



Security and Interoperability

Danny De Cock
January 16th, 2012
Moldova

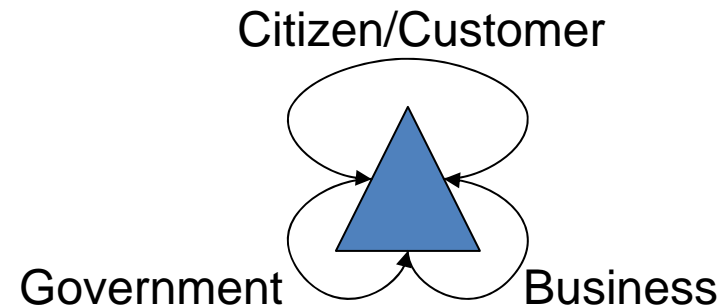
E-mail: Danny.DeCock@esat.kuleuven.be

Slides: godot.be/slides



Secrets of Successful eID Environments

- 3 High-level actors
- Different sectors
 - eGovernment
 - Collect and store data once, reuse where possible
 - eHealth
 - Make patient records available to health care service providers
 - eCommerce & eBusiness
 - Provide ability to correctly identify involved parties
 - Avoiding online fraud, preparing effective anti-spam measures





Secrets of Successful eID Environments

- Success depends on joined forces of public and private sector
 - Private sector requires return on investment (ROI)
 - Number of contacts between a citizen and its eGovernment only does not justify huge investments
 - Public sector prefers eID enablers for use in public **and** private sector
- Avoid reinventing the wheel
 - Need to exchange of experience with successes and ***failures***
 - Risk of lacking focus to create interoperable solutions
 - Caveat: Systems focusing on any single sector are inherently incompatible with ***similar*** systems



Design Decisions – Basic Concepts

- Federated architecture
 - Each sector operates autonomously
 - Interfaces with other sectors through bus system
- Built around authoritative sources
 - Master copy of data is available at exactly one repository
 - Master copy = authoritative source
- Maximal reuse of information
 - No data replication
 - Administrations cannot re-request data already available
- Integrated system for user and access management
 - eID for all – Citizens & organizations
 - Autonomous management of access & use policies



Design Decisions – Benefits

- Guaranteed interoperability enhances security!
 - Modularity respects each organization's sovereignty
 - Prevents vendor-lock-in
 - Exchanging information using standard and open protocols and data formats
- Guaranteed flexibility
 - Modularity allows updating and following
 - Security standards
 - Good/best practices



Identification & Authentication

- Unique identification of
 - Citizens
 - Professionals
 - Companies and other Service Providers (public and private sector)
- eID for all: Authentication & Identification tokens
 - Federal token
 - eID card – Belgian citizens & foreigners
 - Other tokens – companies, organizations, individuals



