THALES
Building a future we can all trust

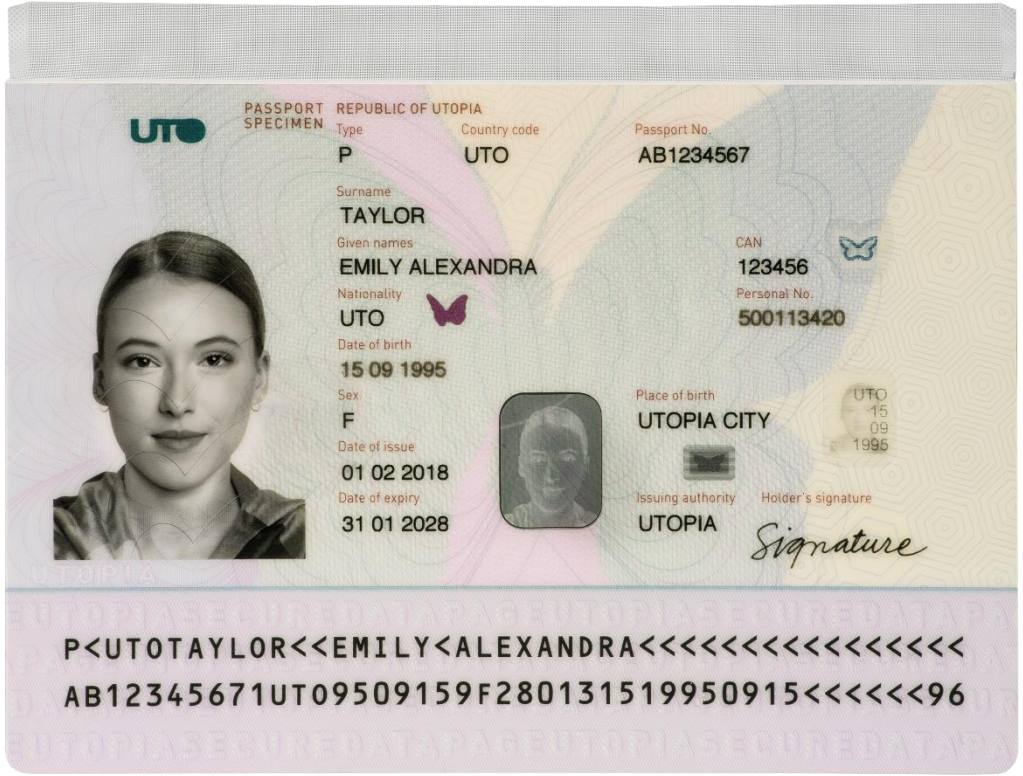
A path towards Quantum Safe eDocuments

PQC4eMRTD

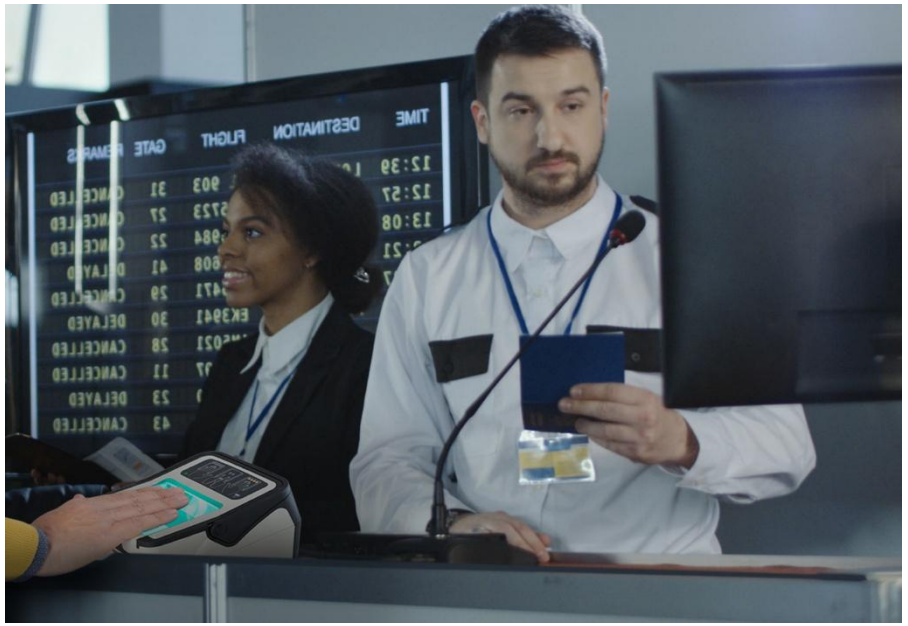
www.thalesgroup.com

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Introduction to MRTDs….



