

Contributions to the Analysis and Design of Large-Scale Identity Management Systems

Public Defense

9th June 2011

Danny De Cock

Promotor: prof. Bart Preneel

Jury: prof. Pierre Verbaeten (chairman)

prof. Jos Dumortier, dr. Walter Fumy, prof. Frank Piessens,

prof. Vincent Rijmen, prof. Joos Vandewalle

Basic Identity Management (IDM) System

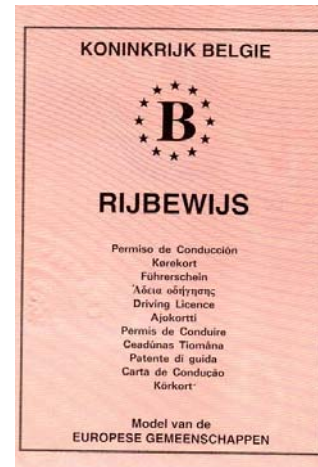
- ▶ **Before:** Archives and libraries store information in folders
- ▶ **Now:** Organizations manage information using servers and databases
- ▶ **Problems**
 - ▶ Finding the right file efficiently
 - ▶ Protecting integrity of archive
 - ▶ Tracing who accessed the archive
 - ▶ Merging archives is complex



Outline

- ▶ Introduction
 - ▶ Basic Identity Management (IDM) System
 - ▶ Typical IDM examples
 - ▶ Research Contributions
 - ▶ Identity Management
 - ▶ Electronic Voting
 - ▶ Conclusions
 - ▶ Publications Checklist
- ▶ Questions & Answers

Typical examples of Large-Scale IDM Systems



Outline

- ▶ Introduction
 - ▶ Basic Identity Management (IDM) System
 - ▶ Typical IDM examples
 - ▶ **Research Contributions**
 - ▶ Identity Management
 - ▶ Electronic Voting
 - ▶ Conclusions
 - ▶ Publications Checklist
- ▶ Questions & Answers

Research Contributions (RC)

- ▶ Can multiple IDM Systems interact with one another in a privacy-respecting manner?
- ▶ Can a set of privacy concerns wrt Belgian eID cards be mitigated?
- ▶ Is it possible to improve a voter's confidence in Belgian eVoting?

Can IDM Systems Respect Privacy?

- ▶ **What are the privacy concerns?**
 - ▶ Is all stored information used according to the rules?
 - ▶ How can one be sure that the rules are being enforced?
 - ▶ Can users be linked when using multiple IDM systems?
 - ▶ Do multiple identification numbers really decrease efficiency of IDM systems?

RC: Can Privacy be Preserved?

▶ Answer: yes

▶ Contribution: design of generic IDM system

- ▶ Supports policy enforcement

- ▶ Supports context specific identification schemes

- ▶ Is compatible with multiple IDM systems that have been analyzed

 - European Member states' eGovernment services

 - Belgian healthcare services

▶ Usefulness of generic system has been validated

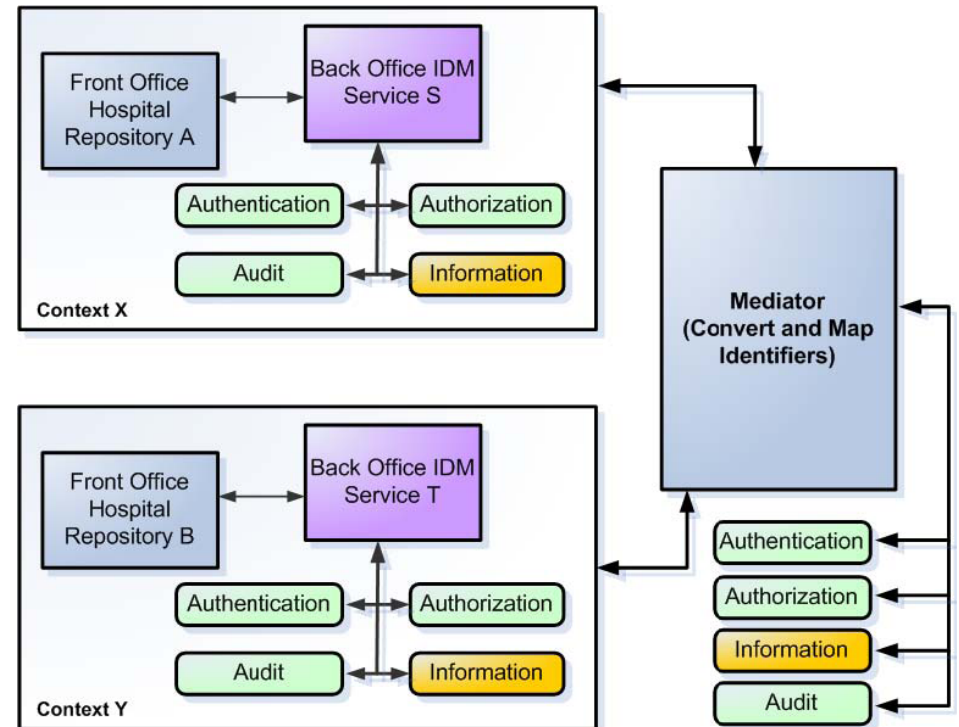
- ▶ Healthcare: eHIP project (IBBT)

- ▶ eGovernment: IDEM project (IBBT)

- ▶ Employability & Healthcare: TAS3 project (EU)

Federated IDM System for eHealth – eHIP

- ▶ Each hospital uses its own identification scheme for patients
- ▶ Doctors of multiple hospitals treat same patient
- ▶ Hospitals communicate through identifier mapping mechanism
- ▶ Patients are identified uniquely without exchanging unique identifiers
- ▶ Work has been acknowledged with
 - ▶ Prize of “outstanding achievement award for student research paper,” by the New Zealand State Services Commission