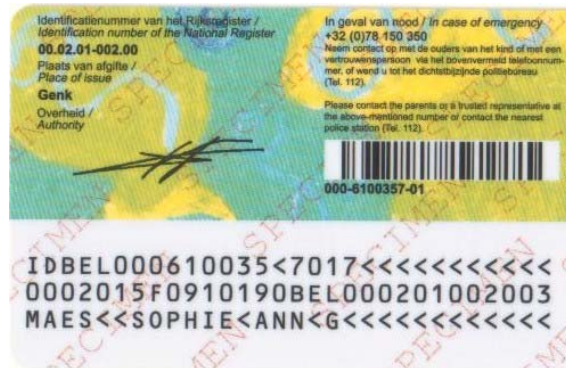
eID Card Types

Citizens



eID card

Kids



Kids-ID

Aliens



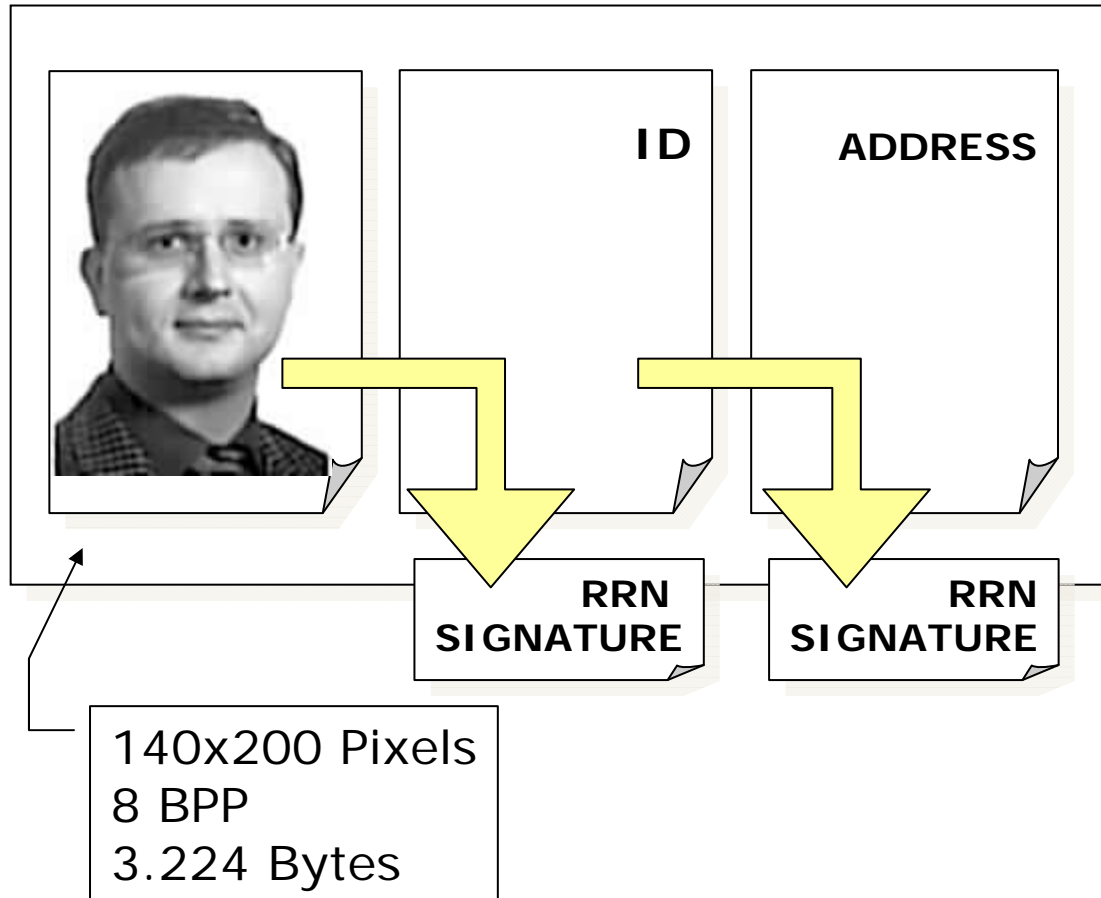
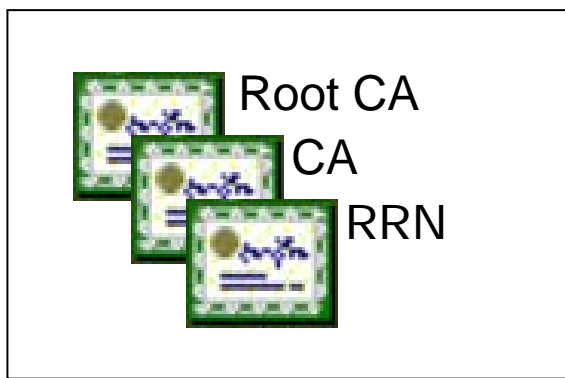
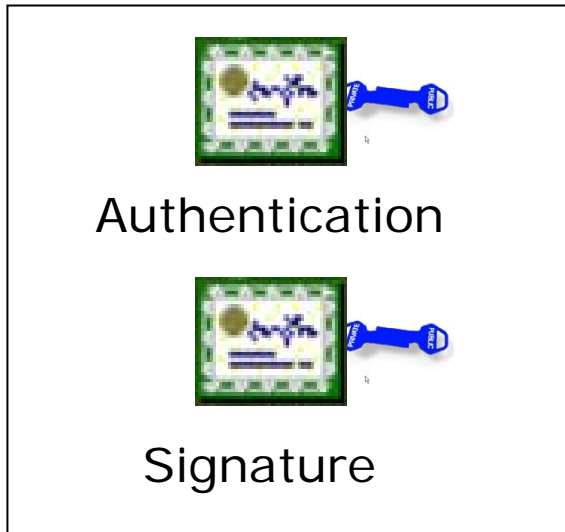
Foreigners' card



eID Card Content

PKI

Citizen Identity Data



RRN = National Register



eID Card = 4 Functions

- Non-electronic
 1. Visible Identification of a person
- Electronic
 2. Digital identification
 - Data capture
 3. Prove your identity
 - Authentication signature
 4. Digitally sign information
 - Non-repudiation signature

**Enabler of
eServices**

eFunctionality



Levels of Assurance (LoA) of Authentication

- Federated identity management model
 - E.g., Shibboleth, Liberty Alliance, CardSpace...

