TRIDENT HSM is the first in the world to offer multi-party cryptography

Verified by the globally recognized Common Criteria EAL 4+ certification

eIDAS Certified Qualified Signature and Seal Creation Device
Post-Quantum crypto support (Sphincs+)

TRIDENT HSM

- WHAT IS AN HSM?
- CONFIGURATIONS
- SPECIAL FEATURES
- RELATED PRODUCTS

HSM

HSM (hardware security module) is:

- a **physical computing device**
- used for safeguarding and managing **cryptographic keys**
- that can be used for cryptographic operations
- **key material never leaves** the protected boundary
- should be **certified** (**CC EAL4+**, FIPS 140)

Compliance requirements

Magyar Elektronikus Aláírás Napja

MPC a HSM-ben (20 percben)

ABOUT TRIDENT

SOLUTION

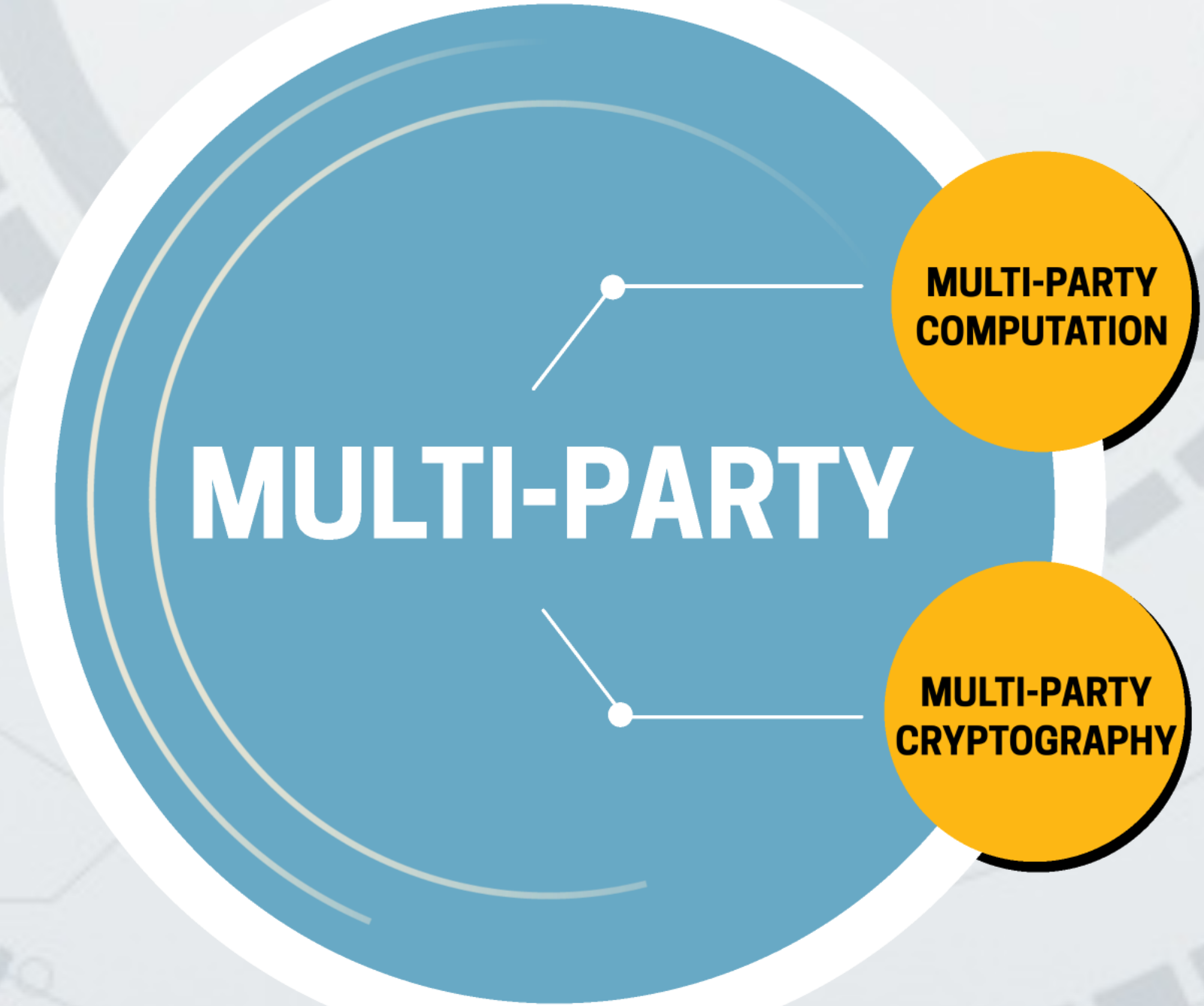
MULTI-PARTY

USECASES

GIST

RÓZSAHEGYI ZSOLT
zsolt.rozsahegyi@i4p.com

I4P
INNOVATING FOR PROTECTION


MULTI-PARTY
MULTI-PARTY COMPUTATION
MULTI-PARTY CRYPTOGRAPHY

SECURE
MULTI-PARTY COMPUTATION

- methods for parties to jointly compute a function over their inputs while keeping those inputs private
- formally introduced in 1982 for the so-called Millionaires' Problem