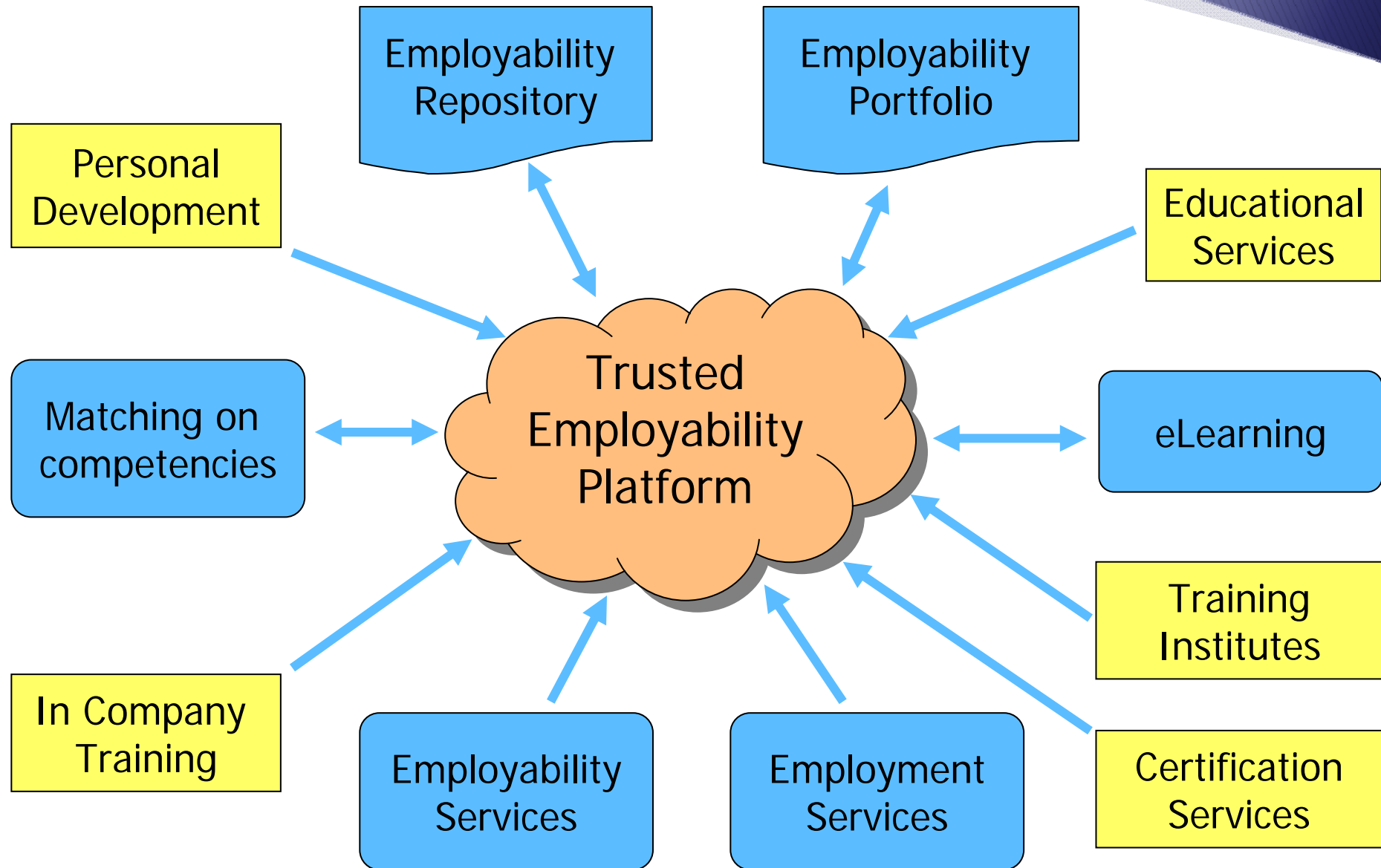


Integrated IDM Project – TAS3

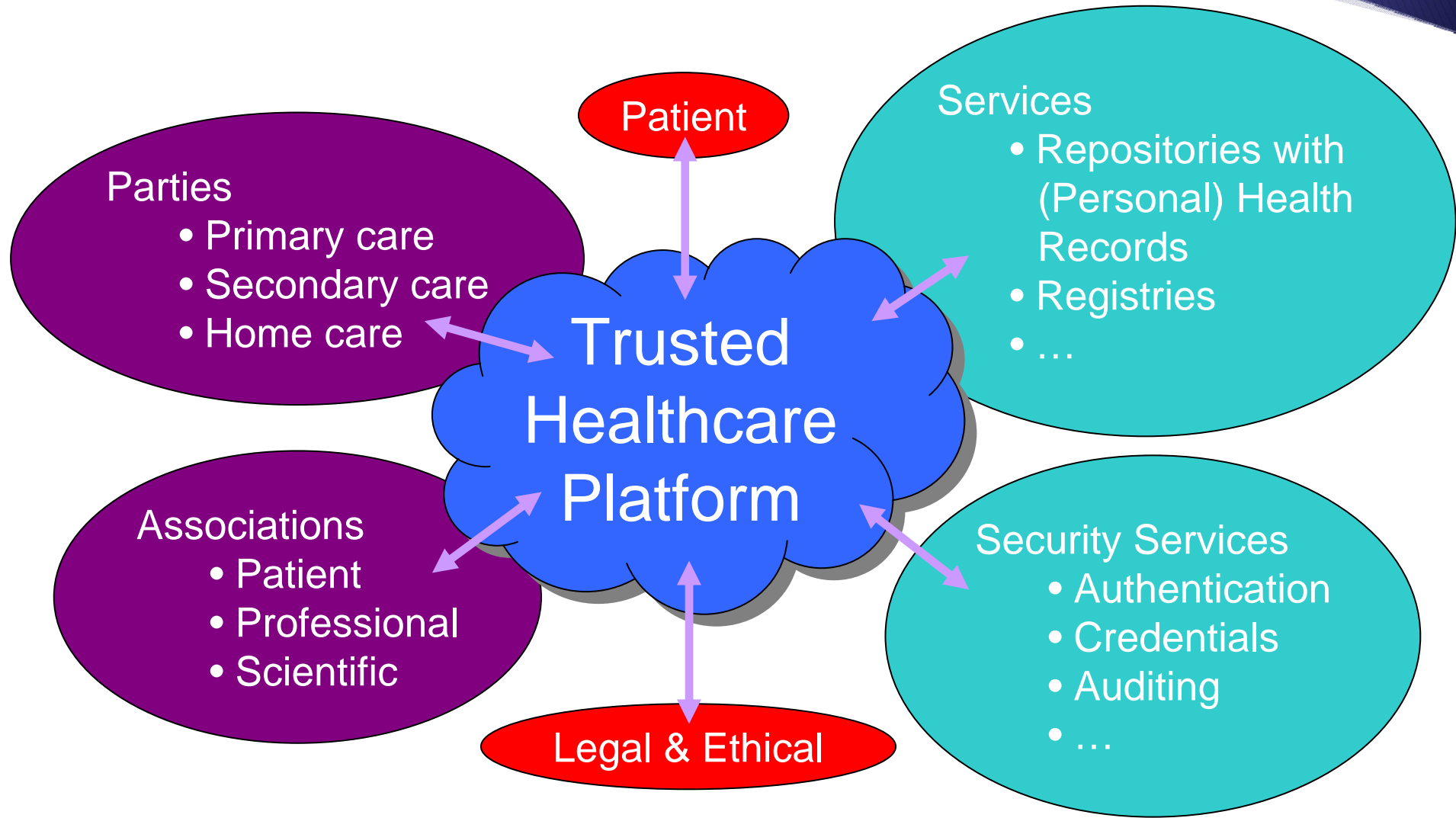


- ▶ **TAS3 = Trusted Architecture for Securely Shared Services**
 - ▶ Integrated Project of EU/FP7, 9.4 million Euro
 - ▶ 18 partners (9 research, 7 SMEs, 2 large organizations)
- ▶ **Consolidates scattered research in Authentication, Authorization, Security, Trust, Privacy using Digital identities**
- ▶ **Harmonizes federated identity management with**
 - ▶ User-centricity & User-control
 - ▶ Fine-grained data-protection policy enforcement
- ▶ **Validates generic IDM system**
 - ▶ 2 cross-border use cases