LoA 4+ (qualified plus biometric)	Setting access policies
LoA 4 (qualified cert with smart card EAL4+)	Sensitive medical records (e.g. HIV), Consultant notes containing opinions. Ability to Break the Glass. Bank to bank transfers
LoA 3 (2-factor authentication, non-qualified cert, EAL4 smart card)	Patient confidential records (non- sensitive)
LoA 2 (one time password)	Some Internet banking applications System administration
LoA 1 (uid/password, Verisign Class 1 cert)	Retrieve degree certificate. Completing public service employment application
LoA 0 (no authentication)	Public data



eID – Level 3 + 4

BELGIË	BELGIQUE	BELGIEN	BELGIUM
IDENTITEITSKAART	CARTE D'IDENTITE	PERSONAL AUSWEIS	IDENTITY CARD

Naam / Name Voornamen / Given names	Dupont Leila Sofie	
 	Geboorteplaats en -datum / Place and date of birth Brussel 01 JAN 1972	Geslacht / Sex V
	Nationaliteit / Nationality Belg	
	Kaartnr. / Card No 590-1234567-89	
Geldig van - tot / Valid from - until 01.04.2003 - 01.04.2013		
Handtekening van de houder / Holder's signature		



Citizen's Federal Token – Level 2

.be **BURGERS**

Anne Dupont

www.belgium.be

1. YUFIQA	9. NEVAHI	17. SAYIWU
2. LEBOXA	10. CIHISO	18. JEPIBU
3. DOWEJO	11. DANIFE	19. HUGEFU
4. YUTOHE	12. KEFUQE	20. XIZUGA
5. QASEWO	13. YATIVU	21. CIZEXA
6. BIWUDA	14. WIYAWO	22. BOVOZU
7. XUQUNO	15. POMUZA	23. KAPESE
8. BIYUNA	16. XIREWO	24. BANULI



How to Choose a Security Level?

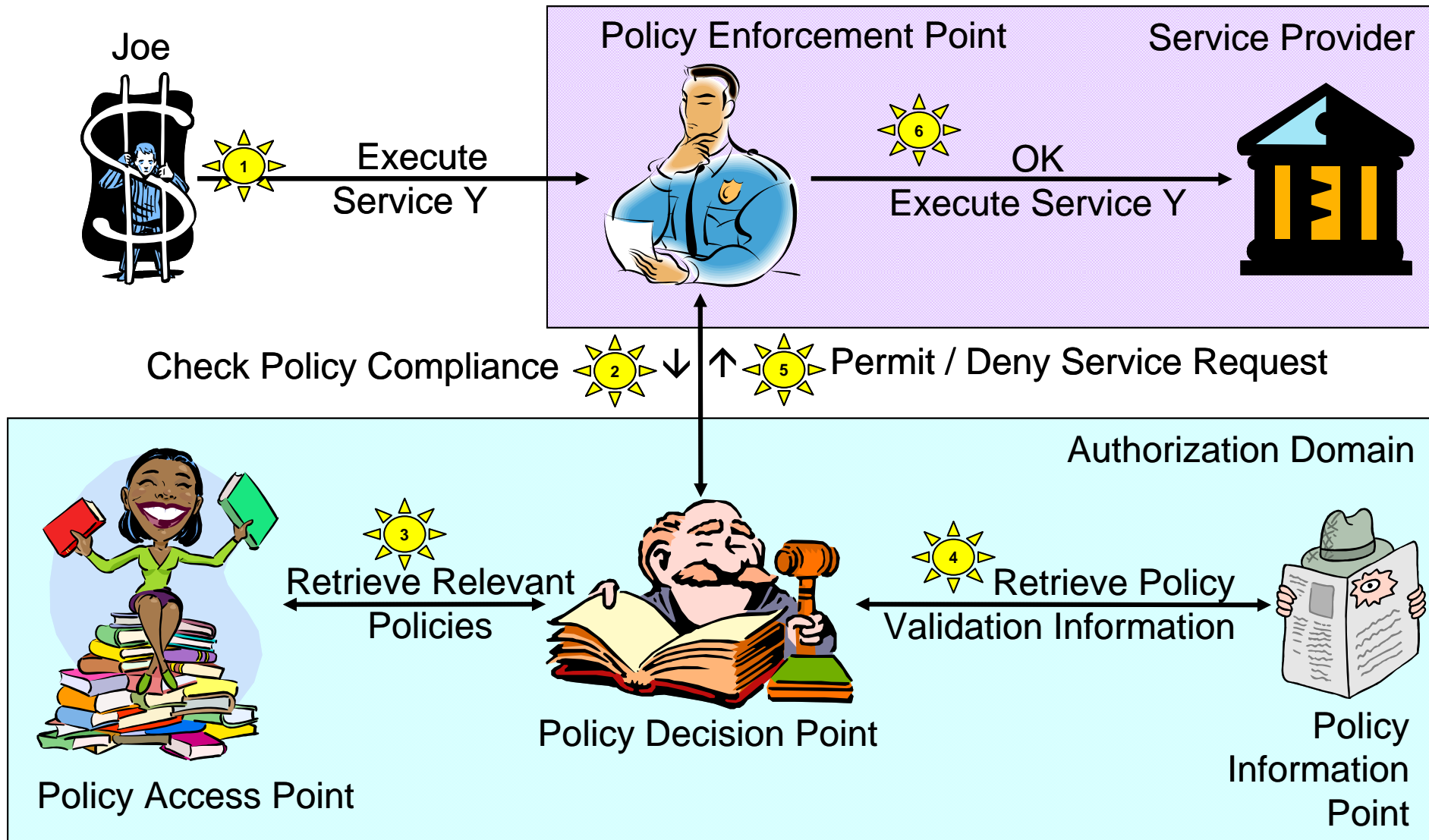
- Responsibility of the service provider under supervision of the Privacy Commission
- Based on **risk assessment** and depending on
 - Type of processing: communication, consultation, alteration,...
 - Scope of the service: does the processing only concern the user or also concern other persons ?
 - Degree of sensitivity of the data processed
 - Possible impact of the processing
- In addition to right security level
 - Use of an electronic & time-stamped signature might be needed



Interoperable & Secure by Design

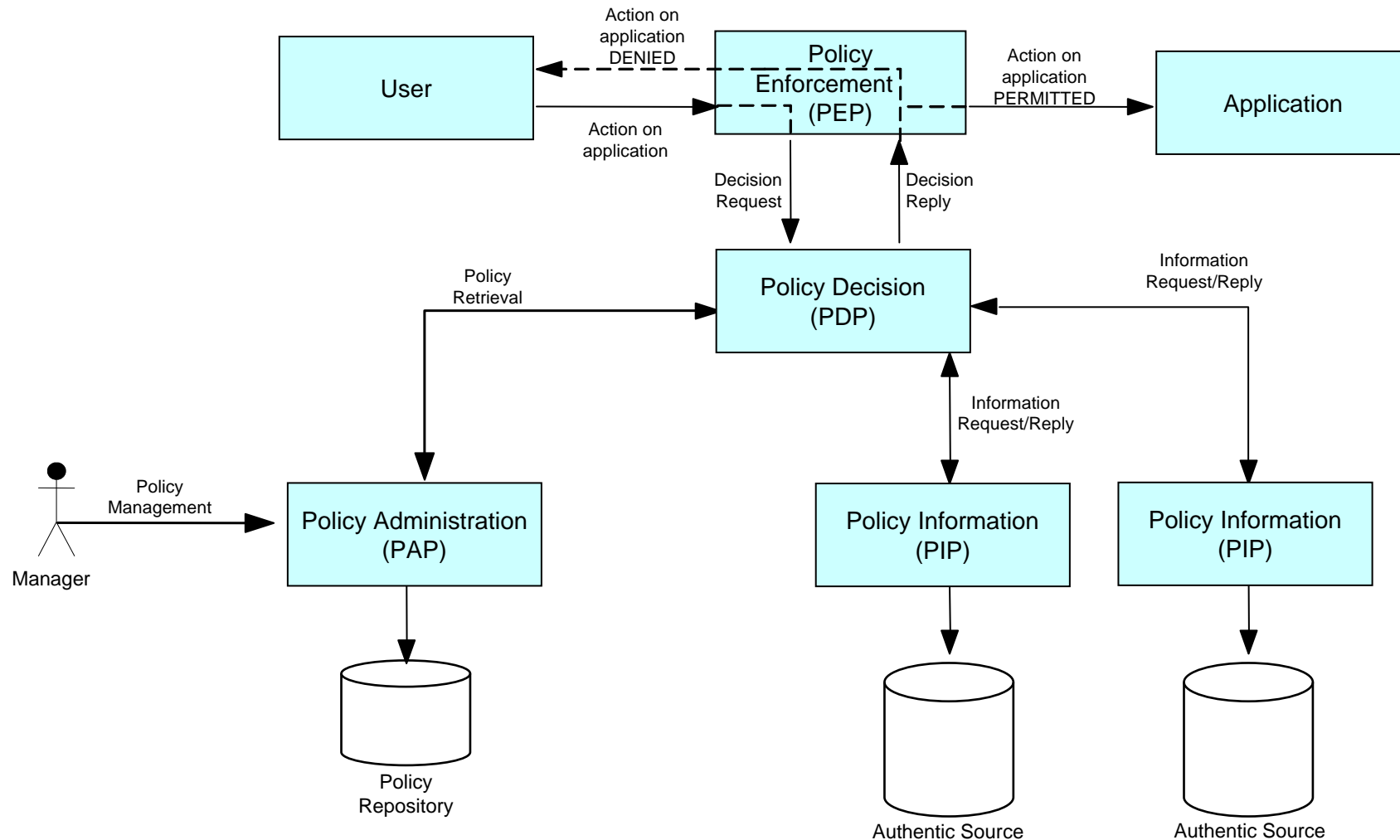
- Mandates & authorization credentials based on open standards, e.g.,
 - XACML
 - SAML
- Revocation services setup by mandate manager and certification authority
 - OCSP
 - CRL
- Certificates, Signatures and timestamps, e.g.,
 - X.509
 - XADES-*
- Communication protocols
 - SSL/TLS

XAXML – Allow/Deny Service Requests...





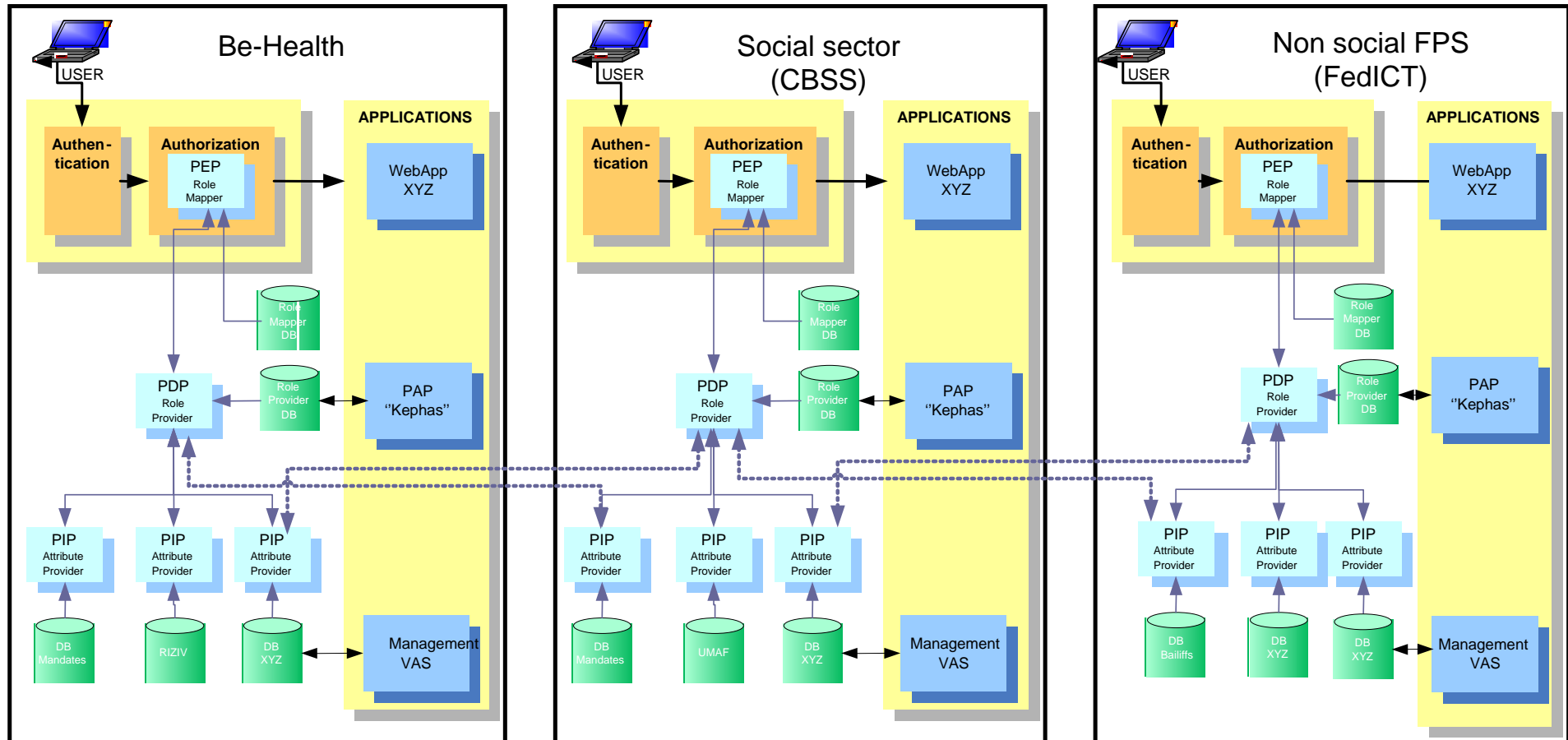
Generic Policy Enforcement Model XACML-based



