



Privacy Enhancing National ID Cards

Digital Identity Forum
November 7th, 2001

Andrew Drapp
Chief System Architect
Hitachi Europe Ltd.
andrew.drapp@hitachi-eu.com

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Alternatively:

Why a Smartcard based National ID
card does not necessarily reduce
privacy.

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



NOT

Is a National ID card right or wrong?

BUT

If a National ID card system is implemented, how can it be implemented correctly?

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next

Agenda

- Government IDs Today
- Biometrics
- Blunkett on ID cards
- Online versus Offline
- Blind Signatures
- Doing it Right

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Government ID Cards

- Most countries today currently issue many types of ID cards.
- I personally have 9 different official government issued ID cards.
- Governments WILL issue some form of ID

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Government ID Cards (cont.)

- US:
 - Social Security Card
 - Passport
 - INS Pass/Port PASS
 - Driver's License
- Japan:
 - Alien Registration Card
 - Driver's License
 - Insurance Card
- UK:
 - National Insurance Card
 - NHS Card

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Government ID Concerns

- Will it invade people's rights or privacy?
- Will it be a crime not have an ID?
- The "optional" mandatory card:
 - Driver's Licenses
 - Banking
 - Hospitals

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Misuse of Government IDs

Last night my friend and I stopped at a Venice club/bar. At the door they were doing the normal ID check, but then took my driver's license and swiped it into a little Palm-like device...and all the info popped up on the screen. I was startled, amused and outraged all at the same time. My friend knows the new owners of the building and told me that the owners had rented part of the upstairs space to a guy with a youth marketing company. What are they doing with this information?

Source: Posting 20/10/01 on Cypherpunks mailing list by Giovanna Imbesi

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Biometrics Review

- Biometrics uses physiological or behavioral characteristics to do one of two things:
 - Identify: the subjects identity is determined
 - Authenticate: a claimed identity is verified

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Biometric Problems

- FTE (Failure to Enroll)
 - Ranges from 0.2% - 20%* on currently available biometric solutions
- FAR (False Acceptance Rate)
 - Ranges from 0% - 15%*
- FRR (False Rejection Rate)
 - Ranges from 0% - 60%*
- FAR and FRR are inversely proportional
- FRR increases over time*

*Source: International Biometric Group

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Biometric Problems (cont.)

- From the October 6th Economist:
Those about to invest in iris-scanning security technology will be disappointed to learn of recent developments in the treatment of glaucoma...An innocuous side-effect of this drug is to cause a change in both iris color and morphology...Apart from rendering iris scanning potentially useless for these people, unscrupulous types without glaucoma may be tempted to use the drugs to “change” identity.

Simon Longstaff
Consultant Ophthalmic Surgeon
South Yorkshire

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Biometric ID Concerns

- What do you do with the significant portion of the population who cannot use biometrics?
- How will the data be protected?
- How will the data be used?
- Will various IDs be linked together?

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Blunkett on ID Cards

- [Blunkett] also maintained that improvements in electronic thumb or fingerprint technology or even "iris-prints" meant the threat of forgery would not make the system redundant.

Source: BBC

http://news.bbc.co.uk/1/hi/english/uk_politics/newsid_1559000/1559245.stm

- [Blunkett] claims that plans for a national ID card had been ditched were "not true".

Source: Breakfast with Frost

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Blunkett on ID Cards (cont.)

- So, it appears that Blunkett is suggesting a National iris and/or fingerprint code database.
- Given such a database, what is the need for a card? Hand held iris/fingerprint scanners could look up the identity and any information that would have been on the card.

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Online vs. Offline

- For an online biometric identity check, NO card is necessary.
- An online biometric DB has significant privacy/security issues.
- An offline system is harder and more expensive to implement *correctly*
- A *poorly* implement offline system faces greater threats of fraud

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Online vs. Offline (cont.)

- EMV example:
 - SDA (Static Data Authentication)
 - Online
 - Cheaper to implement
 - Less secure
 - DDA (Dynamic Data Authentication)
 - Offline
 - More expensive to implement
 - More Secure

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Blind Signatures

- Certificates/IDs can be anonymous
 - An “of age” certificate could indicate the holder is of legal age to purchase alcohol/tobacco/etc, without divulging any personal information (including age)
 - A “resident of X” certificate could prove that the holder has the right to services of X, again, without divulging any personal information

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Doing it Right

- Use high spec, DPA resistant, crypto coprocessor smartcard
- Store digitally signed identity on the card
 - Identity can be certificate
 - Identity can be “blind”
 - Identity can store rights/roles/etc.
- Built in Authentication function on card
 - Biometric
 - PIN or Password

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Doing it Right (cont.)

- Make both ID and Authentication functions only accessible to authorized requests
- Terminals can read identity, and verify owner.
 - Terminal reads fingerprint
 - Sends fingerprint to card
 - Card verifies fingerprint
 - Card responds with digitally signed Valid/Not Valid response
 - Same as above for IRIS/PIN/etc.

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Doing it Right (cont.)

- Benefits:
 - Highly Secure, difficult to forge, ID card
 - Card identity strongly linked to card holder (much stronger than photo)
 - No online biometric DB
 - User in control of biometric data

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Doing it Right (cont.)

• Benefits Continued:

- Authentication function can be different from user to user
- PIN/Password can be used as “backup” for failed biometric checks
- Only government agents have access to ID. Not accessible by hotels/landlords/etc.
- Solves all concerns related to biometric ID cards

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next



Questions?

Andrew Drapp
Chief System Architect
Hitachi Europe Ltd.
andrew.drapp@hitachi-eu.com

©2001 Hitachi Europe Ltd. All Rights Reserved

HITACHI
Inspire the Next