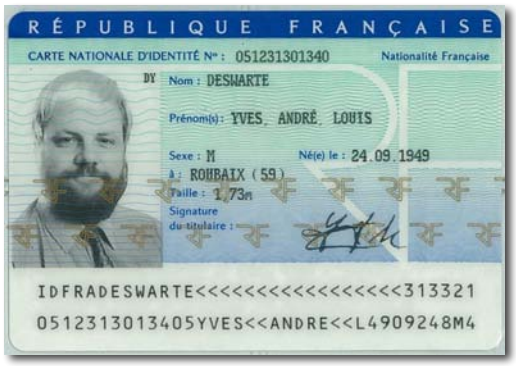
Towards a Privacy-Preserving National Identity Card

Yves Deswarte, Sébastien Gambs
yves.deswarte@laas.fr, sebastien.gambs@irisa.fr

LAAS-CNRS

Toulouse, France

National Identity Card



- ☹ Discloses more information than needed (privacy)
- ☹ Can be used by a similar looking person (weak biometrics)
- ☹ Forgeable, clonable

- ☺ No information leakage (privacy)
- ☺ Untraceable
- ☺ Cannot be used by anybody else (strong biometrics)
- ☺ Unforgeable, clonable ?

Current Electronic ID cards

w.r.t. traditional cards:

- More secure (tamper-resistant chip)
  - Difficult to forge
  - Protection against identity stealing if using stronger biometrics (e.g., fingerprint)
- … but more privacy intrusive (online use)
  - Readable identity information
  - Risk of abuse --> tracing, information crossing
    ex. e-administration, e-commerce, …

What an Id Card is used for ?

- Proof of Nationality
  e.g. border control
- Proof that a document is valid for a person
  e.g. credit card, bank check, boarding pass, …
- Proof of rights
  e.g. senior citizen, free access to a local library, swimming pool…
- Proof of identity for sensitive registration (liability)
  e.g. bank account, new business, …
- Proof of not being on a wanted person list
  e.g. police control, …
- … and many abusing usage :
  e.g. monitoring, tracing, information crossing, marketing, …

Using a Privacy-Preserving ID Card

- The card is issued by an authority (e.g., local government)
  the chip is supposed to be tamperproof (confidentiality, integrity)
- The chip contains the identity information + biometry template
- Contact card (no risk of RFID skimming, owner's consent)
- Mutual authentication between chip ① and (certified) reader ②
  with unlinkability (there is no ID card number !)
- User authentication through biometry scan ③
  - By the card (*fingerprint*) or by the reader (*fingerprint*, *iris*, *voice*, …)
  - Biometric templates stored and verified by the chip
- Basic principles:
  - The stored information never leaves the chip
  - Questions are asked to the chip ④ (according to *reader's clearance*),
    the replies are only binary : yes or no ⑤

P-P ID Card use

- Nationality proof :
  - Reply = YES (as soon as biometry verification ③)
- Identity verification (e.g. boarding pass, bank check…) :
  - Question : Name & First Name = "Doe, John" ?
  - Reply : YES or NO
- Vicinity verification : city, county, state, …
  (e.g., free access to library)
  - Question : Home Town = "Saint Malo" ?
  - Reply : YES or NO
- Majority verification, senior citizenship, …
  - Question : today = 09/24/2009; age ≥ 18 ?
  - Reply : YES or NO
- Police control (e.g. wanted people)
  - Question : Name & First Name = "Bin Laden, Usama" ?
  - Reply : NO

