THALES
Building a future we can all trust

Electronic document in the Quantum era

November 2024

JAVA CARD Forum

THALES GROUP EXTERNAL

Agenda

- Introduction
- Electronic document overview
- Impact of CRQC on electronic document
- PQC algorithms for electronic document

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Introduction

- The first electronic passport compliant to ICAO specifications was introduced in 2004. There are more than 140 States and non-state entities (e.g. United Nations, European Union) currently issuing ePassports, and over 1 billion ePassports in circulation.

- The ICAO specifications for the electronic data (Doc 9303) have been adopted and adapted for other electronic documents: Identity card, Driving License, EU-Resident Permit.

- It's time to review the ICAO security mechanisms to face Quantum era and the different threads it will bring.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©thales 2020 Tous Droits réservés.

Electronic document in the Quantum era

1st part

Electronic Document 101 training

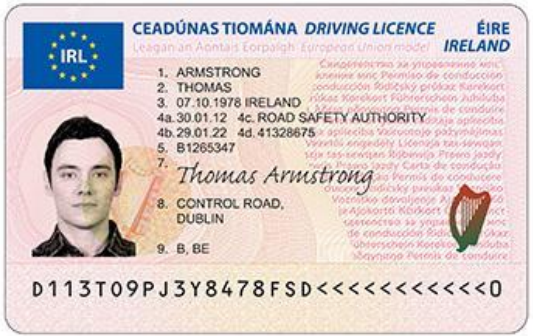
Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Identity documents

Passport

Identity Card

Driving License



Resident Permit

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©thales 2020 Tous Droits réservés.

Standardized passport timeline


TYPE OF "INTERNATIONAL" OR "STANDARD" PASSPORT RECOMMENDED BY THE LEAGUE OF NATIONS PASSPORT CONFERENCE HELD IN PARIS IN OCTOBER 1920. (The model is that of a passport such as would be delivered by the Spanish Government.)

PASAPORTE
PASSEPORT
NOMBRE DEL PAIS
NOM DU PAYS

SEÑAS PERSONALES
SIGNALEMENT

HIJOS · ENFANTS

1920 — The *League of Nations* International Conference on Passports agrees on a new book format for passports

1944

1946 — **ICAO created**

1968 — *ICAO Panel on Passport Cards* created.

1980 — ***ICAO Document 9303*** *Passport with Machine Reading Capability* issued

1997 — ***ICAO New Tech. Working Group*** Starts study on biometric identification, data storage and contactless IC

1998 — **First biometric passport** (non-ICAO compliant) Malaysia

2001 — 9/11 Patriot act

2004 — **First ICAO e-Passport** Belgium

ICAO Doc 9303 Part 1, Vol2 *Specification for Electronically Enabled Passport with Biometric Identification Capability*

2006 — **EU-EAC (BSI)** to protect the access to Fingerprint and Iris

2009 — **EU** Fingerprint mandatory in EU protected with EU-EAC

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Why do we need standards - Passports

Before 2004

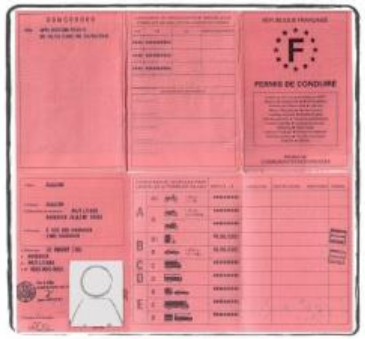
- Different ways to print the information.
- Not many security features.
- Very easy to counterfeit.

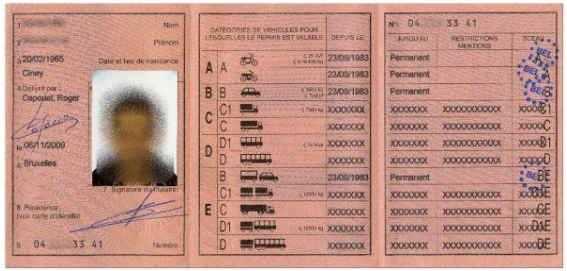
Since 2004

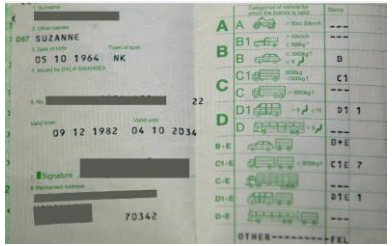
- Identical format allowing an automatic process to read the document.
- More difficult to counterfeit.
- Contactless chip is strongly recommended!

