



Wednesday, May 14

Track A
Identification Applications & Policy

Session: Identification & Privacy Policy

Time: 10:15 AM – 12:00 PM

Room: W202 B&C

Moderator:

James Sheire

Manager, Government Programs
NXP

Speakers:

Gilles Lisimaque

Partner

Identification Technology Partners, Inc.

Neville Pattinson

VP, Government Affairs & Standards
Gemalto

Peter Sand

Director, Privacy Technology
Department of Homeland Security

Catherine Johnston

President & CEO
ACT Canada



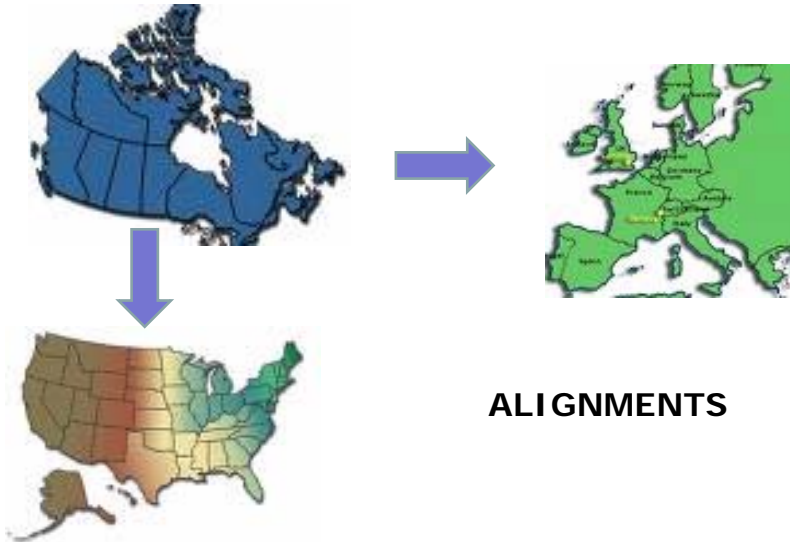
Canada and Privacy

A Presentation to
CTST 2008

Catherine Johnston
President & CEO ACT Canada
Chair, ISCAN

Federal and Provincial Legislation

- 2 federal laws
 - Privacy ACT 1983
 - PIPEDA 2001
- Provincial and Territorial Laws
- Private Sector
- Sector Specific



Enhanced Driver's Licences and other cross border ID

- personal information of participating drivers must remain in Canada
- meaningful and independent oversight
 - regular reporting of oversight activities and corrective measures

RFID Privacy Concerns

- Potential surreptitious location tracking of individuals carrying an EDL
- Potential of unencrypted or unprotected unique identifier number
- Vulnerability of personal information

Steps to Protect Privacy on EDLs

- robust privacy and security
- thorough privacy impact assessments and threat risk assessments at the outset
- Compliance with applicable local privacy legislation
- Consultation with the appropriate privacy oversight officials

Principles & New Technology

- Fair Information Practices
 - Use appropriate safeguards
 - Disruptive transformative technologies
 - Revocable biometrics
- Systemic Design and Protection

Join us and let us ACT on your
Behalf

ACT Canada

85 Mullen Drive
Ajax, Ontario, Canada L1T 2B3
905 426-6360

www.actcda.com

info@actcda.com



***Identity and Access control
privileges applied to Smart Cards***

Gilles Lisimaque
Partner
Identification Technology Partners, Inc.
GLisimaque@idtp.com



CTST 2008 - Orlando, FL

1



The various players in Identity


- Identity certifier (Identity Authority)
 - Certify the attributes claimed by a given individual (identified by his/her biometrics) are indeed correct (citizen, employee, military, etc.)
- Privilege verifier
 - Verifies a given individual is entitled to be in a given role based on claimed identity attributes (being paid by his/her employer, entering his/her own country, wearing a uniform, etc..)
- The individual (person) in a given capacity

Identity defines who we are in the eyes of others



© 2008 All Rights Reserved ID Technology Partners, Inc.

2




Attributes of Identity

- **Physical attributes**
 - Face, Gender, Race, Eye color, Hair color, Gait, Height, Weight, Hand Geometry, Fingerprints, DNA, Iris, etc.
- **Inherited attributes**
 - Family name, Native Language, Place and Date of Birth, Parents names, blood relatives, Mother's maiden name, etc.
- **Ascribed attributes**
 - First and Middle names
 - Identity numbers (SSN, Driver's License #, Passport #, Etc.)
 - Account numbers (Credit Card #, Bank Account #, Telephone #, Frequent Flyer #, Ez-Pass #, e-mail address, etc.)
- **Historical attributes**
 - Address, previous addresses, friends, bank and credit record, spending habits, public records, video rentals, etc.

