Overcoming Barriers in the field of Authentication and Identification

Dr. Sjaak Nouwt
TILT – Tilburg Institute for Law, Technology, and Society
Tilburg University, the Netherlands
j.nouwt@uvt.nl

Information Society and Media

Roadmap

- Authentication and Identification
- Barriers
- Solutions
  - From the solutions report
  - From the US eGovernment Act
  - From the OECD
  - From the Austrian model
  - From experts
- Next

Electronic Authentication

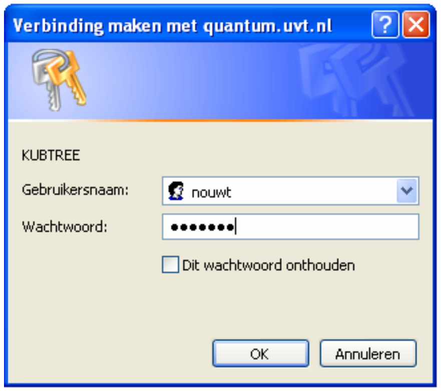
“Electronic authentication provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment. Thus, electronic authentication plays a key role in the establishment of **trust relationships** for electronic commerce, electronic government and many other social interactions. It is also an essential component of any strategy to **protect** information systems and networks, financial data, personal information and other assets **from unauthorised access or identity theft**. Electronic authentication is therefore essential for establishing **accountability online**.”

OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007.

TILBURG UNIVERSITY

Authentication

- Establishing or confirming someone or something as authentic
- Any process through which one proves and verifies certain information



Verbinding maken met quantum.uvt.nl

KUBTREE

Gebruikersnaam: nouwt

Wachtwoord: •••••••

□ Dit wachtwoord onthouden

TILT

Tilburg Institute for Law, Technology, and Society

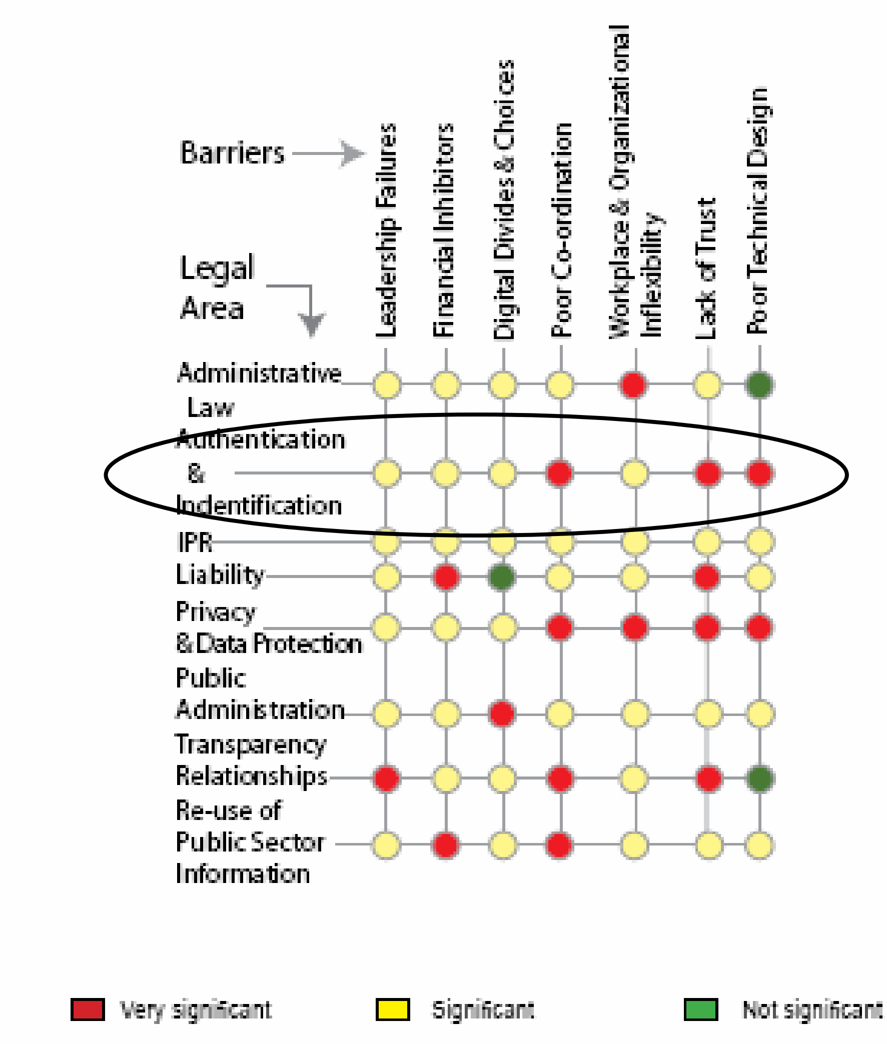
Information Society and Media

Identification

- Identification is an act of establishing or confirming the identity of a person.