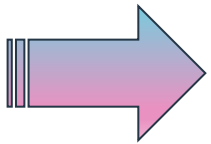
Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales - 2020 Tous Droits réservés.

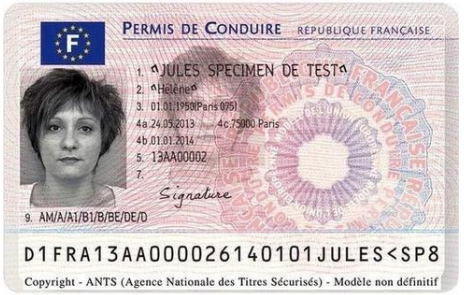
Why do we need standards – Driving license in European Union

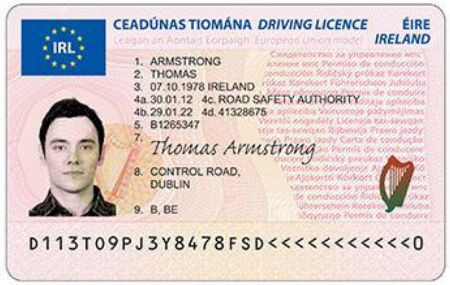












Before 2013

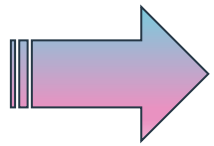
- Different paper/card formats.
- Very easy to counterfeit.

Since 2013

- Polycarbonate ID1 card format with security features; more difficult to counterfeit
- Identical format allowing an automatic process to read the document.
- Chip is not mandatory

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'

Why do we need standards – Identity card in European Union



Before 2021

- Different ID1 or non-ID1 card formats.
- With or without chip

Since 2021

- Polycarbonate ID1 card with security features; more difficult to counterfeit
- Identical format allowing an automatic process to read the document.
- Chip is mandatory

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Security – Document Holder's protection

Tracing passport chip

- The chip shall always return a random Chip Serial Number for each new session of the contactless communication

Unauthorized access to the passport

- A Mutual Authentication sequence shall take place at the beginning of the Document verification process. Document and Personal details are used to create a password to initiate this sequence.
- The mechanism is called **Password Authenticated Connection Establishment (PACE)**

Eavesdropping a passport

- After the Mutual Authentication, a Secure Messaging session is established to encrypt and secure the exchanges between the Document and the Terminal.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Security – Issuing Authority's protection

Modifying data of a given passport

- Data in the chip are hashed and then digitally signed by the issuing country
- Signature is stored in the chip along with the public key of the issuing country.
- The mechanism is called **Passive Authentication (PA)**

Cloning a passport

- Readable data in the chip contains a public key
- Corresponding private key is stored securely in the chip (can't be retrieved)
- To ensure originality of the chip a signature with the private key is requested and verified.
- The mechanism is called **Active Authentication (AA)**

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

What do we store inside the chip

Personal Details

Surname : TAYLOR (unicode)

Given Name : EMILY ALEXANDRA (unicode)

Sex : Female Nationality : Utopia

Date of Birth : 15/09/1995 Custom -- Select Custom Date of Birth Option --

Passport Details

MRZ Type : ID3

Type : P Country Code : UTO

Passport No : AB1234567

Date of Expiry : 31/01/2033

Optional Data :

