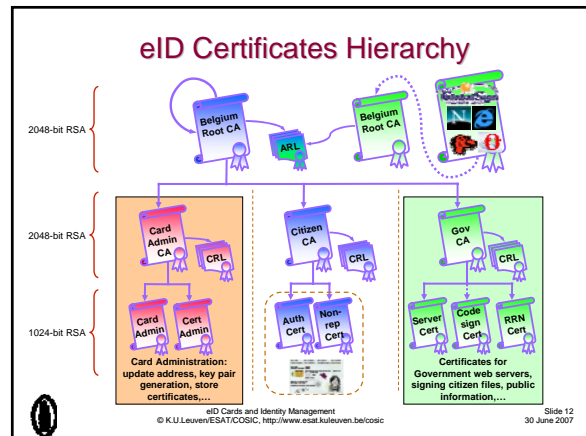
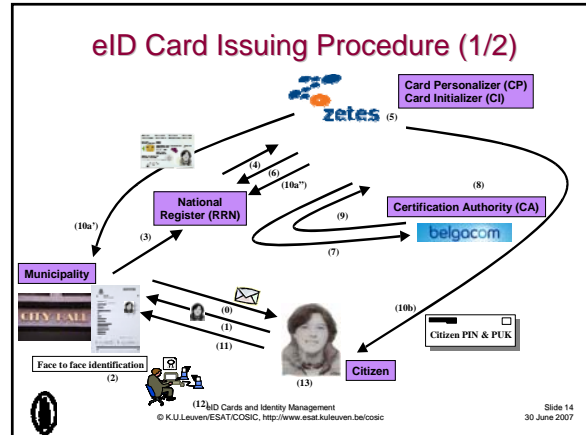
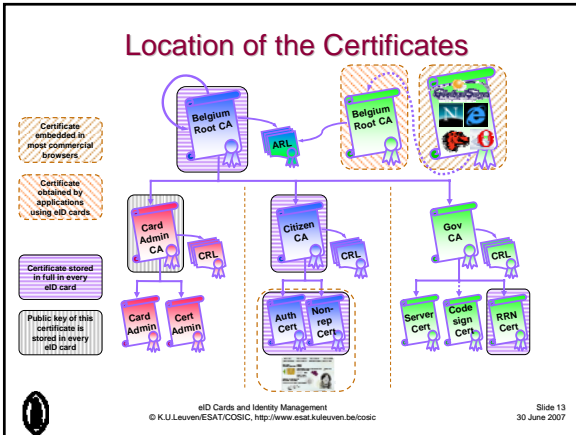


- ### PKI Content – Keys & Certificates
- 2 key pairs for the citizen:
 - Citizen-authentication
 - X.509v3 authentication certificate
 - Advanced electronic (non-repudiation) signature
 - X.509v3 qualified certificate
 - Can be used to produce digital signatures equivalent to handwritten signatures, 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
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic
Slide 10
30 June 2007

- ### Identity Files Content
- 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/machings card
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic
Slide 11
30 June 2007





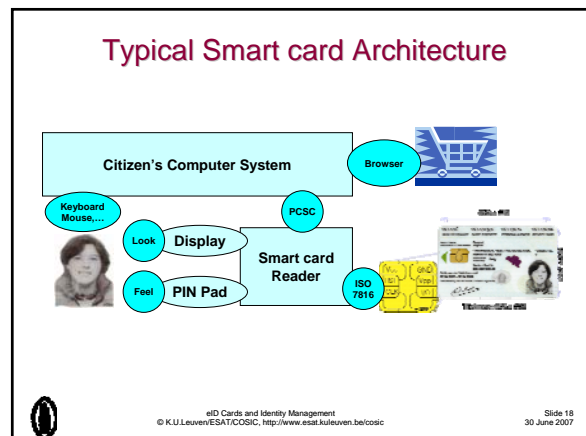
- ### eID Card Issuing Procedure (2/2)
- 0: Citizen receives a convocation letter or takes the initiative
 - 1: Visit municipality with photo
 - 2: Formal eID request is signed
 - 3,4: CP receives eID request via RRN
 - 5: CP prints new eID card, CI starts on-card key pairs generation
 - 6: RRN receives part of the eID card activation code PUK1
 - 7: CA receives certificate requests
 - 8: CA issues two new certificates and issues new CRLs
 - 9: CI stores these certificates on the eID card
 - 10a: CI writes citizen data (ID, address,...) to the card, deactivates the card
 - 10b: CI sends invitation letter with citizen's PIN and activation code PUK2
 - 11: Citizen receives invitation letter
 - 12: Civil servant starts eID card activation procedure
 - 13: eID card computes a signature with each private key, CA removes certificates from CRL
- © K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic> Slide 15 30 June 2007

