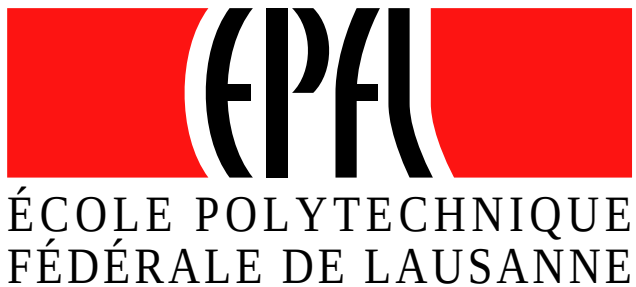
The Biometric Passport Standard

What's all this Mess About?

Serge Vaudenay



http://lasecwww.epfl.ch/

LASEC


Schweizer Pass
Passeport suisse
Passaporto svizzero
Passaport svizzer
Swiss passport

Arrêté Fédéral

2008, June 13

1. Loi du 22 juin 2001 sur les documents d'identité[5]

Art. 2, al. 1, let. a, al. 2bis à 2quater et 4

[1] Chaque document d'identité doit comporter les données suivantes:

a. nom d'état civil;

[2bis] Le document d'identité peut être muni d'une puce. La puce peut contenir la photographie et les empreintes digitales du titulaire. Les autres données prévues aux al. 1, 3, 4 et 5, peuvent également être enregistrées dans la puce.

[2ter] Le Conseil fédéral définit les types de documents d'identité munis d'une puce et les données qui doivent y être enregistrées.

[2quater] Ces documents peuvent en outre contenir une identité électronique utilisable à des fins d'authentification, de signature et de cryptage.

[4] Sur demande du requérant, le document d'identité peut en outre comporter le nom d'alliance, le nom reçu dans un ordre religieux, le nom d'artiste ou le nom de partenariat, et la mention de signes particuliers tels que handicaps, prothèses ou implants.

Art. 2a Sécurité et lecture de la puce

[1] La puce doit être protégée contre les falsifications et la lecture non autorisée. Le Conseil fédéral fixe les exigences techniques.

[2] Le Conseil fédéral est autorisé à conclure des traités avec d'autres Etats concernant la lecture des empreintes digitales enregistrées dans la puce, pour autant que les Etats concernés disposent d'une protection des données analogue à celle appliquée par la Suisse.

[3] Il peut autoriser les compagnies de transport, les exploitants d'aéroports et d'autres services adéquats qui doivent vérifier l'identité de personnes à lire les empreintes digitales enregistrées dans la puce.

Referendum (October 2)

Référendum contre le prélèvement obligatoire de données biométriques et d'empreintes digitales pour tous les nouveaux passeports et cartes d'identité

Voulez-vous que vos empreintes digitales soient centralisées ? Voulez-vous que votre carte d'identité ou votre passeport contienne une puce permettant la localisation ?

NON? Alors agissez pendant qu'il est encore temps!

- **NON** à la collecte forcée de données biométriques pour tous les nouveaux passeports et cartes d'identité!
- **NON** à la sauvegarde de vos données personnelles biométriques dans une base de données centrale.
- **NON** à l'accès de gouvernements étrangers et d'entreprises privées à vos données biométriques!
- **NON** à l'instauration de puces de radio-identification (RFID) dans tous les nouveaux passeports suisses et cartes d'identité!
- **NON** à la centralisation bureaucratique et au démantèlement des bureaux de contrôles des habitants!
- **NON** à l'extension du contrôle de l'Etat sur les citoyens!

Chaque citoyen suisse doit pouvoir décider s'il veut d'un passeport suisse et d'une carte d'identité, avec ou sans données biométriques et puce RFID.

Les citoyennes et citoyens suisses soussignés ayant le droit de vote demandent, en vertu de l'art. 141 de la constitution fédérale du 18 avril 1999 et conformément à la loi fédérale du 17 décembre 1976 sur les droits politiques (art. 59s.), que l'arrêté fédéral du 13 juin 2008 portant approbation et mise en oeuvre de l'échange de notes entre la Suisse et la Communauté européenne concernant la reprise du Règlement (CE) 2252/2004 relatif aux passeports biométriques et aux documents de voyage (Développement de l'Acquis de Schengen) soit soumis au vote du peuple.

Seuls les électrices et électeurs résidant dans la commune indiquée en tête de la liste peuvent y apposer leur signature. Les citoyennes et les citoyens qui appuient la demande doivent la signer de leur main. Celui qui se rend coupable de corruption active ou passive relativement à une récolte de signatures ou celui qui falsifie le résultat d'une récolte de signatures effectuée à l'appui d'un référendum est punissable selon l'article 281 respectivement l'article 282 du code pénal.

Canton:	**N° postal:**	**Commune politique:**

	Nom (à la main et en majuscules)	**Prénom** (à la main et en majuscules)	**Date de naissance** (jour/mois/année)	**Adresse exacte** (rue et numéro)	**Signature manuscrite**	**Contrôle** (laisser en blanc)
1						
2						
3						

TSR Show

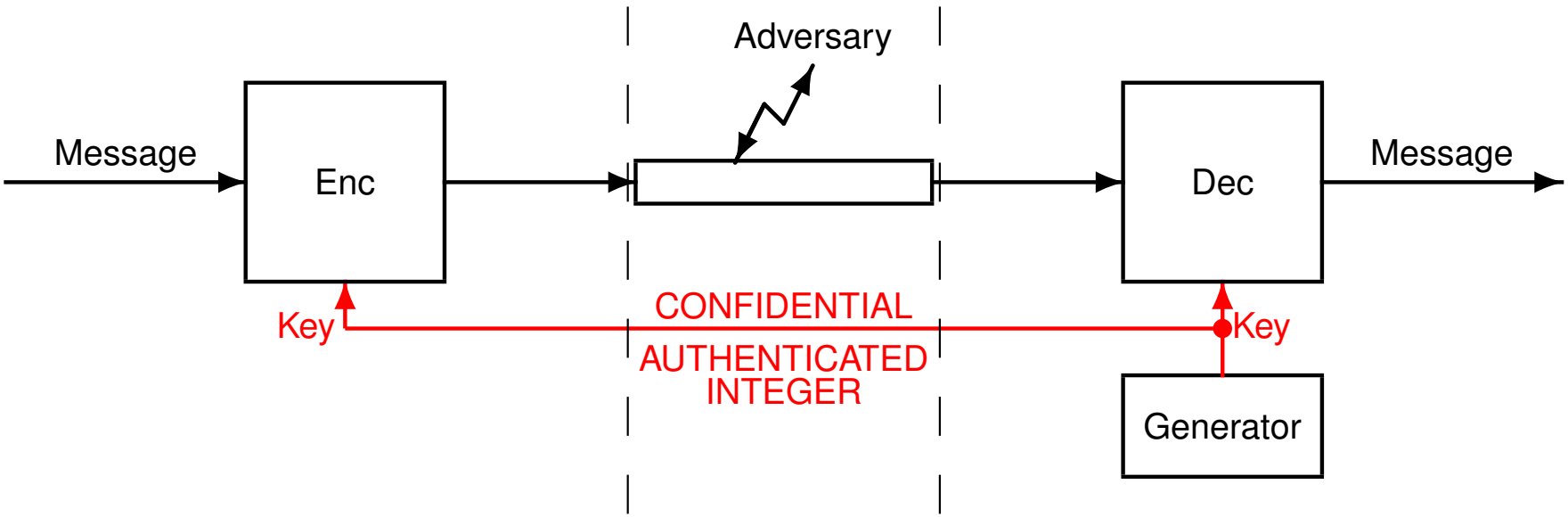
2008, October 9

- in many newspapers since last week
- on TV broadcast tonight

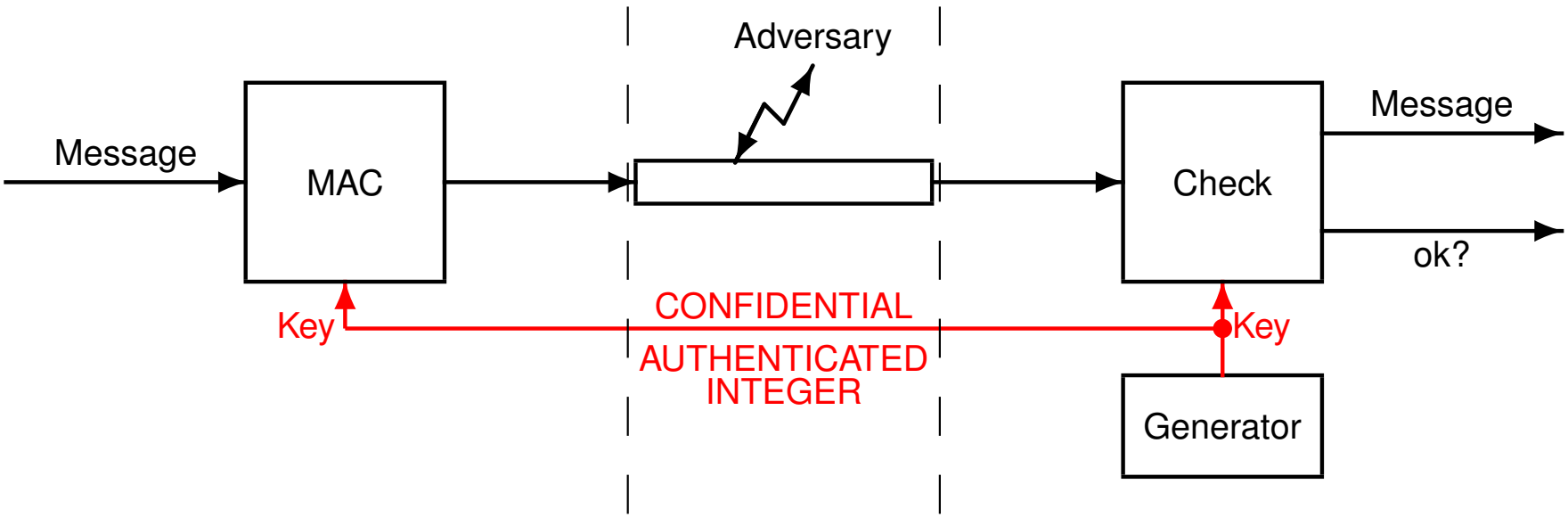
Cryptographic Primitives

conventional crypto	public-key crypto
symmetric encryption	public-key cryptosystem
message authentication code	digital signature
hash function	key agreement protocol