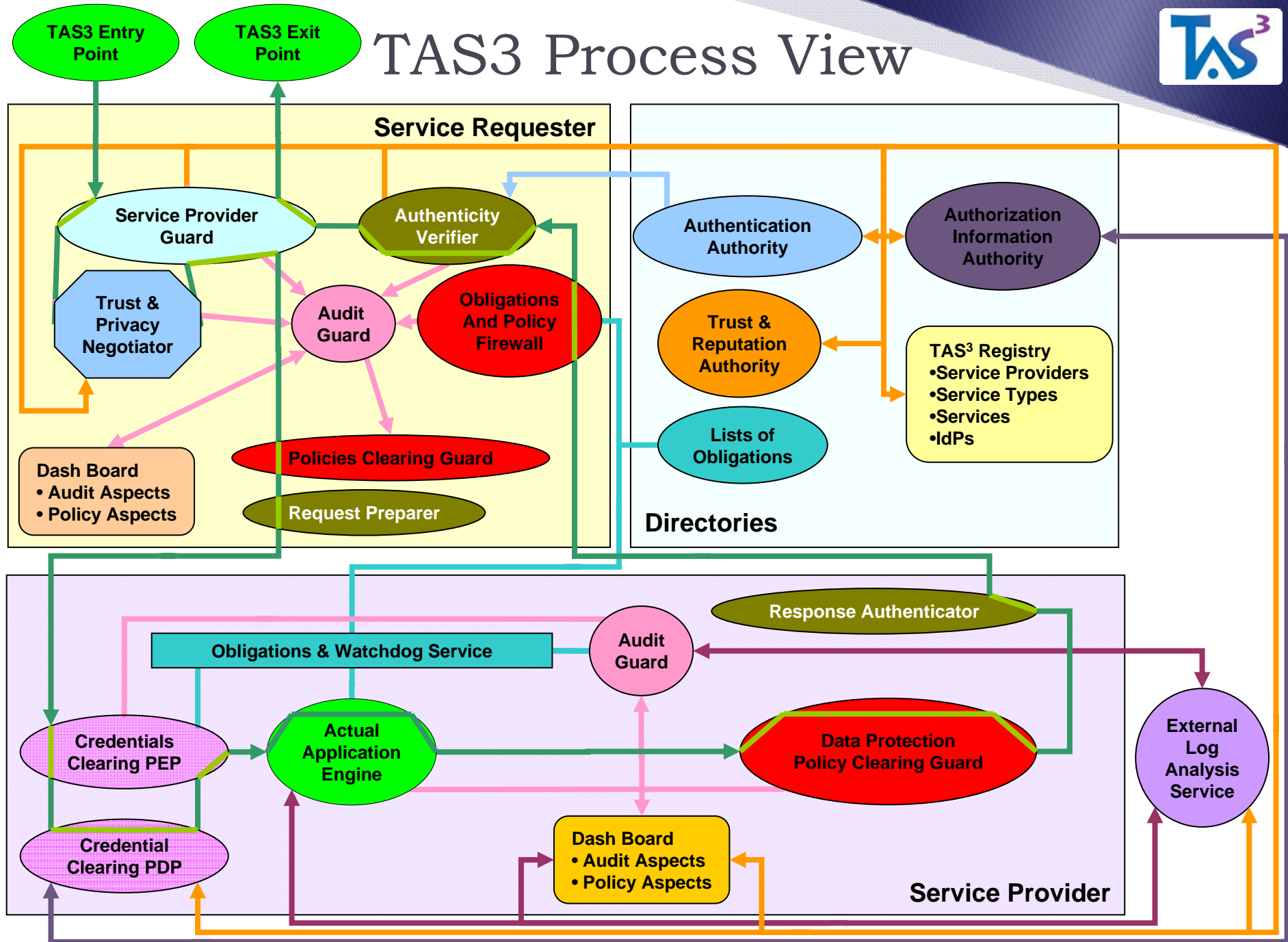
Employability Demonstrator Platform



Healthcare Demonstrator Platform



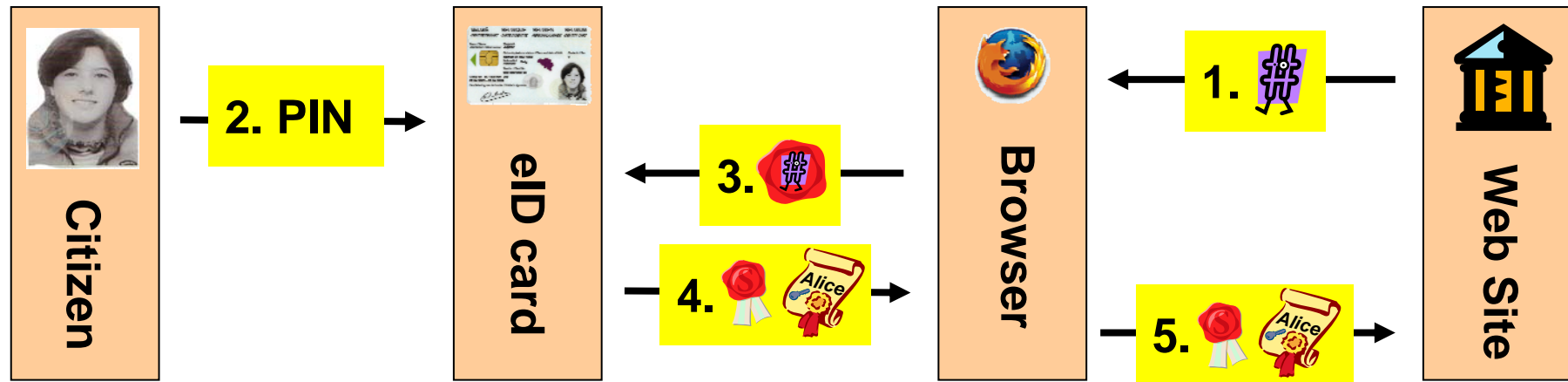
TAS3 Process View



RC: Must eID certificates include National Number?

