THALES

Magyar Elektronikus Aláírás Napja

Piaci trendek a gyártó szemüvegén keresztül

Hirsch Gábor és Paksi Attila

30th of June, 2022

Agenda

- HSM trends
- eIDAS2
- Autentikáció
- Post-Quantum

THALES

THALES
Building a future we can all trust

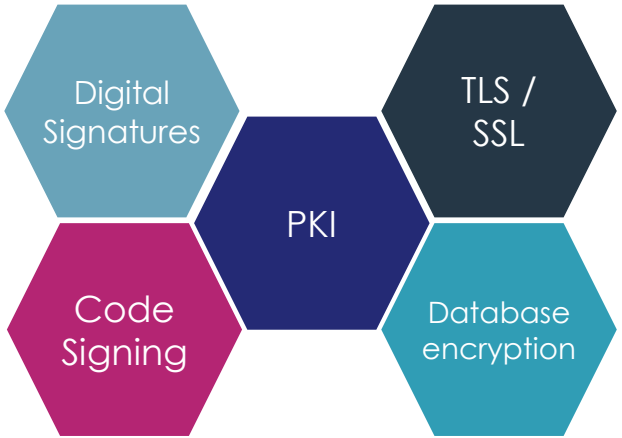
HSM trends

HSMs are the foundation of trust

For over 30 years Enterprise and government have used Luna HSMs to protect critical data and digital identities

The need for HSMs hasn't changed…

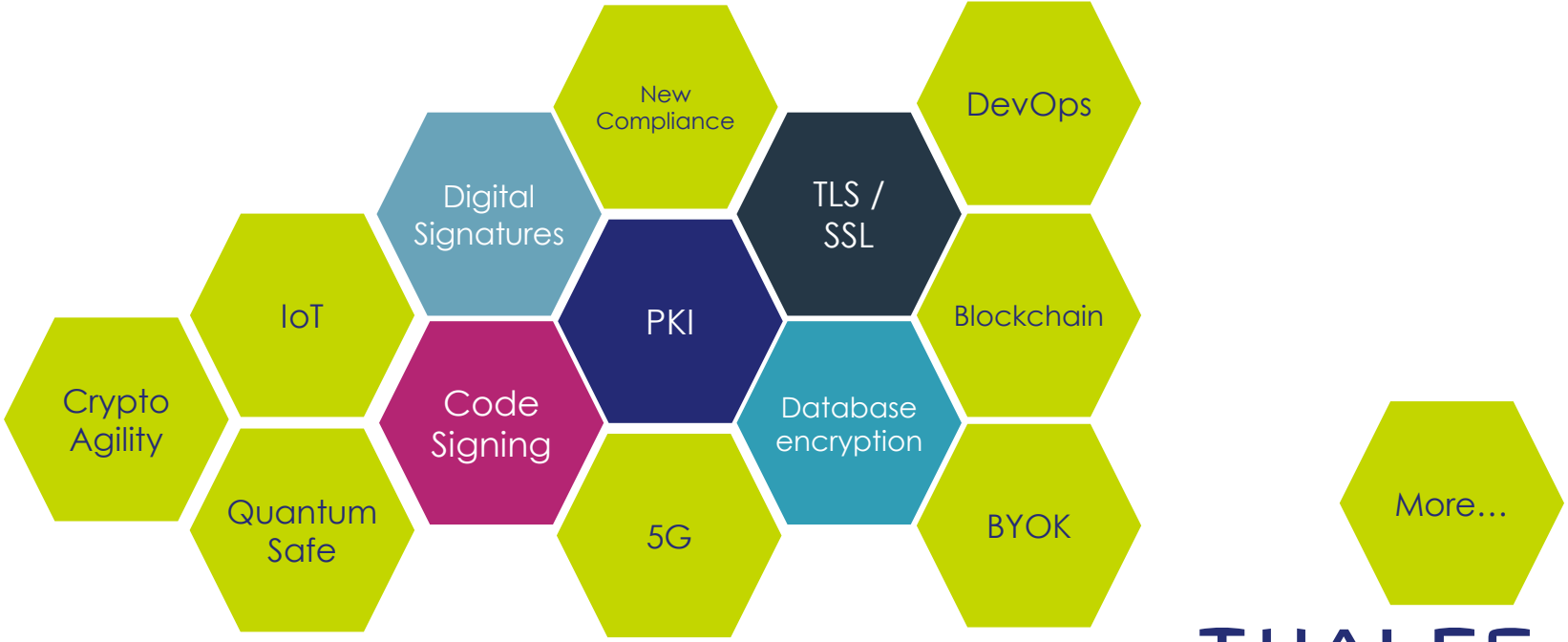
- still required to meet security, compliance and audit needs



