

Identity management 2.0

using

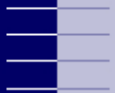
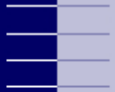
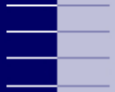
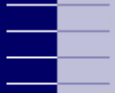
Identity tokens 1.0

Or: How to use your passport for Web client authentication

Martijn Oostdijk + Dirk-Jan van Dijk

SafeNL, Nijmegen, 12-12-2008

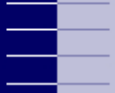
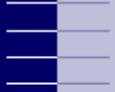
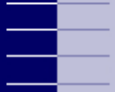
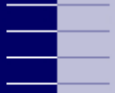




Contents

- Identity
- The ePassport
- Identity 2.0 + CardSpace
- Conclusions





What is identity?

- Identity is what you and others *claim* about you
- In real life, whether you trust a claim
 1. Usually depends on contextual factors,
 2. sometimes on authorities (reputation),
 3. and sometimes on *authorities by proxy*
- In online life there is little context (1), so identity is defined using trust in authorities (2, 3)!



Identity in ~~“real”~~ ^{online} life

KONINKRIJK DER NEDERLANDEN

Dordrecht

DigiD
Je eigen inlogcode voor de hele overheid

Aanvragen van een DigiD gebruikersnaam

- U ontvangt binnen 5 dagen een activeringscode per post waarmee u uw DigiD gebruikersnaam kunt activeren.
- Na het activeren kunt u bij aangesloten overheidsinstellingen met uw DigiD gebruikersnaam inloggen.
- Activeer uw DigiD gebruikersnaam binnen 20 dagen, anders vervalt deze.

Gebruikersnaam vergeten? Wachtwoord vergeten? Opnieuw een DigiD gebruikersnaam aanvragen.

[Hulp bij invullen](#) >

Burgerservicenummer: *

Geboortedatum: * 01 januari 1960

Postcode: *

Huisnummer: *

Huisnummertoevoeging:

E-mailadres:

E-mailadres herhalen:

Ik accepteer de gebruiksvoorwaarden *

Annuleren Verder >

Meer informatie vindt u op www.burgerservicenummer.nl. Een burgerservicenummer bestaat uit 9 cijfers. Hebt u een achttienjarig burgerservicenummer? Toets dan eerst een nul.

Geef het adres op waar u staat ingeschreven bij uw gemeente.

Bijvoorbeeld: A, bis, hs, III.

U bent niet verplicht uw e-mailadres op te geven. Met het invullen van uw e-mailadres geeft u DigiD toestemming om via uw e-mailadres op de hoogte te worden gehouden van ontwikkelingen ten aanzien van DigiD. Mocht uw DigiD-account na 10 werkdagen nog niet geactiveerd zijn, dan ontvangt u een herinneringsmail.

Als u de gebruiksvoorwaarden niet accepteert, kunt u niet verder.

Velden met een * gemarkeerd zijn verplicht. Hebt u geen postcode en/of huisnummer? Kijk dan bij [Hulp bij invullen](#) >.

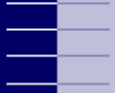
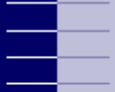
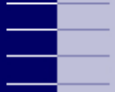
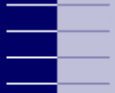
14. opmerkingen

15. handtekening bewaarden

16. opmerkingen

Sorruit.

Telematica
Instituut



Electronic passport

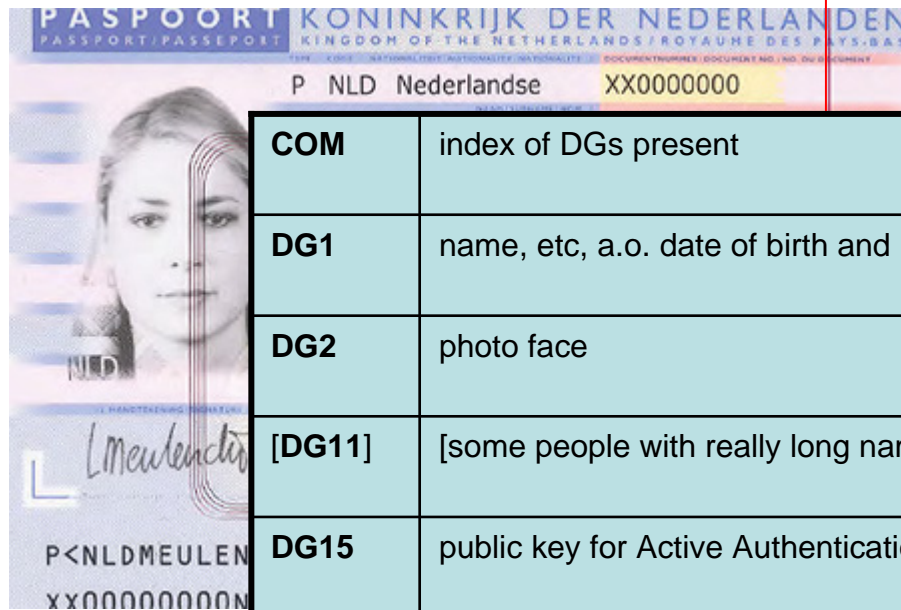
- Issued by government
- Standardized by ICAO
- Contains chip with
 - Information about card holder
 - Mechanism to verify *integrity* of that information
 - Mechanism to verify *authenticity* of chip
 - Mechanism to communicate *confidentially*
- Not intended for online verification
- Dutch version was tested in 2006 by RU Nijmegen (and other test labs)

Can we use an ePassport as Information Card inside Windows Card Space™?



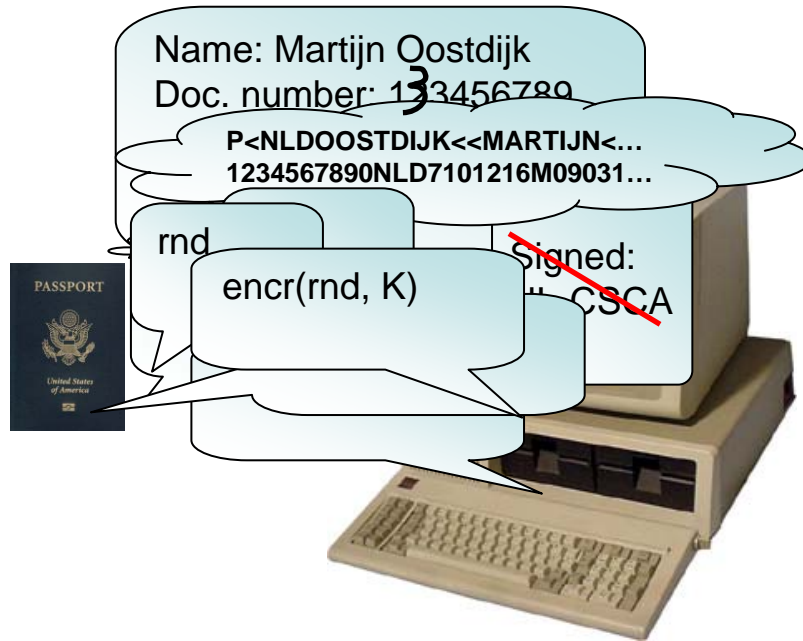
What's inside?

Chip



Antenna

Logo



Threats



- Skimming (privacy)
- Eavesdropping (privacy)
- Tracking (privacy)
- Altering (integriteit)
- Cloning (authenticiteit)
- Look-a-like fraude

Controls

- Basic Access Control (access & confidentiality)
- Passive Authentication (integrity contents)
- Active Authentication (authenticity chip)
- Extended Access Control (confidentiality biometric features)
- Biometry (link to card holder)



Identity 2.0

- User-centric
 - just like “Web 2.0”: emphasis is on user control
- Standards are open & simple
- Examples:
 - OpenID 
 - Information cards 
- It's hot (like everything 2.0)
 - <http://www.identityblog.com>
 - <http://www.links.org/>
 - <http://self-issued.info>
 - <http://eternaloptimist.wordpress.com>
 - <http://identity20.com>
 - <http://virtualsoul.org/blog/category/identity>
- Microsoft has learned its lesson from MS Passport...





Laws of Identity

By Kim Cameron of Microsoft

Explained for dummies:

- People using computers should be in control of giving out information about themselves, just as they are in the physical world.
- The minimum information needed for the purpose at hand should be released, and only to those who need it. Details should be retained no longer than necessary.
- It should NOT be possible to automatically link up everything we do in all aspects of how we use the Internet. A single identifier that stitches everything up would have many unintended consequences.
- We need choice in terms of who provides our identity information in different contexts.
- The system must be built so we can understand how it works, make rational decisions and protect ourselves.
- Devices through which we employ identity should offer people the same kinds of identity controls - just as car makers offer similar controls so we can all drive safely.

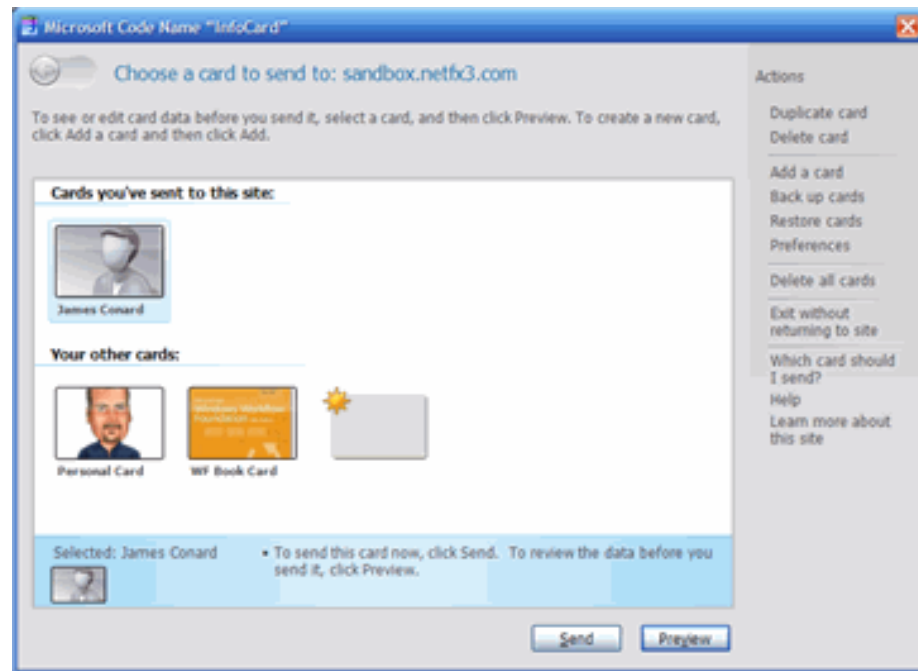
<http://www.identityblog.com/>



Telematica
Instituti



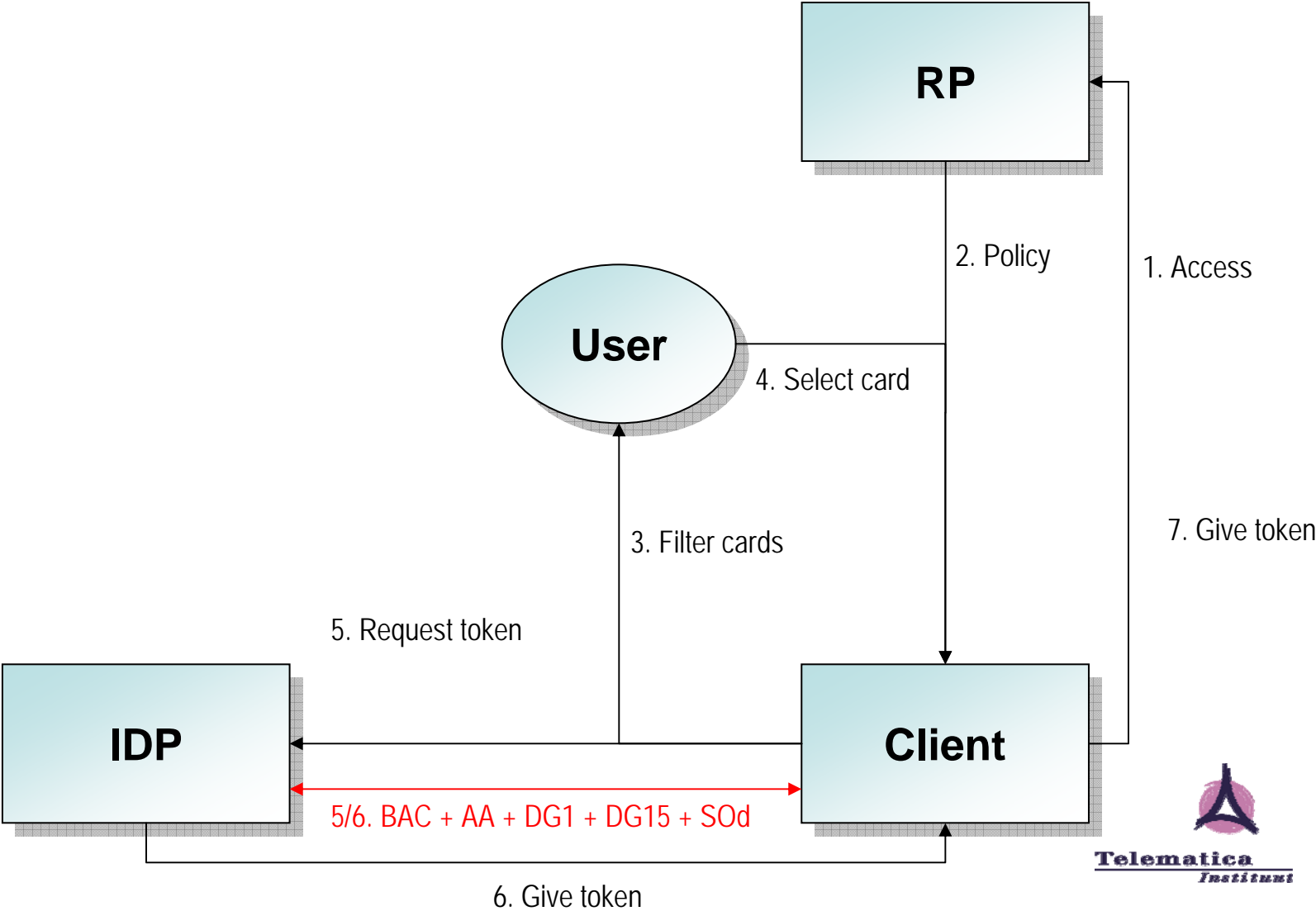
Information Cards



- Open standard (Identity Selector Interop Profile)
- Windows Card Space is Microsoft's implementation
- Some credentials kept at client, some at IdP
- To prevent phishing: dialog leaves context of OS



CardSpace managed card scenario







