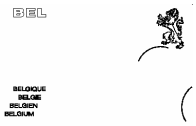



- Choix de conception: adresse pas écrite physiquement
  - Évite la réémission d'une carte à chaque changement d'adresse
  - Nécessite la présente d'un lecteur pour tous les contrôles officiels

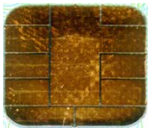
6

# Sécurité

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


- Electronique

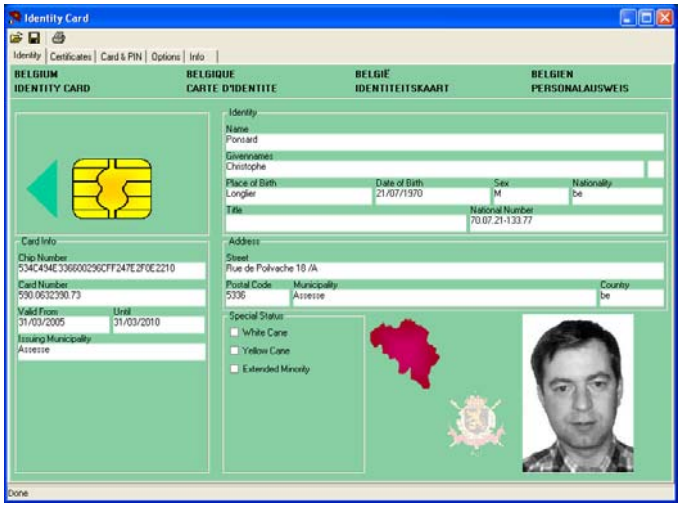


- SHA-1
- RSA
- SPA/DPA/… resistent
- EAL5+ certified
- …

7

# Contenu de la puce

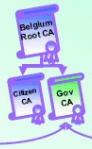
- Applicatif FEDICT (cf. démo)
- Lecteur: standard PC/SC (USB, PCMCIA…) largement supporté




8

## 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 → King, Prince, Count, Earl, Baron,…
    - Special status → No status, white cane (blind people), yellow cane (partially sighted people), extended minority, any combination
    - SHA-1 hash of citizen photo
  - Card-specific:
    - Card number
    - Validity's begin and end date
    - Card delivery municipality
    - Document type → Belgian citizen, European community citizen, non-European community citizen, bootstrap card, habilitation/machtigings card
- 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




9

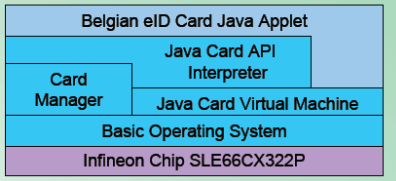
## Contenu PKI– clefs & certificats

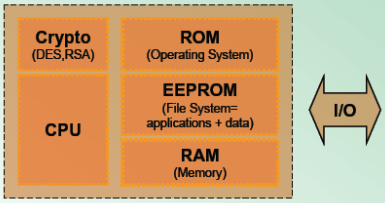
- 2 key pairs for the citizen:
  - Citizen-authentication
    - X.509v3 authentication certificate
  - Advanced electronic (non-repudiation) signature
    - X.509v3 qualified certificate
    - Can be used to produce digital signatures equivalent to handwritten signatures, cfr. European Directive 1999/93/EC
- 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

10

# Spécifications de la puce

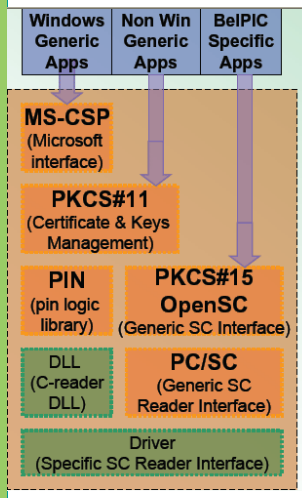
- Cryptoflex JavaCard 32K
  - CPU (processor): 16 bit Microcontroller
  - Crypto-processor:
    - 1100 bit Crypto-Engine (RSA computation)
    - 112 bit Crypto-Accelerator (DES computation)
  - ROM (OS): 136 kB (GEOS Java Virtual Machine)
  - EEPROM (Application + Data): 32 KB (Cristal Applet)
  - RAM (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)