Slide inspired by Frank Robben



Re-using Architecture



Slide inspired by Frank Robben



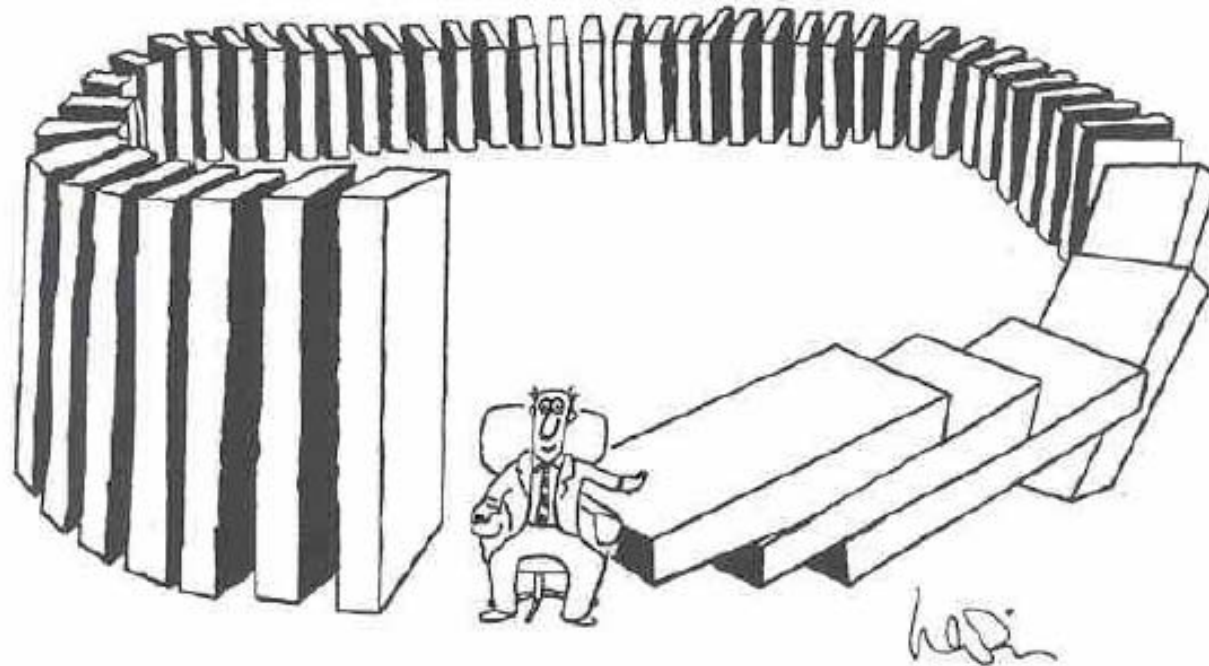
Conclusion

- eGovernment Services are accessible
 - Via open standards
 - With strong authentication & access management
- Federated system permits use of common basic services securely
 - Without losing any autonomy!
- System allows permanent evolution
 - Continuously changing user & organization requirements



Food for Thought

- Trust is Good – Control is Better!





Th@nk you!

Danny De Cock

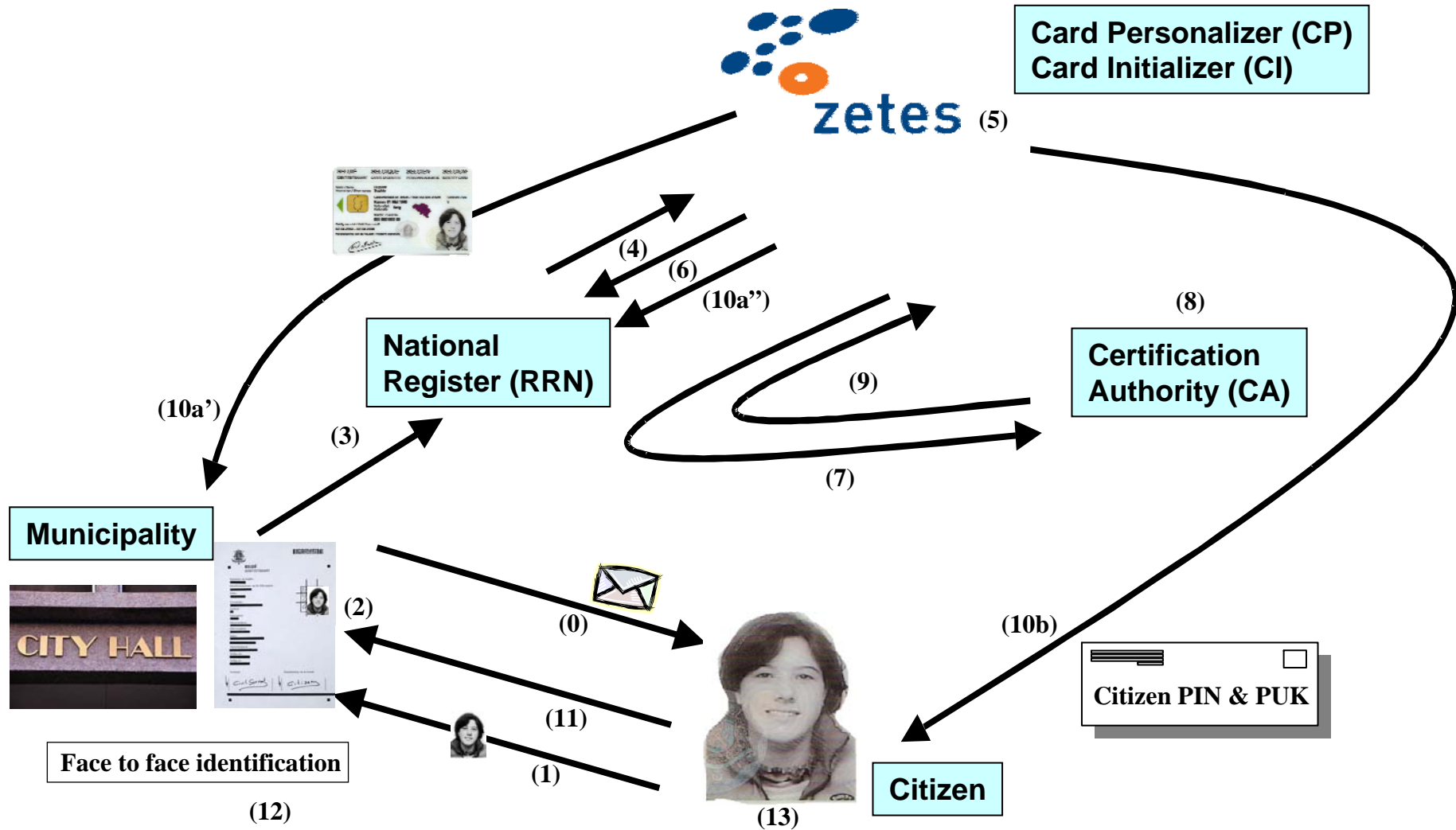
Researcher Applied Cryptography

Danny.DeCock@esat.kuleuven.be

Slides: www.godot.be/slides



eID Card Issuing Procedure