- ▶ **Why eID card certificates include National Number**
 - ▶ Allows service provider to
 - ▶ Identify returning customers
 - ▶ Map customer/user to their file
 - ▶ Benefits for service providers
 - ▶ Citizen is uniquely identified by National Number
- ▶ **Privacy concerns**
 - ▶ Unnecessary disclosure of citizen's unique identifier
 - ▶ Enables linking users across service providers
- ▶ **Can this number be omitted from eID certificates?**
 - ☺ Extending OCSP system
 - ☹ Introduces re-registration problem of new eID cards

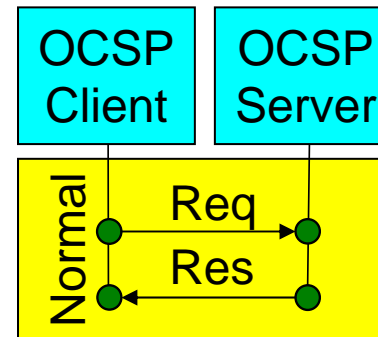
Using an Authentication Certificate



1. Web server asks signed challenge
2. Citizen Alice permits signature generation
3. eID card creates signature
4. Browser retrieves signature and certificate
5. Web server receives signed challenge and certificate
 - Web server verifies signature and certificate

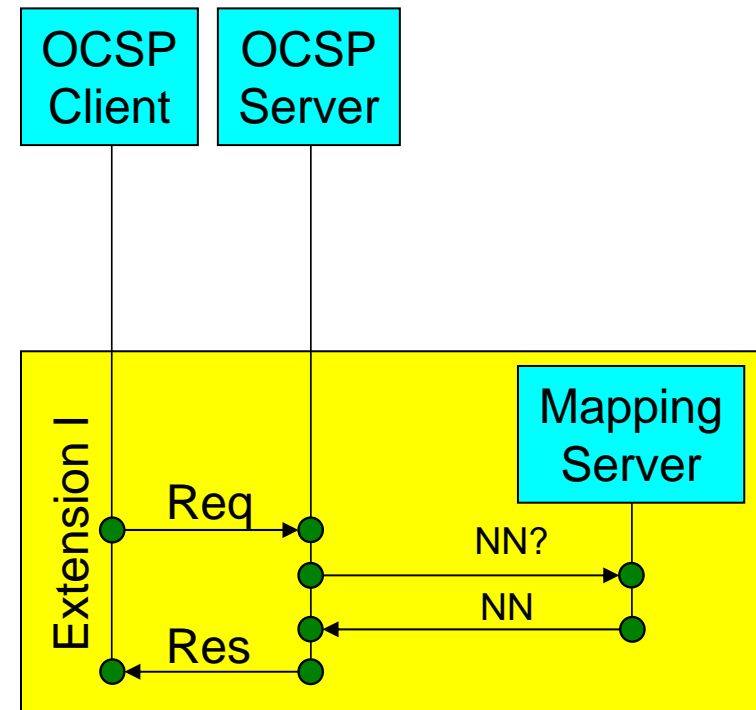
Checking Validity of Certificates

- ▶ Use of Online Certificate Status Protocol (OCSP)
- ▶ Web server asks OCSP Server to check certificate
- ▶ OCSP Server answers with signed response
 - ▶ Valid
 - ▶ Invalid
 - ▶ Unknown
- ▶ Advantage:
 - ▶ Very popular mechanism
 - ▶ Easy to extend



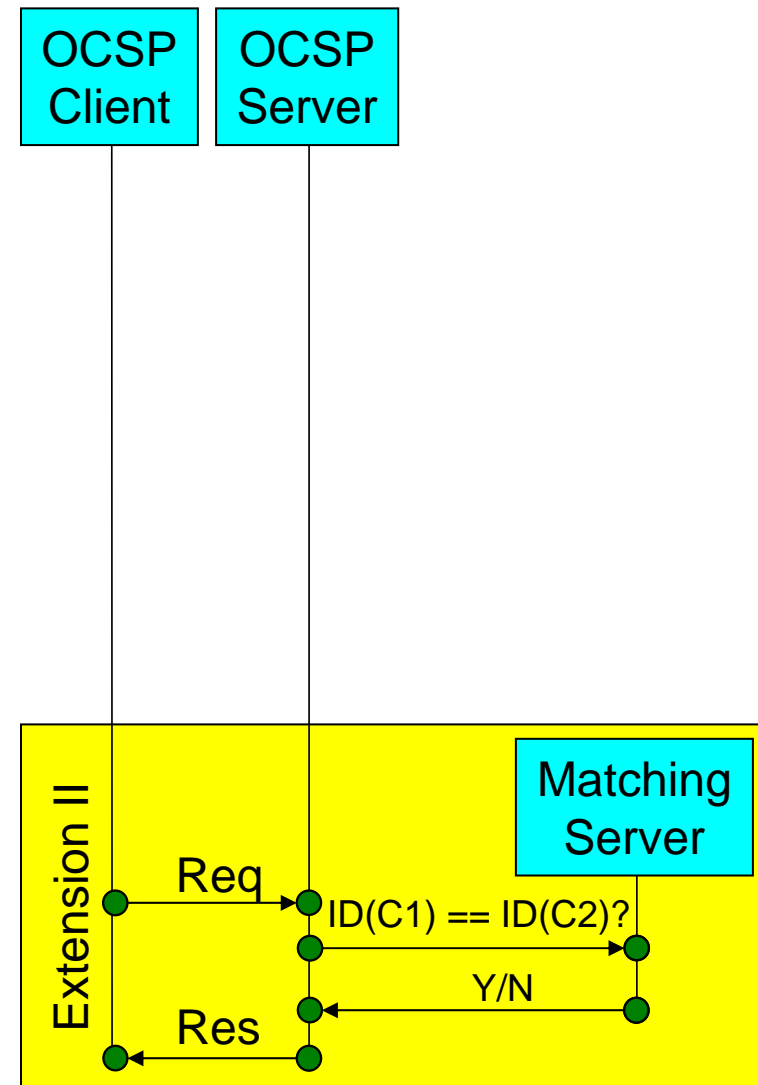
OCSP Extension I – Querying National Number

- ▶ Signed OCSP request also queries NN of citizen's certificate
- ▶ If requester authorized
 - ▶ Response includes NN
- ▶ Remaining problems
 - ▶ NN remains very attractive to link citizens
 - ▶ Service providers without authorization to use NN cannot link subsequent eID cards to one citizen
- ▶ Solution: OCSP Extension II



OCSP Extension II – Matching Cardholder?

- ▶ Signed OCSP request includes two cardholder references
 - ▶ C1 – currently used certificate
 - ▶ C2 – previously used certificate
- ▶ If requester is authorized
 - ▶ Signed OCSP response indicates
 - ▶ Match: C1 and C2 match one citizen
 - ▶ No match



RC: Protect Use of eID card from Malicious Use?

- ▶ Is it easy to copy identity information of eID card?

- ▶ Answer: Yes!