THALES

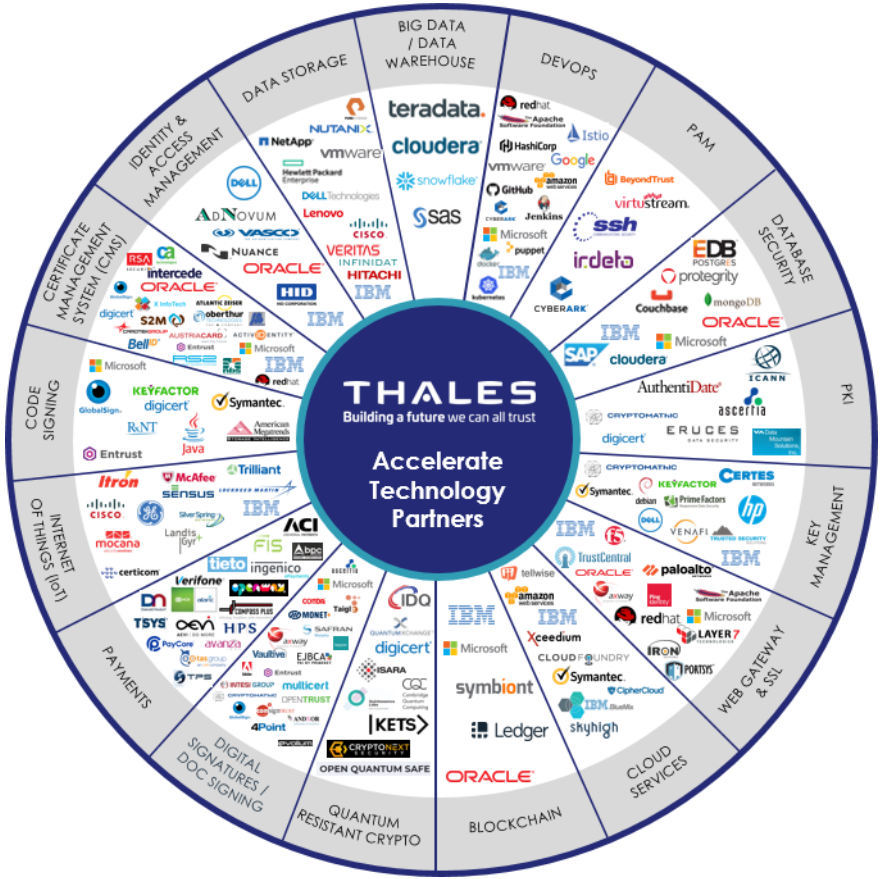
Building on our successes

Luna HSMs are also evolving to meet modern emerging technology needs



THALES

HSM Integrations – Thales Accelerate Partner Network



Industry-leading ecosystem of over **400** Tech Partners and **500+** Integrations