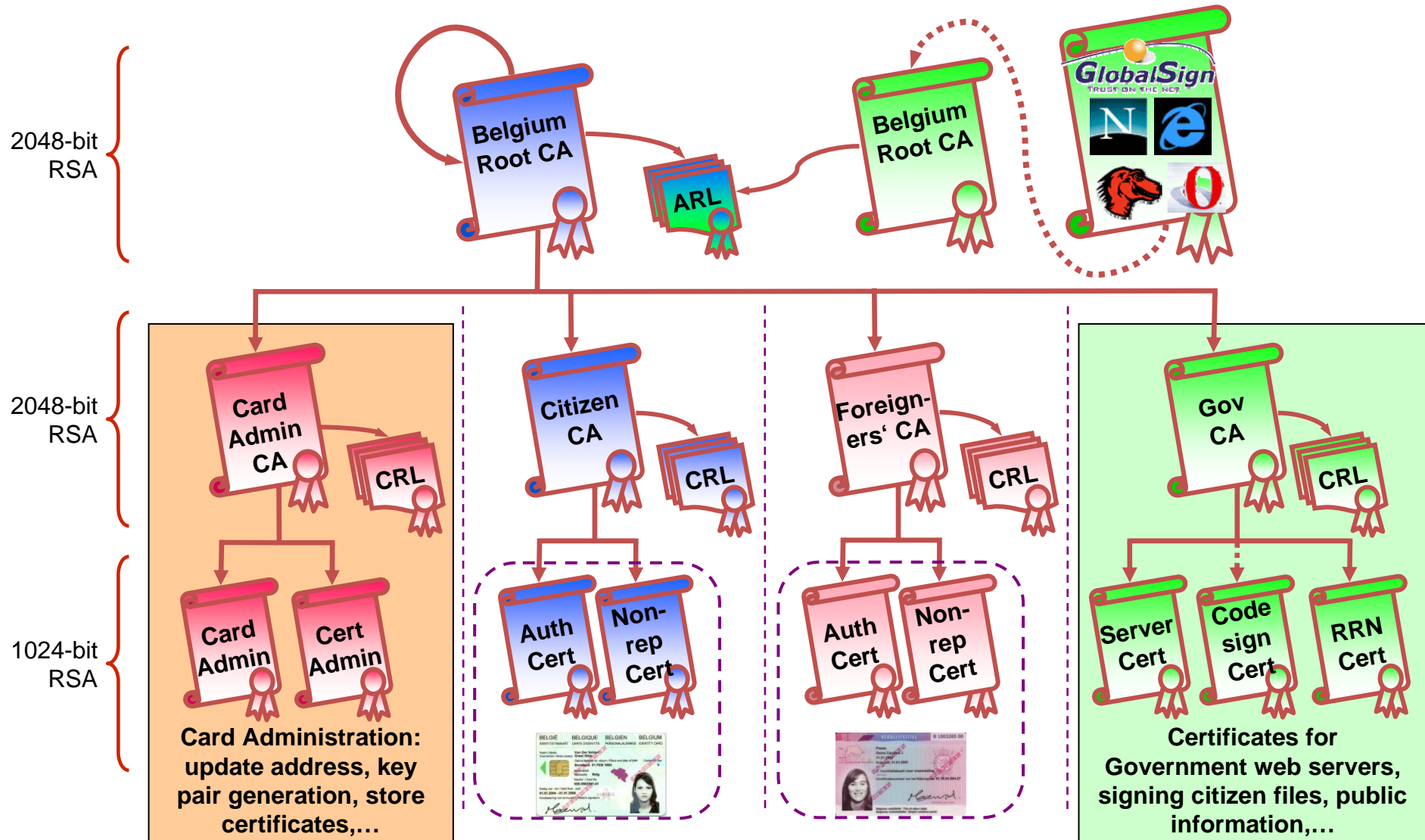


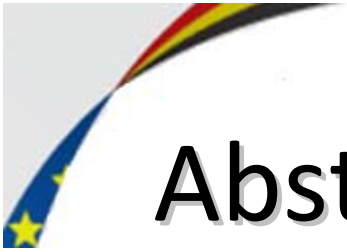
eID Card Issuing Procedure

- 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



eID Certificates Hierarchy





Abstract eGovernment Ecosystem