Personal and document details

Picture

```
P<UTOTAYLOR<<EMILY<ALEXANDRA<<<<<<<<<<<<<<<
AB12345671UTO9509159F3301317<<<<<<<<<<<<<<06
```

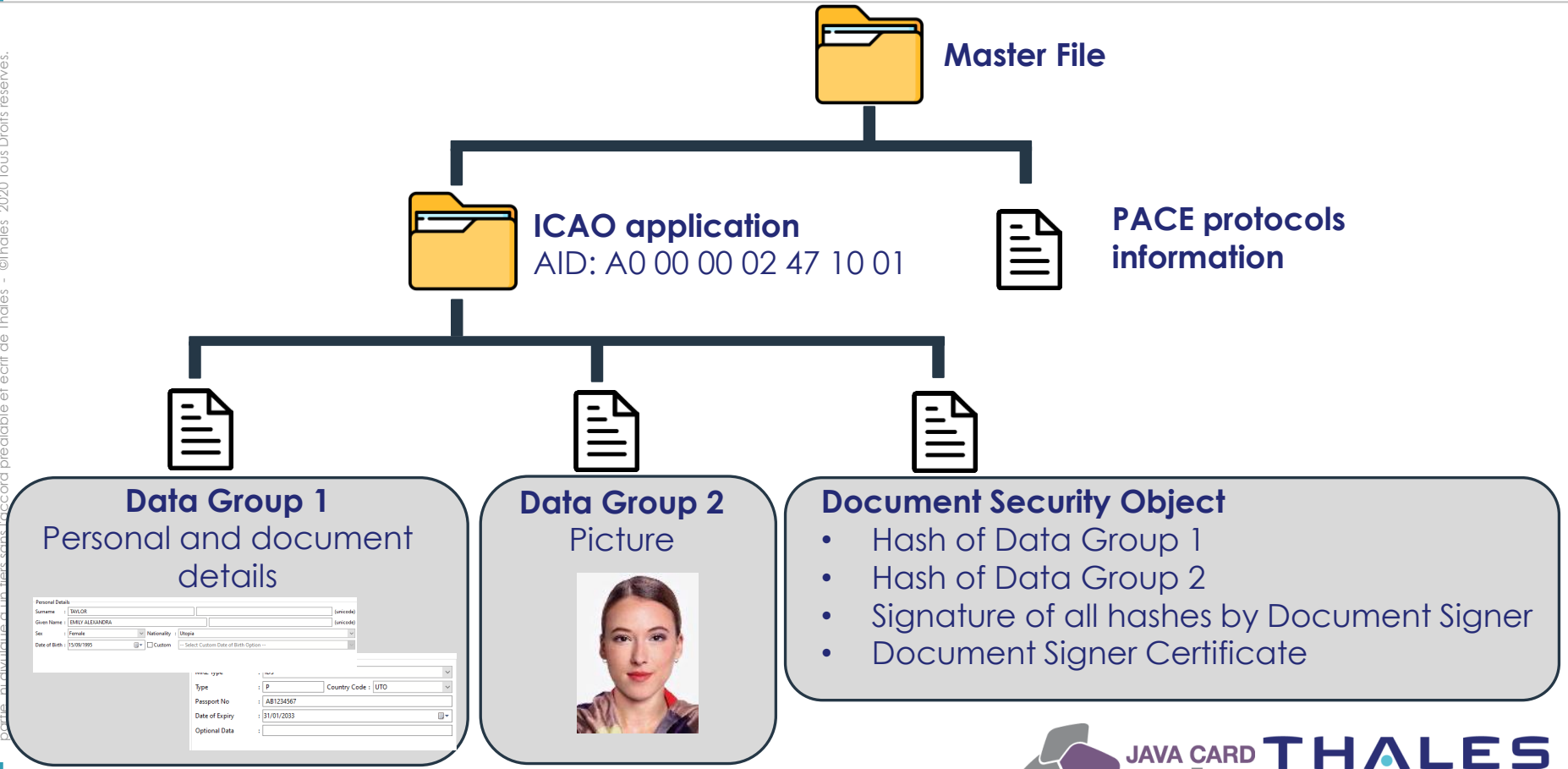
Fingerprint (mandatory in EU)

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

THALES GROUP LIMITED DISTRIBUTION - SCOPE

THALES
Building a future we can all trust

File structure inside the chip



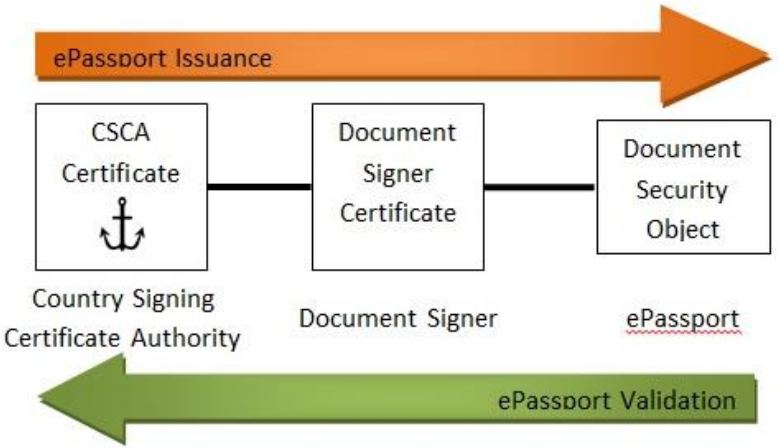
Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

THALES GROUP LIMITED DISTRIBUTION - SCOPE

ePassport Trust Chain for Passive Authentication

- A digital signature on an ePassport is derived from the issuing State's security certificate, the **Country Signing Certification Authority** (CSCA) Certificate and the **Document Signer Certificate** (DSC).