THALES

THALES
Building a future we can all trust

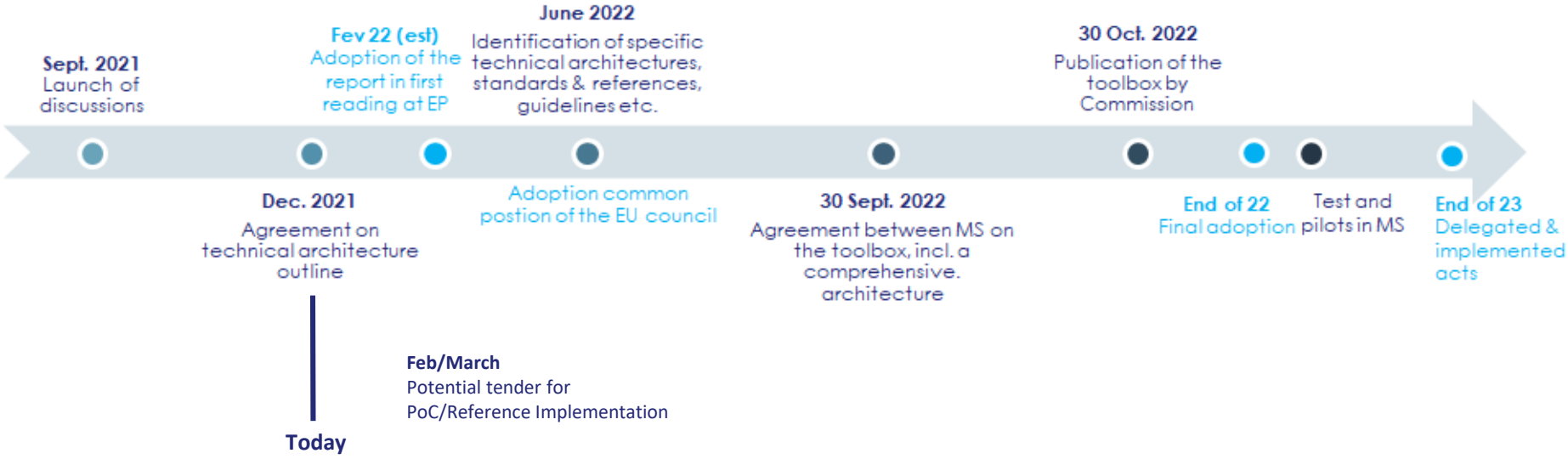
eIDAS 2

eIDAS2 timeline

PREVIEW

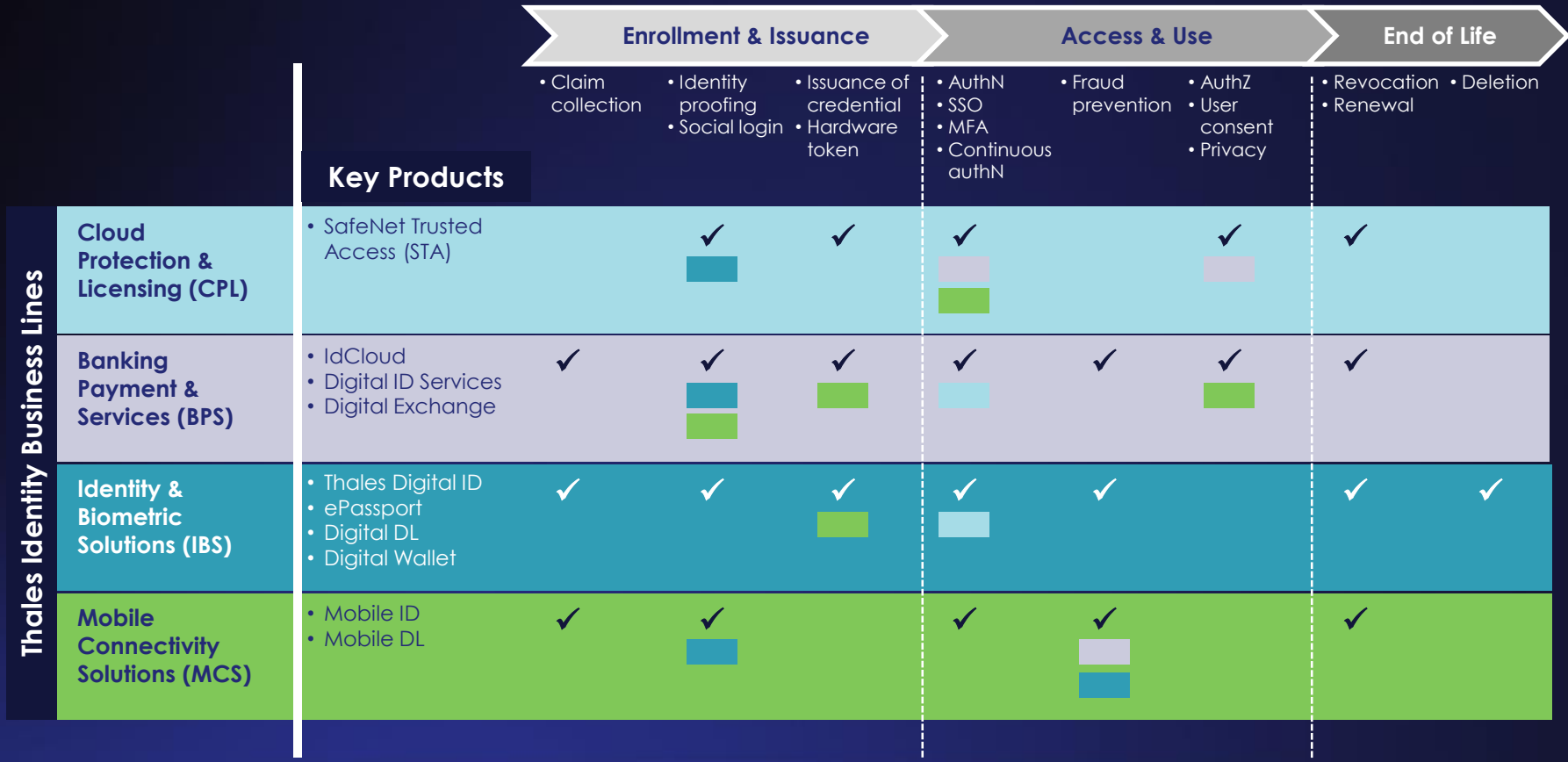
Defined till end of 2022

Implemented by end of 2023 by each Member State



THALES

Strong Thales DIS Assets



EU Digital Identity Wallet – EDIW

PREVIEW

Main change of eIDAS2

Can be used for accessing Remote Services

- Login to Utility providers and GovServices
- Easier user registration to Digital Services (since it contains valid credentials)

- ❑ Secure wallet app
- ❑ Personal identification data (~eID)
- ❑ Online authentication credential

- ❑ Mobile Driver License ~mDL
- ❑ Health card ~mHC
- ❑ Electronic diploma

- ❑ Electronic signature certificate
- ❑ Sole control of remote signature

- ❑ Proof of address
- ❑ Certified IBAN
- ❑ etc.