- ▶ Software library & smart phone application to mimic genuine eID cards
 - ▶ eGovernment Innovation Award 2010
 - ▶ Collaboration with FedICT



- ▶ Can one hijack an eID card's authentication session?

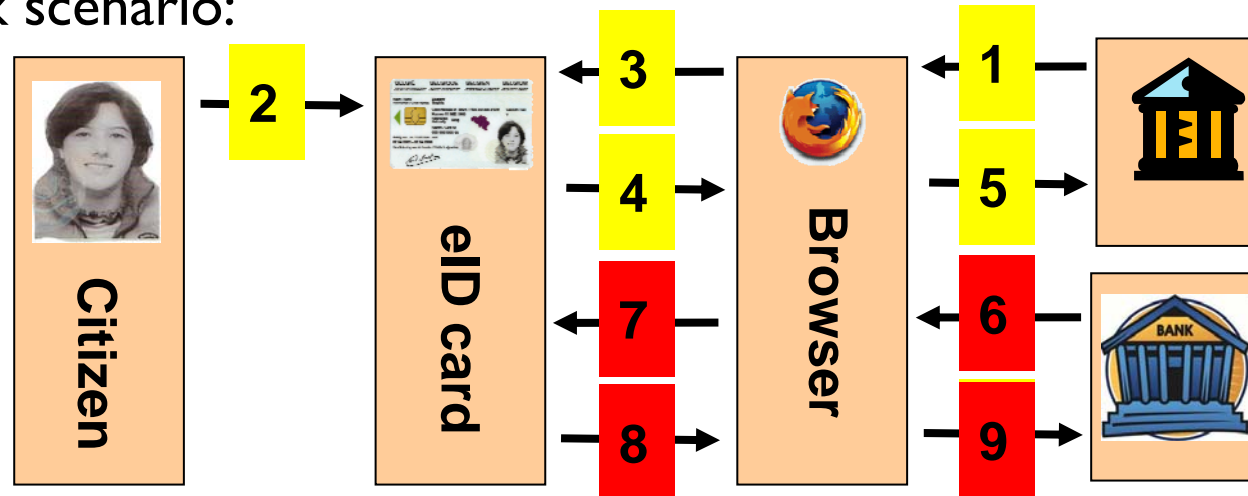
- ▶ Answer: Yes... ☹️

- ▶ Solution:

- ▶ Design of dedicated smartcard reader to prevent hijack

Preventing Hijacking eID Authentication Session

▶ Attack scenario:



▶ Protocol designed to prevent attack:

- ▶ Smartcard reader acts as firewall – filters potentially malicious smartcard commands
- ▶ Card reader provides sensible feedback to citizen
- ▶ Citizen provides consent to send command to her smartcard

▶ Remaining issue:

- ▶ Awareness training of citizen

Outline

- ▶ Introduction
 - ▶ Basic Identity Management (IDM) System
 - ▶ Typical IDM examples
 - ▶ Research Contributions
 - ▶ Identity Management
 - ▶ **Electronic Voting**
 - ▶ Conclusions
 - ▶ Publications Checklist
- ▶ Questions & Answers

RC: Enhance Confidence in Belgian eVoting

- ▶ Can the current eVoting system be improved to enhance the voter's confidence?
 - ▶ Answer: Improved paper-based voting system provides required guarantees
- ▶ Issues with current eVoting system
 - ▶ Does the technology function correctly?
 - ▶ Did the voting officials validate the configuration?
 - ▶ Is the vote correctly recorded?
 - ▶ Is the vote correctly counted?
 - ▶ Is the election result correct?
 - ▶ Did independent auditors validate the elections?

Classic Electronic Voting Computer



Issues with Magnetic Stripe Cards Voting

- ▶ Lack of transparency
 - ▶ Magnetic stripe card = voter's choice?
 - ▶ Voting computer may have stored different ballot
- ▶ Lack of verifiability
 - ▶ Is ballot on magnetic stripe card also counted?
 - ▶ Voting urn may have overwritten the magnetic stripe

Organizational and procedural measures
neutralize these potential issues

Required eVoting Booth Components



Smartcard
Reader to activate
Voting process

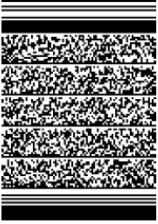


Simplest
Computer Possible



Printer


Design of Improved Paper-based Voting System



Cast in Leuven

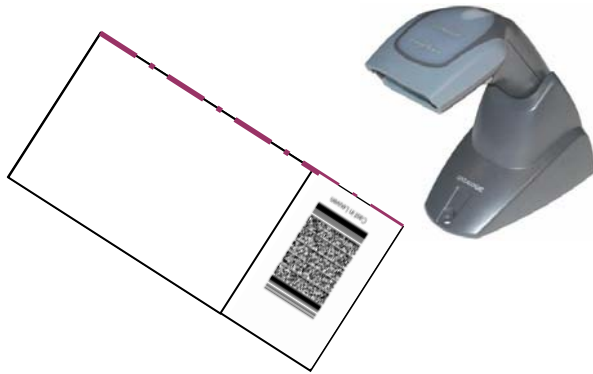
Senate Election <i>Selected Party</i>	Chamber Election <i>Selected Party</i>	European Election <i>Selected Party</i>	Province Election <i>Selected Party</i>	Region Election <i>Selected Party</i>	Local Election <i>Selected Party</i>
1. First Name	17. First Name	33. First Name	49. First Name	65. First Name	81. First Name
2. Second Name	18. Second Name	34. Second Name	50. Second Name	66. Second Name	82. Second Name
3. Third Name	19. Third Name	35. Third Name	51. Third Name	67. Third Name	83. Third Name
4. Fourth Name	20. Fourth Name	36. Fourth Name	52. Fourth Name	68. Fourth Name	84. Fourth Name
5. Fifth Name	21. Fifth Name	37. Fifth Name	53. Fifth Name	69. Fifth Name	85. Fifth Name
6. Sixth Name	22. Sixth Name	38. Sixth Name	54. Sixth Name	70. Sixth Name	86. Sixth Name
7. Seventh Name	23. Seventh Name	39. Seventh Name	55. Seventh Name	71. Seventh Name	87. Seventh Name
8. Eighth Name	24. Eighth Name	40. Eighth Name	56. Eighth Name	72. Eighth Name	88. Eighth Name
9. Ninth Name	25. Ninth Name	41. Ninth Name	57. Ninth Name	73. Ninth Name	89. Ninth Name
10. Tenth Name	26. Tenth Name	42. Tenth Name	58. Tenth Name	74. Tenth Name	90. Tenth Name
11. Eleventh Name	27. Eleventh Name	43. Eleventh Name	59. Eleventh Name	75. Eleventh Name	91. Eleventh Name
12. Twelfth Name	28. Twelfth Name	44. Twelfth Name	60. Twelfth Name	76. Twelfth Name	92. Twelfth Name
13. Thirteenth Name	29. Thirteenth Name	45. Thirteenth Name	61. Thirteenth Name	77. Thirteenth Name	93. Thirteenth Name
14. Fourteenth Name	30. Fourteenth Name	46. Fourteenth Name	62. Fourteenth Name	78. Fourteenth Name	94. Fourteenth Name
15. Fifteenth Name	31. Fifteenth Name	47. Fifteenth Name	63. Fifteenth Name	79. Fifteenth Name	95. Fifteenth Name
16. Sixteenth Name	32. Sixteenth Name	48. Sixteenth Name	64. Sixteenth Name	80. Sixteenth Name	96. Sixteenth Name