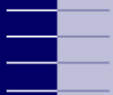
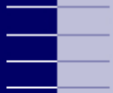
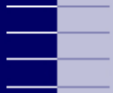
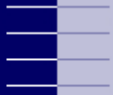






Demo

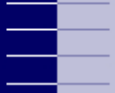
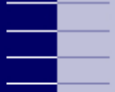
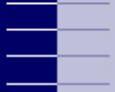
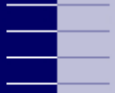




Future? Enough loose ends...

- From prototype to robust application
 - Local application or browser plugin instead of Java applet?
- Works for Dutch ePassport, also for other countries?
 - AA is optional in EU, CSCA not public everywhere
- Support OpenID?
- Privacy issues (KC's law 2)
 - What if I only want to claim "above 18" or "Dutch citizen"
 - Why do we need (to trust the) IdP?
- Who pays for the card reader?
 - Business case?
 - NFC?





Conclusions

- User-centric Identity (Identity 2.0) is hot
- At the same time governments are rolling out large scale PKIs
 - using hardware tokens
 - in case of ICAO ePassport: worldwide!
 - banks and credit card companies will follow?!?
- Such PKIs are very 1.0 but we (the normal users) can re-use infrastructure for Identity 2.0 purposes
- Source code for using ePassport with Information cards will be available GPL or LGPL
 - Check <http://jmrtd.org> and <http://nl.net.nl/>
- Privacy issues are something for future work













Q (& A)

