Security of Biometric Passports
ECE 646 Fall 2013

Team Members :

Aniruddha Harish
Divya Chinthalapuri
Premdeep Varada

Contents

- Introduction to ePassports
- Infrastructure required for ePassports
- Generations of ePassports
- First generation
  - Protocols
  - Drawbacks and attacks
- Second generation
  - Protocols
  - Improvements over the previous generation
  - Drawbacks and attacks
- Third generation
  - Protocols
  - Improvements over the previous generation
- Conclusion
- Questions

Introduction to ePassports

- ePassports are biometric identification documents that use RFID tags.
- Used for Border security.
- Based on ICAO(International Civil Aviation Organization) standards.
- RFID has cryptographic functionality.
- Goal is to enhance security, protect against forgery, manipulation of travel documents and ease of identity checks.
- Biometrics are used a form of individual recognition

INFRASTRUCTURE REQUIRED FOR EPASSPORTS

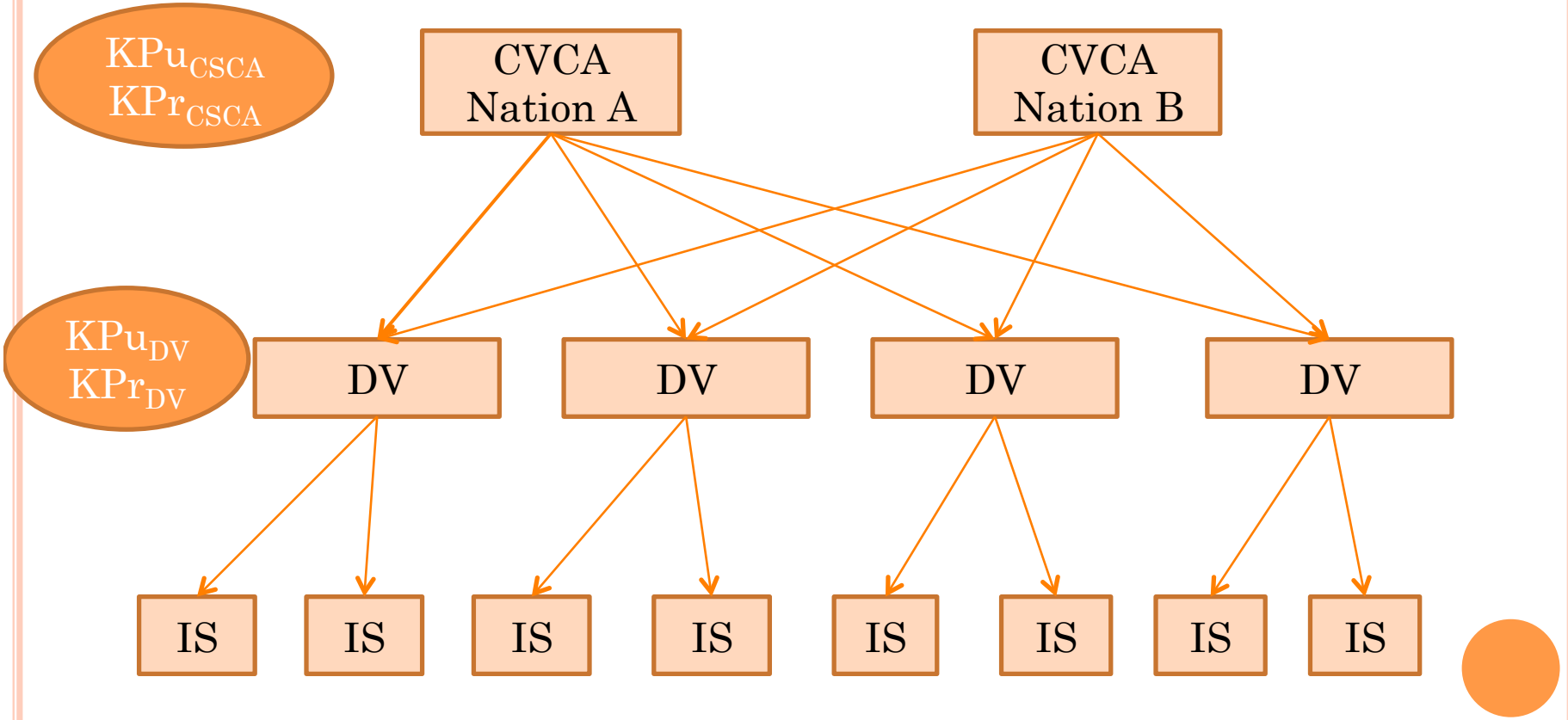
- 16 DG's are write protected
- A hash of DGs 1-15 are stored in the SDE.
- Each of these hashes should be signed by the issuing state.

Data Group	Data Element
DG1	Document details
DG2	Encoded headshot
DG3	Encoded fingerprint
DG4	Encoded iris
DG5	Displayed portrait
DG6	Reserved for future use
DG7	Signature
DG8-10	Data features
DG11-13	Additional details
DG14	CA Public key
DG15	AA Public key
DG16	Persons to notify
SOD	Security Data Element(SDE)

ePassport Logical data structure

Infrastructure required for ePassports

- **ePassport PKI**



First generation of ePassports: protocols

- 3 Cryptographic protocols
  - Passive Authentication (mandatory)
  - Active Authentication
  - Basic Access Control

First generation of ePassports : Protocols

- **Passive Authentication (PA)** :
  - For the reader to verify that the data in the ePassport is authentic.

Signature on LDS on the ePassport ⟸ Inspection System verifies

Hash values on SDE ⟹ Reader computes hash of data elements and compares them with the hashed values stored on the SDE.

  - If there is a match, then the data on the Tag was not manipulated.

First generation of ePassports : Protocols

- **Active Authentication(AA)(optional)**
  - To detect if a tag has been substituted or cloned.
  - Tag stores a public key (KPu_{AA}) in DG15 and its hash in SDE.
  - The (KPr_{AA}) is stored in the secure section of Tag memory.

Tag ⟸ Reader (random 64 bit string)

Tag ⟹ Reader

(sign-KPr_{AA})

Tag ⟸ Reader (public key KPu_{AA} from Data Group 15)

First generation of ePassports : Protocols

- Basic Access Control
  - It prevents eavesdropping.
  - Reader needs to prove the knowledge of secret keys(access keys(K_{ENC};K_{MAC})) that are derived from data on the Machine Readable Zone (MRZ) of the passport.
    - **MRZ** : The Passport Number (Doc No), Date of Birth of the Passport Holder (DOB), Valid Until Date of Passport expiry (DOE).
  - From these keys, a session key is obtained.
  - The access keys are derived from :
    - K_{seed}=128msb(SHA 1(DOCNo||DOB||DOE||C))
      - K_{ENC}=128msb(SHA-1(K_{seed}||1))
      - K_{MAC}=128msb(SHA-1(K_{seed}||2))

First generation of ePassports : Protocols

Basic Access Control

- Tag (Rt) ⟹ Reader

  Reader receives Rt and generates Rr, Kr
  Reader Rr||Rt||Kr using K_{ENC}.
  Reader MAC using K_{MAC}.

- Tag ⟸ Reader

  cipher and MAC

- Tag

  MAC and decrypts the cipher extracts Kr
  Tag Rt||Rr||Kt using K_{ENC}
  Tag MAC using K_{MAC}

- Tag ⟹ Reader

  cipher and MAC

- Reader

  MAC and decrypts the cipher extracts Kt

- Tag ⟺ Reader

K_{seed}=Kr^Kt K_{seed}= Kr^Kt

All communication is secured using these KS_{ENC} and KS_{MAC} keys.

First generation of ePassports : Attacks

- Just the passive authentication ??
  - Skimming attack and
  - Eavesdropping attacks are possible
  - Therefore Basic access control.

First generation of ePassports : Attacks

- Privacy attack(because of the weakness in BAC):
  - Dutch passport
    - » Can be read from a distance of <0.5m
    - » Hence can acquire the user's MRZ data
    - » Static keys derived from MRZ (used in the key derivation for BAC(encryption key and session key))
      - DOE of ePassport : 5 years : 5*365=1825 values
      - DOB of the passport holder : 10*365 = 3650 values
      - One character followed by 8 digits gives an entropy of 50 bits. Therefore 10^15 possible values.
      - Passports were issued sequentially

ENTROPY CALCULATION

Document Number	7 variable characters (letters + digits)	(26 + 10)^7	36.19 bits
Date of birth	2 digits for year	365*100	15.16 bits
Date of expiry	validity period of 5 years	5*365	10.83 bits
Total			62.18 bits

BAC of MRTD(machine readable travel document): Architecture consisting of RF based communication and for cryptanalysis in real-time a **cost optimised parallel code breaker hardware (COPACOBANA)** is used to trace the user.

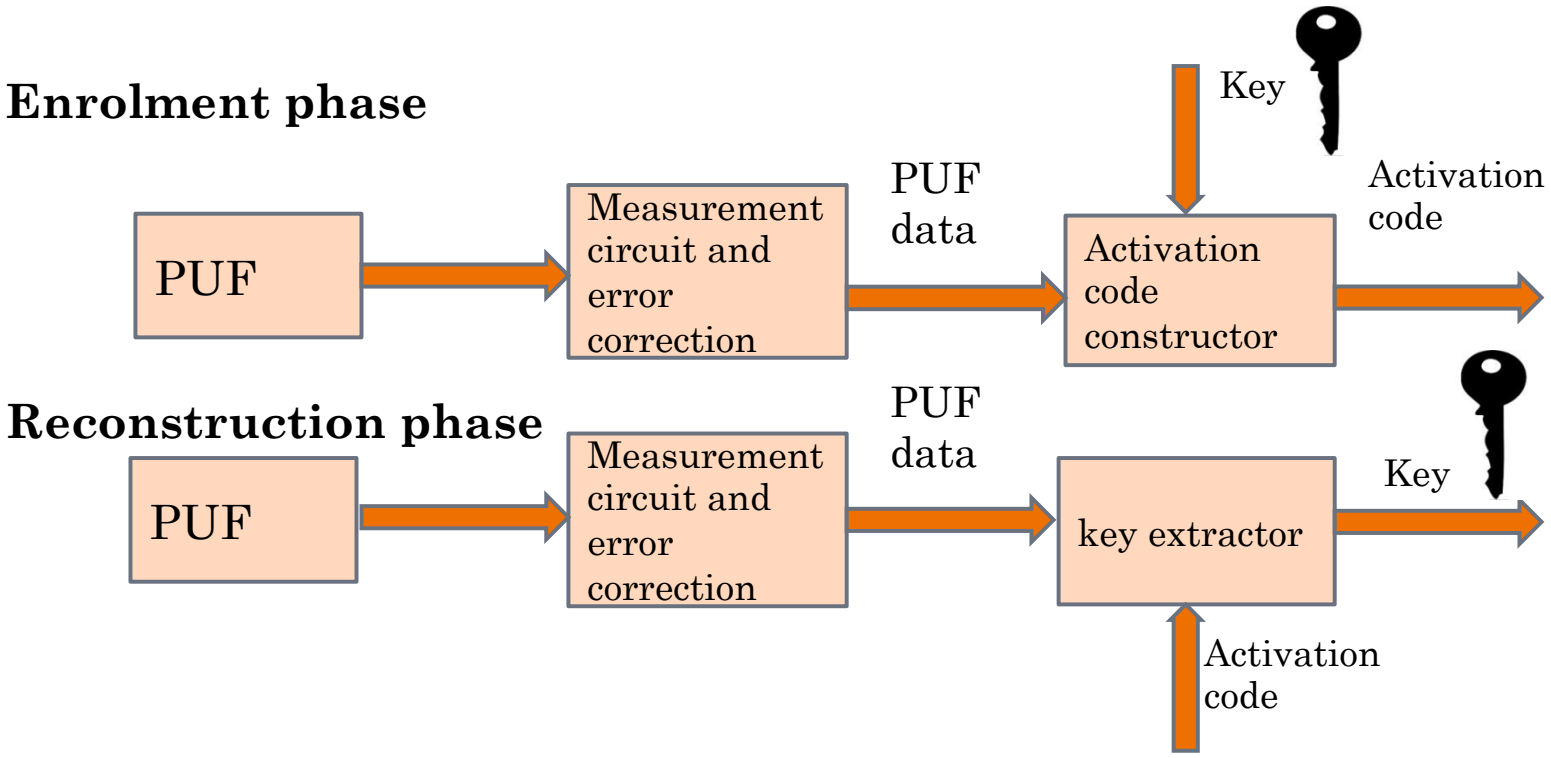
PROTECTION AGAINST CLONING

- **Active authentication** for protection against cloning attack
- The authentication relies on a private key hidden in the chip's secure memory.
- Physical unclonable function(PUF) can protect the key and prevent reverse engineering or cloning.

PUFs are functions based on physical characteristics which are :

- Unique for each chip and practically impossible to duplicate.
- A characteristic that fluctuates can be turned into a PUF.
- SRAM-based- On powering the Smart Card IC each specific bit in SRAM getting zero or one as an initial value - is different for every individual chip
- Monitor the environment.

PHYSICAL UNCLONABLE FUNCTION



SECOND GENERATION OF EPASSPORTS : PROTOCOLS

- **Extended Access Control** :
- Tag and Reader authentication protocols.
- Implementation of secondary biometrics for additional security.
- To achieve mutual authentication :
  - Chip Authentication and
  - Terminal Authentication

SECOND GENERATION OF EPASSPORTS : PROTOCOLS

- **Chip Authentication**
- Replaces Active Authentication. It is the process of checking the possession of a private key in the chip of the passport by the reader.
- Uses a public key (in DG 14) and private key (in secure memory) (TK_{PuCA}, TK_{PrCA}).

  - Tag ⟹ Reader
    (TK_{PuCA}, D)

    Verifies the correctness of the key using PA.
    Uses the data in D to generate its own RK_{PuCA} and RK_{PrCA}
  - Tag ⟸ Reader
    (RK_{PuCA})
  - Tag(K_{seed}) ⟺ Reader (K_{seed})
  - The new encryption and MAC keys are generated.

SECOND GENERATION OF EPASSPORTS :PROTOCOLS

Terminal Authentication

- Access to more sensitive data (secondary biometrics).
- Allows Tag to validate the Reader used in CA.
- The Reader proves to the Tag using digital certificates that it has been authorized by the home and visiting nation to read ePassport Tags.

- Tag ⟸ Reader

  Inspection System certificate (which was received from the local DV) and the DV's certificate (which was received from the CVCA).

- Tag

Extracts (RK_{PuTA}) from the IS certificate.

- Tag(R) ⟹ Reader

  Reader computes hash of RK_{PuCA} derived in the CA
  Reader signs the message (R||SHA-1(RK_{PuCA})) with (RK_{PrTA}).

- Tag

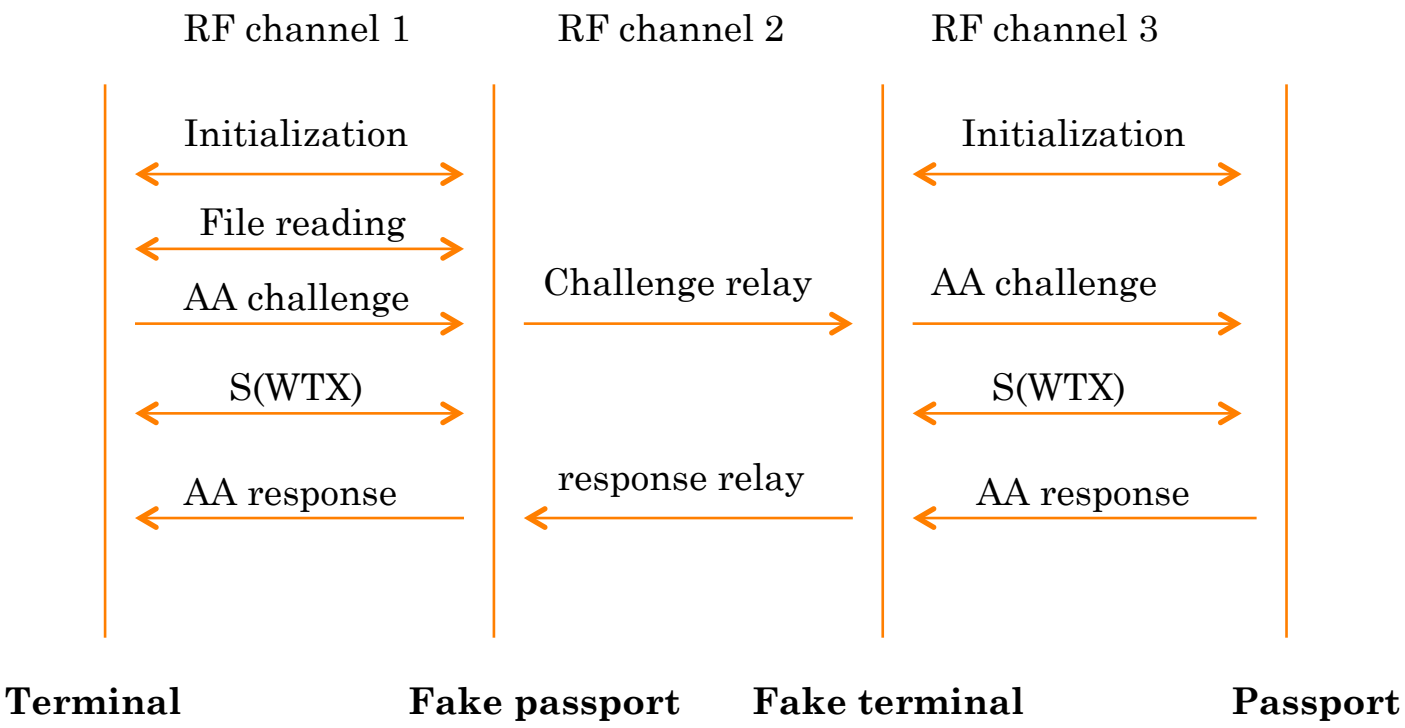
R and RK_{PuCA} using the key RK_{PuTA} and grants access to secondary biometrics.