**Check and
fold this
ballot**

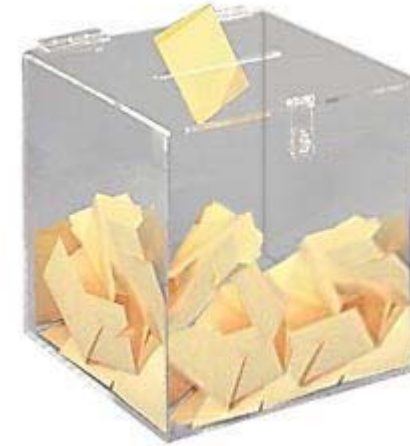


Cast in Leuven

Proposed Voting Office's Equipment



Ballot Verifier



Ballot Box

© George Patton Associates, Inc.

Properties of Improved Paper-based Voting Ballots

- ▶ Barcode represents same information as human readable part
- ▶ Barcode digitally signed by voting computer
 - ▶ Signature not linkable to voter
- ▶ Barcode encrypted under public key of election administration
 - ▶ Photographed barcodes do not compromise voter's secrecy
- ▶ Extension of this system can be fully verifiable
 - ▶ Voter gets a copy of the cryptographic hash value of barcode
 - ▶ Ballot has been counted if hash value is listed online
- ▶ Patent request filed for EU and US wrt generalized version of ballots

System Validated by Council of Europe

- ▶ Requirements for Free and Fair Elections
 - ▶ Universal
 - ▶ Everybody can cast a vote
 - ▶ Equal
 - ▶ Everybody has just one vote
 - ▶ Freedom
 - ▶ Everybody can cast his/her vote of his/her choice
 - ▶ Secrecy
 - ▶ Only the voter knows who he has voted for
 - ▶ Transparency
 - ▶ All procedures are simple, publicly available and known
 - ▶ Verifiability
 - ▶ Voting and counting systems are verifiable
- ▶ Only recommendation
 - ▶ Voters and external observers must check correctness of voting ballots

Outline

- ▶ Introduction
 - ▶ Basic Identity Management (IDM) System
 - ▶ Typical IDM examples
 - ▶ Research Contributions
 - ▶ Identity Management
 - ▶ Electronic Voting
 - ▶ **Conclusions**
 - ▶ Publications Checklist
- ▶ Questions & Answers

Identity Management Systems

- ▶ Good technical solutions exist to build scalable and user-centric IDM systems
- ▶ Remaining issues
 - ▶ Usability of IDM systems
 - ▶ All users must be able to use user-centric systems
 - ▶ Challenge: Default privacy settings to match needs and expectations of “most” users
 - ▶ Transparency
 - ▶ Challenge to find right balance between easy-to-use, easy-to-understand and information granularity
 - ▶ Linkability
 - ▶ Using services online still exposes relationships between users and service providers
 - ▶ Technical solutions to limit these are not yet mature for large scale implementation

Conclusions – Electronic Voting

- ▶ Requirements for free and fair elections can be met with technical means
 - ▶ Correctness of election result still depends on technically skilled validators
 - ▶ Transparency requirement conflicts with use of advanced cryptographic techniques
 - ▶ Cryptographic techniques need to be made understood by the layman
- ▶ Unanswered questions:
 - ▶ Can one guarantee the correct functioning of a voting computer?
 - ▶ Does it matter?
 - ▶ Can one guarantee that a voting computer does not remember votes cast?
 - ▶ Can one use an Internet voting system for large scale and important elections?

Outline

- ▶ Introduction
 - ▶ Basic Identity Management (IDM) System
 - ▶ Typical IDM examples
 - ▶ Research Contributions
 - ▶ Identity Management
 - ▶ Electronic Voting
 - ▶ Conclusions
 - ▶ **Publications Checklist**
- ▶ Questions & Answers

Publications Checklist

- ▶ LNCS: 1
- ▶ LNI: 2
- ▶ International Conferences: 6
- ▶ Journal Papers: 5
- ▶ Book Chapters: 2
- ▶ Patents: 1

Publications (1 / 4)

▶ eArchiving

- ▶ C. Troncoso, D. De Cock, and B. Preneel, “Improving Secure Long-Term Archival of Digitally Signed Documents,” In 4th International Workshop on Storage Security and Survivability (StorageSS 2008), Y. Kim, and B. Yurcik (eds.), pp. 27-36, 2008

▶ eAuthentication

- ▶ D. De Cock, K. Wouters, D. Schellekens, D. Singelée, and B. Preneel, “Threat Modelling for Security Tokens in Web Applications,” In Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security (CMS 2004), IFIP International Federation for Information Processing 175, D. Chadwick, and B. Preneel (eds.), Springer, pp. 183-193, 2005
- ▶ J. Iliadis, S. Gritzalis, D. Spinellis, D. De Cock, B. Preneel, and D. Gritzalis, “Towards a Framework for Evaluating Certificate Status Information Mechanisms,” Computer Communications 26(16), pp. 1839-1850, 2003

▶ eBanking

- ▶ J. Claessens, D. De Cock, V. Dem, B. Preneel, and J. Vandewalle, “On the Security of Today's Online Electronic Banking Systems,” Computers & Security 21(3), pp. 253-265, 2002

Publications (2/4)

▶ eIDM

- ▶ M. Deng, D. De Cock, and B. Preneel, “Towards a Cross-Context Identity Management Framework in E-Health,” *Online Information Review* 33(3), pp. 422-442, 2009
- ▶ B. Van Alsenoy, D. De Cock, K. Simoens, J. Dumortier, and B. Preneel, “Delegation and Digital Mandates: Legal Requirements and Security Objectives,” *Computer Law and Security Review* 25(5), pp. 415-431, 2009
- ▶ B. Van Alsenoy, D. De Cock, J. Dumortier and B. Preneel, “Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card,” *Datenschutz und Datensicherheit*, pp. 178-183, March 2008
- ▶ M. Deng, D. De Cock, and B. Preneel, “Towards cross-context identity management framework in e-health,” In *Managing Identity in New Zealand – identity conference 2008*, 10 pages, 2008

Publications (3/4)