- The signature and certificates form a **trust chain** wherein one end is securely anchored in the authority of the issuing State and the other end is securely stored in the chip of the ePassport.

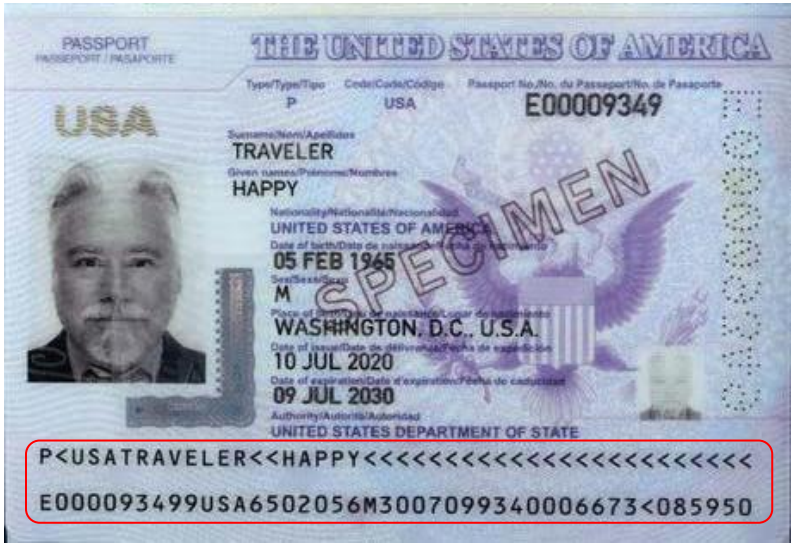


Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

How do we verify a document

Step #1 – Scan the data page of the passport

- Retrieve different items: Personal and Passport data, Photo, MRZ (2 lines on passport)



Step #2 – Gain access to the chip

- Perform PACE using some items in the MRZ as a password
- Read all the accessible files

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

How do we verify a document

Step #3 – Authentication of the data

1. Hashes of each files read are compared with the one stored in the chip
2. Signature of the hashes compared with the one stored in the chip
3. Document Signer Certificate (DSC) verified against Country Signing Certification Authority (CSCA)
4. CSCA and DSC verified against Certificate Revocation List (CRL)

Step #4 – Comparison of the chip content and data printed

- Compare Personal and Document details, picture and any additional data stored on the chip

Step #5 – Authentication of the chip (anti cloning)

- Perform Active Authentication procedure

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Details on ICAO Security mechanisms

Password Authenticated Connection Establishment (PACE)

- PACE is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and password-based authentication of the eMRTD chip and the inspection system

- Key Agreement Algorithms:
  - Diffie-Hellman: PKCS#3, RSA 1024 and 2048 bits
  - Elliptic Curve Diffie-Hellman: TR-03111, ECC NIST/Brainpool 192/224/256/320/384/512/521 bits

- Secure Messaging Algorithms:
  - Key 3DES 112 bits, Secure Messaging CBC/CBC, Auth. Token CBC
  - AES 128/192/256 bits, Secure Messaging CBC/CMAC, Auth. Token CMAC

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Details on ICAO Security mechanisms

Passive Authentication (PA)

- Ensure that the contents of the Data Group are authentic and unchanged by hashing the contents and comparing the result with the corresponding hash value in the Document Security Object

- Hashing algorithms:
  - SHA2: 224/256/384/512 bits
- RSA signature mechanisms: RSASSA-PSS (recommended) and RSASSA-PKCS1_v15
- Digital Signature according to FIPS 186-4
- ECDSA according to X9.62 or ISO/IEC 15946

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Details on ICAO Security mechanisms

Active Authentication (CA)

- Active Authentication authenticates the contactless Chip by signing a challenge sent by the Terminal with a private key known only to the Chip.