THALES

Autentikáció

Gartner Identity & Access Management Summit

11 May 2022/London, U.K., Europe

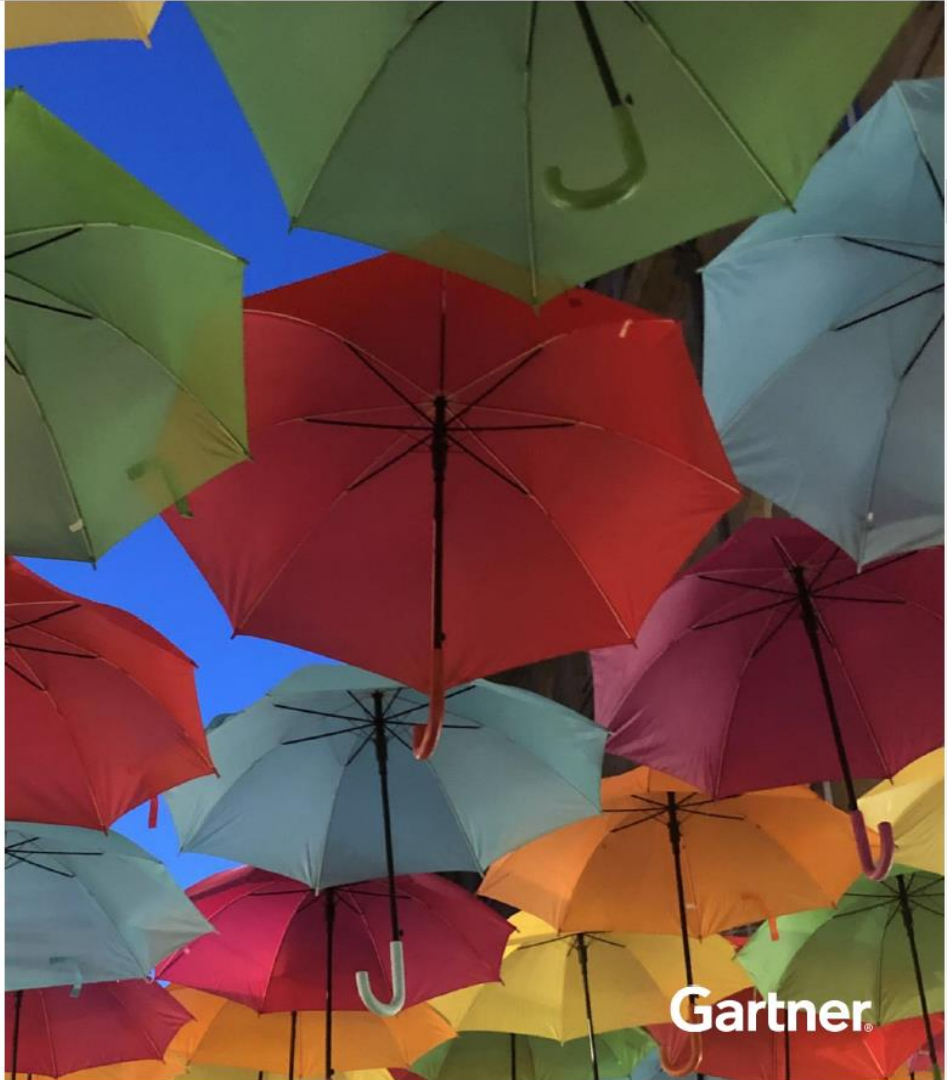
Gartner Opening Keynote: How to Digitally Accelerate When You're So Freaking Tired

Mary Mesaglio

Gartner®

Multifactor Authentication Is Not Optional

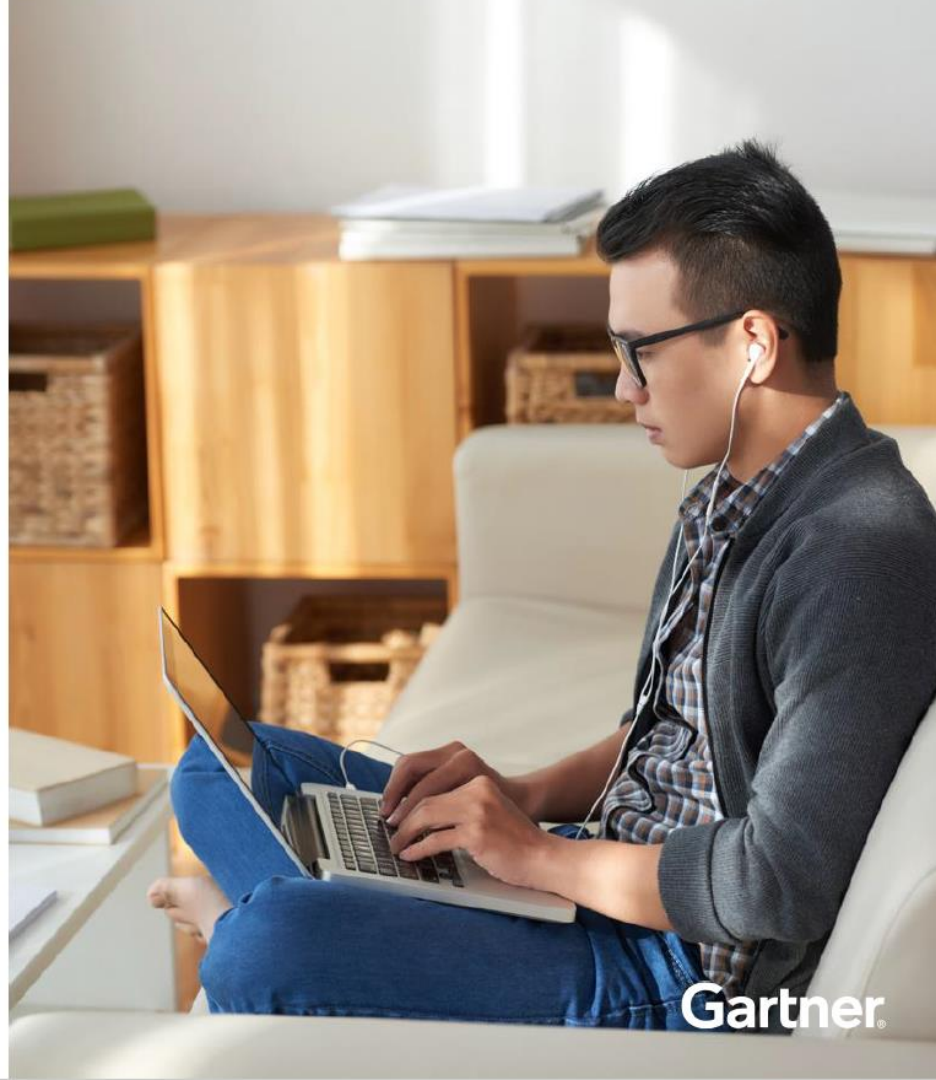
- Passwords are completely insufficient
- Remote access **must** be protected with MFA
- Privileged access **must** be protected with MFA
- Cybersecurity insurance increasingly requires MFA