▶ eHealth

- ▶ M. Deng, D. De Cock, B. Preneel, “An interoperable cross-context architecture to manage distributed personal e-Health information,” Handbook of Research on Developments in e-Health and Telemedicine: Technological and Social Perspectives, ISBN: 978-1-61520-670-4, M. M. Cunha, R. Simoes, A. Tavares, Eds., Hershey, PA, USA: IGI Global, Inc., pp.~576-602, chapter 27, 2009
- ▶ M. Deng, R. Scandariato, D. De Cock, B. Preneel, and W. Joosen, “Identity in federated electronic healthcare,” In 1st IFIP Wireless Days (WD 2008), IEEE, pp. 1-5, 2008
- ▶ D. De Cock, M. Deng, S. Faust, S. Nikova, D. Schellekens, D. Vandevenne, and K. Wouters, “Applicability of e-ID and alternative identification mechanisms,” Deliverable 3.2.1: E-Health Information Platforms (E-Hip), 48 pages, 2007
- ▶ M. Deng, and D. De Cock, “Feasibility of federated identity and roadmap for integration in e-Health,” Deliverable 3.2.2: E-Health Information Platforms (E-Hip), 32 pages, 2007

▶ eVoting

- ▶ A. Bosselaers, D. De Cock, F. Vercauteren, B. Preneel, “Selection Systems,”
 - ▶ US Patent Application US 2010/0237151 A1, Sep 23, 2010;
 - ▶ European Patent Application EP2186065, May 19, 2010
- ▶ D. De Cock, and B. Preneel, “Electronic Voting in Belgium: Past and Future,” In E-Voting and Identity - 1st International Conference, VOTE-ID 2007, Lecture Notes in Computer Science 4896, A. Alkassar, and M. Volkamer (eds.), Springer-Verlag, pp. 76-87, 2007

Publications (4 / 4)

▶ eID

- ▶ D. De Cock, B. Van Alsenoy, B. Preneel, J. Dumortier, “The Belgian eID Approach,” Handbook of eID Security Concepts, Practical Experiences, Technologies, W. Fumy and M. Paeschke (eds.), pp.~117-139, Erlangen, Publicis Publishing, 2011
- ▶ R. Peeters, K. Simoens, D. De Cock, and B. Preneel, “Cross-Context Delegation through Identity Federation,” In Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Lecture Notes in Informatics (LNI) P-137, A. Brömme, C. Busch, and D. Hühnlein (eds.), Bonner Köllen Verlag, pp. 79-92, 2008
- ▶ D. De Cock, K. Simoens, and B. Preneel, “Insights on identity documents based on the Belgian case study,” Information Security Technical Report 13(2), pp. 54-60, 2008
- ▶ M. Hansen, M. Meints, I. Angell, D. De Cock, P. De Hert, D. Demetis, C. Diaz, S. Freh, M. Gasson, X. Huysmans, M. Jacomet, G. Karjoth, E. Kindt, E. Kosta, A. Pfitzmann, B. Preneel, W. Scheurs, S. Steinbrecher, R. Thomas, and C. Wolf, “Study on ID Documents,” FIDIS Deliverable 3.6, 160 pages, 2006
- ▶ D. De Cock, C. Wolf, and B. Preneel, “The Belgian Electronic Identity Card (Overview),” In Sicherheit 2005: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3rd Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI), Lecture Notes in Informatics (LNI) LNI P-77, J. Dittmann (ed.), Bonner Köllen Verlag, pp. 298--301, 2006
- ▶ D. De Cock, K. Wouters, and B. Preneel, “Introduction to the Belgian EID Card: BELPIC,” In Public Key Infrastructure - 1st European PKI Workshop: Research and Applications, EuroPKI 2004, Lecture Notes in Computer Science 3093, S. Gritzalis, S. K. Katsikas, and J. Lopez (eds.), Springer-Verlag, pp. 1-13, 2004

Outline

- ▶ Introduction
 - ▶ Basic Identity Management (IDM) System
 - ▶ Typical IDM examples
 - ▶ Research Contributions
 - ▶ Identity Management
 - ▶ Electronic Voting
 - ▶ Conclusions
 - ▶ Publications Checklist
- ▶ **Questions & Answers**



**Thanks for your
attention**

Danny.DeCock@esat.kuleuven.be

Thesis Outline, Part I

- ▶ **Topic 1 – Analysis of IDM Systems**
 - ▶ Main drivers to introduce IDM systems
 - ▶ Issuance, use and issues of identifiers of users, service providers
 - ▶ Authentication mechanisms of users & other entities, digital and electronic signatures
 - ▶ Introduction of use case: Belgian eGovernment
 - ▶ Authoritative sources as core components
 - ▶ Privilege and Mandate management
- ▶ **Topic 1 – Design of IDM-related systems**
 - ▶ Archival of digitally signed information
 - ▶ Dedicated smartcard reader for use with Belgian eID card
 - ▶ Limiting uncontrolled propagation of National Number
- ▶ **Topic 2 – Design of Improved paper-based voting system**
 - ▶ Analysis of classic electronic voting system
 - ▶ Design of improved paper-based voting system
- ▶ **Conclusions & Open Issues**
 - ▶ Identity Management
 - ▶ Electronic Voting

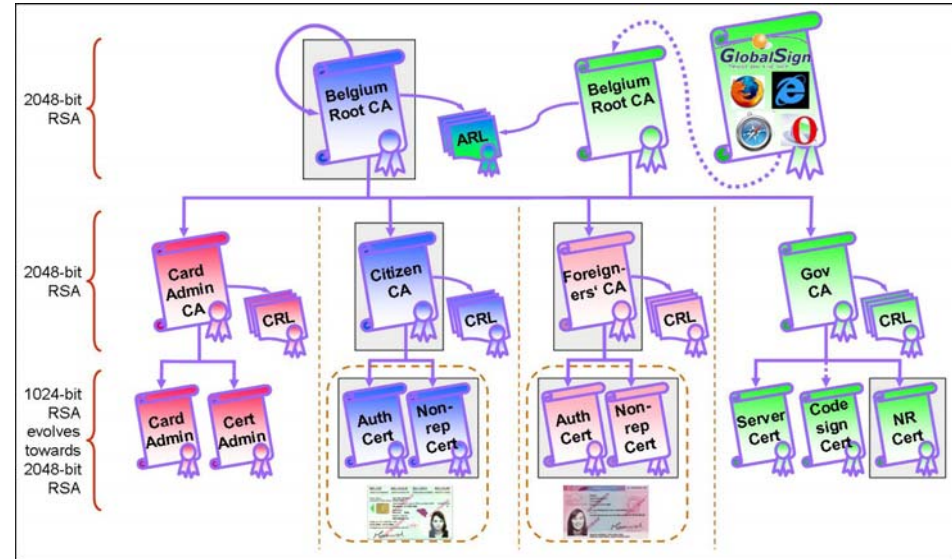
Thesis Outline, Part II

▶ Part II: Publications

- ▶ *Chapter 1: List of Publications*
- ▶ *Chapter 2: Belgian eID Approach*
- ▶ *Chapter 3: Towards a cross-context IDM Framework in eHealth*
- ▶ *Chapter 4: Delegation and digital mandates*
- ▶ *Chapter 5: Insights on Identity Documents based on Belgian Case Study*
- ▶ *Chapter 6: Improving Long-term Archival of Digitally Signed Documents*
- ▶ *Chapter 7: Electronic Voting in Belgium: Past and Future*

