UNIK
UNIVERSITETSSTUDIENE
PÅ KJELLER

Privacy protection in biometric passports

György Kálmán
gyorgy@unik.no

Agenda

- Biometric passports overview
- RFID applications
- BAC weaknesses
- Image related problems
- Enhancements in EAC
- Watermarking, image hash

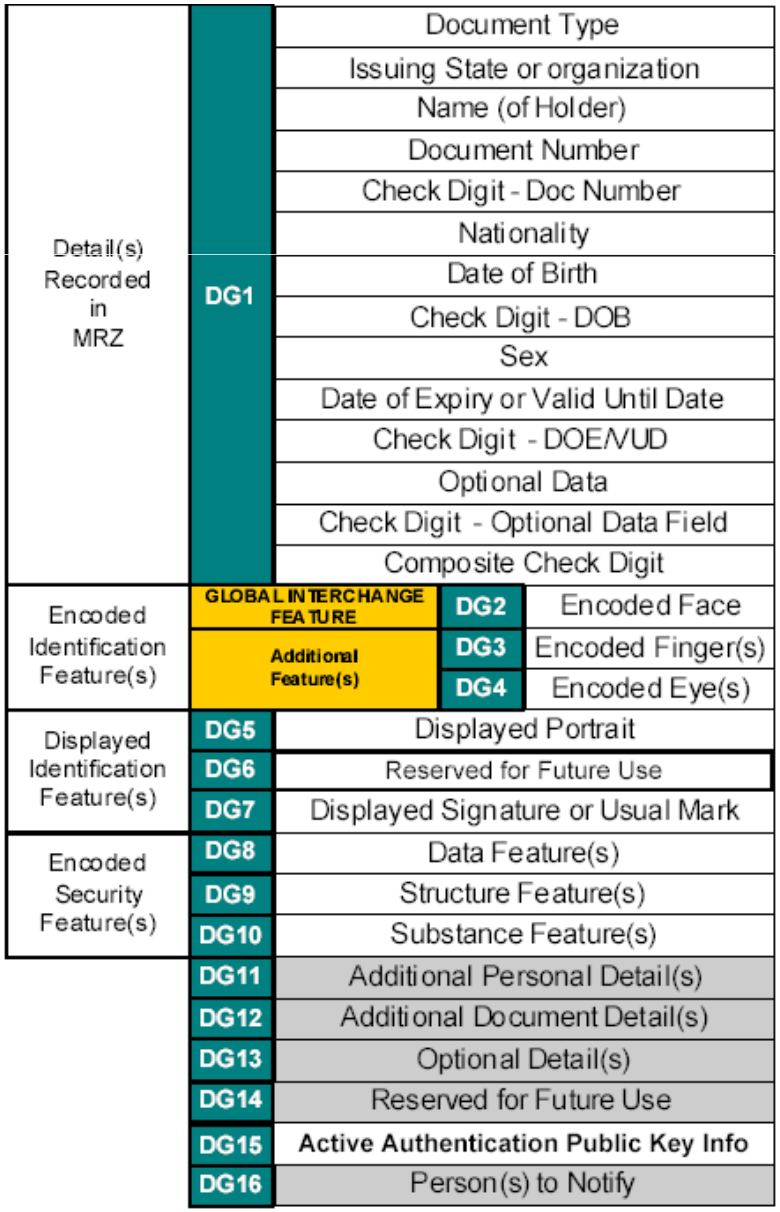
UNIK

Past RFID problems

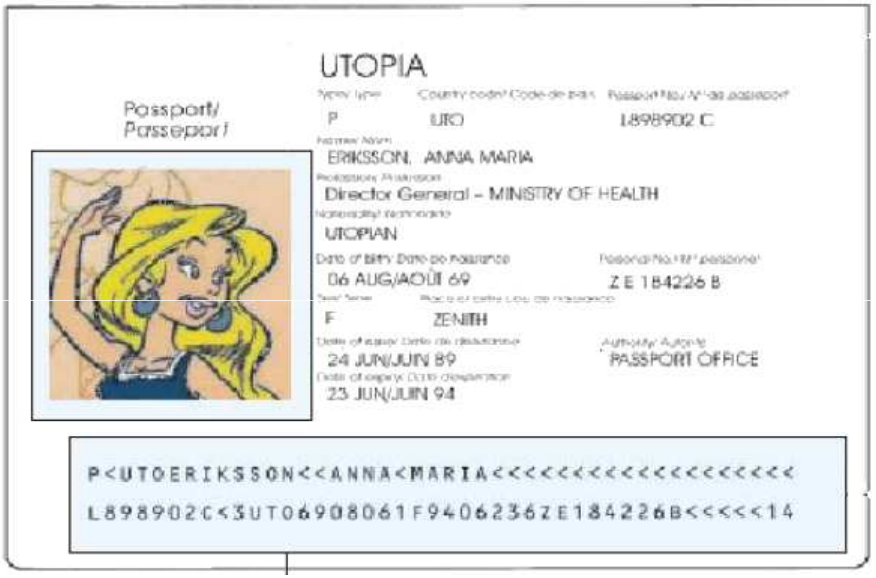
- Ticketing, storage, shop
- Overheated expectations
- Barcode faced similar problems, but RFID extends this with an additional dimension
- Similar problems in all implementations