Source: Gartner

User Experience Matters

- Adding MFA can add friction (but it doesn't have to)
- Employee and customer experience is more important than ever
- Offering multiple options for diverse users is necessary
- Password less MFA is one possible answer



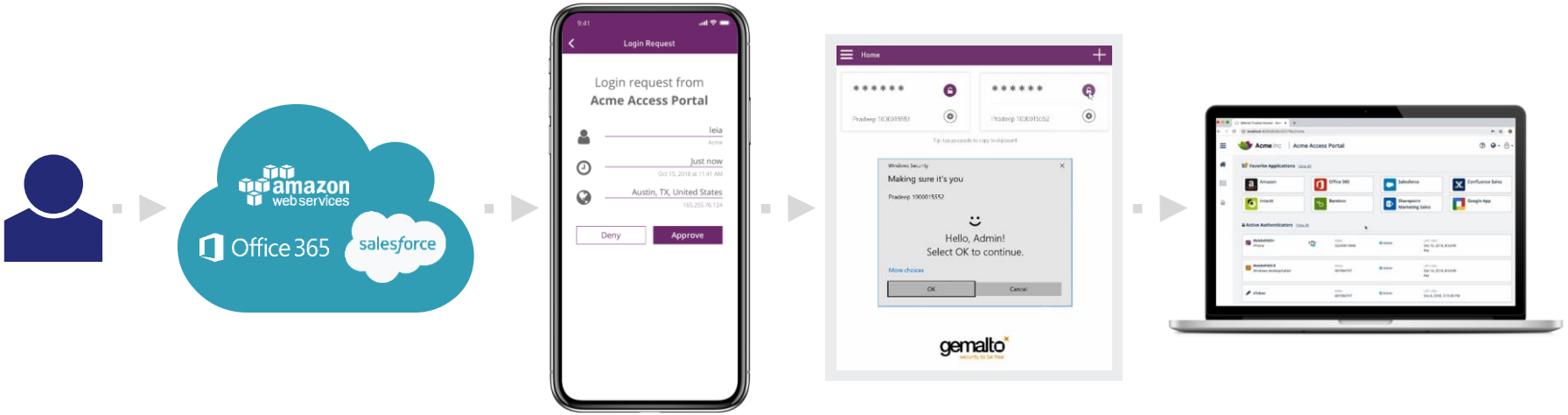
Source: Gartner

Zero-Trust és modern hozzáférés-kezelés

THALES

Passwordless Authentication

Push OTP és PIN kombinációja (Windows Hello / Biometria)



THALES

Mire figyeljünk technológia szempontból?

- Csak a **VPN-hez** kell, vagy van más **use case-ünk is?**
- Segítenék az **automatizációk** az adminisztrációt?
- Mennyire **biztonságos** a tokenek kiadása?
- Függhetek-e **csak egy (felhő) szolgáltatótól**??
- ...