- Hashing algorithms:
  - SHA1: not for ECDSA
  - SHA2: 224/256/384/512 bits
- RSA Digital Signature according to ISO/IEC 9796-2: 1024/1280/1536/2048/3072/4096 bits
- ECDSA plain signature format according to TR-03111: Brainpool/NIST 160/192/224/256/320/384/512/521 bits

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Electronic document in the Quantum era

2nd part

Impact of CRQC on electronic document

and

PQC algorithms for electronic document

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Impact of CRQC on electronic document

- Cryptographically Relevant Quantum Computers (CRQC) will have a colossal impact on the security mechanisms used by electronic documents
- Indeed, ICAO security mechanisms rely on RSA and ECC for Digital Signature and Key agreement. **They will be broken by a powerful CRQC using Shor's algorithms!**
- This means, that someone will be able to forge any electronic document **without the possibility to make a distinction between a forged and a real document!**
- We must specify **new security mechanisms** based on Post Quantum Cryptographic algorithms.
- Their implementation in the electronic document should allow a **smooth migration** in front of legacy **Inspection Systems**.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

THALES GROUP LIMITED DISTRIBUTION - SCOPE

Hybrid Passive Authentication - CSCA

Hybrid signature - PKI implementation

- Hybrid Signature consists of combining asymmetric post-quantum algorithms with well known and well studied pre-quantum asymmetric cryptography (several governmental agencies recommend such implementation).
- For our demonstration today, Thales selected an implementation backward compatible with current Inspection Systems to allow a smooth migration to a full PQC era: multiple-certificates

Multiple Certificates implementation

- Current CSCA (legacy CSCA) remain unchanged
- A new PQC CSCA shall be deployed
- The legacy CSCA and the new PQC CSCA live in parallel for an extended period.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Hybrid Passive Authentication – SOD File

Two signatures

- The SOD File will enclose two signatures: legacy and PQC
- Both signatures will sign the same hash of DGs content. Therefore, the hash algo used for DG contents shall be a legacy one for backward compatibility.
- Example:
  - DGs content hashes: SHA512
  - Signature #1: ECDSA 521 - SHA512
  - Signature #2: ML-DSA Level 5 – SHAKE256
  - SOD File size: 19,250 bytes

	Algorithm	Signature size (bytes)	Public Key (bytes)
Legacy	ECDSA 521	139	133
	RSA 4096	512	526
PQC	FIPS 204 (ML-DSA Dilithium) - Level 3	3,309	1,952
	FIPS 204 (ML-DSA Dilithium) - Level 5	4,627	2,592
	Falcon 1024	1,273	1,793

Backward compatible

- The second signature in the SOD File is ignored by legacy Inspection Systems

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Hybrid Passive Authentication – Impacts

Back-end system

- Upgrade of the Document Issuer PKI system for the support of the PQC-CSCA
- Upgrade of the Document Issuance system for dual signature of the SOD file
- Upgrade of the ICAO PKD to share PQC-CSCA public keys
- Upgrade of Inspection Systems for the verification of both signatures

Document

- Current electronic passport can support the hybrid Passive Authentication.
- The chip must have enough Non-Volatile Memory to store larger SOD file.
- Example: total amount of memory used to store DG1, DG2 and corresponding security mechanisms
  - Legacy (ECDSA 521 - SHA512): 1,637 bytes for the SOD File → **Total memory: 24KB**
  - Dual Signature (ECDSA 521 - SHA512 and ML-DSA Level 5 – SHAKE256): 19,250 bytes for the SOD File → **Total memory: 41KB**

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Password Authenticated Key Exchange (PAKE)

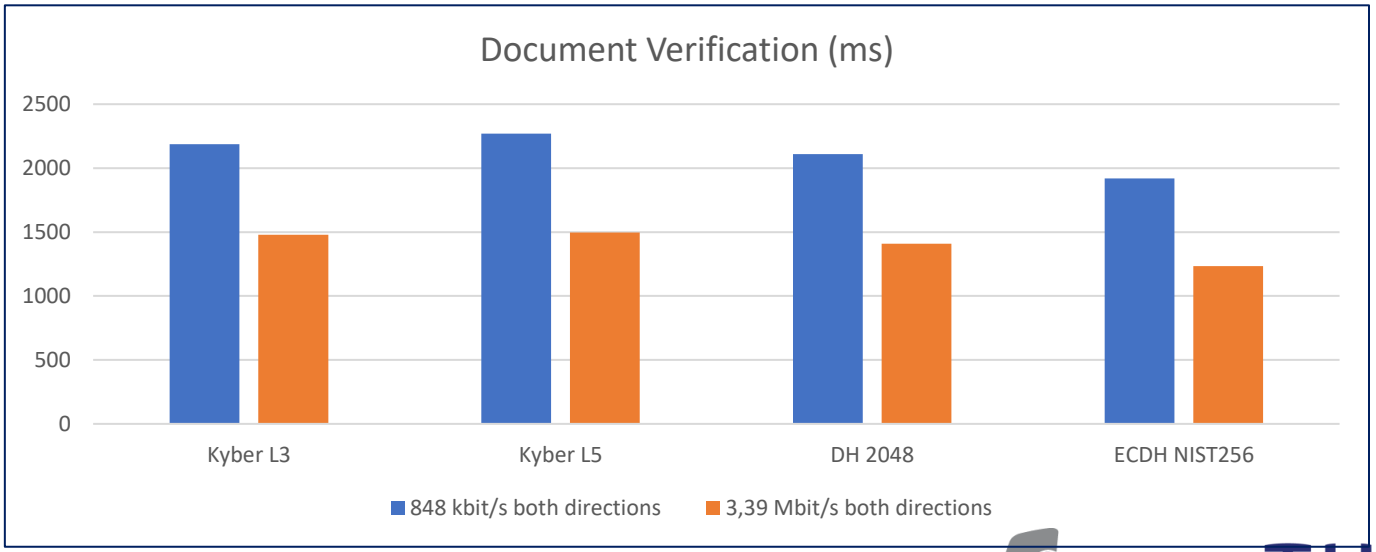
- **Password Authenticated Key Exchange (PAKE) allows to dispense with the heavy public key infrastructures and its efficiency and portability make it well suited for applications such as Internet of Things or e-passports.**
- **PAKE will allow establishing a secure channel between the terminal and the chip**
- **Different research papers on Cryptology have been recently published regarding PAKE and PQC**
  - **2023 - GeT a CAKE:** Generic Transformations from Key Encapsulation Mechanisms to Password Authenticated Key Exchanges - Ecole Normale Supérieure, CNRS, Inria, Université Paris Panthéon, ANSSI, Thales: 470.pdf (iacr.org)
  - **2023 - Randomized Half-Ideal Cipher on Groups with applications to UC (a)PAKE:** University of California, Irvine: 295.pdf (iacr.org)
  - **2024 - C'est trés CHIC: A compact password-authenticated key exchange from lattice-based KEM:** University of Porto, Irvine CA, Luxemburg and Institute for Security and Privacy: 308.pdf (iacr.org)
  - All these recent papers triggered a lot of interest in Thales Security Labs, and then decided to implement the **PAKE CHIC** protocol in a chip.
  - PAKE CHIC uses **NIST FIPS 203** Key Encapsulation Mechanism (KEM).

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

PAKE CHIC with Kyber – Some benchmarks

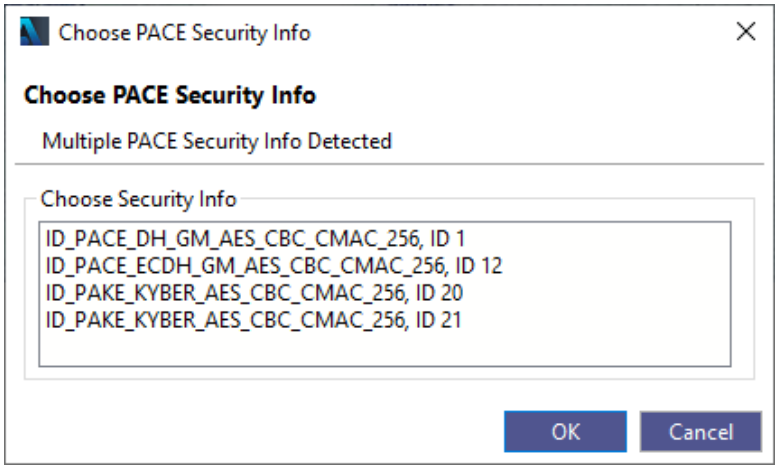
Configuration of the document

- PACE and PAKE
  - **PAKE CHIC Kyber L3 - AES-CBC-CMAC-256**
  - **PAKE CHIC Kyber L5 - AES-CBC-CMAC-256**
  - PACE DH GM (RSA 2048) - AES-CBC-CMAC-256
  - PACE ECDH GM (NIST P256) - AES-CBC-CMAC-256
- Chip Authentication: ECDH 512 Brainpool - ECDH-AES-CBC-CMAC-256
- Passive Authentication: Hybrid ECDSA521-SHA512 and ML-DSA (Level 5) SHAKE256
- DG files total size: 41KB