Passports overview

- Biometric identifiers
  - Availability
  - Deployment
- Implementation
  - ICAO standards
  - BAC
  - EAC



EU standard biometric passport



- Extends ICAO with BAC
- Key is generated from the MRZ
- DGs encrypted with the BAC key, signed with the authority's key
- EAC
- No shielding
- Entropy limiting key generation
  - Passport numbering, fix bits, checksums, names, dates

Cryptograpic problems

- Uses good crypto, SHA-256 for signature generation
  - Designed to work on high-entropy binary data
- The inclusion of the picture is weakening the implementation
- Encryption key is calculated from the MRZ
- Weakens assym. crypto with large number of data packets
- Passive unit, no revocation, no try limit

Picture ”validity”

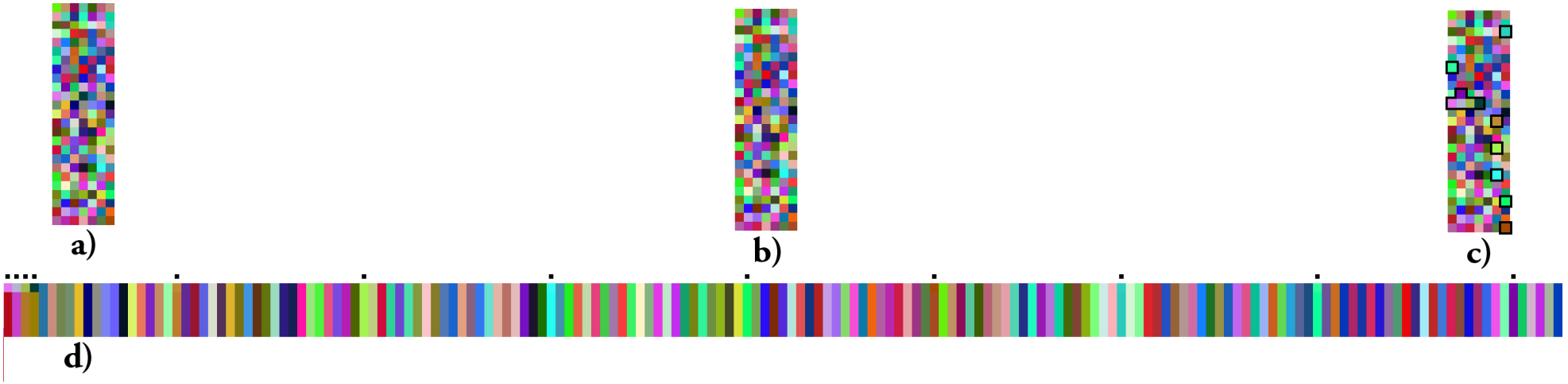
Images seems to be the same for the border guard person

The left image differs in 100 pixels from the right one

UNIK

Crypto attack – hash collisions

- Unnoticeable modifications possible
- Vectorprocessors (Cell, nVidia)
- Attacks to MD5 crypto presented on HashClash
  - Not directly applicable to SHA
  - Colliding X.509 certificates



Privacy concerns

- Distributed.net statistics
- MacG4 export limited ”supercomputer”, PentiumD830 approx. 2 times faster
- Passive element
- No revocation
- Unlimited validity
- Not possible to replace

Watermarking

- Special hash function designed for authenticity check
- Designed to result in the same hash in case of bit-level differences
- Captures the perceptual properties of the image
- Similar images have small Euclidean distance
- Possible replacement of the fingerprint image itself

Limited length image hash

- Long hash size may result in just an other kind of unique identifier
- An avoided hash property might be the solution
  - Forcing collisions leads to a probabilistic identifier
- Choosing the right tradeoff between hash length and uniqueness of the identifier leads to better privacy and revoke possibility

An image hash example

- 32 bit -> practically one ID/person on Earth
- Birthday attack: only 110.000 tries are required to reach a collision with 75% probability

- This solution is not lowering the probability of a successful check: allowed false-negative rate for biometric passports is 0,3% -> every 333th check is providing a false-negative 1/333>>1/110000

Image space of picture hash

- To use the Euclidean-distance properties of image hash, a bigger image-space hash is needed
- Objective is to accept fingerprints which differ only a few bits from the hash stored in the pass

Summary and future work

- Privacy protection is needed
- Current implementation suffers from severe weaknesses, EAC is only delaying the problems

- Future work will focus on finding the right tradeoff between hash length, privacy and reliability

Questions?