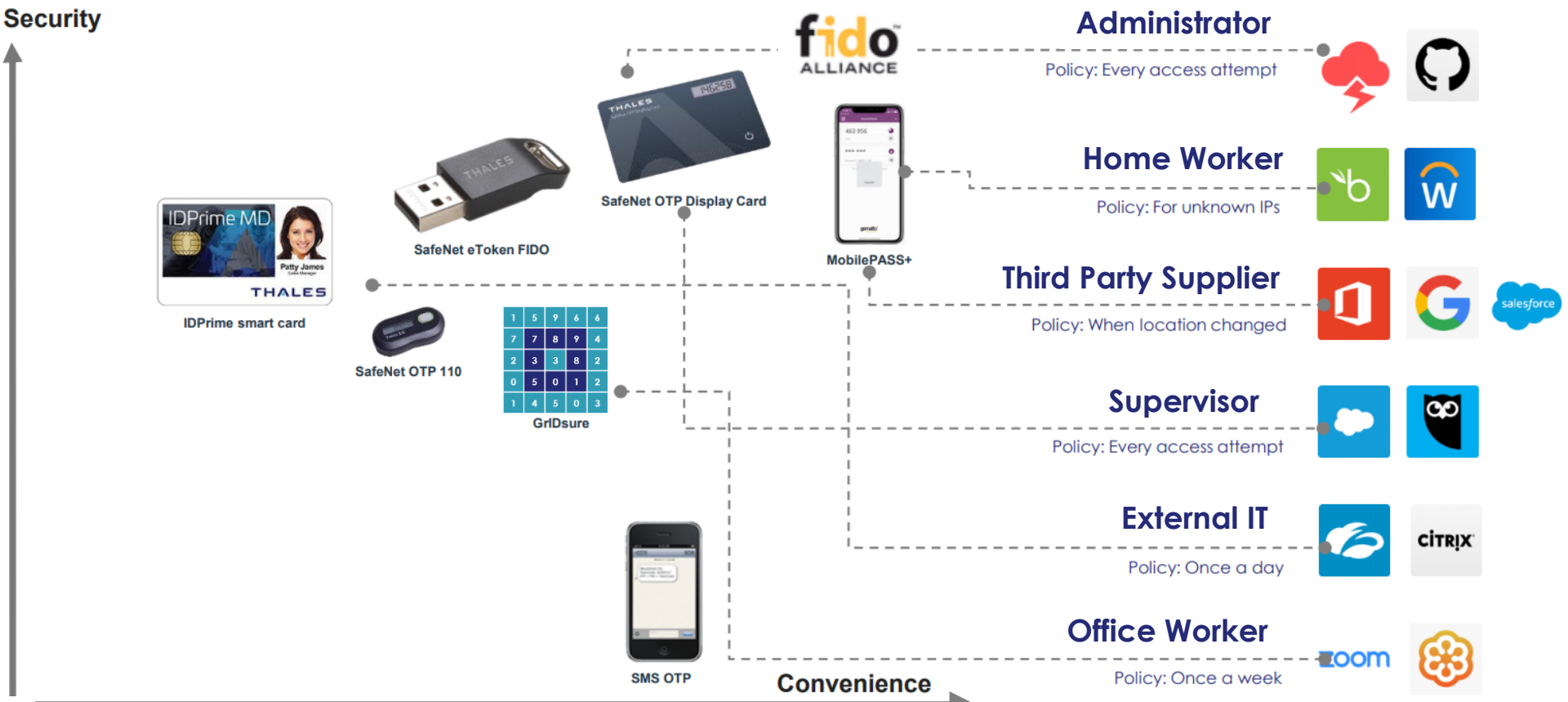
THALES

Mire figyeljünk üzleti szempontból?

- Mit kell **TCO**-mba beleszámítanom? Transzparensek a költségeim?
- Van **elég** (kipihent!) **kolléga** egy IAM-megoldás bevezetéséhez és üzemeltetéséhez?
- Külön **szabályokra** van szükségem bizonyos alkalmazásokhoz és felhasználókhoz?
- Elegendő **csak egy mobil tokent** az összes felhasználómnak?
- ...

THALES

Eltérő autentikációs utak



THALES

Univerzális autentikációs lehetőségek

A meglévő MFA telepítések újrafelhasználása

A PKI autentikáció kiterjesztése a felhőre

Az adott kockázatnak megfelelő biztonsági szint garantálása

THALES

Vezető szereplő a PKI alapú hitelesítés területén

Fejlődés

Új felhasználási esetek témogatása

IDPrime Virtual

FIDO hardver autentikátorok

Karbantartás

A legerősebb MFA portfólió

Smartkártyák
Middleware

Tokenek

THALES

SafeNet IDPrime Virtual

- A fizikai smartkártya szoftver alapú, biztonságos változata
- Csökkenti a fizikai eszközök operatív kihívásait
- Kiterjeszti a tanusítvány alapú autentikációt és tranzakciókat új felhasználási esetekre:
  - VDI
  - BYOD és mobil eszközök
  - Ideiglenes smartkártyák
  - Könnyű smartkártya pótlás

FIDO2 megoldások a Thales-től

- PKI és FIDO2 támogatás egy eszközben
- Meglévő PKI befektetések felhasználása
- Gyors üzembe helyezés a Thales Middleware és a meglévő PKI infrastruktúra alapján

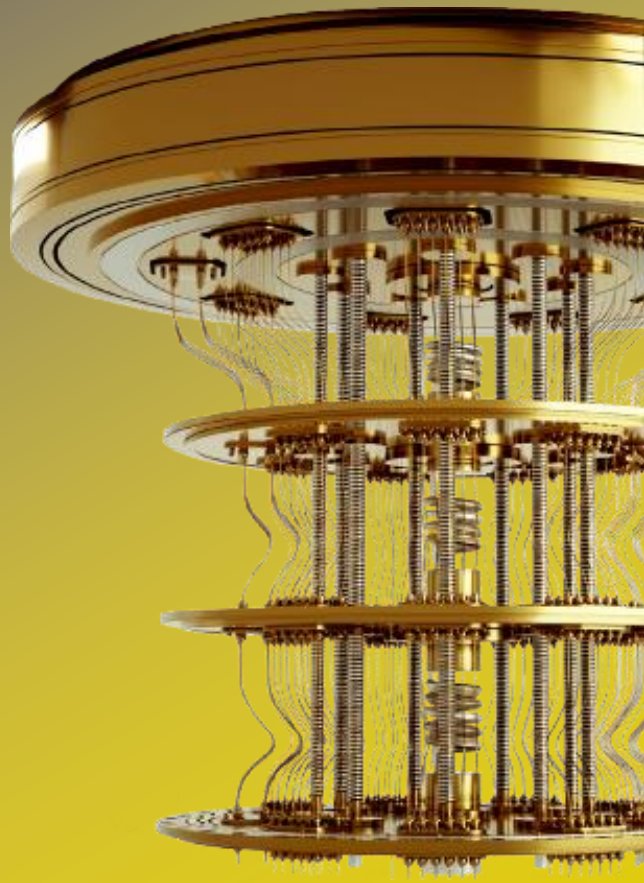
PKI + FIDO2 eszközök

- Kombinált FIDO – PKI Smartkártya
- FIDO USB token

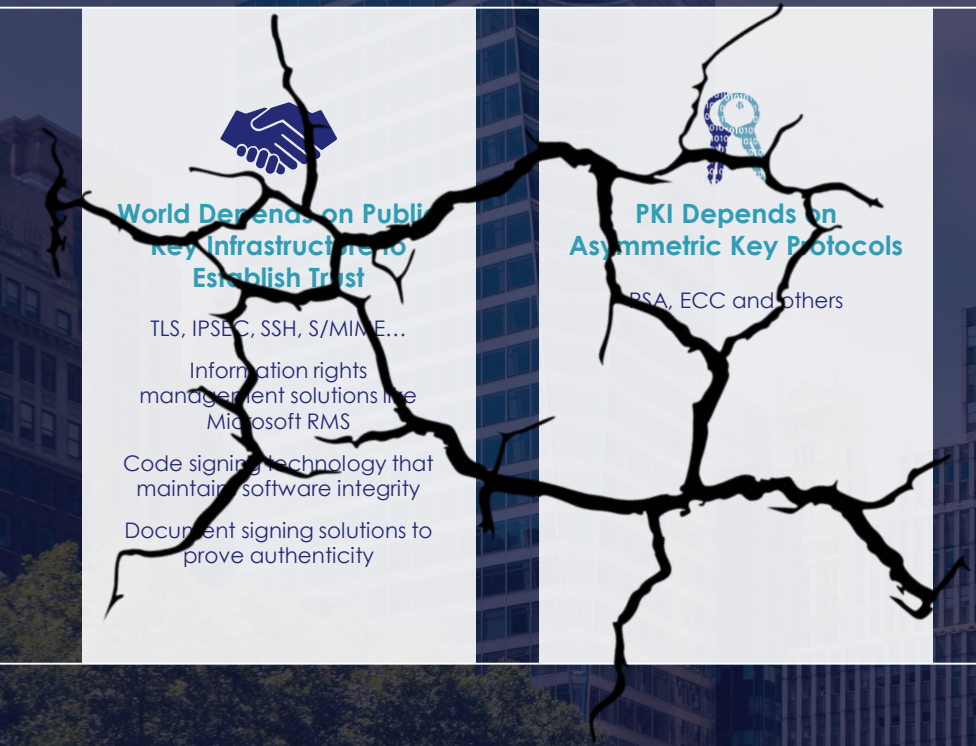
„Quantum.
Quantum Everywhere.”

Emerging threats: quantum computing

Of respondents said they were concerned with ‘tomorrow’s decryption of today’s data’ when asked to identify security threats from quantum computing.
Only **2%** said they were not presently concerned.



Why are we talking about this topic?



World Depends on Public Key Infrastructure to Establish Trust

TLS, IPSEC, SSH, S/MIME…

Information rights management solutions like Microsoft RMS

Code signing technology that maintains software integrity

Document signing solutions to prove authenticity

PKI Depends on Asymmetric Key Protocols

RSA, ECC and others

Quantum computers and research will efficiently crack PKI and weaken encryption

We don't know exactly when

Quantum Safe Crypto (QSC) will maintain our "way of life"

QSC is also called Post-Quantum, Quantum-Proof or Quantum Resistant Cryptography Crypto agile products allow us to use QSC algorithms and keys today

THALES

Long lifetime data confidentiality requirements

THALES

Quantum defenses

#1 Quantum safe cryptography

- Quantum Signature schemes
  - Dilithium, Falcon, Rainbow
- Key Encapsulation Mechanisms
  - SABRE, NTRU, Kyber, McEliece


NIST

Search NIST

Menu

NEWS

NIST's Post-Quantum Cryptography Program Enters 'Selection Round'

Chosen algorithms will become part of first standard devised to counter quantum decryption threat.