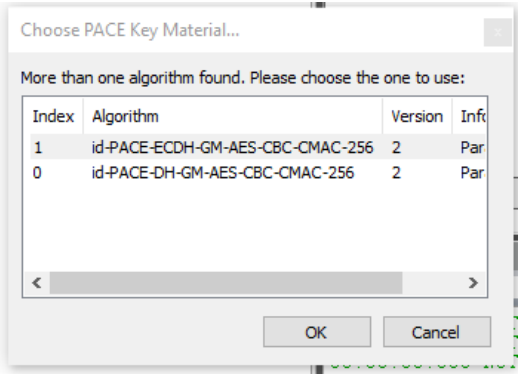


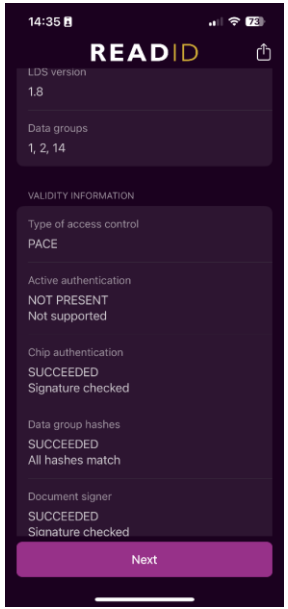
Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

PAKE Kyber– Demonstration



PQC enabled Inspection System





Legacy Inspection Systems (Platinum GRT, ReadID me)

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

PAKE – Impacts

Back-end system

- Upgrade of the Document Issuance system for the personalization of PAKE parameters
- No impact on the PKI solutions (CSCA, CVCA)
- Upgrade of Inspection Systems for the support of PAKE algorithm

Document

- For this demonstration Thales used a standard “high-end” **chip 32 bits CPU with around 25KB of RAM**

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Evolution of the chips used for electronic passports

2004 to 2011

- 8 bits CPU
- 5 to 6 Kbytes RAM
- Type of Memory: ROM and EEPROM
- RF Communication: Up to 848 kbps

2012 to 2020

- 16 bits CPU
- 8 to 12 Kbytes RAM
- Type of Memory: ROM and EEPROM or Flash
- RF Communication: Up to 848 kbps and few VHBR products (up to 3,39Mb/s)

Since 2021

- 32 bits CPU
- 12 to 20 Kbytes RAM
- Type of Memory: Flash
- RF Communication: Up to 848 kbps and VHBR products (up to 6,78Mb/s)

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

PQC4eMRTD

Post-Quantum Cryptography for electronic Machine- Readable Travel Documents

- Funding: **EU - Digital-ECCC-2024–Deploy-Cyber-06-StandardPQC**
- 24 months project starting January 2025

The vision of the PQC4eMRTD project is to:

- Join forces of world leading European players in the field of security solutions in hardware and software, as well as PQC experts from academia and industry to push previous PQC research results up in the technology readiness scale towards the international standardization working groups to facilitate future deployments
- Demonstrate the secured implementation and integration of QRC algorithms and protocols in the fields of digital identities and PKI infrastructures.

5 Partners from 6 countries

- Infineon – Coordinator (Germany), CryptoNext (France), University of Lubiana (Slovenia), Barcelona Supercomputing Center - Centro Nacional de Supercomputación (Spain), Thales (France)

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

Conclusion

- This Electronic Document PQC enabled prototype based on NIST PQC algorithms confirms that there is no technical barriers to make Electronic Documents systems ready for Quantum era.
- It also confirms that existing document verification solutions can accept new type of documents allowing a smooth migration when introducing PQC enabled documents.
- European projects such as PQC4eMRTD will support ICAO on the specification of news security mechanisms.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2020 Tous Droits réservés.

THALES
Building a future we can all trust

Thank you

Electronic document in the Quantum era

JAVA CARD Forum

THALES GROUP EXTERNAL