Yao's Millionaires' Problem

Multi-party computation on shared secret

https://en.wikipedia.org/wiki/Secure_multi-party_computation

Millionaires' Problem

Andrew Yao

The problem discusses two millionaires, Alice and Bob, who are interested in knowing which of them is richer without revealing their actual wealth.

https://en.wikipedia.org/wiki/Yao%27s_Millionaires%27_Problem

Shared secrets

Additive sharing:
Each party has its own part of the secret and the sum of these parts is the global secret that is not known by any of the parties.
E.g. global secret is 18, can be shared as -5, 30, -7 (and in unlimited other ways)

Other ways of sharing: binary sharing, Shamir's polynomial sharing etc.

Add constant to a shared secret

Multiply a shared secret by constant

Add 2 shared secrets

Threshold

MULTI-PARTY CRYPTOGRAPHY

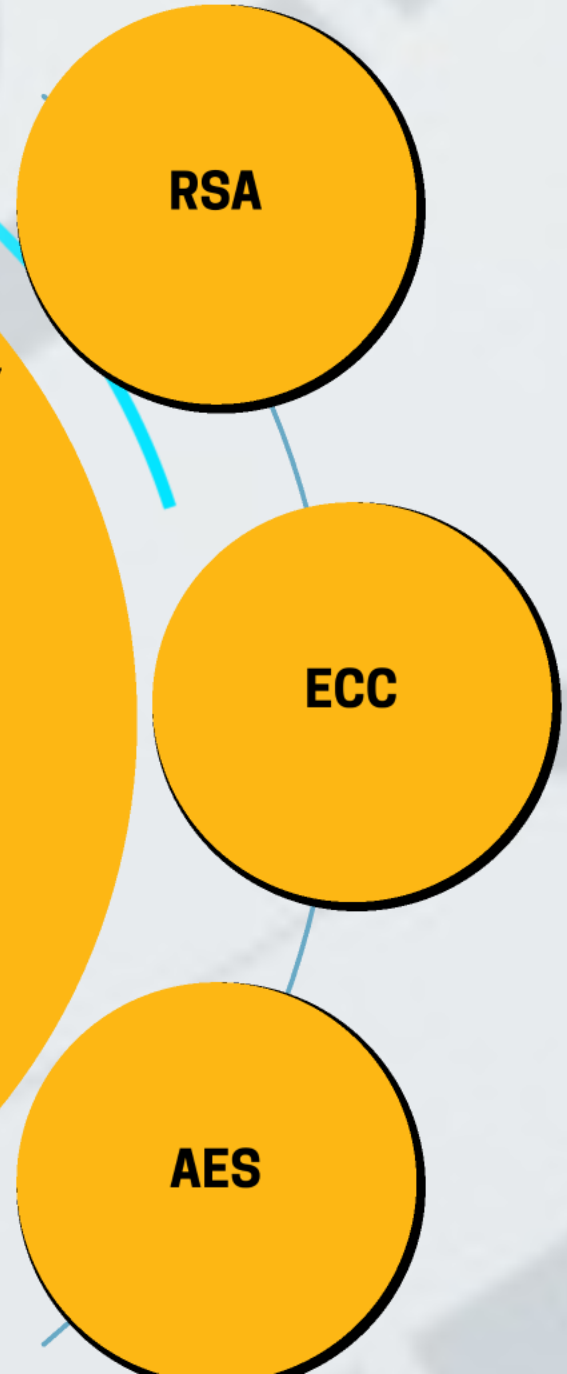
Goals:

key generation:

- whole key is never in one place

key usage:

- secret-key parts never assembled, only used to separately creating one cryptographic function



RSA

Key generation:

Distributed Miller–Rabin primality test

Each of the parties have primes and so the private key (d) as shared secret

Key usage

ECC

Key generation:

No need for complex multi-party key generation methods. Random number generation by each parties