July 22, 2020

Performance in real-world protocols varies

- Key sizes, padding schemes, latency

First NIST draft QRA standards expected in 2022

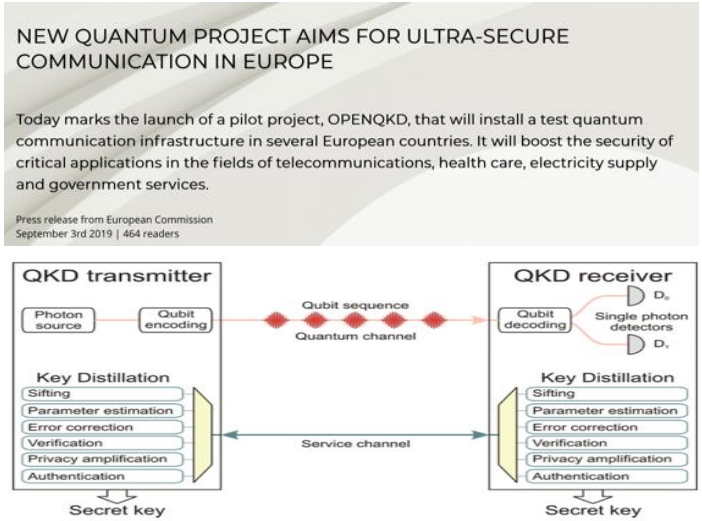
- Digital signatures, Public key encryption, Key encapsulation mechanisms
- Best used in hybrid modes initially

THALES

Quantum defenses

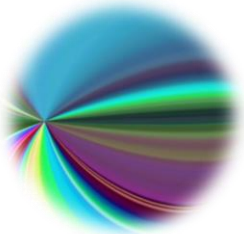
#2 Quantum key distribution

- Harnesses properties of quantum mechanics
- Fundamentally different approach to key sharing
- Distributes keys based on principles of physics not mathematics



#3 Quantum RNG

- True and unpredictable randomness at high entropy rates up (10+ Mbps)



THALES

Luna HSM Approach to Quantum

Work with our Accelerate Technology Partners

Current Luna 7 HSMs

- External QRNG
  - Ability to seed internal DRBG
- Add Quantum-Safe Algorithms using FMs
  - Available now from Thales & Partners
- Once standardized, add algorithms into FW
  - FIPS certification

THALES

Commercially Available Quantum-Safe Luna HSM

ISARA Quantum Resistant Algorithms and Luna's PQC FM

- Secure storage of quantum-resistant keys within the secure, tamper-resistant HSM
- Perform digital signatures with a hardware root of trust
- ISARA's Quantum-Safe digital signature technology is implemented as a secure software update to Luna HSMs

ISARA

Thales Luna HSM Customer Quantum Implementation

- Implement your own Post Quantum Crypto mechanism using Luna's Functionality Module (FM)

THALES

IDQ Quantum Random Number Generation with Luna HSMs

- Generate unique and truly random, high entropy numbers with ID Quantique's QRNG and Luna HSM's secure key storage
- Address critical applications where high quality random numbers are absolutely vital
- Use case examples: cloud; cryptographic services; compliance; gaming; IoT-scale device authentication and managed end-to-end encryption

IDQ
FROM VISION TO TECHNOLOGY

THALES

THALES

“Hope is not a strategy”

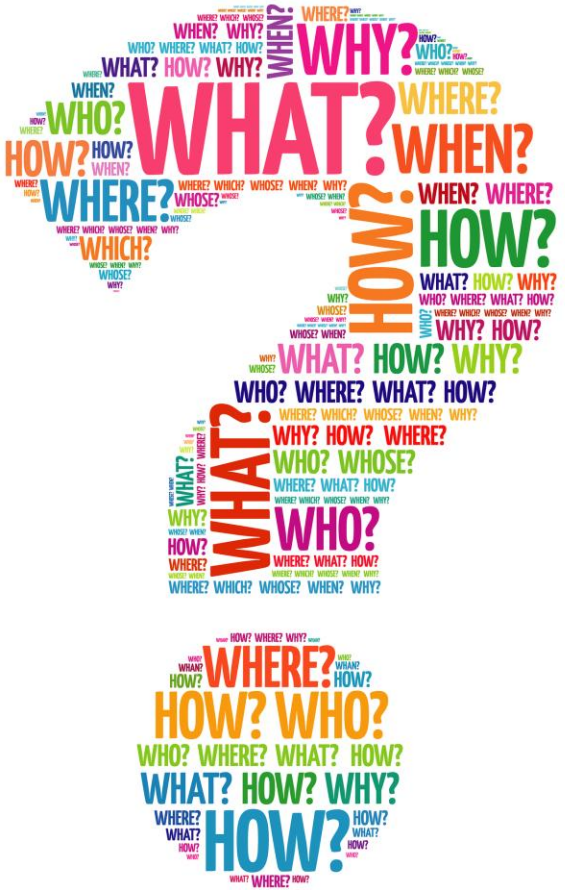
Keressen bennünket, hogy segíthessünk

Access Management

Paksi Attila
+36 30 202 6000
attila.paksi@thalesgroup.com

Data protection

Hirsch Gábor
+36 30 526 3024
gabor.hirsch@thalesgroup.com



THALES

Köszönjük a figyelmet!