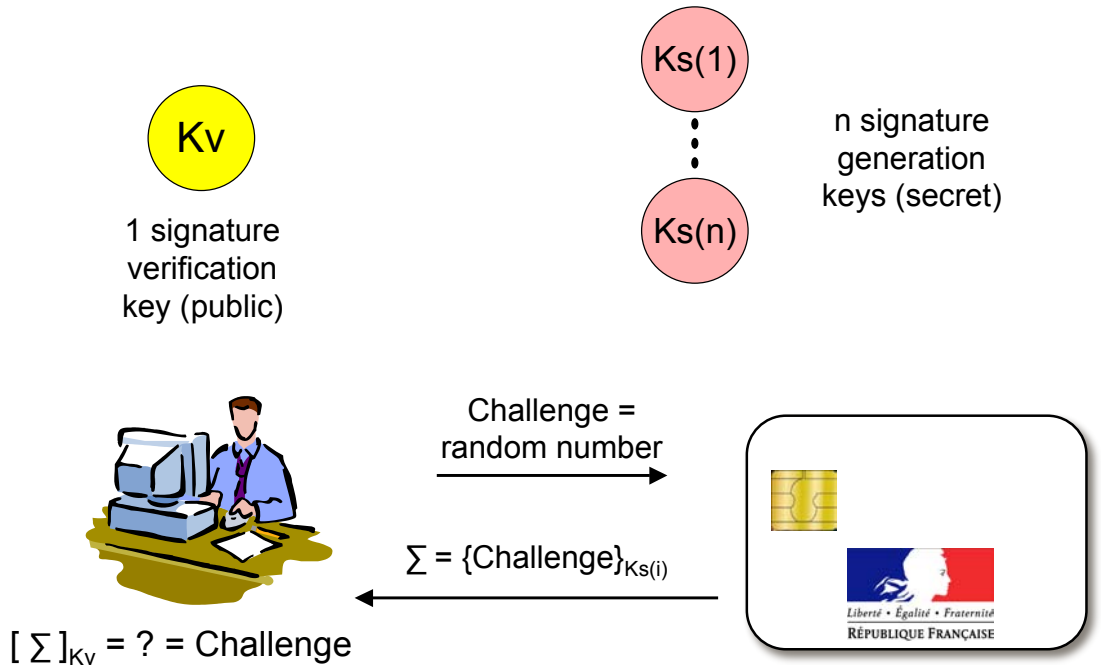
Hardware Technologies

- Smartcard reader + biometry :

Software & algorithms

- PK Certificate
  - Reader authentication
- Group signature
  - Card authentication
- Fuzzy commitment
  - Biometry verification
- Secure channel (between card and reader)
  - Reader public key, card-generated session public key
  - Semantically secure binary reply
- To relax tamperproof requirement :
  - Biometry verification: fuzzy extractor --> decrypt stored data
  - Non-interactive zero-knowledge proofs of statements

Group Signature



Fuzzy Commitment / Extraction

- Biometry scan (sent to the chip)
  "11001010110001101101010101...10101001011110010101101101 1"
- Transformation : ECC encoding
  "01101001001110001011010011"
- Error Correction --> Closest Code word
  "01111000101110011011010010"
- Is it equal to the stored template ? Yes/No

Extensions (1)

- Biometric sensor + display on the smartcard itself
  - Better trustworthiness ?
  - Other uses: e.g., display the owner's picture, display the question, …

Extensions (2)

- Remote identity proofs
  - e-Administration: income tax declaration, official document printing, …
  - e-Voting
  - e-Commerce, …
- Problems
  - Limits of unsupervised biometry ?
  - Phishing with stolen reader ?

Extensions (3)

- Integrate the ID card into a cell phone
  - Wireless connection (NFC, Bluetooth, WiFi, 3G)
  - Biometry through phone sensors (voice, iris)
  - More capability on the user side (e.g., display, audit log)
- Problems
  - Trustworthiness of the phone ?
  - More risks of linkability (IMEI, MAC@, …)

Conclusion

- Users can be confident that this card disclose as little information as possible
- It is more secure than current cards
  - Cannot be used, except by the owner
    --> low risk of stealing
    --> no need for revocation
    --> no burden for recreation
- The technology exists today
- Would it be adopted by states ?

More information

- Extended version at

http://hal.archives-ouvertes.fr/hal-00411838/fr/

- Mailto: deswarte@laas.fr