Key usage:
SMPC operations with the shared secrets and domain parameters

AES

Key generation:
Random number generation by each parties

Key usage:
SMPC operations with the exciting problem of using lookup tables with an index that is to remain a shared secret*

*patent pending by i4p

Magyar Elektronikus Aláírás Napja

MPC a HSM-ben (20 percben)

ABOUT TRIDENT

SOLUTION

MULTI-PARTY

USECASES

GIST

RÓZSAHEGYI ZSOLT
zsolt.rozsahegyi@i4p.com

I4P
INNOVATING FOR PROTECTION

MULTI-PARTY
USE CASES

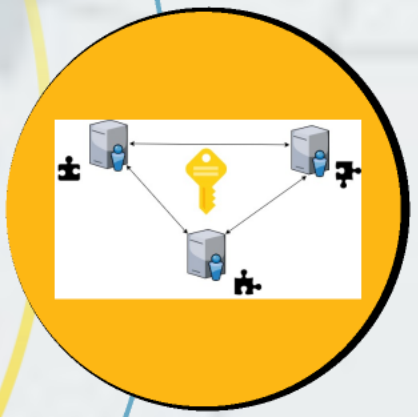
ELASTIC HSM

- Enhanced protection
- Cloud configuration
- Possession factor

Enhanced protection of your crypto keys

Instead of storing your keys in one single place, you can store it in a distributed cluster

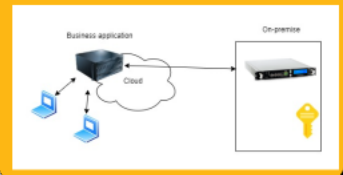
MOST VALUABLE KEYS



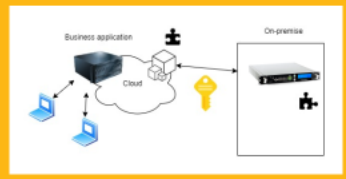
GO TO THE CLOUD

Without entrusting and revealing your keys to cloud providers.

Regular way

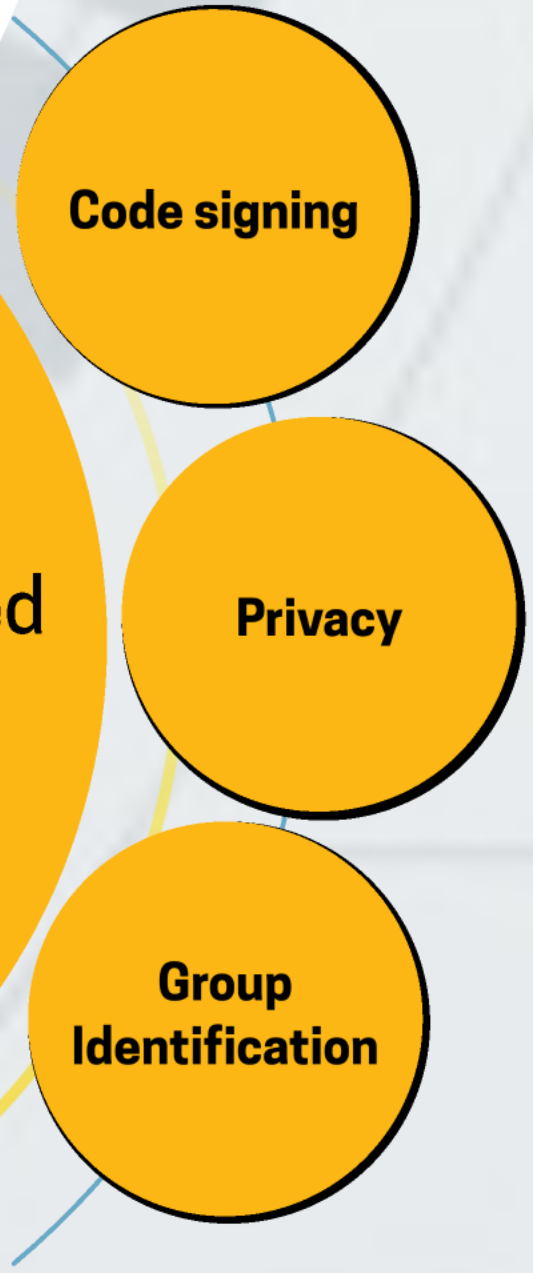


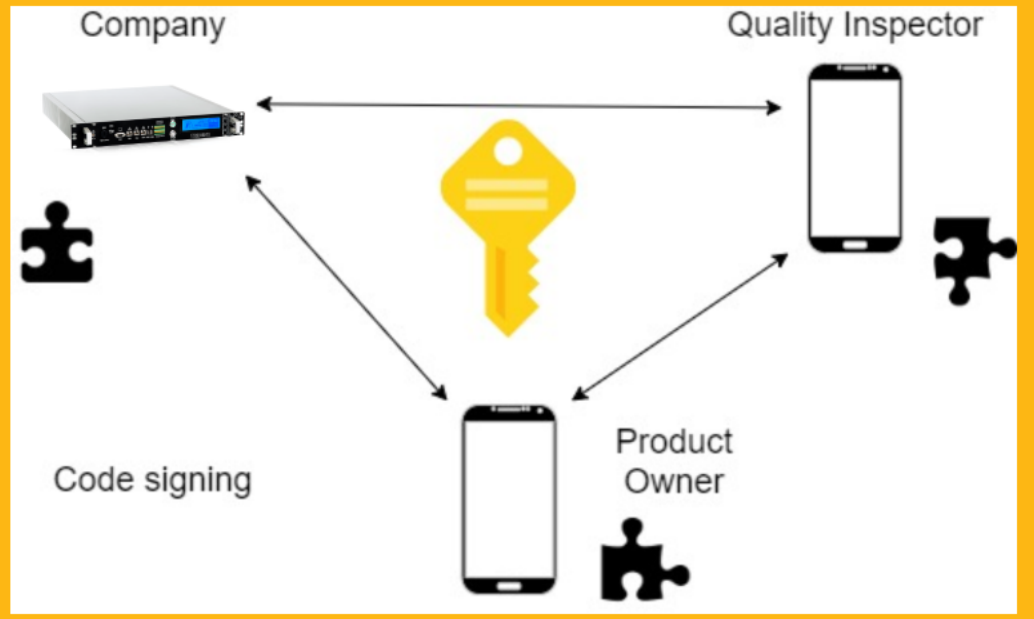
Elastic HSM

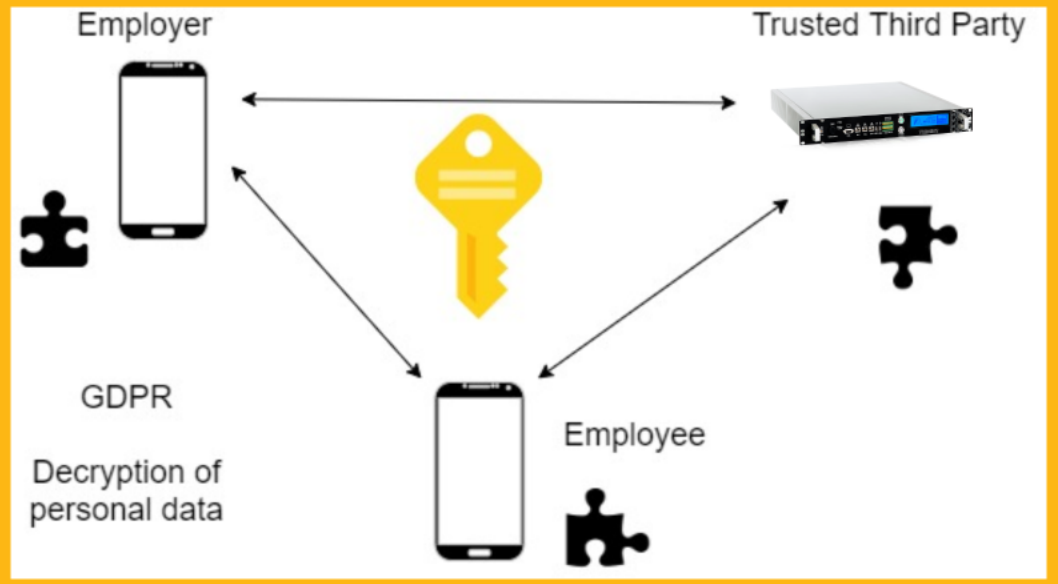


Possessing a key part

parties maybe in an untrusted environment and (even) with conflicting interests to perform a single crypto operation




Company
Quality Inspector
Code signing
Product
Owner


Employer
Trusted Third Party
GDPR
Decryption of personal data
Employee

Magyar Elektronikus Aláírás Napja

MPC a HSM-ben (20 percben)

ABOUT TRIDENT

SOLUTION

MULTI-PARTY

USECASES

GIST

RÓZSAHEGYI ZSOLT
zsolt.rozsahegyi@i4p.com

I4P
INNOVATING FOR PROTECTION

JUST THE GIST

Secure multi-party computation helps you to protect your secret in a way that is never seen before

Possessing at least one part of your secret can provide you possessing the whole secret

Physical protection of that secret is essential