Introduction to « e » MRTDs…



Digital mechanisms

> PACE / Anti Skimming & Anti Eavesdropping	➢ (EC)DH + 3DES or (EC)DH + AES
> Passive Authentication / Digital Seal	➢ SHA2 + RSA or SHA2 + ECC
> Active Authentication / Anti-cloning	➢ DSA or ECDSA
> Chip Authentication / Anti-cloning	➢ (EC)DH + RSA or (EC)DH + ECC
> Terminal Authentication / Access to “Biodata”	➢ Chip Auth then DSA or ECDSA

Digital mechanisms

=

PQC4eMRTD

https://pqc4emrtd-project.eu/

https://www.linkedin.com/company/pqc4emrtd-project

https://x.com/pqc4emrtd

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

This project has received funding from the European Union's Cybersecurity Competence Centre under Grant Project No 101190400.

infineon

BSC Barcelona Supercomputing Center Centro Nacional de Supercomputación

THALES

CRYPTONEXT SECURITY

inštitutzaprimerjalnopravo

Objective: propose new quantum safe protocols to secure eMRTDs

PQC4eMRTD Objectives

> Draft PQC-solutions for all protocols used in the Doc9303 eMRTD-arena

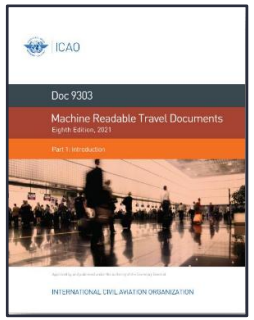
- Study state of the art protocols & Standardized Quantum Safe algorithms to upgrade 4 mechanisms
  - Skimming & Eavesdroping protection – PACE
  - Ensuring passport data are genuine – Passive Authentication
  - Anti-cloning mechanisms – Active Authentication & Chip Authentication
  - Data Access protection – Terminal Authentication
- Diversified approach
  - Single PQC algorithm
  - Hybrid (conventional + Quantum Safe) – concatenated & imbricated
  - Backward compatibility
- Demonstrate the security proof of proposed mechanism and ensure that new solutions preserve key properties from legacy ones

ICAO, ISO/IEC JTC1/SC17 & PQC4eMRTD

Joint Technical Committee 1
Sub Committee 17
Cards and security devices for personal identification
(JTC 1/SC 17)

Working Group 3
Traveler identification
(WG3)

Doc 9303



Technical Advisory Group on the Traveler Identification Program
(TAG/TRIP)

New Technologies Working Group
(NTWG)

PQC4eMRTD

First Achievements

> ICAO PQC Proof of Concept presented @NTWG.

> Password Authenticated Key Exchange (PAKE)

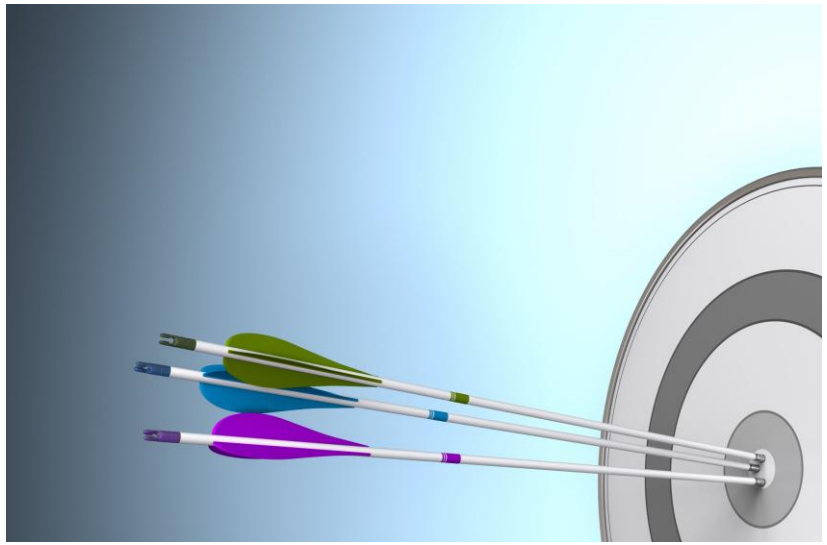
- PAKE will allow to establish a secure channel between the terminal and the eMRTD; to replace PACE.
- Protocol used is PAKE CHIC designed by 3 cryptographic researchers (**University of Porto, UC Irvine CA and University of Luxemburg**)
- Based on NIST FIPS 203 Key Encapsulation Mechanism (ML-KEM) & AES 256