Symmetric Encryption

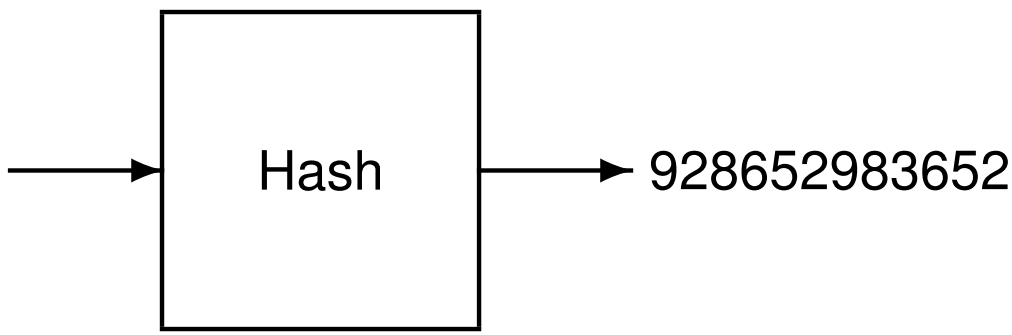


Message Authentication Code

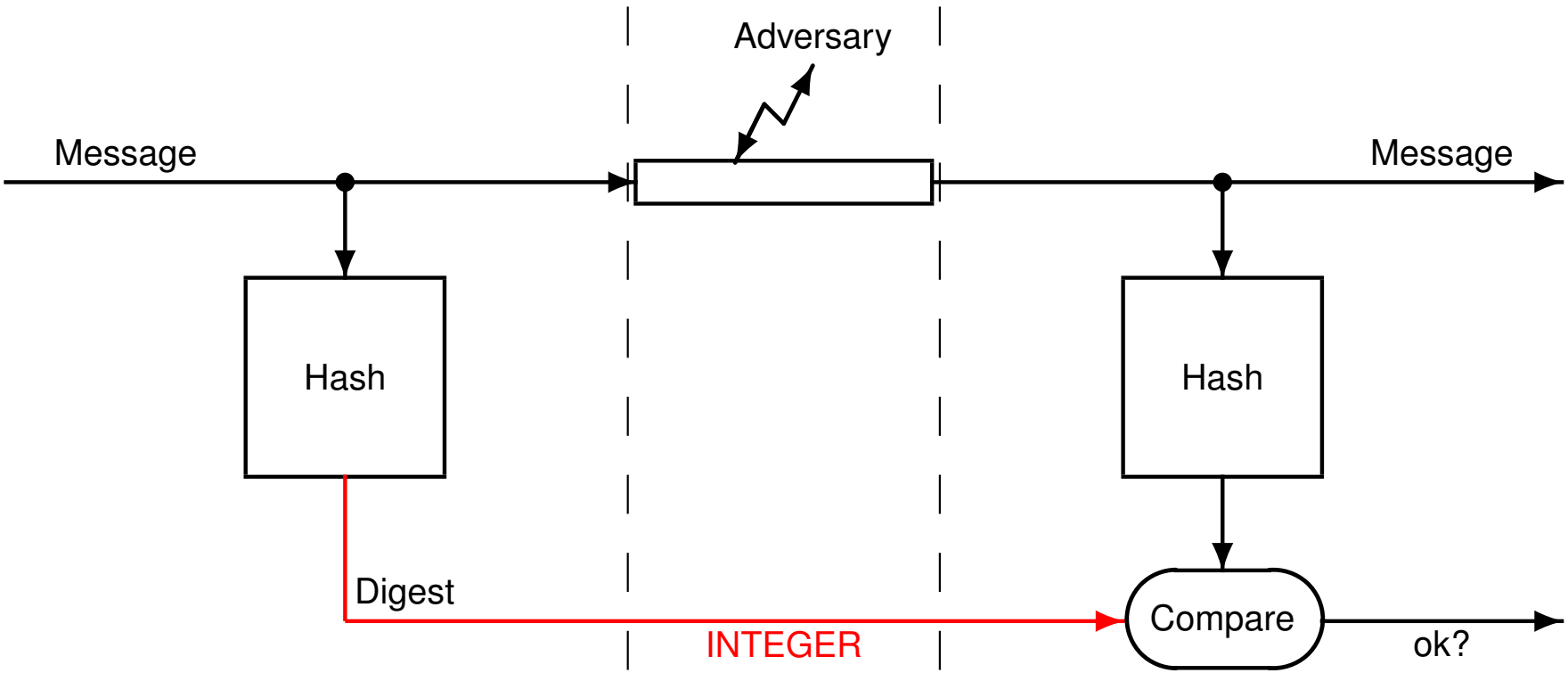


Hash Function

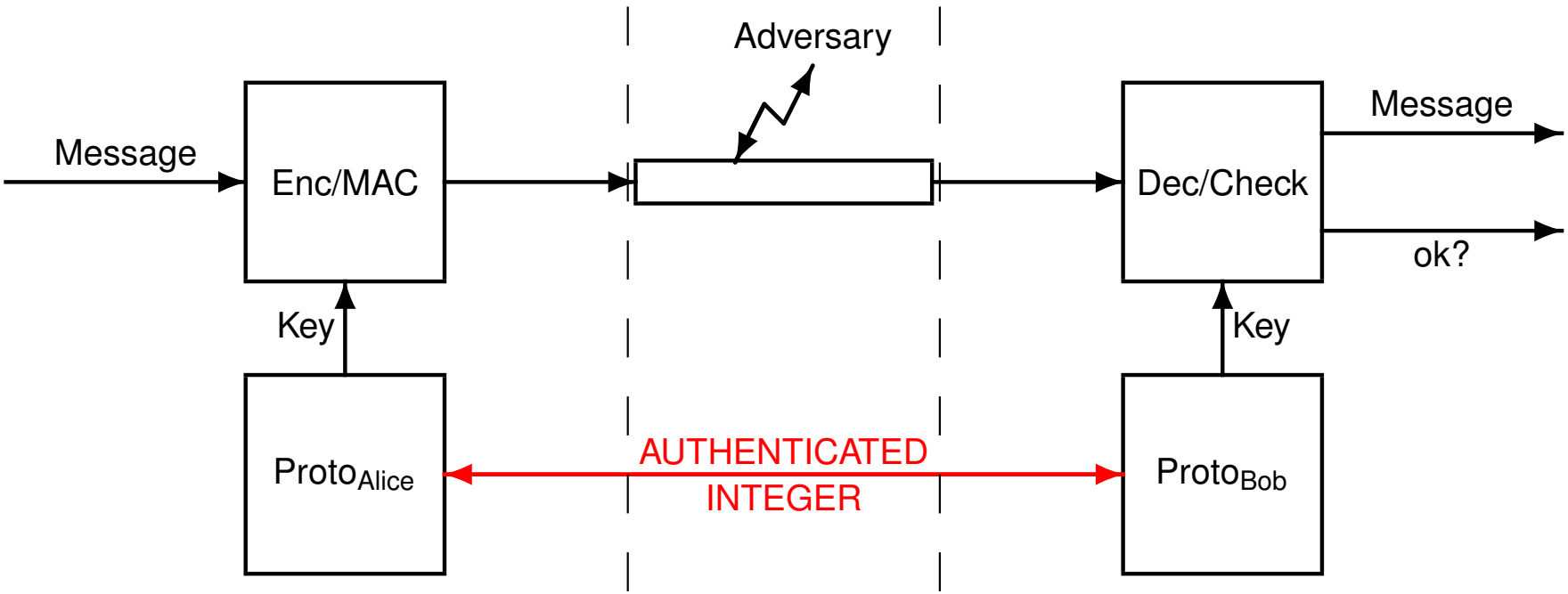
La cigale ayant chanté tout l'été se trouva fort dépourvue quand la bise fut venue pas un seul petit morçeau de mouche ou de vermisseau elle alla trouver famine chez la fourmie sa voisine ...



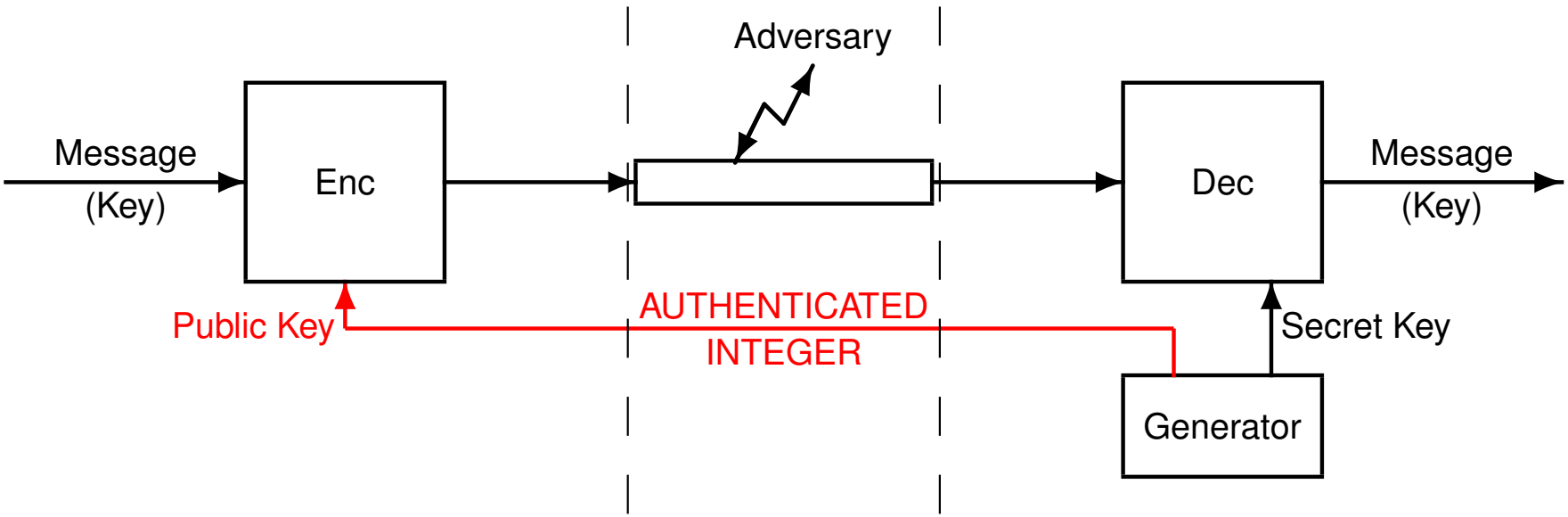
Integrity by Hash Function



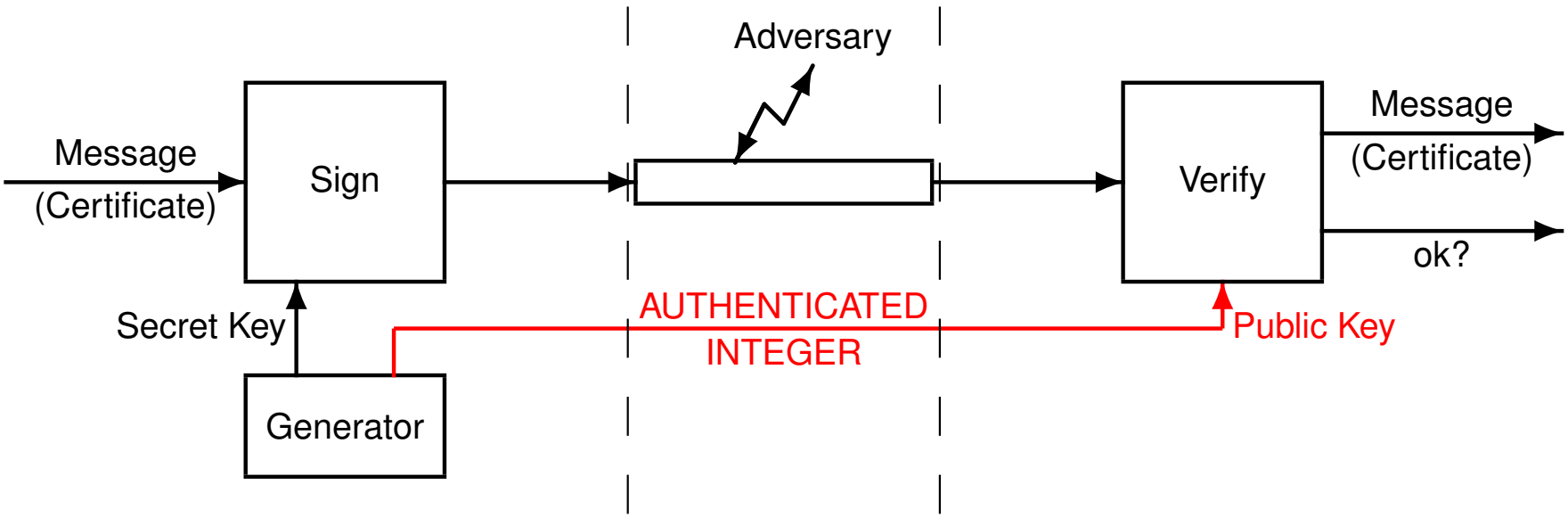
Key Agreement Protocol



Public-Key Cryptosystem (Key Transfer)



Digital Signature (Public-Key Certificate)




2002
X-RAY

Objectives

more secure identification of visitors at border control

- $\longrightarrow$ biometrics
- $\longrightarrow$ contactless IC chip
- $\longrightarrow$ digital signature + PKI

maintained by UN/ICAO (International Civil Aviation Organization)

MRTD History

- 1968: ICAO starts working on MRTD
- 1980: first standard (OCR-B **Machine Readable Zone (MRZ)**)
- 1997: ICAO-NTWG (New Tech. WG) starts working on biometrics
- 2001 9/11: US want to speed up the process
- 2002 resolution: ICAO adopts **facial recognition**
  (+ optional fingerprint and iris recognition)
- 2003 resolution: ICAO adopts MRTD with **contactless IC media**
  (instead of e.g. 2D barcode)
- **2004: version 1.1** of standard with ICC
- 2005: deployment of epassports in several countries
- 2006: **extended access control** under development in the EU
- 2007: deployment of extended access control (+ more biometrics)

Why Face Recognition?

- disclose no information that people does not routinely disclose
- facial image is already socially and culturally accepted
- already collected and verified in passports
- people already aware of capture and use for ID verification purpose
- non-intrusive: no need for physical contact
- requires no new enrolment procedure
- feasability of fast deployment
- many states already have database of people images
- can be captured from an endorsed photograph only
- children need not be present for capture
- human verification is feasible and easy

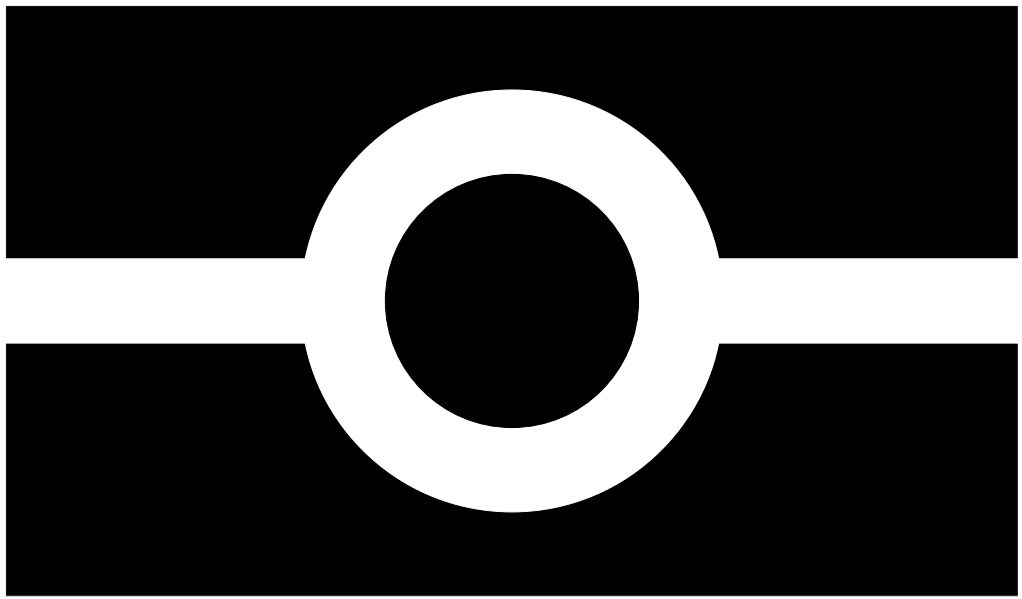
Why Contactless IC Chip?

- useability: no need for swiping or sensing, requires no contact
  ($\neq$ magnetic strip, optical memory, contact IC chip)
- data storage: can store over 15 kilobytes
  ($\neq$ 2D barcodes)
- performance: random access feasible as information will grow

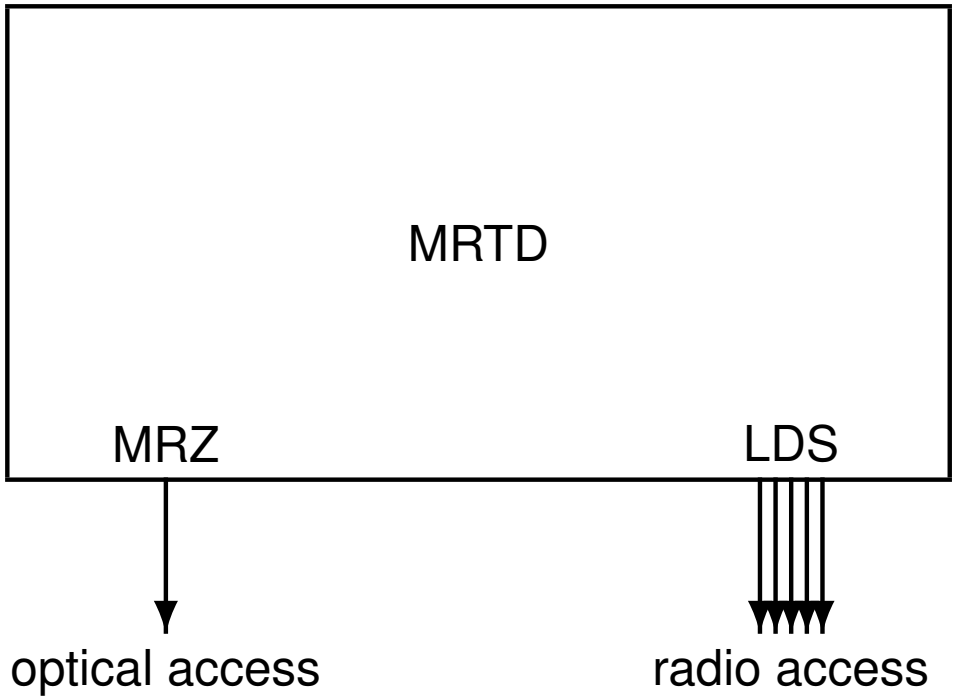
Recommendation:

- on-board operating system (ISO/IEC 7816–4)
- ISO 14443 type A or B compliance
- very high ($>$64K) capacity (minimum: 32K, recommended: 512K)
- minimum set of commands
- data stored in LDS format with encryption, hashing, and signature
- high speed retrieval (50K in $<$5sec)
- read distance range 0–10cm

How to Distinguish a Compliant MRTD



MRTD in a Nutshell



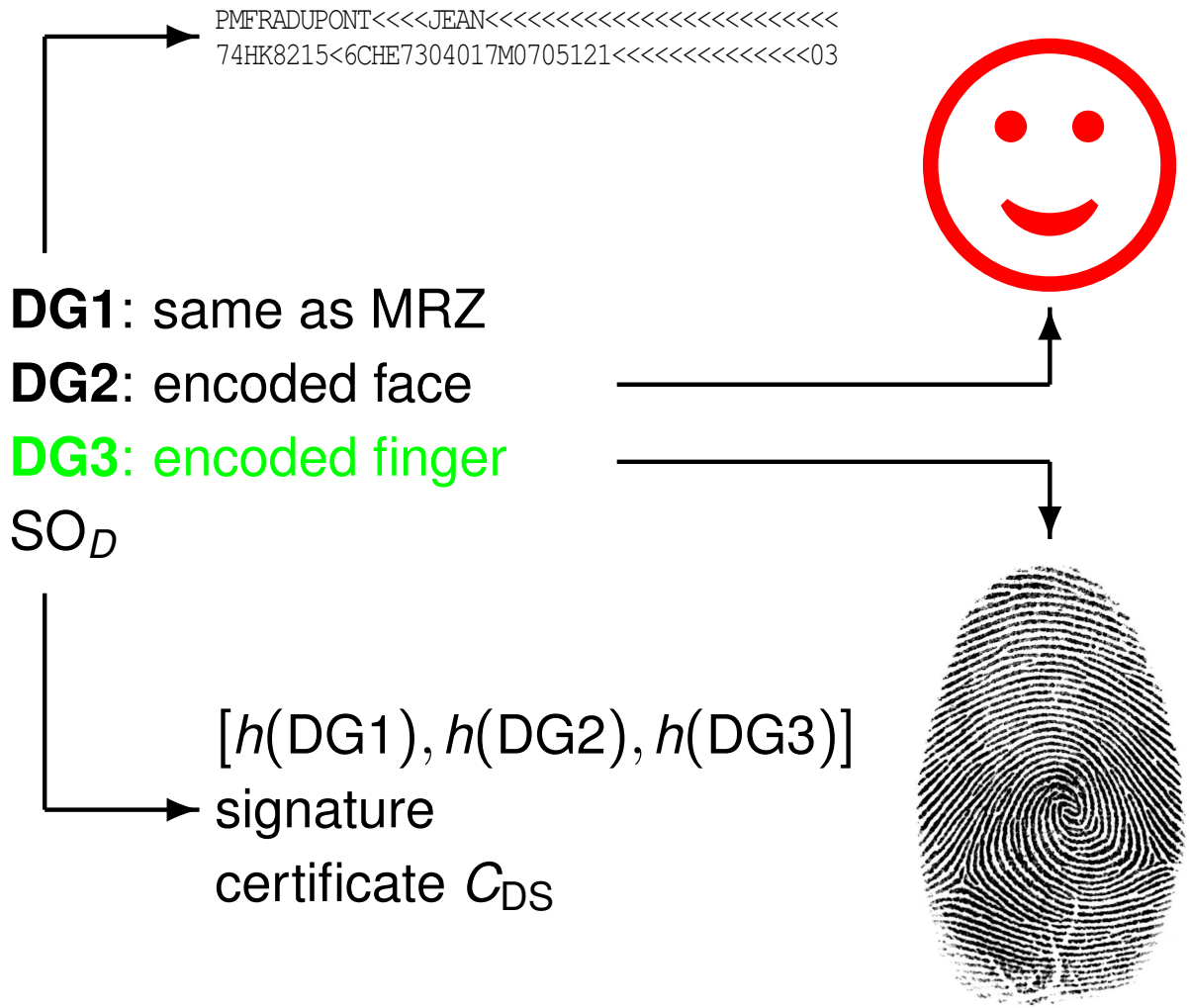
- data authentication by digital signature + PKI
  aka **passive authentication**
- access control + key agreement based on MRZ_info
  aka **basic access control (BAC)**
- chip authentication by public-key cryptgraphy
  aka **active authentication (AA)**

MRZ Example

```
PMFRADUPONT<<<<JEAN<<<<<<<<<<<<<<<<<<<<<<<<
74HK8215<6CHE7304017M0705121<<<<<<<<<<<<<<03
```

- document type
- issuing country
- holder name
- doc. number + CRC
- nationality
- date of birth + CRC
- gender
- date of expiry + CRC
- options + CRC

LDS Example


PMFRADUPONT<<<<JEAN<<<<<<<<<<<<<<<<<<<<<<<<
74HK8215<6CHE7304017M0705121<<<<<<<<<<<<<<03
DG1: same as MRZ
DG2: encoded face
DG3: encoded finger
SO_D
[h(DG1), h(DG2), h(DG3)]
signature
certificate C_DS

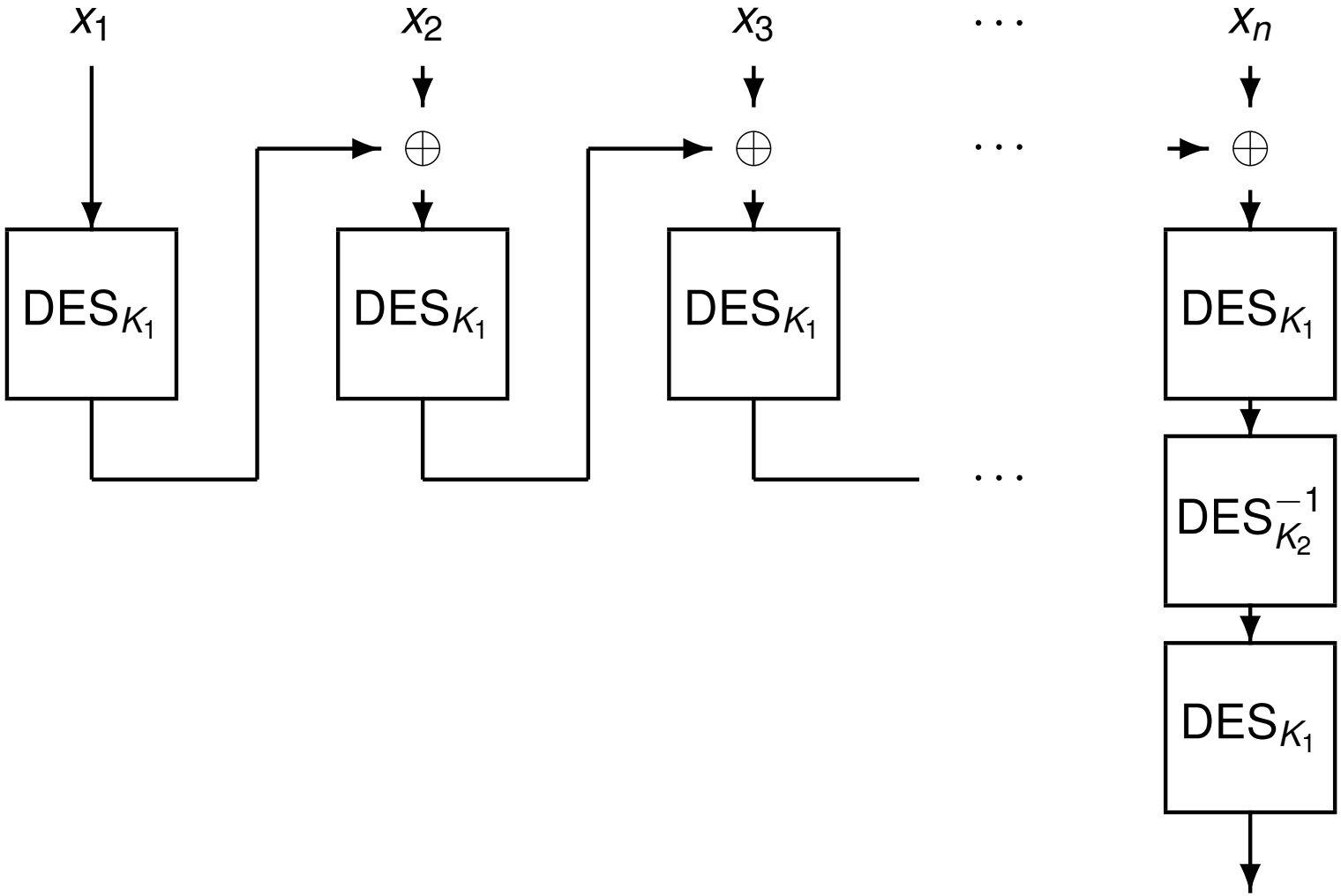
Underlying Cryptography

- RSA signatures (ISO/IEC 9796, PKCS#1), DSA, ECDSA
- X.509
- SHA1 and sisters
- DES, triple-DES, CBC encryption mode
- one of the ISO/IEC 9797-1 MAC (next slide)

ISO/IEC 9797-1

(MAC algorithm 3 based on DES with padding method 2)

(concatenate message with bit 1 and enough 0 to reach a length multiple of the block size)



LDS Structure

- K_{ENC}, K_{MAC}, KPr_{AA}
- COM: present data groups
- DG1: same as MRZ
- DG2: encoded face
- DG3: encoded finger(s)
- DG4: encoded eye(s)
- DG5: displayed portrait
- DG6: (reserved)
- DG7: displayed signature
- DG8: data feature(s)
- DG9: structure feature(s)
- DG10: substance feature(s)
- DG11: add. personal detail(s)
- DG12: add. document detail(s)
- DG13: optional detail(s)
- DG14: (reserved)
- DG15: KPu_{AA}
- *DG16: person(s) to notify*
- DG17: autom. border clearance
- DG18: electronic visa
- DG19: travel record(s)
- SO_D

SO_D Structure

- list of hash for data groups DG1–DG15
- formatted signature by DS (include: information about DS)
- (optional) C_{DS}

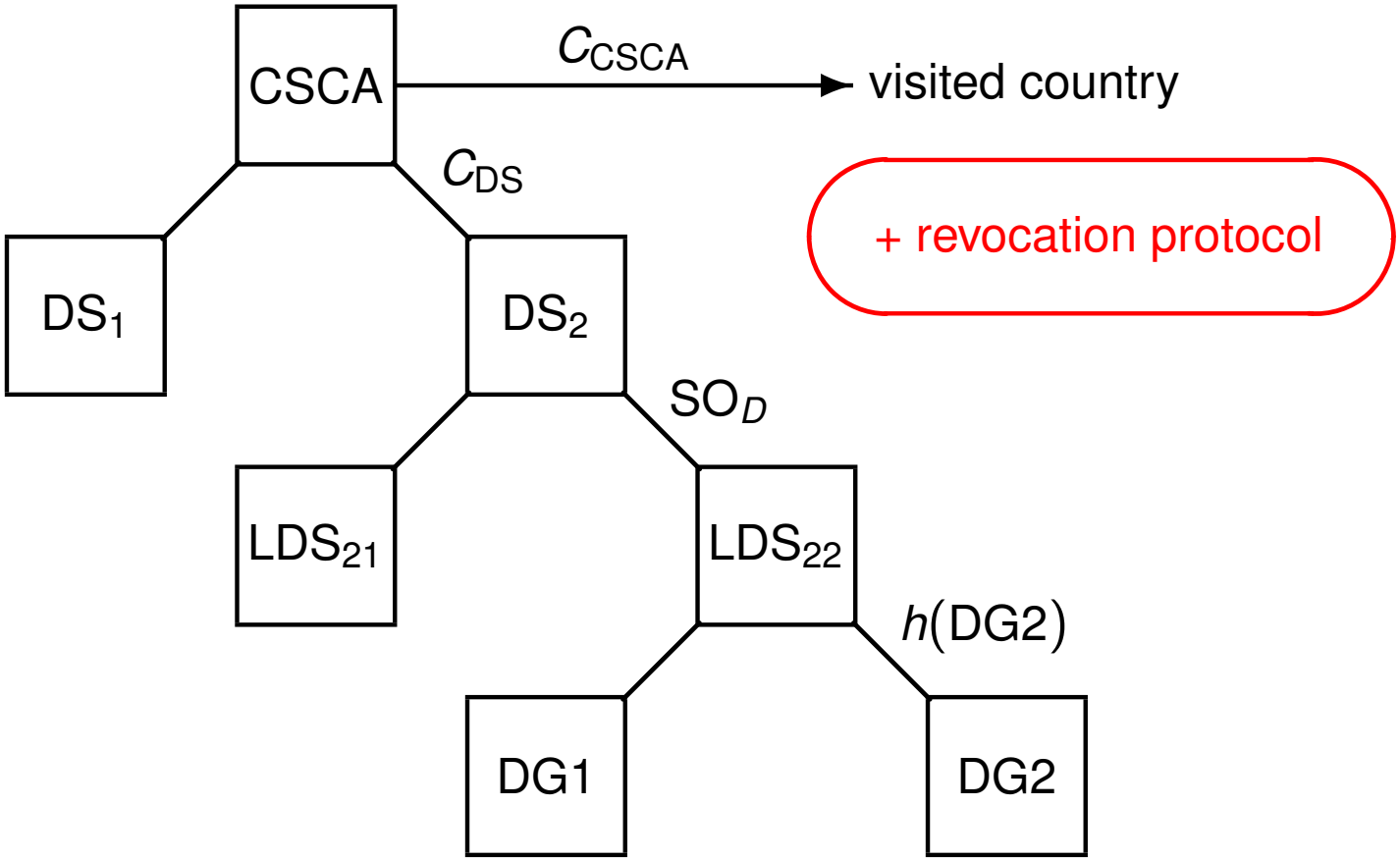
Passive Authentication

goal authenticate LDS

- after getting SO_D, check the included certificate C_{DS} and the signature
- when loading a data group from LDS, check its hash with what is in SO_D

$\longrightarrow$ stamp by DS on LDS

(Country-wise) PKI



- one CSCA (*Country Signing Certificate Authority*)
- several DS (*Document Signer*) per country
- SO_D: signature of LDS
- fingerprint of a DG

Revocation

- incident must be reported within 48 hours to all other countries (and ICAO)
- “routine” CRL to be distributed every 3 months to all other countries (and ICAO)

ICAO Server

- collection of C_{CSCA}'s (not available online)
- online public-key directory of C_{DS}'s (primary directory)
- online CRL of C_{DS}'s (secondary directory)

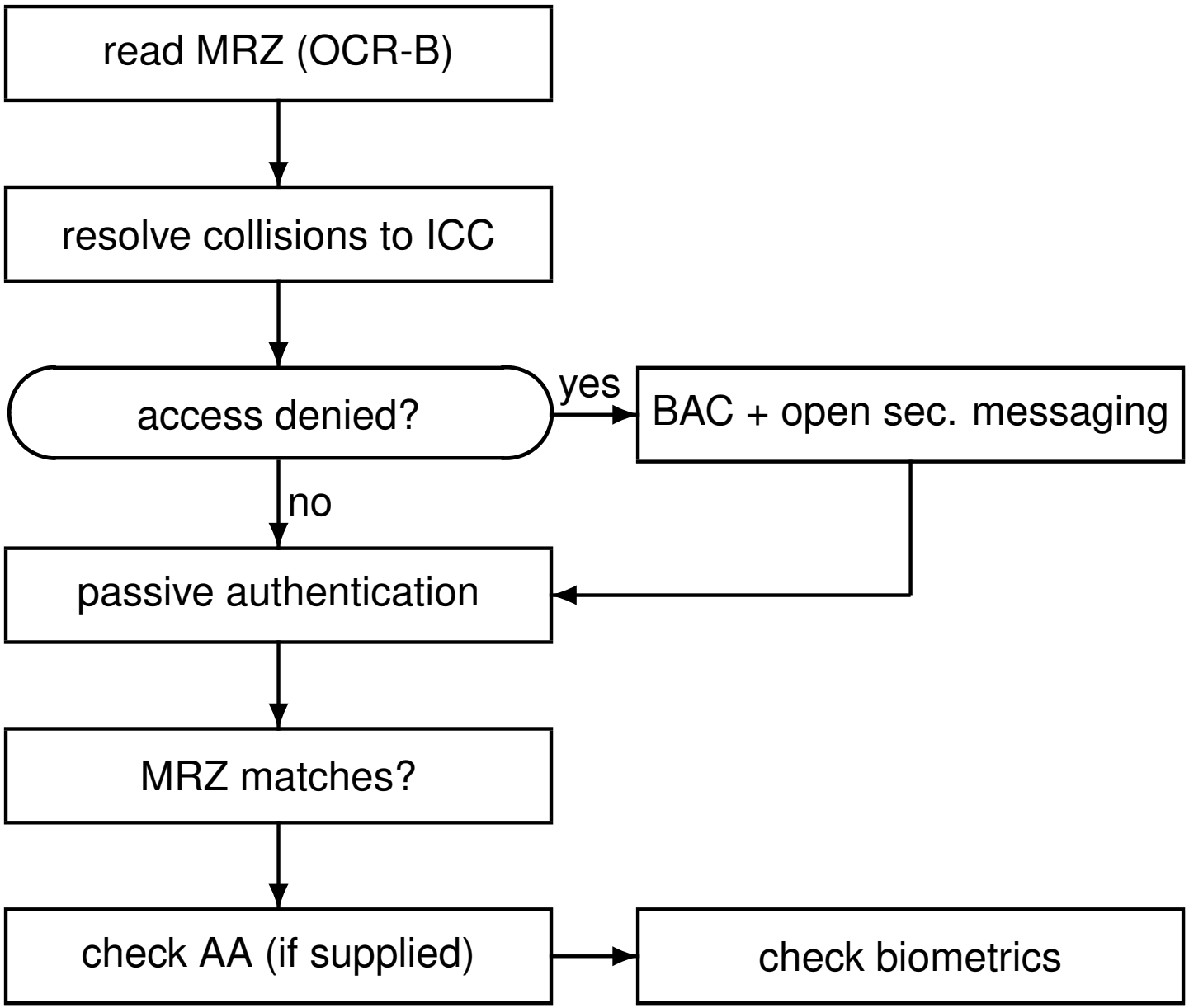
MRZ vs LDS

- LDS does not replace MRZ (interoperability)
- MRZ must still be used in identification
- MRZ used by access control to LDS

Access Control Options

- **none**: anyone can query the ICC, communication in clear
- **basic**: uses secure channel with authenticated key establishment from MRZ
- **extended**: up to bilateral agreements (no ICAO standard)
  EU common criteria: now being implemented

Sequence of Steps for Identification



Basic Access Control

goal prevent from unauthorized access by the holder (privacy)

- read MRZ (OCR-B)
- extract MRZ_info
- run an authenticated key exchange based on MRZ_info
- open secure messaging based on the exchanged symmetric key

$\longrightarrow$ proves that reader knows MRZ_info

MRZ_info

```
PMFRADUPONT<<<<JEAN<<<<<<<<<<<<<<<<<<<<<<<<
74HK8215<6CHE7304017M0705121<<<<<<<<<<<<<<03
```

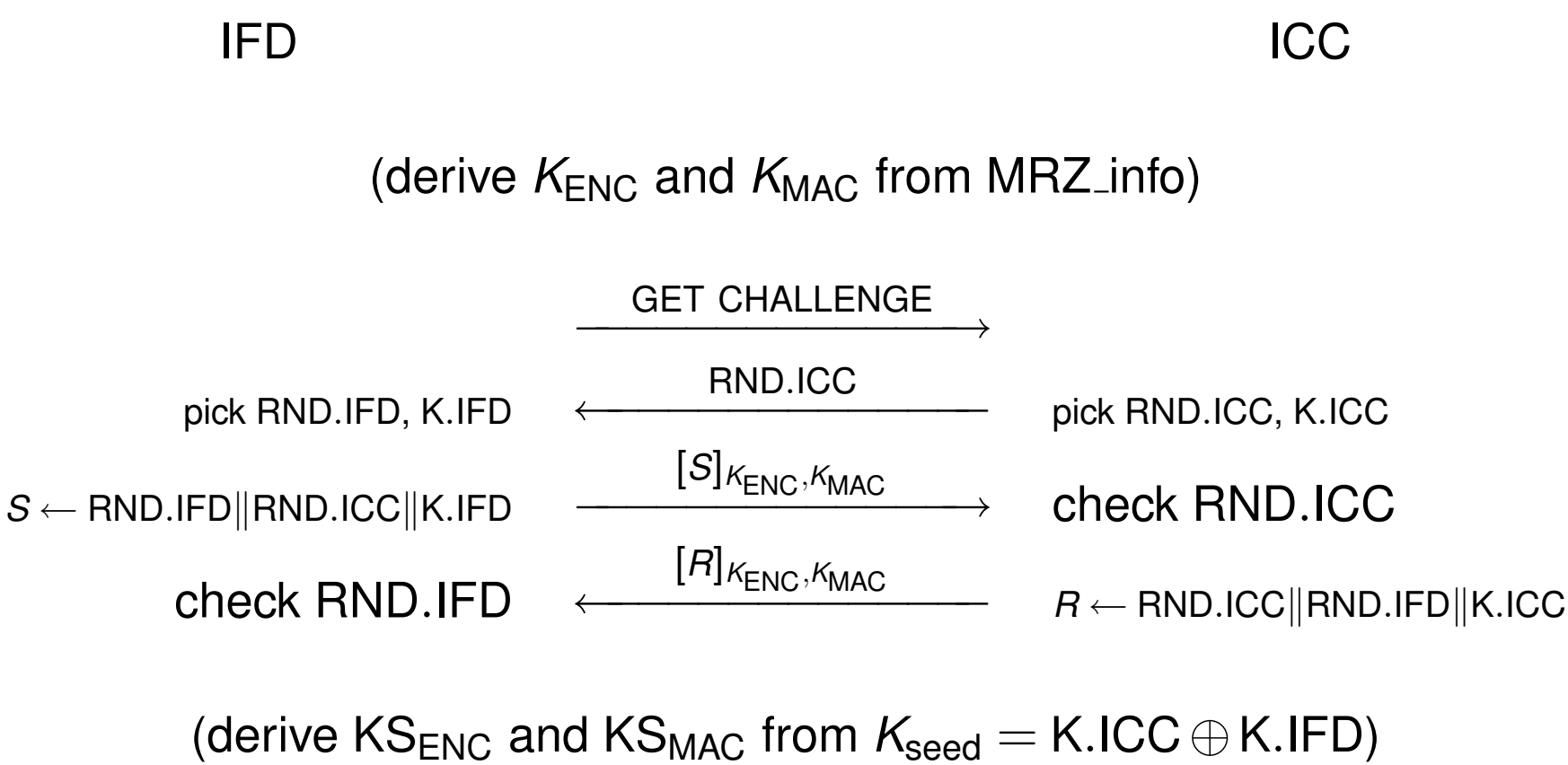
- document type
- issuing country
- holder name
- doc. number + CRC
- nationality
- date of birth + CRC
- gender
- date of expiry + CRC
- options + CRC

(Pre)key Derivation from MRZ (Basic Access Control)

- set $K_{\text{seed}} = \text{trunc}_{16}\left(\text{SHA1}(\text{MRZ\_info})\right)$
- set $D = K_{\text{seed}} \| 00\,00\,00\,01$
- compute $H = \text{SHA1}(D)$
- first 16 bytes of H are set to the 2-key triple-DES K_{ENC}
- set $D = K_{\text{seed}} \| 00\,00\,00\,02$
- compute $H = \text{SHA1}(D)$
- first 16 bytes of H are set to the 2-key triple-DES K_{MAC}
- adjust the parity bits of the all DES keys

Basic Access Control

Authenticated Key Exchange Based on MRZ_info

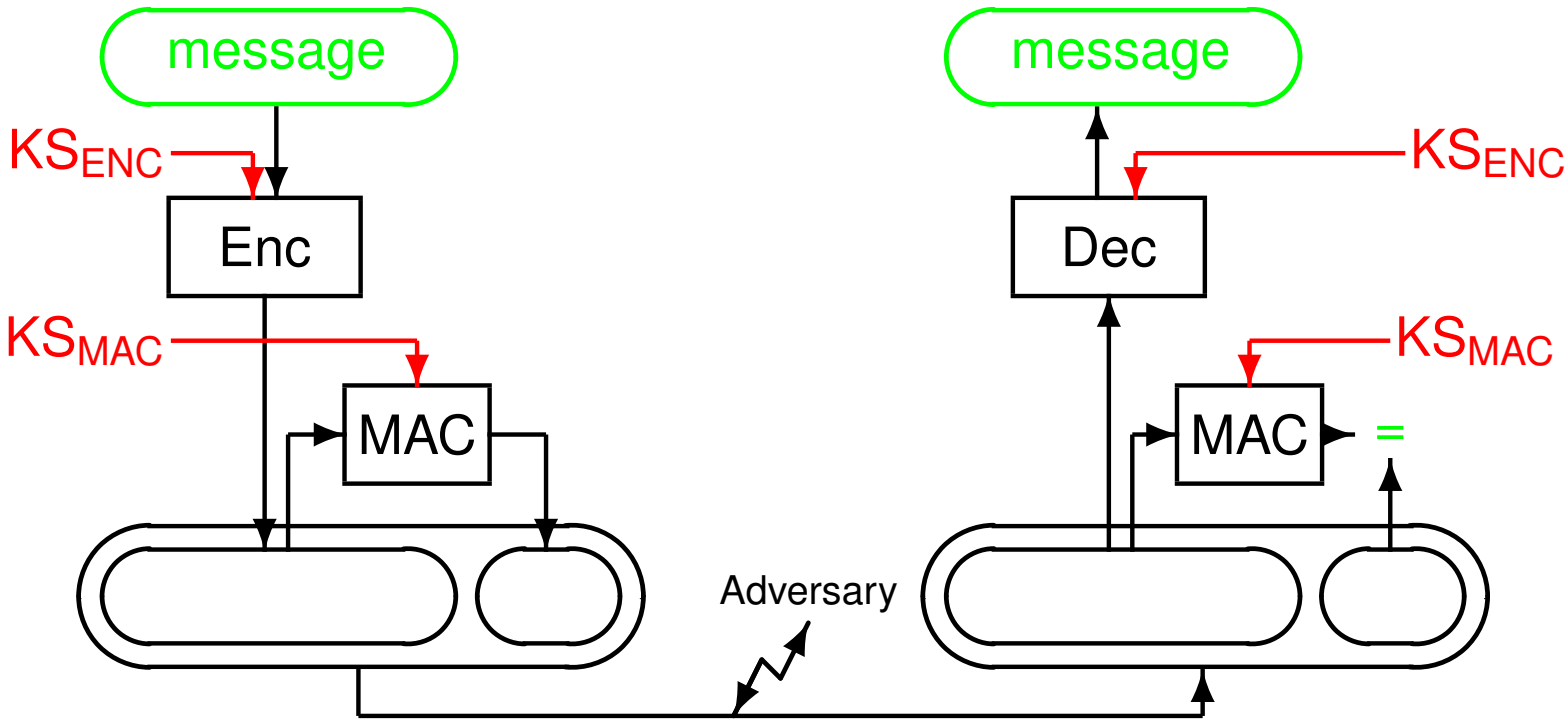


Session Key Derivation (Basic Access Control)

- compute K_{ENC} and K_{MAC} from MRZ_info
- run a protocol to compute K_{seed}
- set $D = K_{seed} || 00\,00\,00\,01$
- compute $H = \text{SHA1}(D)$
- first 16 bytes of H are set to the 2-key triple-DES KS_{ENC}
- set $D = K_{seed} || 00\,00\,00\,02$
- compute $H = \text{SHA1}(D)$
- first 16 bytes of H are set to the 2-key triple-DES KS_{MAC}
- adjust the parity bits of the all DES keys

Secure Messaging

goal authentication, integrity, confidentiality of communication



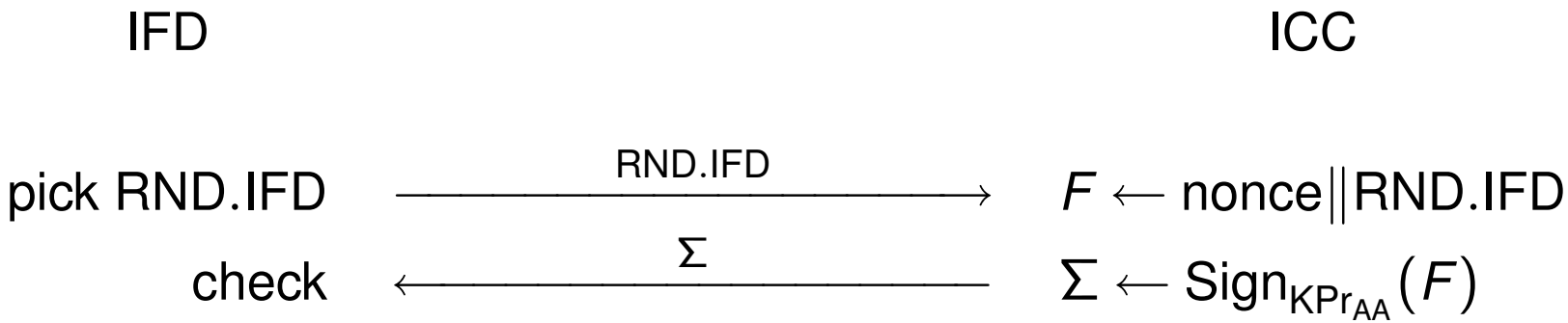
Active Authentication

goal authenticate the chip

- proves that ICC knows some secret key KPr_{AA} linked to a public key KPu_{AA} by a challenge-response protocol
  (KPu_{AA} in LDS authenticated by passive authentication)

$\longrightarrow$ harder to clone a chip

Active Authentication Protocol



With vs Without Active Authentication

No Active Authentication

- ICC can be cloned
- simple computations to perform

Active Authentication

- protection against clones
- requires public-key cryptography in ICC

ISO 14443 with Private Collision Avoidance Protocol

- for each new singulation protocol
  ICC introduces himself with a pseudo (32-bit number)
- singulation to establish a communication link between reader and ICC of given pseudo
- pseudo is either a constant or a random number starting with `08`

With vs Without Faraday Cages

Regular Document

- can access to ICC without the holder approval

Metalic Cover

- document must be opened to access to ICC
- more expensive
- not fully effective
- rings at security gates

Implementation Discrepencies

	shield	singulation	BAC	AA
Switzerland	none	random 08xxxxxx	used	not implemented
United Kingdom	none	random 08xxxxxx	used	not implemented
France	none	random 08xxxxxx	?	?
Australia	none	random xxxxxxxx	used	?
New Zealand	none	constant	used	?
USA	yes	?	?	?
Italy	?	constant	?	?
Belgium	none	?	used	implemented
Czech Republic	none	random 08xxxxxx	used	implemented

Algorithms

	certificate	SO_D	AA
Switzerland	ecdsa_with_sha1 824b	ecdsa 512b	n/a
United Kingdom	sha256withRSA 4096b	RSA 2048b	n/a
Czech Republic	rsaPSS (sha1) 3072b	RSA 2048b	RSA 1024b
Belgium	sha1withRSA 4096b	RSA 2048b	?
Germany	ecdsa_with_sha1 560b	ecdsa 464b	n/a
Italy	sha1withRSA 4096b	RSA 2048b	?
New-Zealand	sha256withRSA 4096b	RSA 2048b	?
USA	sha256withRSA 4096b	RSA 2048b	?

JPEG2000 Format

- many metadata: hackers learn about which software/OS (+bug) used in government agencies
- lack of software diversity: hackers introduce viruses in border control systems from JPEG2000 metadata

Private Collision Avoidance

- when prompted by a reader, the ICC answers with a 32-bit random number (temporary device identity) ISO 14443B of format `08xxxxxx`

  some countries: constant number
- information leakage: `08xxxxxx` tags likely to be e-passports

  some countries: random number not necessarily of format `08xxxxxx`
- the protocol and radio signature (pattern) leaks

Issues in Basic Access Control

- MRZ_info entropy:
  ideally, $\log_2((10+26)^9 \times 365 \times 100 \times 365 \times 5) \approx 70$
  in practice, $\log_2(20 \times 10^6 \times 365 \times 10 \times 365 \times 5) \approx 47$
  at this time, $\log_2(10^4 \times 365 \times 10 \times 365 \times 5) \approx 36$
- online bruteforce attack
  guess MRZ_info and try it with MRTD until it works
  $\longrightarrow$ one experiment reported: it took 4h
  (would make sense in a long haul flight)
- offline bruteforce
  infer MRZ_info from some $(x, \mathrm{MAC}_{K_{\mathrm{MAC}}}(x))$ pair
  decrypt BAC protocol to get $\mathrm{KS}_{\mathrm{ENC}}$
  decrypt passive authentication to get LDS

Unauthorized Wireless Access

Radius:

- easy at a distance less than 5cm
- experiment reported at a distance of 1.5m
- claimed to be possible at a distance up to 10m

Threat:

- (if MRZ_info is known): tracing people
- (if MRZ_info is unknown): identifying people by bruteforce
- in any case: collecting valuable people profiles

Passive Skimming

Radius:

- experiment reported at a distance of 4m
- claimed to be possible at a distance up to 10m

Threat:

- offline bruteforce: identifying people, collecting profiles

Identity Theft

- feasible when only facial biometric is used
- stealing MRTD
- cloning MRTD

$\longrightarrow$ AA should be mandatory

Detecting Passports

- can check if there is an MRTD in the neighborhood
- (if leakage) can detect if there is an MRTD issued by a given country

Relay Attack against AA

- a fake reader and a fake tag can relay AA messages
- authenticate the fake tag to a genuine reader

Denial of Service

- e-bombing: destroy chips
- hammer: destroy your own chip

Unauthorized Biometric Usage

biometric = human-to-computer identification

- digital image $\neq$ small identity picture
  can be copied many times without quality decrease
- biometric digital image $\neq$ digital image
  optimized for automatic face recognition

- department stores can use it for profiling + automatic recognition

Cookies

- some DGs reserved so that border clearance can store data
- space for extra application
- foreign ambassies can store an e-visa

(undocumented so far)

Collecting Digital Evidences

- challenge semantics in AA:

$$\begin{aligned} \text{RND.IFD} &= H(\text{social}(t-1)) \\ \text{evidence} &= \text{timestamp}_t(\text{social}(t-1) \| \text{LDS} \| \Sigma) \end{aligned}$$

  evidence that MRTD did sign a challenge given by IFD at time t
- LDS is an evidence by its own (got from passive authentication)

Circulating Personal Profile Evidence

- signed personal data: transferable authentication proof
- can no longer hide ones name, age, etc
- when DG11 is used: more personal data
  (place of birth, telephone number, profession, etc)
- when DG12 is used: reference to kids
- personal profiles can be sold!

Basic Idea

- use more biometrics after a stronger access control
- reader authentication
- better protocol (chip authentication) based on Diffie-Hellman

- access to private data requires chip AND terminal authentication
- chip authentication could be used alone
  (e.g. to replace AA or to have a better key agreement)

- BUT: terminal authentication requires a heavy PKI for readers

Chip Authentication

- chip has a static Diffie-Hellman key (authenticated by SOD)
- semi-static ECDH with domain parameters D_{ICC}
- replace the secure messaging keys

$\longrightarrow$ resists skimming

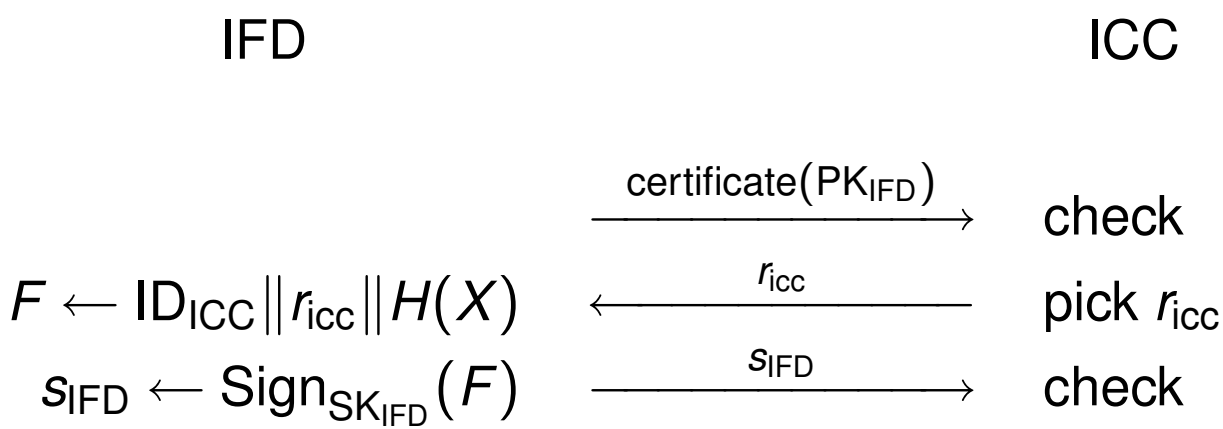
$\longrightarrow$ key with large entropy

IFD		**ICC**
input: m		**secret key**: $\mathrm{SK}_{\mathrm{ICC}}$
	$(g \in D_{\mathrm{ICC}})$	**pub key**: $\mathrm{PK}_{\mathrm{ICC}} = g^{\mathrm{SK}_{\mathrm{ICC}}}, D_{\mathrm{ICC}}$
pick x at random	$\xleftarrow{\mathrm{PK}_{\mathrm{ICC}}, D_{\mathrm{ICC}}}$	
$X = g^x$	$\xrightarrow{X}$	
$K = \mathrm{KDF}(\mathrm{PK}_{\mathrm{ICC}}^x)$		$K = \mathrm{KDF}(X^{\mathrm{SK}_{\mathrm{ICC}}})$
output: K		**output**: K

Terminal Authentication

- terminal sends a certificate to chip (ECDSA)
- terminal signs a challenge + the ECDH ephemeral key

$\longrightarrow$ strong access control



Overall Process

1. do as before with MRZ and facial image
2. run chip authentication (replace the secure messaging keys)
3. run terminal authentication
4. load fingerprint, iris, ...

Terminal Authentication: Revocation

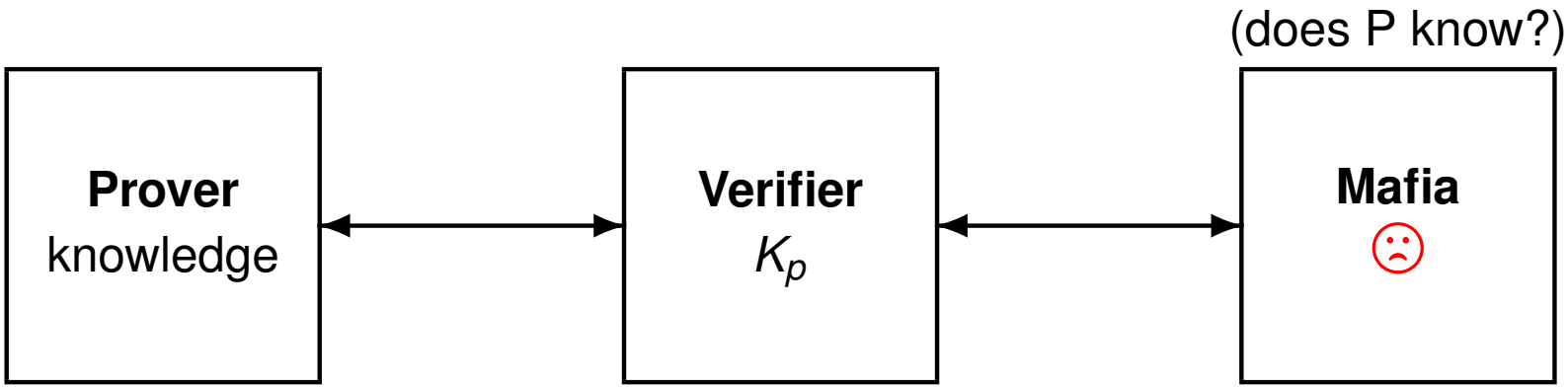
- MRTD are not online!
- MRTD have no reliable clock

$\longrightarrow$ MRTD must trust readers to revoke themselves

Information Leakage

- SO_D leaks the digest of protected DGs before passing EAC
- could be used to recover missing parts from exhaustively search
- could be used to get a proof if DG is known

Mafia Fraud + Fully Non-Transferable Proof



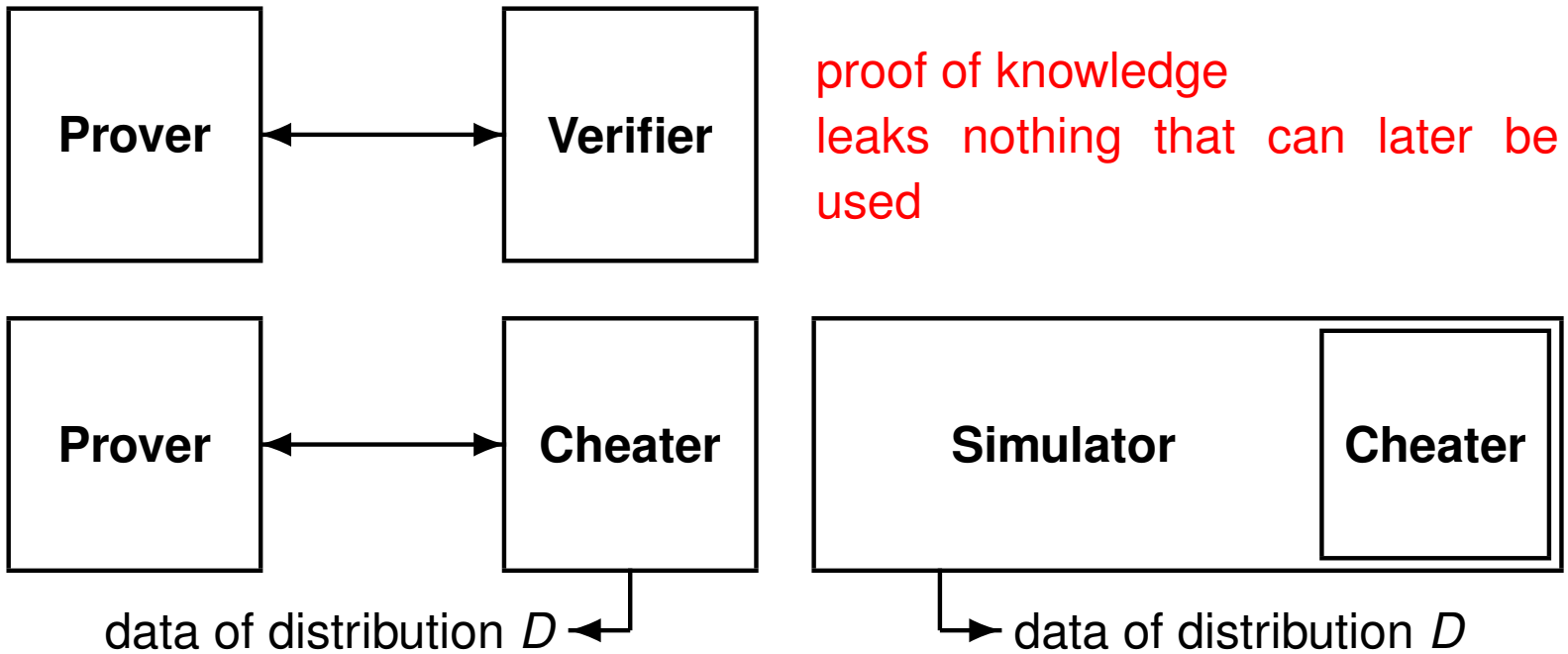
proof of knowledge

↓

proof of knowledge or of knowing a secret key attached to K_p

$\longrightarrow$ need PKI for verifiers: maybe an overkill

Zero-Knowledge: Offline Non-Transferability



Proof of Signature Knowledge based on GQ

Prover		**Verifier**
formated message: X **private signature**: x	**public key**: N, e	**formated message**: X
pick $y \in \mathbf{Z}_N^*$		pick $c \in \{0,1\}^\ell$, pick δ
	$\xleftarrow{\gamma}$	$\gamma \leftarrow H(c\|\|\delta)$
$Y \leftarrow y^e \bmod N$	$\xrightarrow{Y}$	
$\gamma \stackrel{?}{=} H(c\|\|\delta)$	$\xleftarrow{c,\delta}$	
$z \leftarrow yx^c \bmod N$	$\xrightarrow{z}$	$z^e \stackrel{?}{\equiv} YX^c \pmod N$

does not work when only HVZK: $c = F(Y)$ transforms into signature

full ZK with a prior commitment round

Conclusion

- **LDS**: leaks to much private information
- **passive authentication**: leaks digital evidences of LDS
  $\longrightarrow$ need zero-knowledge proof of valid signature knowledge
- **BAC**: does a poor job
  $\longrightarrow$ need PAKE
- **secure messaging**: OK (old crypto from the 1980's)
- **AA**: leaks evidences, subject to MITM
  $\longrightarrow$ need zero-knowledge ID proof
- **EAC**: much better, but still leaks + revocation issue
- **RFID**: leaks
  $\longrightarrow$ need a privacy standard or an off/on switch
- **biometrics**: leaks patterns
  $\longrightarrow$ need onboard matching

Related Academic Work

- **Avoine-Oechslin**: Financial Cryptography 2005
  privacy issues related to RFID collision-avoidance protocols
- **Juels-Molnar-Wagner**: SecureComm 2005
  survey of security and privacy for MRTD
- **Hoepman-Hubbers-Jacobs-Oostdijk-Schreur**: IWSEC 2006
  entropy of MRZ + extended access control
- **Carluccio-Lemke-Rust-Paar-Sadeghi**: RFID Security 2006
  bruteforce on MRZ_info for basic access control
- **Hancke**: S&P 2006
  unauthorized access and skimming experiments
- **Vuagnoux-Vaudenay**: Journal of Physics vol. 77, 2007
  survey + privacy issues related to passive authentication
- **Vaudenay**: IEEE Security & Privacy vol. 5, 2007
  survey + better protocol for passive authentication

Q & A