Advantages over First Generation

First Generation	Second Generation
Use of static keys	Ephemeral keys derived from Diffie Hellman
Biometrics not included	Biometrics included
Use of MRZ to derive the session key	MRZ data not used
Less entropy	Comparatively more entropy

Second generation of ePassports: Attack

- Relay Attack on Active Authentication



Second generation of ePassports: Drawbacks

- Vulnerability to attack by once valid readers - since a passive RFID tag doesn't have a clock, the clock still has the value it had when it was active the previous time.
- Since Terminal Authentication is performed after Chip Authentication, it is vulnerable to Denial of Service Attacks.
- It is still vulnerable to side channel attacks/skimming attacks.

THIRD GENERATION OF EPASSPORTS: PROTOCOLS

- **Password Authenticated Connection Establishment(PACE)** protocol as a replacement to BAC.
- Also updated CA and TA.
- Uses asymmetric cryptography
- CAN(Card access number) & MRZ

types of passwords are used. CAN may be static or dynamic

- CA carried out after TA so that it can have the key pair generated in TA.

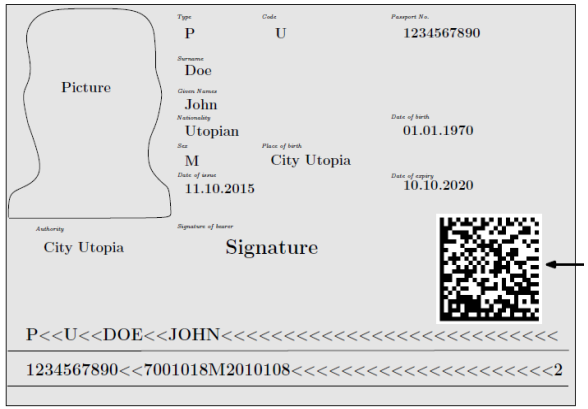
Third Generation e-passports: Protocol

PACE(share a common password “π”)

TAG		READER
Encrypts “s” by K_{π}	D, K_{π} →	Decrypts “s” by password
Computes D' by D and S		Computes D' by D and S
(Pr_{Tag}, Pu_{Tag})	Pu_{Tag} →	Reader
Tag	← Pu_{Reader}	$(Pr_{Reader}, Pu_{Reader})$
K_{Seed}	↔	K_{Seed}
Derive session keys K_{ENC} and K_{MAC}		

BIOPACE

- It is implemented by using facial image, fingerprints, iris, etc
- Biometric reference comprising of a pseudonymous identifier PI and auxiliary data AD
- BioPACE claims that no unauthorised data retrieval is possible
- Faster verification
- Improving privacy



THIRD GENERATION E-PASSPORTS SOLUTION: WDDL

- Information related to the physical implementation of the device can be used to find the secret key in the side-channel attacks.
- Wave Dynamic Differential Logic (WDDL) is a practical technique to thwart side-channel attacks.
- Measurement based experimental results show that attack on a IC fabricated in CMOS does not disclose the entire secret key
- Side –channel attacks can be mounted on to ASICs, FPGAs, DSPs .
- By using the Secure digital design flow we can have constant power dissipation by balancing the power consumption (independent of the signal).

Third Generation e-passports: Drawback

- The password is picked up by users from a small space, and therefore the protocol is vulnerable to dictionary attacks.
- An online dictionary attack (guess the password and try to execute the protocol with one of the parties) can be prevented through latency or smart card blocking.

Third Generation e-passports: Solution and conclusion: PACE v2

- PAKE is implemented using elliptic-curve cryptography
- Representing numeric values(here passwords) as points on an elliptic curve.
- Uses encoding functions(encoding passwords to curve points) for authenticated key agreement.
- Groups are defined with the points in such a way that the discrete-logarithm problem in that group (the problem of retrieving integer l from point G on the curve and lG = G + … + G) is believed to be computationally hard.
- This means that elliptic-curve-based protocols can use shorter keys and more efficient arithmetic than protocols

Third Generation e-passports: Solution and conclusion: PACE v2

- The two parties have therefore obtained a common high-entropy secret: point Z on the elliptic curve. Then the key is derived, confirmed, and a secure session is establishment.
- This encoding is more efficient and protects against side channel attacks.

Questions