11

# 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,…

12

# 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 !)

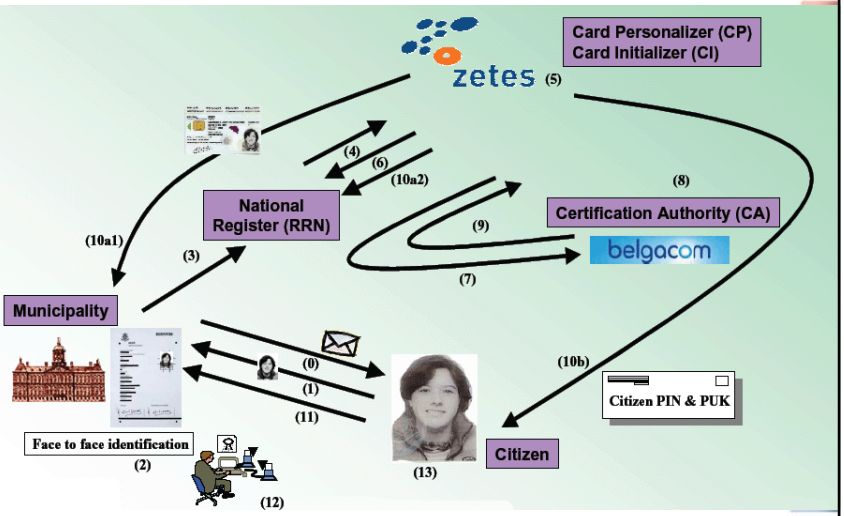


Do you trust this ?


And this ?

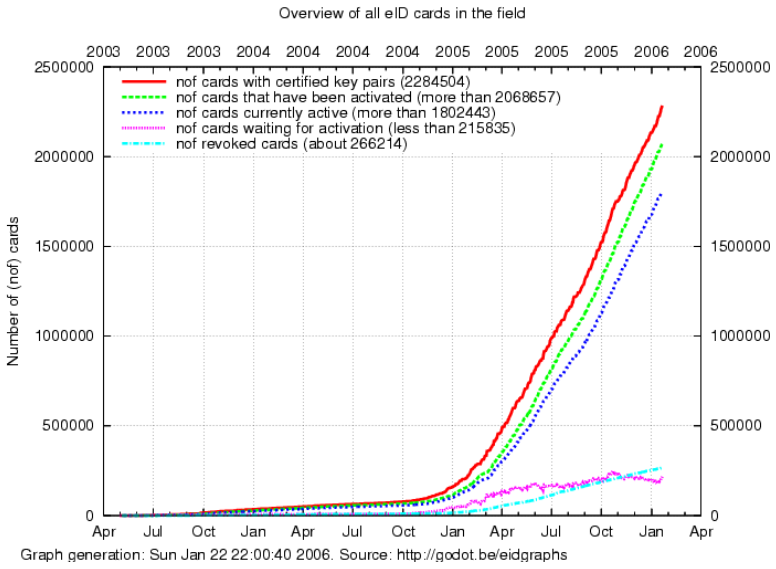


# Processus de délivrance




- 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




15

# Applications citoyennes

16

# Aperçu des applications

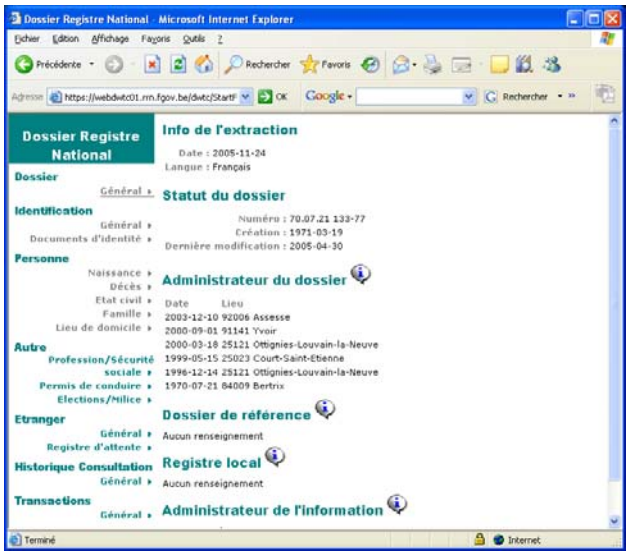
- Contrôle d'accès physique: parc à conteneurs, bibliothèque, police,…
- Authentification électronique: login sur une station de travail, SSH, SFT
- Signatures digitales: emails, fichiers PDF,…

- 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, …

17

# Consultation du Registre National

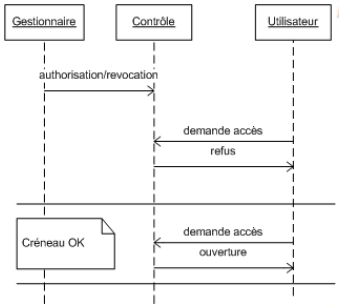
## https://mondossier.rrn.fgov.be/




Accès au dossier personnel + historique de consultation !

