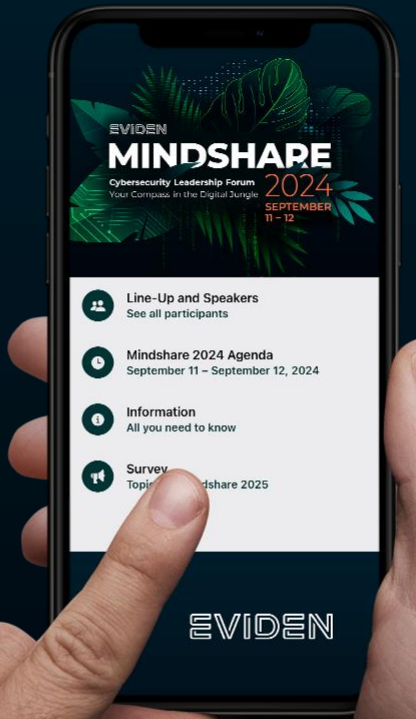
MINDSHARE 2024 AGENDA

SCAN NOW !



EVIDEN

Making Hardware Security Modules Quantum-ready

Antoine Schweitzer-Chaput
Head of Trustway BU
Eviden

EVIDEN
MINDSHARE
2024

About Trustway

What is Trustway ?

More than
20 years
of expertise in Cryptography

The only HSM with **ANSSI reinforced qualification**

First cryptographic provider of the **French government**

100%
Certified European manufactured

A key player in **European sovereignty projects**
SMiEQ, µPQRS projects

A key player **in Post-Quantum Cryptography, homomorphic encryption** and **blockchain cryptography.**

Data protection solutions

Trustway products

Secure data

Safeguard sensitive data and perform cryptographic operations.

Provide a unified encryption solution to secure data at rest and ensure an end-to-end secure infrastructure

- Proteccio HSM range
- DataProtect

Secure transactions

Ensure a secure connection and transaction environment for payment and IoT solutions

- Crypt2pay

Secure communications

Secure network communication across IP networks between devices geographically separated to protect data in transit

- IP protect – IP Sec

What does Trustway do?

Google CSE

Azure DKE

Salesforce KMS

External Key Storage for AWS

As-a-Service

HSM

Trustway Proteccio™
General purpose HSM

Trustway Proteccio™
OEM Appliance

Trustway Crypt2pay

IPSec

Trustway IP Protect

Trustway Chronos

KMS

Trustway DataProtect

On-premise

R&D, studies and customized products

Trustway products – Strong DNA

Manufacturer

Hardware cryptographic products
HSM, IP, token

Full control

Product range : **Defense & Civil**

Defense security requirements **benefiting** Civil products

R&D

Trustway well known crypto player working on cutting edge technologies : **PQC, homomorphic**

Some successes:

90% of payment by card in France are secured by Crypt2pay

Critical infrastructures

Creation of a **National Datacenter** that will host government cloud environment

Military aircraft

Design, development and manufacturing of a secure Gateway Interface Boxes embedded in weapon aircraft

Certified cryptography to meet the highest sovereignty needs

The **only HSM** on the market with **ANSSI reinforced qualification**

ANSSI QR + QS

ANSSI Qualification is the French government's recommendation of proven cybersecurity products or services approved by **French national cybersecurity agency (ANSSI).** There are 3 levels of qualification, the highest being the "reinforced qualification", based on the CC EAL4+ evaluation. As of August 2024, Trustway has the only hardware security module with the **ANSSI "reinforced qualification".**

CC EAL4+

ANSSI qualification

"WHILE THERE ARE MANY AND VARIOUS CYBERSECURITY SOLUTIONS AVAILABLE ON THE MARKET, THEY ARE NOT ALL EQUALLY EFFECTIVE AND ROBUST."

ANSSI qualification process

Qualification is the French state's recommendation of cybersecurity products or services that have been tested and approved by ANSSI.

It demonstrates their compliance with the regulatory, technical and security requirements promoted by ANSSI by providing a guarantee for the **product's robustness** and the service provider's **competency**, as well as the product or service supplier's commitment to comply with **trust** criteria:

1. The evaluation of the product's robustness and a service provider's competency
2. Trust evaluation

3 levels of ANSSI qualification

Basic

the product must be able to prevent basic attacks performed by an attacker with limited ressources.

Standard

the product must be able to prevent advanced attacks performed by an attacker with substantial resources

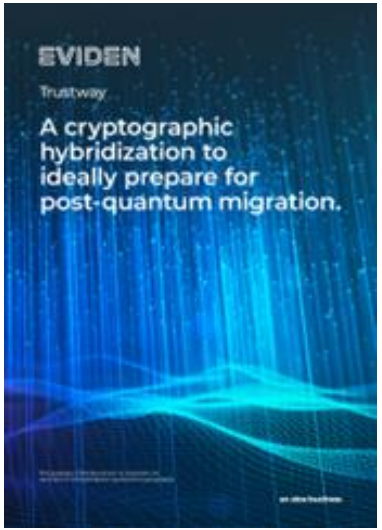
Enhanced

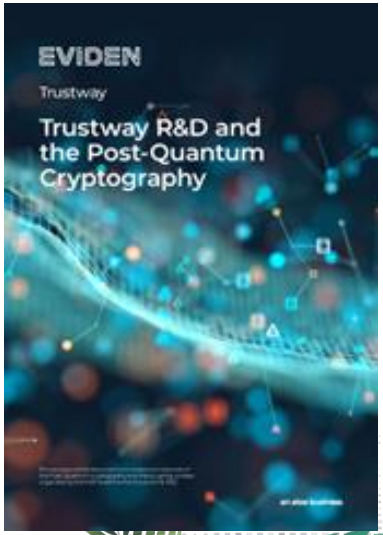
the product must be able to prevent sophisticated attacks performed by an attacker with unlimited resource with etatic or criminal organization support.

Trustway expertise on PQC

Trustway is promoting R&D for future evolutions

- Cutting-edge technology
- 3 PHD in cryptographic domain in R&D
- Future-proof devices, manufactured in France
- Partnership with Cryptonext and commitment for certifying PQC solution
- Ecosystem: end-to-end around quantum





Trustway partnership ecosystem

Research Laboratories

Inria
UGA Université Grenoble Alpes
FONDAZIONE BRUNO KESSLER
FUTURE BUILT ON KNOWLEDGE
CentraleSupélec
université PARIS-SACLAY
if INSTITUT FOURIER
LIRMM
TELECOM Paris
IP PARIS
cea
UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Technology & Commercial partners

STORMSHIELD
THEGREENBOW
MBDA MISSILE SYSTEMS
snowflake
menta
NOKIA Connecting People
seclab -cybersecurity-
DuoKey
salesforce
amazon web services
ORACLE CLOUD
THALES
CRYPTONEXT SECURITY

Trustway PQC developments

Released – April 2024

The Open Quantum Safe (OQS) project is an open-source project that aims to support the transition to quantum-resistant cryptography.
OQS is part of the Linux Foundation's Post-Quantum Cryptography Alliance.

Among organizations, that have supported and continue to support OQS: academic, industry, public sector, and individual contributors who participate in the project.

Release – H2 2024

Trustway Proteccio HSM

CC EAL4+ eIDAS NATO SECRET ANSSI QR SOG-IS EU RESTRICTED

Trustway IP Protect VPN

CRYPTONEXT SECURITY

Solutions in partnership with Cryptonext

PQC primary schemes by H2 2024 (Dilithium / ML-DSA for signature and Kyber / ML-KEM for key exchange)

PQC primary key exchange scheme by H2 2024 (Kyber / ML-KEM)

Overview of performance tests results at similar security level

Dilithium / ML-DSA (signature) facing pre-quantum algorithms

	Key pairs generation	Signature	Verification
ML-DSA Vs RSA	+ + +	+ +	+
ML-DSA Vs ECC	-	- -	+ +

Various encouraging results despite a few remaining concerns

\+ Worldwide optimisation efforts

KEYFACTOR	CLOUDFLARE	NXP	Qualcomm
Tests on **IT PKI using HSM**	Large scale tests on **WebPKI**	Tests on chips for **secure boot** and **secure updates** use cases	Tests on **Mobile ecosystem**
\+ Low impact on signing/verification (without optimization)	\+ Very promising results for TLS, no performance impact	\+ Reduced memory usage for signature verification	\+ Praised the strategy to offload PQC operations from the main CPU to a "crypto-agile PQC co-processor" until main CPUs are PQC optimized and crypto-agile
\- Database size increases 4x (but optimization possible)	\- More complexity (multiple algorithms, extra round-trips) for signatures, DNSSEC and ZKP	\- Verification speed halved as trade-off	

Eviden's full range of post-quantum ready cybersecurity products

CC EAL4 · ANSSI QS · ANSSI DR

Trustway Proteccio HSM

Trustway IP Protect VPN

CC EAL4+ · eIDAS · NATO SECRET

ANSSI QR · SOG-IS · EU RESTRICTED

IDnomic PKI

Cybersecurity Consulting Services

- PQC Maturity Assessment
- Cryptographic Inventory
- Quantum Risk Assessment
- PQC Migration Roadmapping

Cryptovision GreenShield mail & file

Cryptovision & CardOS eID, cards & tokens

EAL4+ · SOG-IS · eIDAS

Evidian IAM suite

Innovative & dynamic partners

short security shelf life

Questions?

Antoine Schweitzer-Chaput, Trustway, Eviden

TAKE A MINUTE AND GIVE US FEEDBACK …

RATE NOW!