ID TECHNOLOGY
PARTNERS

© 2008 All Rights Reserved ID Technology Partners, Inc.

3



Identity Credentials

- Combine most often:
 - **Physical attributes** (biometry) allowing to link the credential to the legitimate bearer
 - **Inherited attributes** (e.g. name) allowing to link the bearer to other documents presented
 - One **ascribed attribute** (e.g. driving license number) given by the identity authority which issued the document. Is often a pointer/index to a data base
- Nearly always an **implicit privilege** is attached to the identity credential

ID TECHNOLOGY
PARTNERS

© 2008 All Rights Reserved ID Technology Partners, Inc.

4

Ascribed Attributes & Authentication



- *Attributes used for identification* should not be mixed up with *methods used for authentication*.
- *Ascribed attributes should not be secrets*. They are identification attributes but in themselves should never be used to authenticate their owner (e.g. SSN)
- *Ascribed attributes need to be disclosed* (they are equivalent to indexes in databases) but in case they are compromised or renewed, they should be changed (e.g. Passport number)



Authentication elements used often have often chances of being compromised



© 2008 All Rights Reserved ID Technology Partners, Inc

5



Credentials & Implicit Privileges

- A *passport* is an identity credential allowing the legitimate bearer to enter the country of *citizenship*
- A *driving license* is a privilege credential allowing the legitimate bearer to *drive a vehicle*
- A *pilot license* is a privilege credential allowing the legitimate bearer to *fly a certain type of plane*
- A *membership card* is a privilege credential allowing the legitimate bearer to enter the corresponding *club*
- A *boarding pass* is a privilege credential allowing the person whose name is on it to *board a plane*

Most privilege credentials have attributes of identity in order to link the privilege to the legitimate bearer. Because of these attributes, they are (too) often called Identity Credentials



© 2008 All Rights Reserved ID Technology Partners, Inc


6




Identity is different than Privilege

- I have the *privilege to vote because I am a US citizen* but I need to register in order to exercise this privilege
- I am allowed to *travel abroad* and come *back to the US* because I am a US citizen (implicit privilege attached to my passport) but in order to enter some *other countries* I may need to apply for a *visa* (explicit privilege)
- An employee is allowed to *enter his/her company site* (implicit privilege) but most likely needs to register in order to enter another company's site

Privileges define what we are allowed to do




© 2008 All Rights Reserved ID Technology Partners, Inc. 7

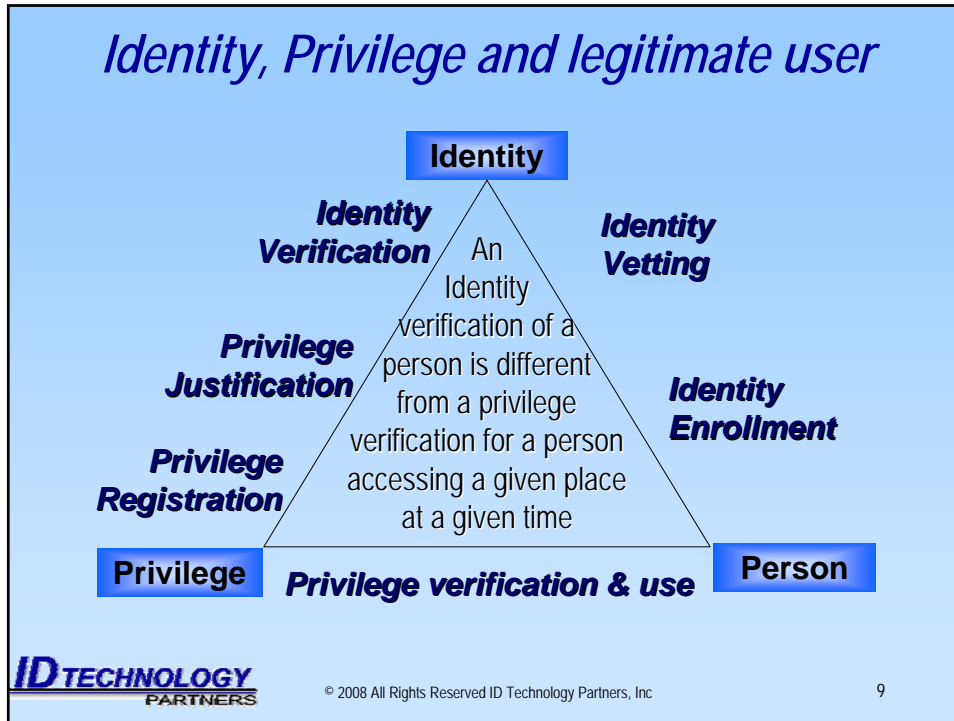


ID Smart Cards are not all privilege cards


- Having a PIV card most likely allows the legitimate cardholder to enter the building of his/her agency but probably does not grant automatically the privilege for entering another agency's site. This is an *implicit privilege for an identity credential*.
- *Identity credentials* do store information regarding the legitimate cardholder but the privileges (e.g. access rights) are often managed in the back end of each of the systems
- In *privilege credentials* (e.g. Registered Traveler) no identity attribute about the user needs to be stored on the card but only the reference of the privilege(s) granted and a means to identify the legitimate bearer (fingerprints, picture, etc.)



© 2008 All Rights Reserved ID Technology Partners, Inc. 8



- ## Issues and principles
-
- Most of the time, *identity is not required at the time of verification of a privilege* as long as the legitimate privilege holder can be verified (legitimate user authentication)
 - Identity as well as personal information *should not be disclosed (or exposed) to un-trusted entities*
 - *Privilege granting process should be as easy* as it can be but should not happen without user's consent
 - Because *Smart cards* are able to be "smart" they should be *used to enforce the rules and principles of the application* including protecting the user's personal information
- ID TECHNOLOGY PARTNERS** © 2008 All Rights Reserved ID Technology Partners, Inc 10




Identity Verification

When an **identity credential** is used to verify the user's identity (and/or the implicit privilege attached to the credential), the main objectives of the verification are:

1. Is the **issuing identity authority** of the document trusted by the verifier?
2. Is this person the **legitimate bearer** of this identity document?
3. Is this person listed (wanted) on any **black list** the verifier has?

Identity verification deals with the past (person on a wanted list) or the future (re-course if things go wrong) but has often little to do about allowing what is the person doing in the present.

ID TECHNOLOGY PARTNERS © 2008 All Rights Reserved ID Technology Partners, Inc 11



Identity Verification example

- When using my Passport entering the US, my identity will be verified and the implicit privilege (citizenship) will be invoked.
- The match between the legitimate bearer and the identity credential is done as thoroughly as possible (e.g. using EAC when implemented)
- A check is made against watch lists to verify the user is not on any of them

ID TECHNOLOGY PARTNERS © 2008 All Rights Reserved ID Technology Partners, Inc 12



Privilege Verification

- When a **privilege credential** is used to verify the user's privilege attached to the credential, the main objectives of the verification are:
 1. If the **privilege verifier** is not the **privilege issuer**, is there is an agreement (trust) between the two?
 2. Is this person the **legitimate user** registered for this privilege?
 3. Is this **privilege still active** for this person?

The complete identity of the person, or attributes not related to the privilege verification have no need to be used or disclosed



© 2008 All Rights Reserved ID Technology Partners, Inc

13



Privilege Verification example


- When entering CHINA with my US passport (Identity credential), I have to present a VISA (privilege credential).
- My passport is the link between me (as a person) and the VISA I had to apply for at the Chinese embassy in the US.
- The Chinese immigration officer verifies I am the legitimate user of this VISA (using the picture the name from my US passport (e.g. BAC)) and verifies the VISA has not been revoked.
- They will also most likely verify (also) I am not on any of their watch lists as they have a "some" attributes of my identity (Name, DoB, Citizenship) in their hands

In this example, China is not doing an identity vetting (they rely on the US for that part) but they do a privilege verification for the VISA



© 2008 All Rights Reserved ID Technology Partners, Inc

14




Example: the “age” privilege

- Being over 21 allows to buy tobacco and/or alcohol in the US.
- The merchant is required to verify this “privilege” by law but does not need to know about the identity of the person
- A correctly constructed Identity Credential should be able to answer such a question (is bearer older than 21?) by providing a proof (digital signature of the answer) but with no other information about the credential bearer.

ID TECHNOLOGY
PARTNERS

© 2008 All Rights Reserved ID Technology Partners, Inc

15



The three points of interaction

- In all Identity or privilege applications, there are always three very different points of interactions between the legitimate user and the rest of the system:
 - **Enrollment & Identity vetting:** verifies the Identity (back ground checks) and links it to the user’s biometric (FIPS 201 is a very good model)
 - **Privilege granting:** Verifies the user has being enrolled by a trusted authority (Identity verification) and has a legitimate reason to apply for the given privilege. The system then “activates the privilege” for that given user either in the back end system, in the card, or in both
 - **Verification station:** Verifies there is a valid privilege for the token presented and it is used by the legitimate bearer