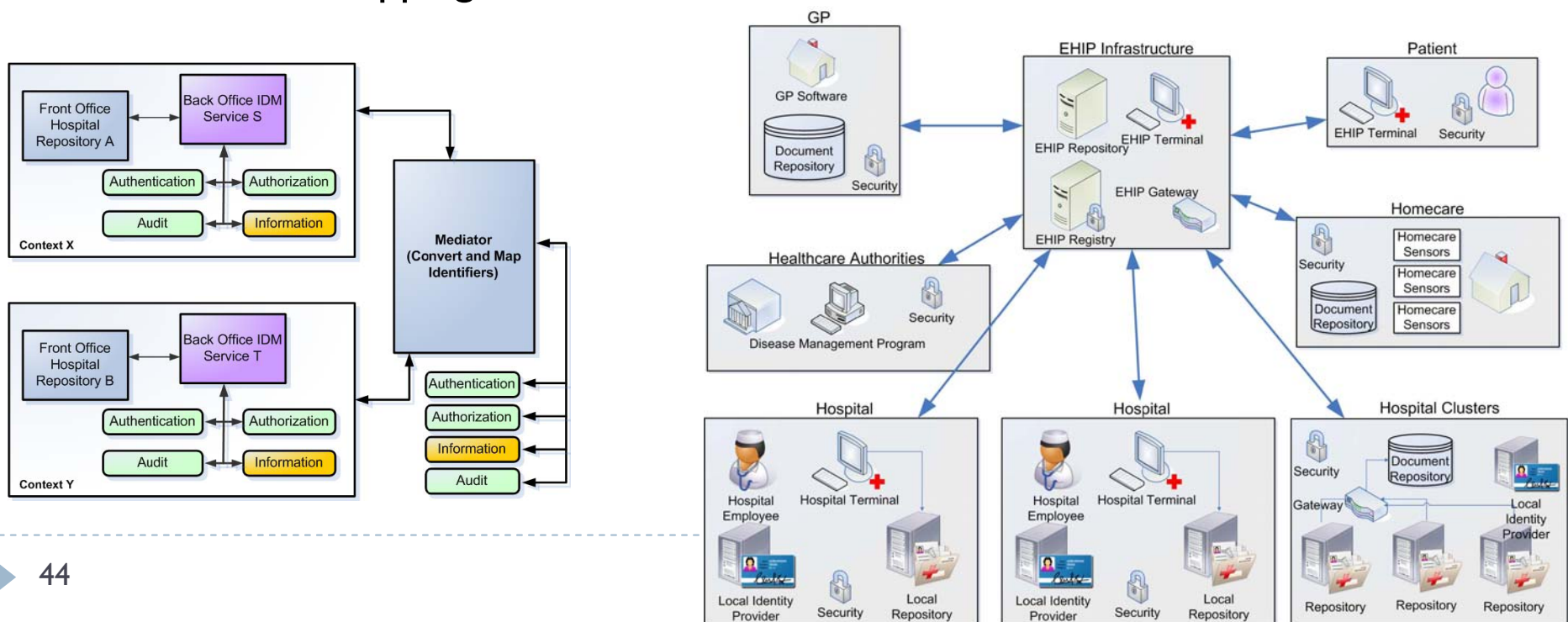
1. Approach & Insights on Belgian eID & ID Documents

- ▶ **Multiple electronic identities credentials issued in Belgium**
 - ▶ Userid/Password, Federal Token, eID Card, ePassports
- ▶ **Enabler of eServices offered to Belgian citizens & aliens**
- ▶ **Life-cycle of information available at National Register**
- ▶ **eID card & ePassports issuance and use**
 - ▶ Document security
 - ▶ Access control mechanisms
 - ▶ Digital identification
 - ▶ Entity authentication
 - ▶ Non-repudiation of origin
 - ▶ Terminal Authentication



2. Towards a Cross-Context IDM Framework in eHealth

- ▶ New model for IDM with identifiers conversion to ensure interoperability in federated eHealth environment
 - ▶ Collaboration between multiple healthcare service providers
 - ▶ Each refers to a single patient using its own identification scheme
 - ▶ Service providers communicate sensibly about the same patient using identifier mapping mechanisms



3. Delegation and Digital Mandates

- ▶ Integration of legal mandates within identity and information management systems
- ▶ Outlines
 - ▶ Legal framework surrounding delegation (main contributor: Brendan Van Alsenoy)
 - ▶ Identification of basic requirements to technically implement delegation and digital mandates – very close relationship with certificates
 - ▶ Delegation scenarios
 - ▶ Risk analysis
- ▶ Representation of technical capabilities vs. legal representation
 - ▶ Delegated administration: offloading responsibility wrt well defined legal actions to a delegate
 - ▶ Use-case with online tax declaration
 - ▶ Lack of authority – dealing with presumed mandate holder exceeds his authority or acts without any authority
 - ▶ First time that it is mentioned that technical controls can help reduce the impact of these issues

4. Improving Long-term Archival of Digitally Signed Documents

- ▶ **Goal:**

- ▶ Protection of digitally signed documents against decay of signing algorithm, signing format, hash functions

- ▶ **Approach:**

- ▶ Verifiable storage of proofs of validity of certificates of digitally signed documents
- ▶ Archive timestamps, documents, proofs of validity
- ▶ Regularly re-timestamp whole package with “today’s” algorithms and mechanisms to protect against degradation of cryptographic strength of any of the components

- ▶ **Property:**

- ▶ First proposal in literature providing timely evidence on document’s existence

5. Electronic Voting in Belgium – Past & Future

- ▶ Overview of electronic voting system used in Belgium
- ▶ Reasons why magnetic-stripe card system needs to be replaced
 - ▶ Lack of transparency wrt integrity of the voter's ballot
 - ▶ System is not usable by people who are, e.g., blind
 - ▶ Availability of hardware components – design based on hardware available in the nineties
- ▶ Recommendations for new voting system
 - ▶ 4 options: improved paper-base voting system, optical scanning, remote voting through Internet, Intranet voting in kiosk/voting booth
- ▶ Introduction of improved paper-based voting system
 - ▶ Taking into account accessibility concerns