Tilburg University

Barriers



Barriers
Legal Area

Legal Area	Leadership Failures	Financial Inhibitors	Digital Divides & Choices	Poor Co-ordination	Workplace & Organizational Inflexibility	Lack of Trust	Poor Technical Design
Administrative Law	🟨	🟨	🟨	🟨	🟥	🟨	🟩
Authentication & Indentification	🟨	🟨	🟨	🟥	🟨	🟥	🟥
IPR	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Liability	🟨	🟥	🟩	🟨	🟨	🟥	🟨
Privacy & Data Protection	🟨	🟨	🟨	🟥	🟥	🟥	🟥
Public Administration	🟨	🟨	🟥	🟨	🟨	🟨	🟨
Transparency Relationships	🟥	🟨	🟨	🟥	🟨	🟥	🟩
Re-use of Public Sector Information	🟨	🟥	🟨	🟥	🟨	🟨	🟨

🟥 Very significant 🟨 Significant 🟩 Not significant

TILT
Tilburg Institute for Law, Technology, and Society

Information Society and Media

Barrier: Leadership failures (*significant*)

- “a lack of leadership could result in slow development and implementation of authentication and identification processes.”

- “Knowledge and vision on technological developments seems to be important elements for leaders to guarantee the use of state-of-the-art authentication and identification processes.”

Barrier: Financial inhibitors (*significant*)

- “It seems clear that higher security demands result in higher costs for authentication and identification.”

- “At a pan-European scale, investments in effective, secure and trustworthy systems might be better affordable than at a national level.”

Barrier: Digital divides and choices (*significant*)

- “Authentication and identification processes should be easy to use and not too expensive to apply…”
- “…a process like a digital signature should not be too expensive for an organization to apply or too difficult to be used by any of its customers. Otherwise, a digital signature could result in digital divides.”

Barrier: Poor coordination (*very significant*)

- “Within EU Member States, different rules still exist because of different interpretations of the Directive’s provisions. This has also resulted in the failure to agree and implement standards for electronic signatures.”

- “the Commission will continue to encourage the development of e-signatures services and applications and will monitor the market. Beyond the support through eGovernment activities, particular emphasis will be on interoperability and cross-border use of electronic signatures. The Commission will encourage further standardization work in order to promote the interoperability and use of all kinds of technologies for qualified electronic signature in the internal market.”

Barrier: Workplace and organizational inflexibility (*significant*)

- “When authentication and identification processes are introduced in an organization, management and staff could resist such innovations. In some cases, their resistance could be legitimized by laws.”

- “the question is raised about ways in which the current structure of Employment Law in Member States act as a blockage or facilitator for any restructuring of the public sector labour market that may be needed to realize the full benefits from high levels of ePublic Services delivery and use?”

Barrier: Lack of trust (*very significant*)

- “…trust is an important enabler for eGovernment, especially because governments often process highly sensitive personal data from their citizens.”

- “Therefore, it is also of great importance that access to those personal data is highly secured, with the support of advanced authentication and identification procedures.”

- Government should authenticate itself first?

Barrier: Poor technical design (*very significant*)

- “…the standardization of the European ‘Qualified Electronic Signature’, [which] should give users a presumption that an electronic signature which complies with this standard will be presumed equivalent to handwritten signatures throughout Europe.

- “Does a lack of standardization or interoperability of electronic identification and authentication technologies remain a barrier to eCommerce applications in the public sector?”

Remaining barriers

- The unavailability of a secure authentication process
- Governments' uncertainty about identity management systems
- Identity theft
- Citizens' uncertainty about identity management systems

Example

- In 2005, the Netherlands introduced DigID: an authentication system (one login code) for Dutch citizens to get access to all government services (tax authorities, social security, student grants, permit applications, etc.).
- Only available for inhabitants of Dutch municipalities, registered in the local population register.
- Not available for citizens with a Dutch nationality, living across the border (in Belgium), but working in the Netherlands. These citizens can not (yet) receive a DigID to return their tax declaration.

Solutions: from the Solutions Report

Poor coordination:

- Keep additional requirements (see Article 3.7 of Directive 1999/93) by the public sector for receiving eSignatures to a minimum.
- Promote interoperability and the cross border use of eSignatures by obliging Member States to notify the European Committee for Standardization (CEN) about national standardization initiatives with regard to eSignatures.

Solutions: from the Solutions Report

Poor coordination:

- Prescribe by legislation that eSignatures that are used in the public sector should comply with a certain standard. This can be a national standard, with the CEN controlling the adequate level of standardization of Member States' national standardization initiatives. The CEN could also take the initiative to develop a European standard for eSignatures in the public sector, based on the national initiatives. The EU could also require Member States to cooperate in this respect.
- Require Member States to mutually recognize the eSignature standards developed in other Member States, when these are approved by the CEN. This legislative change could be achieved by amending the eSignatures Directive 1999/93/EC.
- Ensure other EU legislative initiatives, such as the Procurement Directives and the Invoice Directive, increase the cross border use of eSignatures.

Solutions: from the Solutions Report

Build better trust:

- Manage more effectively the ‘trust tension’ between the citizen’s concern about privacy, security and identity and their obligation to provide personal information to receive eGovernment services;
- Establish agreements, guidelines and frameworks to enhance trust;
- Enable citizens to gain experience with the use of Internet and, thereby, learn to trust it;
- Use Privacy Enhancing Technologies (PETs) to boost trust;
- Design, build, run and evolve sustainable ICT systems;
- Oblige government agencies to conduct Privacy Impact Assessments (PIAs) for new electronic information systems and information collections that involve the use of personally identifiable information.
- Ensure appropriate privacy practices are implemented and the public informed of their nature (e.g. through the posting on a Website of a ‘Privacy Notice’ describing the practices in operation).

Solutions: from the US eGovernment Act of 2002

Purposes of the US eGovernment Act of 2002:

- Provide effective leadership of Federal Government efforts to develop and promote electronic Government services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management and Budget,
- Improve the ability of the Government to achieve agency missions and program performance goals,
- Promote the use of the Internet and emerging technologies within and across the Government agencies to provide citizen-centric Government information and services, and
- Promote access to high quality Government information and services across multiple channels.

Solutions: from the US eGovernment Act of 2002

SEC. 203: COMPATIBILITY OF EXECUTIVE AGENCY METHODS FOR USE AND ACCEPTANCE OF ELECTRONIC SIGNATURES:

a. The purpose of this section is to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government.

b. In order to fulfill the objectives of the Government Paperwork Elimination Act (…), each Executive agency (…) shall ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director.

c. The Administrator of General Services shall support the Director by establishing a framework to allow efficient interoperability among Executive agencies when using electronic signatures, including processing of digital signatures.

Solutions: from the OECD Recommendation and Guidance 2007

- The Guidance sets out the context and importance of electronic authentication for electronic commerce and electronic government and provides a number of foundation and operational principles that constitute a common denominator for cross-jurisdictional interoperability.

- The Recommendation encourages efforts by Member countries to establish compatible, technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities.

Solutions: from the OECD Recommendation and Guidance 2007

Foundation Principles:

1. Systems Approach
2. Proportionality
3. Roles and Responsibilities
4. Security and Trust
5. Privacy
6. Risk management

Solutions: from the OECD Recommendation and Guidance 2007

Operational Principles:

1. Usability
2. Fit for purpose
3. Business continuity
4. Education and awareness
5. Disclosure
6. Complaints Handling
7. Independent audit and assessments
8. Cross-jurisdictional approaches
9. Standards

Solutions: from the Austrian Model

Austrian Identification System:

- Every person gets assigned a unique personal identification number, the so called Source PIN
- For Identification in E-Government Processes, Sector Specific-PINs (ssPIN) are being used
- Each ssPIN is different and it is neither possible to calculate the underlying sourcePIN nor any other sector's ssPIN from a given ssPIN
- For access to a Governmental Application by means of a citizen card:
  - Citizen is uniquely identified (ssPIN)
  - And authenticated by electronic signature

- *Thomas Rössler, Giving an Interoperable Solution for Incorporating Foreign e-IDs in Austrian E-Government. IDABC Conference 2005, 18 February 2005*

Solutions: from the expert #1

- Limit (re)-outsourcing of data processing by government agencies to organizations outside the EU, because this undermines trust.
- It should be easy for citizens to have their incorrect data corrected by government agencies, because time-consuming procedures result in distrust.
- Make sure that public officials (sometimes employed by private agencies) do not use weak authentication / verification systems for obscure purposes. Biometrics might help solving insecurity in online communications.
- Strong message for cross-border interoperability.

Solutions: from the expert #2

- Pan-European standardization and interoperability are at the heart of barriers to European eGov services. Also look at the EU SecurEGOV project.
- Austria (and particularly its citizen card) is perceived as a world leader in providing E-Government e-ID solutions. Also look at e-ID initiatives (ID-cards) in other countries.
- There is no standardization of authentication levels across the EU, which particularly causes barriers for pan-European eGov services. Solution: standardization across Europe, for instance legally accepted minimum standards for specific eGov services).
- Learn from the New Zealand All-of-Government e-Authentication Programme.

To do:

- Comments from the eGov Barriers Expert Group
- Comments from this workshop

- Final version Chapter Authentication and Identification in the final Solutions for eGovernment report

Overcoming Barriers in the field of Authentication and Identification

Dr. Sjaak Nouwt
TILT – Tilburg Institute for Law, Technology, and Society
Tilburg University, the Netherlands
j.nouwt@uvt.nl

Information Society and Media