18

# 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

19

# 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

20

# Exemple: Mons


21

# Exemple: Chaudfontaine

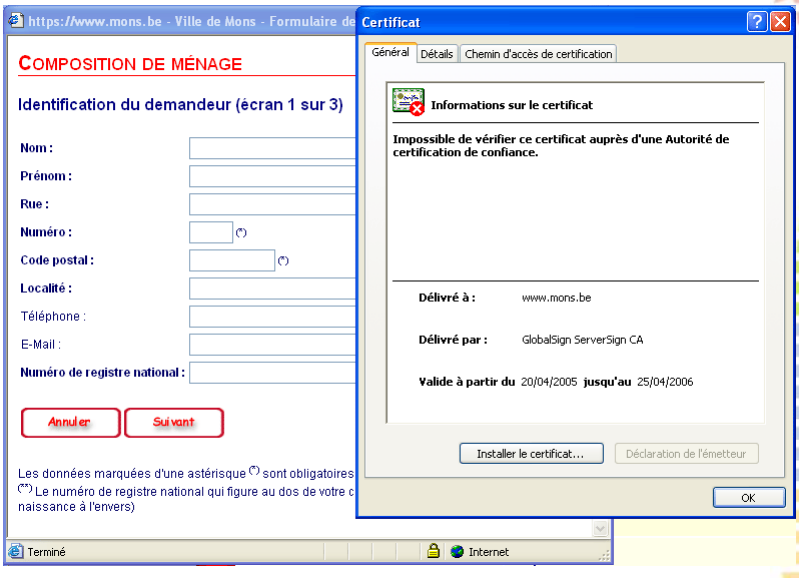

22

# 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

23

# Authenticité du site communal




24

# 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)

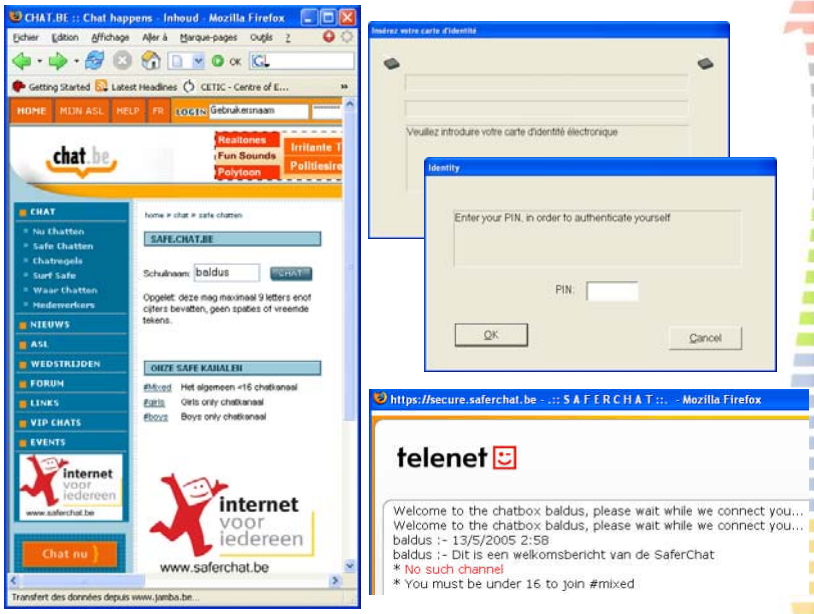
25

# 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




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.chaudfontaine.be
- www.gent.be
- www.geraardsbergen.be
- www.jabbeke.be
- www.lasne.be
- www.leuven.be
- www.olln.be (Ottignies - Louvain-la-Neuve)
- www.oudenaarde.be
- www.seraing.be
- www.vilvoorde.be
- www.woluwe.be

29

## 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

30