ID TECHNOLOGY
PARTNERS

© 2008 All Rights Reserved ID Technology Partners, Inc

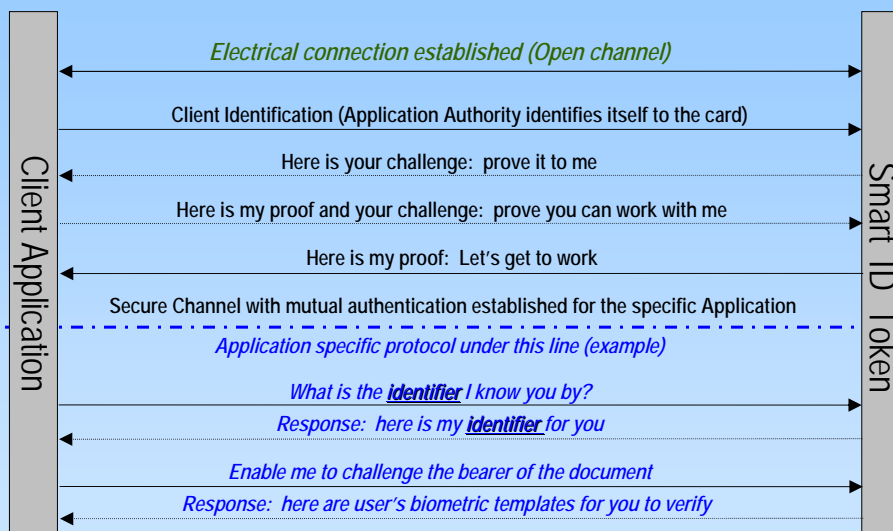
16

Fuel for thoughts




- In an *ideal world a smart ID credential should*
 - *Not reveal any personal information* to an unknown requestor, with or without the user's consent
 - Should *answer about existence of privileges* present in the credential only when asked by an authorized party or when its user explicitly consents to provide an answer
 - Should be a *safe repository of the privileges* the legitimate user has and should be able to accept new (or remove old) privileges when *authorized by its user (and its original issuer)*
 - Should be able to *authenticate authorities* willing to access the identity, privileges or personal information (e.g. biometry) of its legitimate user and limit accordingly the information disclosed.

The ideal credential protocol



Do not search for what you can do with the card but ask the card what it can do for you



The Ideal Smart ID Credential

- Four *different behaviors* depending on who's talking to it.
- Able to *register new privileges* and how to communicate with them
- Communication over the contactless interface protected by *mutual authentication* and a *session key*
- *Personal identifiable information* released only to authenticated requestors or when explicitly authorized by the legitimate user

ID TECHNOLOGY
PARTNERS

© 2008 All Rights Reserved ID Technology Partners, Inc

19




The Ideal Smart ID Credential: Look who's talking

- *The Identity Issuer* has access to all user's personal information allowing the highest assurance of verifications
- An *unrelated identity verifier* has limited access to user personal information if the user consents to share such information.
- A *service provider* (e.g. access control system) can be securely registered in the credential
- *Registered service providers* are allowed to communicate securely with the credential

ID TECHNOLOGY
PARTNERS


© 2008 All Rights Reserved ID Technology Partners, Inc

20



Privileges loaded in Identity cards

- Instead of having separate cards for identity and privileges, a possible solution is to register dynamically privileges in the identity credential:
 - Instead of issuing a “local” access control card, a PIV card could be loaded with a “*virtual access control privilege card*”.
 - Such a PIV card then becomes an “*access control card wallet*” sheltering the “virtual local access control cards” for all the sites the user is allowed to get access to.
 - These “*virtual access control cards*” are just “*active images*” of the local cards which would have been issued (“cards” issued under the authority of the site to access and with the credential identifier allocated by that site to that specific credential. No need to share a universal CHUID anymore for access).




© 2008 All Rights Reserved ID Technology Partners, Inc

21

Same concept for E-Passports & e-Visa

The country has to actively identify itself to the ID card in order to set the context for the privilege it is looking for.

Country Identifier




Country	Authentication	Visa
China	Algo(x)+Key(z)	#13725#
Russia	Algo(3)+Key(4)	AbC45&9
Hong-Kong	Algo(\$)+Key(&)	UFC666

Authentication Mechanism (Algorithm + Key)	Visa Number
---	-------------



e-Passport information (ICAO)

The ID credential contains (and protects) a lookup table for the multiple privileges obtained by the legitimate bearer of the ID credential



© 2008 All Rights Reserved ID Technology Partners, Inc

22



Conclusion

- *Identity* and *privilege* should not be treated the same way in order to protect *privacy*
- *Identity Cards* can be smart and used to load, manage and *use privileges*
- Any sensitive *personal information disclosed to an un-authenticated party*, even with user consent, is not only a *privacy risk* for the credential bearer but may turn into a *security threat* for the whole identity system

ID TECHNOLOGY
PARTNERS

© 2008 All Rights Reserved ID Technology Partners, Inc

23

Thank you for your attention ..



Gilles Lisimaque

GLisimaque@idtp.com



ID TECHNOLOGY
PARTNERS

© 2008 All Rights Reserved ID Technology Partners, Inc

24