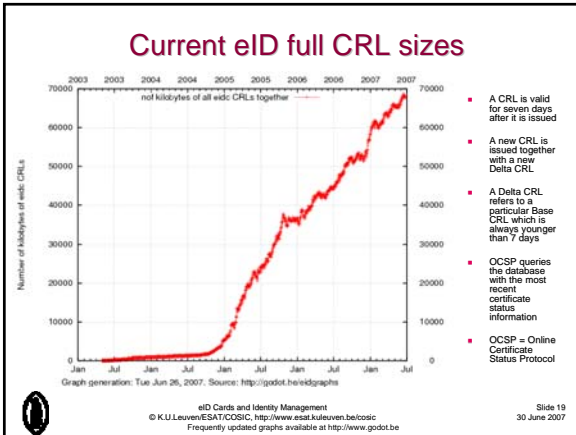
Citizen Certificate Details

Citizen Qualified certificate (~1000 bytes)	Citizen Authentication certificate (~980 bytes)
Version: 3 (0x2) Serial Number: 10:00:00:00:00:8d:8a:fa:33:d3:08:f1:7a:35:a2 Signature Algorithm: sha1WithRSAEncryption (1024 bit) Issuer: C=BE, CN=Citizen CA, SN=200501 Not valid before: Apr 2 22:41:00 2005 GMT Not valid after: Apr 2 22:41:00 2010 GMT Subject: C=BE, CN=Sophie Dupont (Signature), SN=Dupont, GN=Sophie Nicole, SerialNumber=60050100093 Subject Public Key Info: RSA Public Key (Modulus (1024 bit): 4b:e5:7e:6e: ...:86:17, Exponent: 65537 (0x10001)) Certificate Policies: Policy: 2.16.56.1.1.2.1 CPS: http://repository.esat.belgium.be Key Usage: critical, Non Repudiation Authority Key Identifier: [D1:13 ... :7FAF-10] CRL Distribution Points: URIs: http://crl.esat.belgium.be/crl/002.crl Netscape Cert Type: S/MIME Authority Information Access: CA Issuers - http://crl.esat.belgium.be/crl/002.crl OCSP - http://ocsp.esat.belgium.be Qualified certificate statements: [00...:F...] Signature: [74:ae:10: ... :e0:91]	Version: 3 (0x2) Serial Number: 10:00:00:00:00:0a:5d:9a:91:b1:21:d8:00:a2:7a Signature Algorithm: sha1WithRSAEncryption (1024 bit) Issuer: C=BE, CN=Citizen CA, SN=200501 Not valid before: Apr 2 22:40:52 2005 GMT Not valid after: Apr 2 22:40:52 2010 GMT Subject: C=BE, CN=Sophie Dupont (Authentication), SN=Dupont, GN=Sophie Nicole, SerialNumber=60050100093 Subject Public Key Info: RSA Public Key (Modulus (1024 bit): cf:ca:7a:77: ...:5c:d5, Exponent: 65537 (0x10001)) Certificate Policies: Policy: 2.16.56.1.1.2.2 CPS: http://repository.esat.belgium.be Key Usage: critical, Digital Signature Authority Key Identifier: [D1:13 ... :7FAF-10] CRL Distribution Points: URIs: http://crl.esat.belgium.be/crl/002.crl Netscape Cert Type: SSL Client, S/MIME Authority Information Access: CA Issuers - http://crl.esat.belgium.be/crl/002.crl OCSP - http://ocsp.esat.belgium.be Signature: [10:ac:04: ... :e9:04]

© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic> Slide 16 30 June 2007

- ### eID Card Applications
- eGovernment**
 - Official document requests
 - Marital status, Birth certificate,...
 - Access to RRN database
 - eTax**
 - Tax form declaration + consultation
 - VAT declaration
 - eJustice**
 - Electronic submission of conclusions in court cases
 - eAccess**
 - Client authentication for web servers
 - Secure chat for 12-16 year
 - Access control, e.g., container park, library, swimming pool,...
 - eMove**
 - Water invoices
 - Energy contracts
 - eLogin**
 - Windows Glna, Vista, Citrix
 - eCommerce**
 - Online opening of new account
 - Digital Rights Management
 - Qualified signature
 - Contract signing
 - eBanking**
 - Online mortgage request
 - eMail**
 - Registered mail
 - Authenticated email
 - eWork**
 - Time registration
 - eAdministration**
 - Data capture
 - Car matriculation registration
 - Signing eForms
 - Signing PDFs
 - eHealth**
 - Access to patient file
 - Insurance card
- © K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic> Slide 17 30 June 2007





Validation = complex

- Digital Signature**
 - Valid
 - Invalid
- eID Card (Signature Creation Device)**
 - Valid
 - Invalid
 - Suspended
 - Revoked
 - Expired
- CRL, OCSP Response**
 - Valid
 - Invalid
 - Expired
- Certificate**
 - Valid
 - Invalid
 - Suspended
 - Revoked
 - Expired
 - Unknown

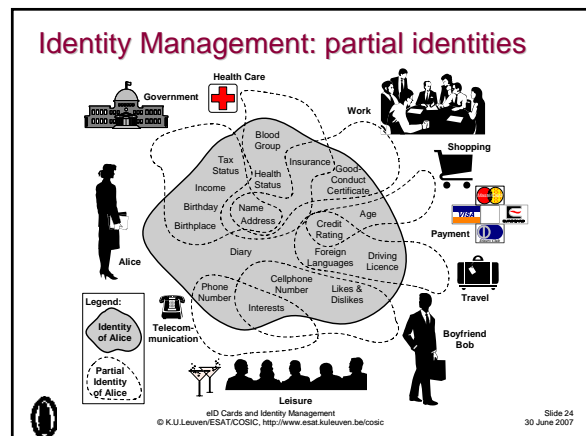
eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 20
30 June 2007

- ### Issues and challenges
- key generation on the card
 - no email address in certificate
 - different PIN for entity authentication and signing
 - RSA PKCS#1 1.5 versus 2.0
 - avoid storage of information on the card
 - encryption/decryption: need private decryption key back-up
 - 20% of first PIN mailers lost
 - certification of card readers
 - certification of smart cards (common criteria)
 - certification of middleware and applications
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>
- Slide 21
30 June 2007

- ### Round-up: Belgian eID card
- big challenge: multiple parties and interfaces
 - 4.5 years for planning and try-out
 - 4.5 years for the roll-out
 - 10% of population is special case
 - critical issues: education and awareness, applications, card readers and middleware
 - it's not about the card
 - can be an enabler: e-government and more
 - privacy concerns about unique ID
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>
- Slide 22
30 June 2007

- ### Outline
- the Belgian eID card
 - identity and identity management
 - eID cards worldwide
 - interoperability
 - concluding comments
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>
- Slide 23
30 June 2007



Identity: definitions (1)

- **attributes:** distinct & measurable properties belonging to a particular entity
- **identity:** dynamic collection of all of the entity's attributes (1 entity: 1 identity)
- **partial identities:** specific subset of relevant attributes
- **identifier:** attribute or set of attributes of an entity which uniquely identifies the entity in a given context
- **entity authentication or identification:** using claimed or observed attributes of an entity to distinguish the entity in a given **context** from other entities it interacts with



Identity: definitions (2)

- **credential:** piece of information attached to an entity and attesting to the integrity of certain stated facts
- **registration:** process in which a **partial identity** is assigned to an entity and the entity is granted a means by which it can be authenticated in the future
- **federated identity:** credential of an entity that links an entity's partial identity in one **context** to an entity's partial identity in another **context**
- **authorization:** the permission of an authenticated entity to perform a defined action

!! these definitions reflect a specific vision on identity and identity management

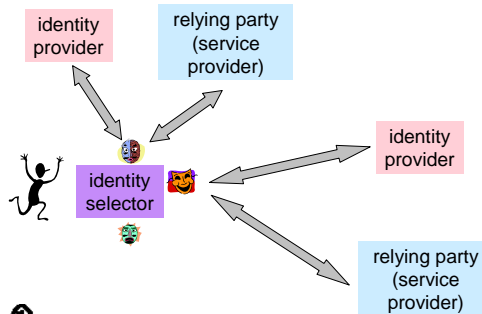


Identity: principles "laws" [Kim Cameron, Microsoft]

1. user control and consent
2. minimal disclosure of information for a constrained use
3. disclosure limited to justifiable parties
4. directed identities: omni-directional and uni-directional
5. open – operators and technologies
6. human integration
7. consistent experience across contexts



Identity management: roles (identity meta-system)



Identity management: business

- too many identities in enterprise, identity problem on the Internet
- need for distributed identification, authentication & authorization across boundaries
- Liberty Alliance: identity service for web
 - emphasis on convenience (single sign on)
 - federation = linking/binding of (partial) identities
 - relies in a critical way on identity provider
 - problem with collusion between service providers
- Microsoft WS.-* CardSpace (f.k.a. InfoCard)
 - Passport was not the correct approach for broad applications
- IBM Higgins (open source version CardSpace)
- OATH
- TLS federation



Federated identity management

- standards
 - token (WS-*, X.509, SAML)
 - profile and services (WS-*, Liberty, SAML)
 - policy and management (WS-*, SAML, XACML)
 - HTTP/TLS
- contracts
 - strength of (entity) authentication
 - privacy
 - certificates and liability
- technology
 - credentials (tokens)
 - federation service (issuing and validating tokens)
 - identity selector



Identity management has many dimensions

.... so it's not sufficient to add an "identity layer" to the Internet

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 31
30 June 2007

Identity management for e-Government

- specific requirements: security, scale, legislation
 - do not copy business solution
- need for federation
 - national
 - regional (states, territory)
 - city
 - international?
 - government sector: tax, social security, health, traffic, voting
 - contexts: government, finance, insurance, public transport
- can this investment be reused by private sector?
 - citizen has 1.5 eGovernment interactions per year on average
- tension: citizen needs versus industry push

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 32
30 June 2007

Identity Management Meta-Framework

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 33
30 June 2007

Outline

- the Belgian eID card
- identity and identity management
- eID cards worldwide
- interoperability
- concluding comments

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 34
30 June 2007

eID cards worldwide

- ID cards in most countries
 - compulsory in 100 countries
 - no ID cards in Australia, Canada, Denmark, Ireland, Latvia, Lithuania, USA
- sensitive topic
 - war, religion, race, insurgents
 - Big Brother
- many countries are rolling out or planning eID cards
- Germany: plans for eID card, health card and job card

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 35
30 June 2007

EU development Nov '06

Austria	16 M		
Belgium	4 M		
Estonia	1.1 M		
Finland	100 K		
Italy	2 M+9.3M		
Spain	300 K		
Sweden	130 K		

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 36
30 June 2007

Status (June 2006) eID card – no eID card

Conceptual/design	Development/roll-out	Update/review	Consolidation
Cyprus	Germany	The Netherlands	Austria
Czech Republic	Latvia	France	Belgium
Greece	Lithuania	Ireland	Denmark
Hungary	Portugal	Malta	Estonia
Luxembourg	United Kingdom	Slovenia	Finland
Poland			Italy
Slovakia			Spain
			Sweden

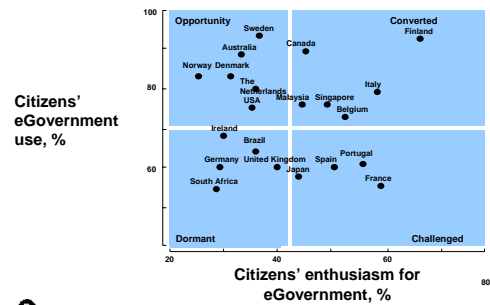
Other issues: private sector involvement, biometrics, local services

See <https://www.cosic.esat.kuleuven.be/modinidm/twiki/bin/view.cgi/Main/NationalProfiles>

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 37
30 June 2007

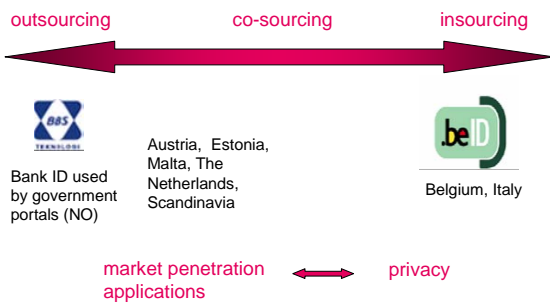
Accenture (2006)



Jaana Kaakola, Prime Minister's Office (source: Accenture)
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 38
16.6.2006

Public/private sector



eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 39
30 June 2007

The challenge...



Slide 40
30 June 2007

Federation

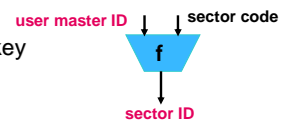
- global unique identifiers: Belgium, Czech Republic, Hong Kong, Ireland, Luxembourg, UK ...
 - illegal in some countries
- identifier per context: the Netherlands (?)
- identifier per sector: Austria, France
- one central database with "all" information: UK
- use of separate databases with controlled linking: Belgium
- very limited central storage: Germany
- use of cryptographic credentials (minimal disclosure)

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 41
30 June 2007

Privacy Enhancing Mechanisms

- Pseudonyms
 - but still 1 public key
- Chaum credentials [Brands, Camenisch-Lysanskaya]
 - can prove in ZK possession of digital signature (certificate)
 - can prove Boolean assertions on data without leaking any additional information (e.g., older than 18)



eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 42
30 June 2007

Smart cards

- smart cards: Austria, Belgium, Finland, France, Spain, UK, Estonia, Italy,...
 - also mobile: Austria
 - no smart card: Bosnia
-
- standardized solution
 - can be easier to deploy nationally/cross-border
 - varying public perception of conventional ID cards and smart cards
 - less flexible



Biometrics

- biometrics (other than photo): Brazil, France, Hong Kong, Italy, Korea, Malaysia, Oman, Spain, UK
 - note: 2 fingerprints needed for ICAO compliant passports
 - fingerprint removed in Greece (2002)
- may enable to detect duplicate registrations
- may offer better security
- but also security and privacy risks particularly if central database



Other criteria

- mobile solutions
- contact or contactless?
- inclusion of non-nationals
- e-vault
- other applications: e-health, payment, driving's license, public transport, passport: Malaysia

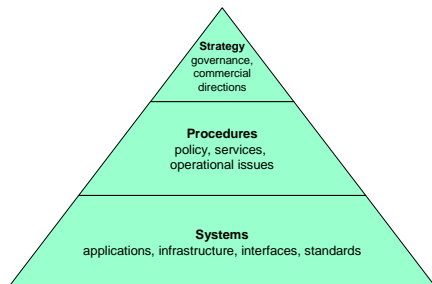


Outline

- the Belgian eID card
- identity and identity management
- eID cards worldwide
- interoperability
- concluding comments



Interoperability



Challenges/barriers (IPTS study – Hyperion)

- **Socio-cultural:** history, information asymmetry and brands, privacy and sharing, e-inclusion
- **Technical:** standards, legacy, usability, technical interoperability
- **Market:** semantic understanding, inertia and incumbents, initial investment and transaction costs, complexity
- **Legal:** e-signature, diversity, liability



eIDM Roadmap: first steps

- Interoperable eIDM in public services was identified as a policy priority in the eGovernment action plan, adopted by the Commission on 25 April 2006
- Member States signed up to an 'eID Timeline' in the so-called 'Signpost towards eGovernment 2010' paper:

"a pan-European eIDM framework that would allow citizens, businesses and administrations to identify and authenticate themselves in a variety of eGovernment applications, [with a view of offering] **secure means of electronic identification** that maximise user convenience while respecting data protection regulations"

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic

Slide 49
30 June 2007

eIDM Roadmap: goals

Meeting this timeline will be very challenging

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic

Slide 50
30 June 2007

The Porvoo Group
international cooperative network
meets twice per year since April 2002

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic

Slide 51
30 June 2007

CEN 15264 e-Authentication
Architecture for a European interoperable eID system within a smart card infrastructure – April 2005

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic

Slide 52
30 June 2007

CEN 15264 e-authentication

- Part 1: Architecture for a European interoperable eID system within a smart card infrastructure [61pp]
- Part 2: Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services [49pp]
 - Privacy: code of conduct – 5 pages
- Part 3 User Requirements for a European interoperable eID system within a smart card infrastructure [49pp]
 - The cardholder needs to feel safe and with a sufficient degree of **privacy** relevant to the transaction. For example, for a cash transaction or account enquiry the cardholder would want a more secure area free of distractions and **with a supportive ambiance so that the PIN entry cannot be overseen by a "shoulder surfer"**, free of distractions with a supportive ambiance. In a public place, the interaction between the machine and the User should be easily learned, simple and clear as some people will be unwilling to experiment or be seen to fail to operate the equipment in public.

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic

Slide 53
30 June 2007

CEN TC224 WG15:
CEN 15480 European Citizen Card ('07-'08)

- Complete smart card specification, covering physical, electrical and security services
- Middleware specification of implementation
- Card profiles around a main service (ICAO traveling card, National ID card, e-Government card)

CEN CWA 14890 (eSign)

eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, http://www.esat.kuleuven.be/cosic

Slide 54
30 June 2007

Outline

- the Belgian eID card
- identity and identity management
- eID cards worldwide
- interoperability
- **concluding comments**



Digital signatures

- still rarely used for signing transactions
- common infrastructure can help
- security level for *generic* digital signature needs to be very high
- legislation (e.g., EU '99 Directive) has increased complexity

- **research: delegation and revocation mechanisms for complex settings**



Privacy

- Privacy
 - Digital signature (1975)
 - Digital certificate (1978)
 - Privacy at network layer (1981)
 - Privacy protecting credentials (1985)
- Individual is losing control
 - Profiling, behavioral targeting, social sorting, dynamic pricing, blacklists, constant surveillance, data-veillance,...
- eID can make it worse
 - unique identifiers used over broad range of applications
 - central database with biometrics
- eID can also be privacy-enhancing tool
 - implement Chaum credentials
- **privacy requires an integrated approach at all layers**
- **research: bring the concepts to applications**



Biometrics

- main drive: law enforcement and e-passports
 - fingerprint is better for forensics than for one-to-many identification
 - not scientifically tested with opponent model as defined in cryptology/security
- ok:
 - local verification and template storage
 - derive key from biometrics (fuzzy key derivation)
 - duplicate matching with fuzzy one-way function
- very risky:
 - central database
 - massive matching for duplicates
 - RFID implants
- **research: integrate biometry with cryptology**



Back to basics: goals

- what are we trying to achieve?
 - cost savings (hard to evaluate)
 - better service (faster, more user-friendly)
 - reduce identity theft
 - bridge digital divide
 - more privacy
 - global interoperability with many applications
 - fraud prevention
 - reduce illegal immigration and terrorism
- set realistic goals
- technology will change yet time scale of any deployment is 6-10 years



The future

- eID could be a virtual concept
 - so it may not need to be carried at all times – or it's there all the time
 - it's not about the card (or the number), it's about the system
 - what about eID in second life?
- couple it to e-passports
- technology can help (**but ignored by 2007 standards**)
 - Chaum-type credentials could make a useful tool to strengthen privacy
 - biometry could be used in a privacy-enhancing way
- ... but it needs to be carefully aligned with view and needs of society
 - need informed public debate
 - balancing interests of citizen, government(s), private companies
 - slow political change (slower than business/social/technology)



The future (2)

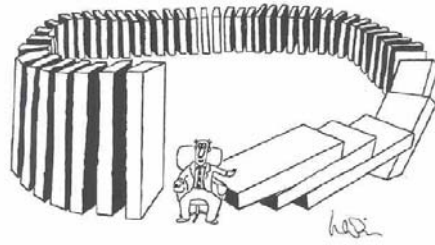
- Designing and deploying a national infrastructure takes 8-10 years
- What will the world look like in 2016?
 - 1 Terabyte of data generated per citizen and per year
 - 4 Terabyte flash drives (a few hundred movies)
 - thousands of CPUs per citizen (RFID)
 - Integration of computers and networks with human body



eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 61
30 June 2007

Get eID right from the start or...



Thank you for your attention.
¡Gracias!



eID Cards
© K.U.Leuven/ESAT/COSIC

Some information sources

- Roadmap http://europa.eu.int/information_society/activities/egovm/ent_research/index_en.htm
- Modinis Study on Identity Management in eGovernment: <https://www.cosic.esat.kuleuven.be/modinis-idm/>
- Advanced Applications for Electronic ID cards <https://www.cosic.esat.kuleuven.be/adapid/>
- PRIME: Privacy and Identity Management for Europe <http://www.prime-project.eu/>
- FIDIS: Future of Identity in the Information Society: <http://www.fidis.net/>
- GUIDE: Government User Identity for Europe: <http://istrg.som.surrey.ac.uk/projects/guide/>



eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 63
30 June 2007

Some information sources

- Liberty Alliance <http://www.projectliberty.org/>
- Infocard <http://msdn.microsoft.com/winfx/reference/infocard/default.aspx>
- Higgins <http://www.eclipse.org/higgins/>
- UK <http://www.identitycards.gov.uk>
- LSE: the identity project: <http://is.lse.ac.uk/idcard>



eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 64
30 June 2007

Belgium eID links

Belgian eID card information on the Internet

- <http://eid.belgium.be>
- <http://www.nriksregister.fgov.be>
- <http://www.fedict.be>
- <http://www.belgium.be>
- <http://www.cardreaders.be>

Test cards can be ordered at

- <http://www.eid-shop.be>



Source code examples are available at

- http://www.belgium.be/zip/middleware_source_code_nl.html
- http://www.belgium.be/zip/middleware_source_code_fr.html

Portal (Danny De Cock) <http://godot.be>  keywords: "godot eID"

- Yourself <https://www.mijn dossier.rm.fgov.be>
<https://www.mondossier.rm.fgov.be>
<https://www.meindossier.rm.fgov.be>



eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

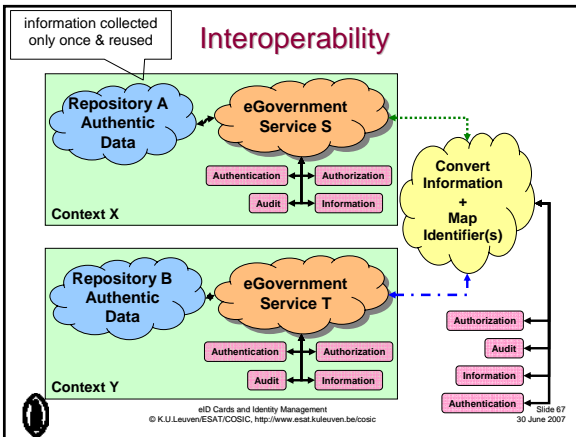
Slide 65
30 June 2007

Backup slides



eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic>

Slide 66
30 June 2007



- ## Technical interoperability challenges
- Lack of common standard
 - Temporary character of most solutions
 - technical choices are typically “medium term”
 - Middleware
 - Management of authorizations
 - even harder in a cross-border context
 - Mapping of partial identities?
 - Free choice of tokens
 - an eID is not equal to a token
 - not everyone wants to use smart cards (only)
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic> Slide 68
30 June 2007

- ## Organizational interoperability challenges
- Multitude of digital identities and attributes
 - Reliability and trust
 - The issues of **delegation/representation**
 - How to model and manage this?
 - Possible conflict between technology and socio-cultural and historical background
 - Inertia w.r.t. local choices
 - Public perception: useful, easy-to-use, privacy
 - Lack of common terminology
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic> Slide 69
30 June 2007

- ## Legal interoperability challenges
- Availability and use of one or more unique identifiers
 - Mismatch between technical/legal concepts
 - E.g. mandates
 - Diversity of legal frameworks vs. the need for technical interoperability
 - eID and European legal competence
 - Article 18.3 of the EC Treaty: no ID cards, residence permits, social security cards...
 - Federation and the law
 - Core concept: circles of trust. However, the law doesn't “trust”...
 - Varying attention to privacy issues
 - ID cards, data exchange or access...
 - Respect socio-cultural backgrounds
- eID Cards and Identity Management
© K.U.Leuven/ESAT/COSIC, <http://www.esat.kuleuven.be/cosic> Slide 70
30 June 2007