> Passive Authentication (PA)

- Hybrid signature. The SOD File encloses two signatures: legacy and PQC
- Dual Signature (ECDSA 521 - SHA512 and ML-DSA-87 (FIPS204) – SHAKE256)

> Active Authentication (AA)

- ML-DSA-65 (FIPS 204) Digital Signature to prevent the copy of the original chip



PQC4eMRTD - Prototype verification (1/2)

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2025/32

Ce certificat est associé au rapport de certification ANSSI-CC-2025/32

MultiApp 5.2 Premium PQC

version 5.2

Développeur : THALES DIS FRANCE SAS
Commanditaire : THALES DIS FRANCE SAS
Centre d'évaluation : CEA - LETI

Critères Communs version 3.1, révision 5

EAL6 augmenté
ALC_FLR.1

conforme au profil de protection :
Java Card System – Open Configuration Protection Profile, version 3.1
certifié BSI-CC-PP-0099-V2-2020, avril 2020

Date de validité : date de signature + 5 ans.

Paris, le 29/9/2025 | 21:08 CEST

Vincent Strubel

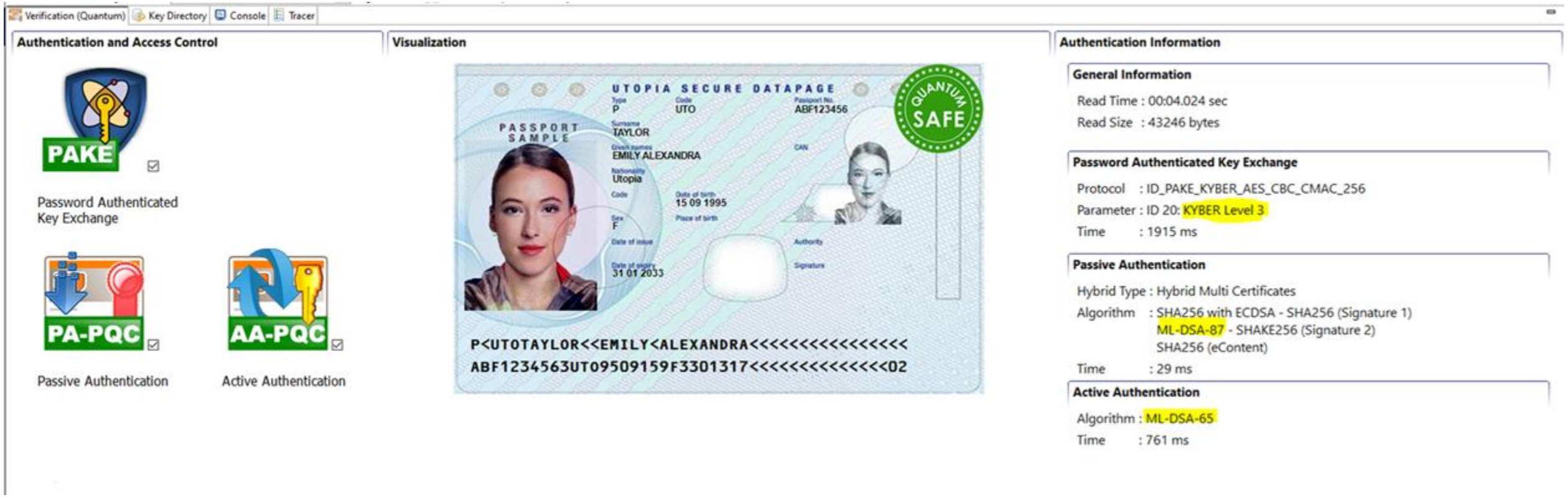
Dans le cadre du CCRA, ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.1.

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Prototype derived from MultiApp 5.2 Premium PQC

PQC4eMRTD - Prototype verification (2/2)



4 seconds to read and verify a full PQC enabled electronic passport

Take Aways & Next Steps

> Time has come to move on.

> Next Steps:

- Demonstrate the security proof of each mechanism and ensure that new solutions preserve key properties from legacy ones
- Propose a hybrid version of each mechanism to ensure continuity during the transition period
- Contribute to the reach of a consensus with key stakeholders (SC17/WG3 & NTWG)

PQC4eMRTD

Post-Quantum Cryptography for electronic Machine-Readable Travel Documents

Contacts:

xavier.banchelin@thalesgroup.com

https://www.pqc4emrtd-project.eu/contact

Thank you

www.thalesgroup.com

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE