



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



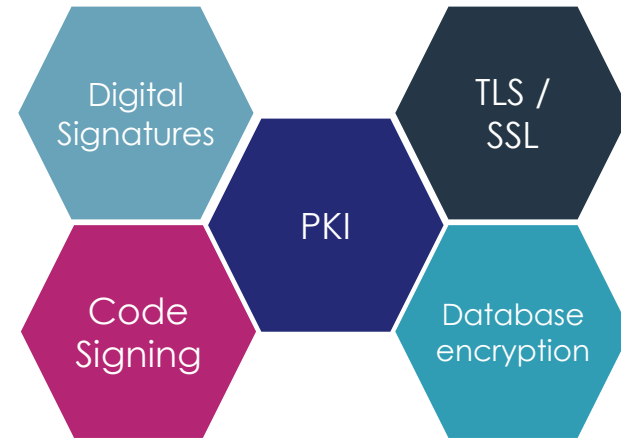
## HSM trends



# HSMs are the foundation of trust

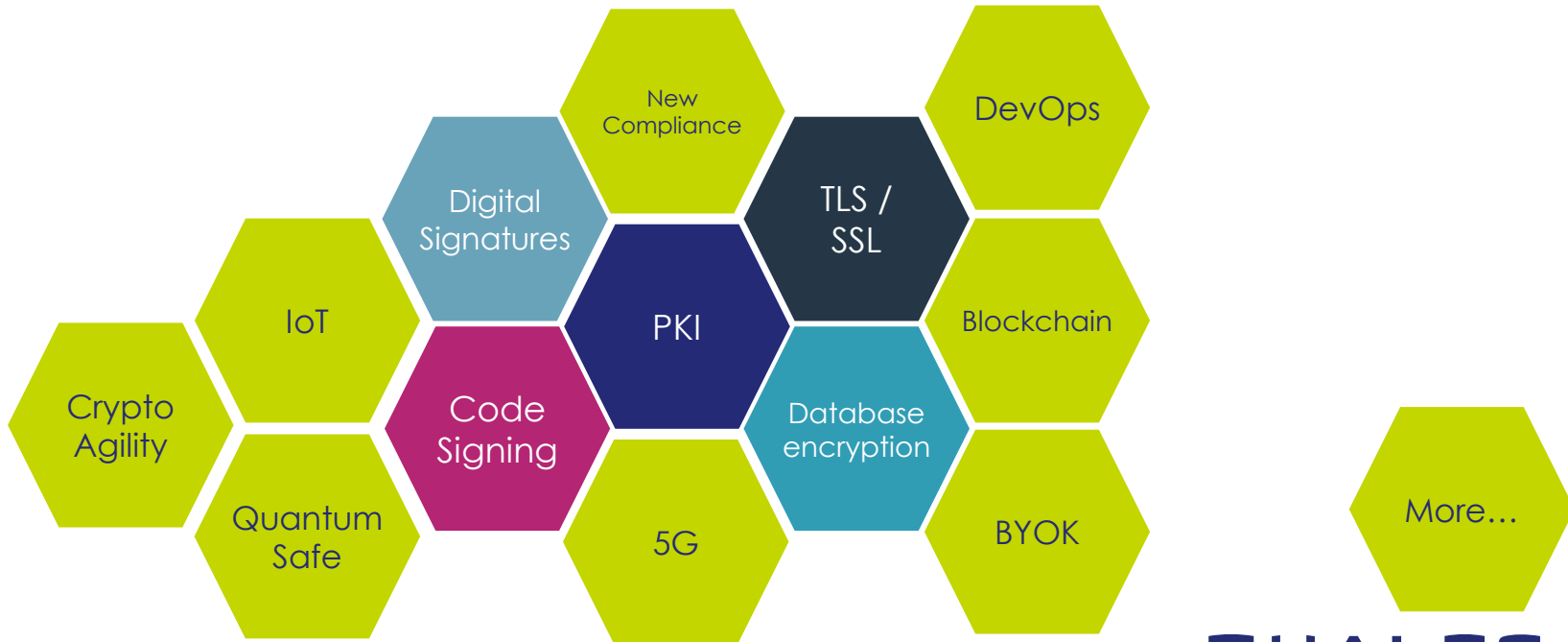
For over 30 years Enterprise and government have used Luna HSMs to protect critical data and digital identities

The need for HSMs hasn't changed...  
still required to meet security, compliance and audit needs

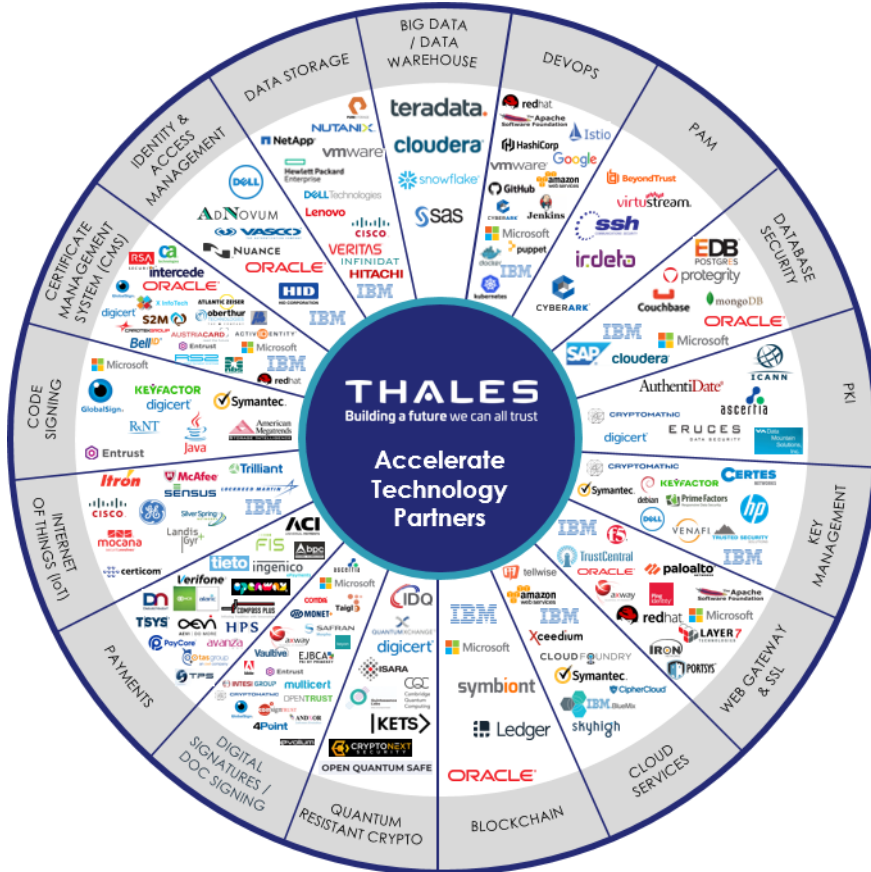


# Building on our successes

Luna HSMs are also evolving to meet modern emerging technology needs



# HSM Integrations – Thales Accelerate Partner Network



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

# THALES

Building a future we can all trust

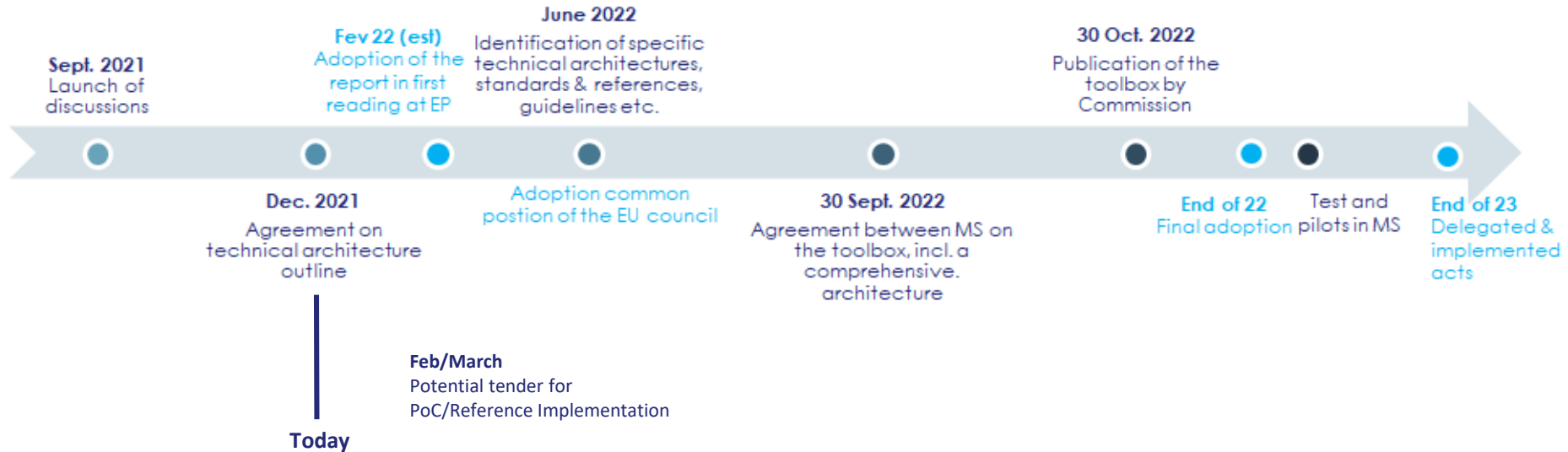


## eIDAS 2



Defined till end of 2022

Implemented by end of 2023 by each Member State





# Strong Thales DIS Assets



- Enrollment & Issuance**
  - Claim collection
  - Identity proofing
  - Social login
  - Issuance of credential
  - Hardware token
- Access & Use**
  - AuthN
  - SSO
  - MFA
  - Continuous authN
  - Fraud prevention
  - AuthZ
  - User consent
  - Privacy
- End of Life**
  - Revocation
  - Deletion
  - Renewal

## Key Products

Thales Identity Business Lines	Enrollment & Issuance			Access & Use			End of Life	
	Claim collection	Identity proofing Social login	Issuance of credential Hardware token	AuthN SSO MFA Continuous authN	Fraud prevention	AuthZ User consent Privacy	Revocation	Deletion Renewal
<b>Cloud Protection &amp; Licensing (CPL)</b>		✓	✓	✓		✓	✓	
<b>Banking Payment &amp; Services (BPS)</b>	✓	✓	✓	✓	✓	✓	✓	
<b>Identity &amp; Biometric Solutions (IBS)</b>	✓	✓	✓	✓	✓		✓	✓
<b>Mobile Connectivity Solutions (MCS)</b>	✓	✓		✓	✓		✓	

## ■ 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.

## 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

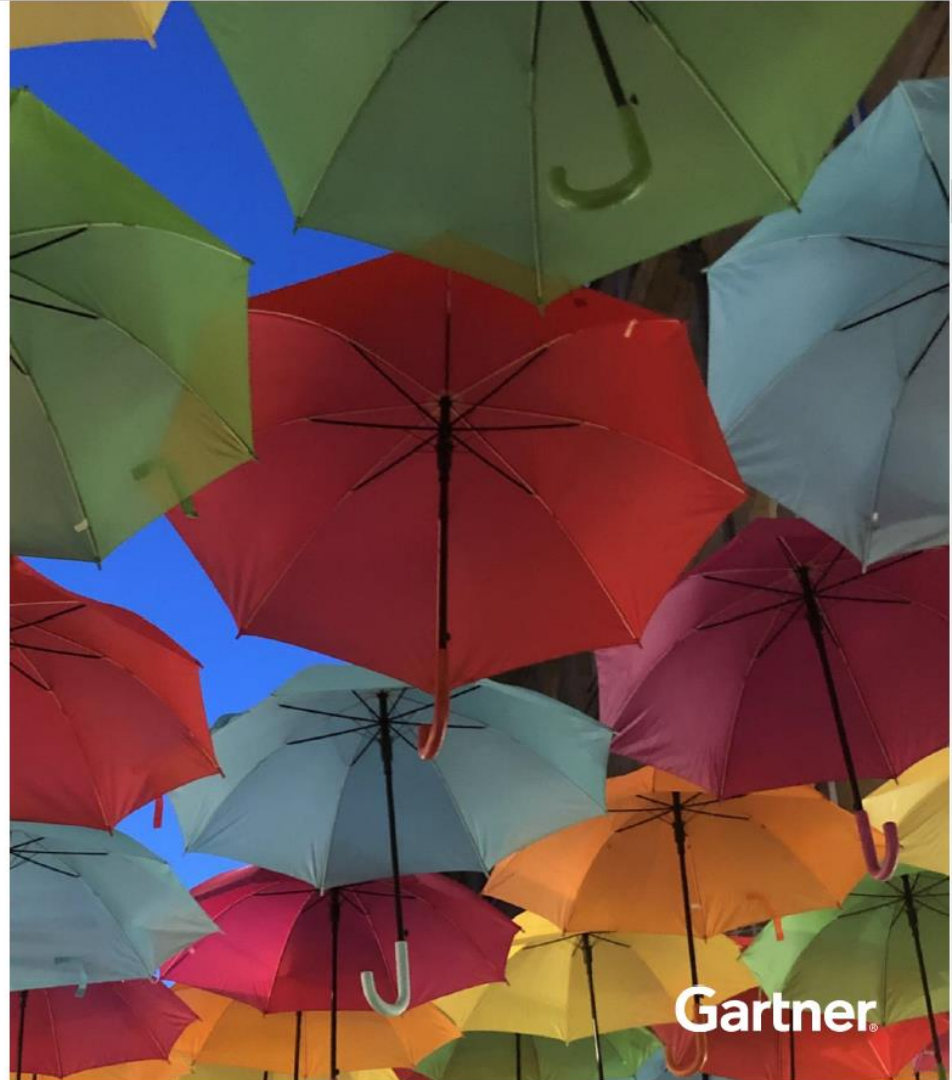
© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see ["Guiding Principles on Independence and Objectivity."](#)

**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

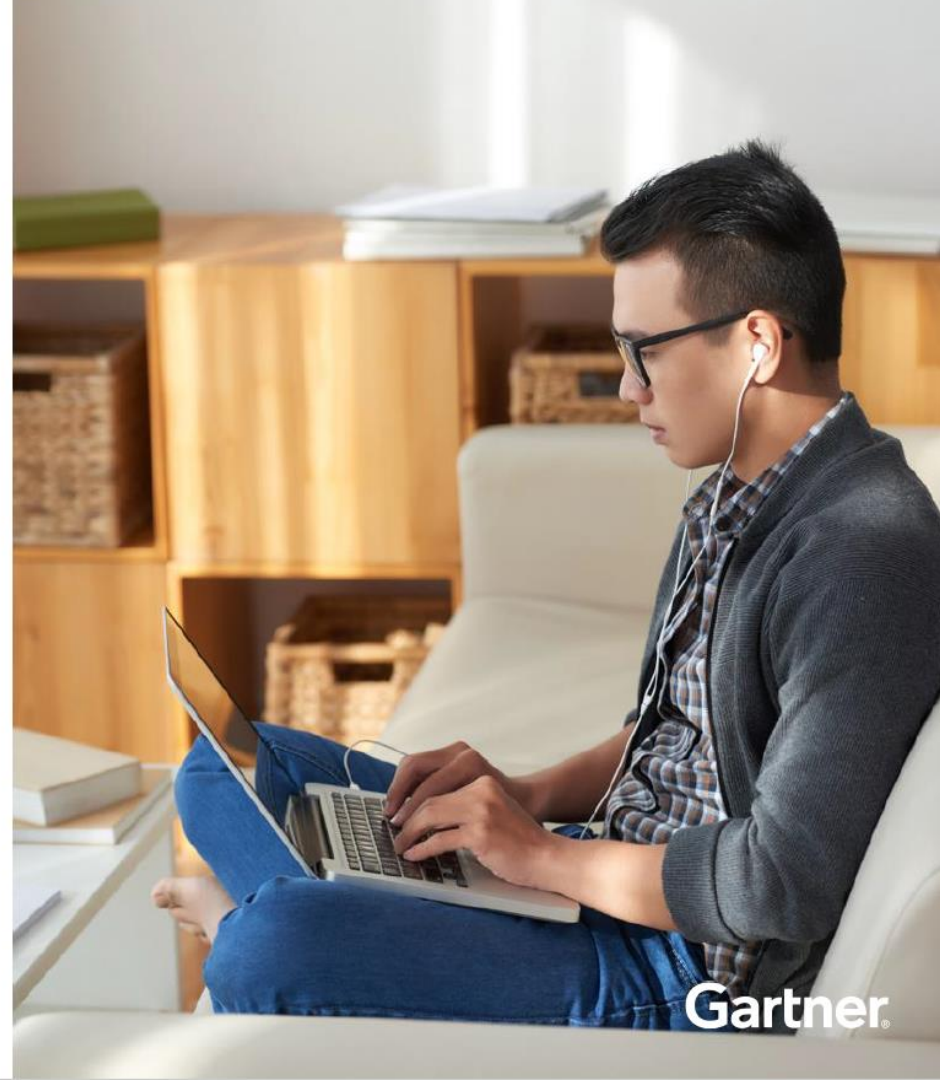
Source: Gartner



# 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



Cloud



BYOD



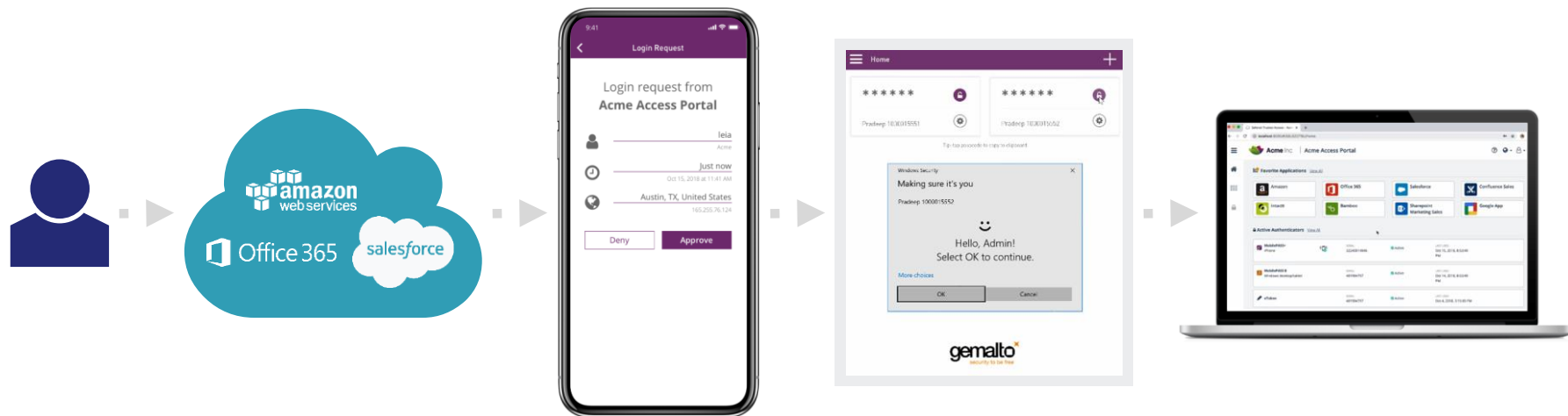
Work From  
Home



Regulations/  
Compliance

# Passwordless Authentication

## Push OTP és PIN kombinációja (Windows Hello / Biometria)





# Mire figyeljünk technológia szempontból?

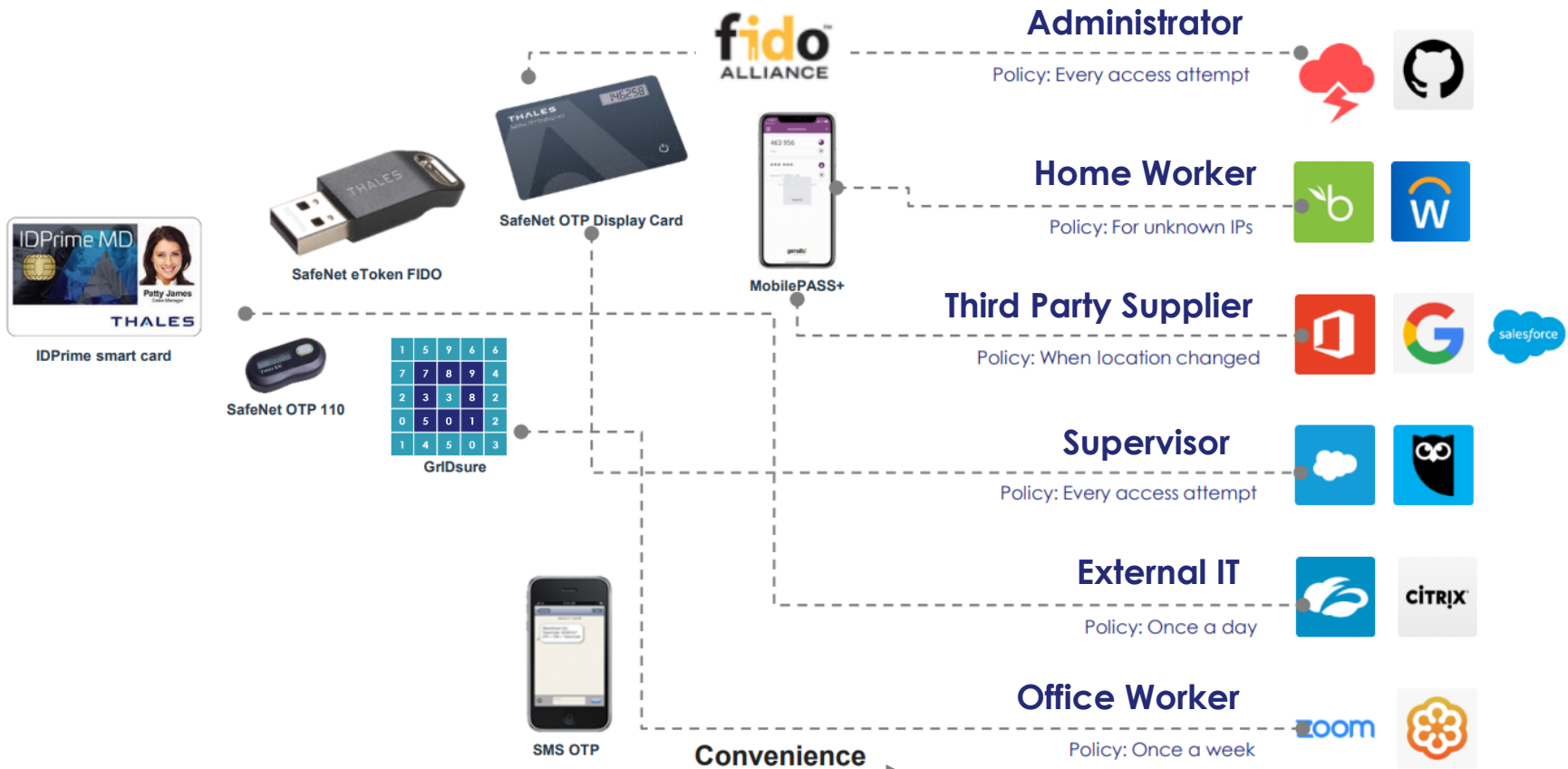
- Csak a **VPN-hez** kell, vagy van más **use case-ünk is?**
- Segítenék az **automatizációk** az adminisztrációt?
- Mennyire **biztonságos** a tokenek kiadása?
- Függhetnek-e **csak egy (felhő) szolgáltatótól??**
- ...

# Mire figyeljünk üzleti szempontból?

- Mit kell **TCO**-mba beleszámítanom? Transzparenssek 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?
- ...

# Eltérő autentikációs utak

Security



Convenience

# Univerzális autentikációs lehetőségek



A meglévő MFA telepítések újrafelhasználása

A PKI autentikáció kiterjesztése a felhőre

Az adott kockázatnak megfelelő biztonsági szint garantálása

# Vezető szereplő a PKI alapú hitelesítés területén

## Fejlődés

### Új felhasználási esetek támogatása



IDPrime Virtual



FIDO hardver  
autentikátorok

## Karbantartás

### A legerősebb MFA portfólió



Smartkártyák  
Middleware



Tokenek



# SafeNet IDPrime Virtual

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



- 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



# THALES

Building a future we can all trust



„Quantum.  
Quantum Everywhere.”

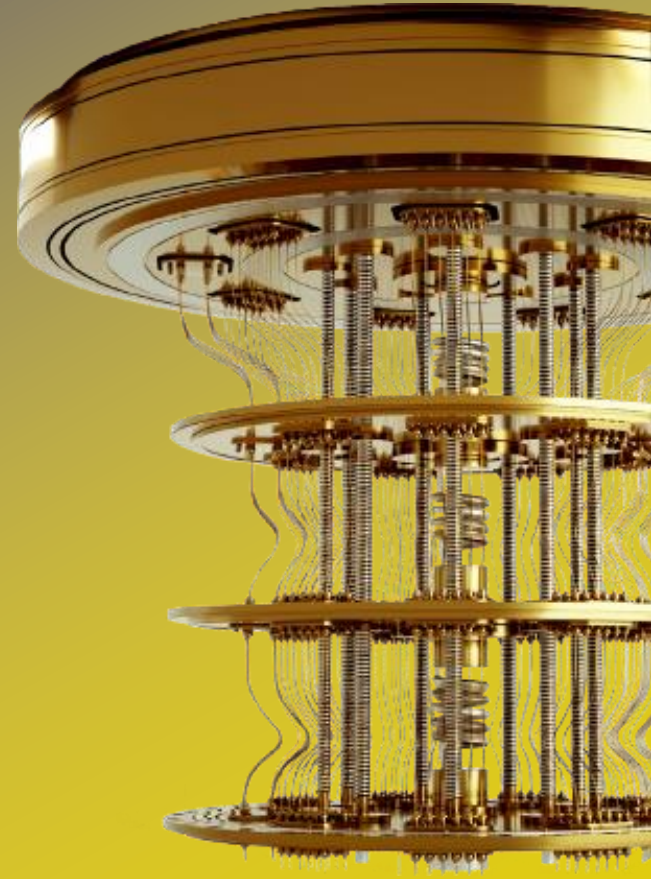




# Emerging threats: quantum computing



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.

# Long lifetime data confidentiality requirements

## Expiration date

Hours – temporary credentials

---

Months – corporate earnings

---

Years – banking information, credit cards, contracts

---

Decades – trade secrets, classified information

---

Lifetime – DNA data, personal information

## #1 Quantum safe cryptography

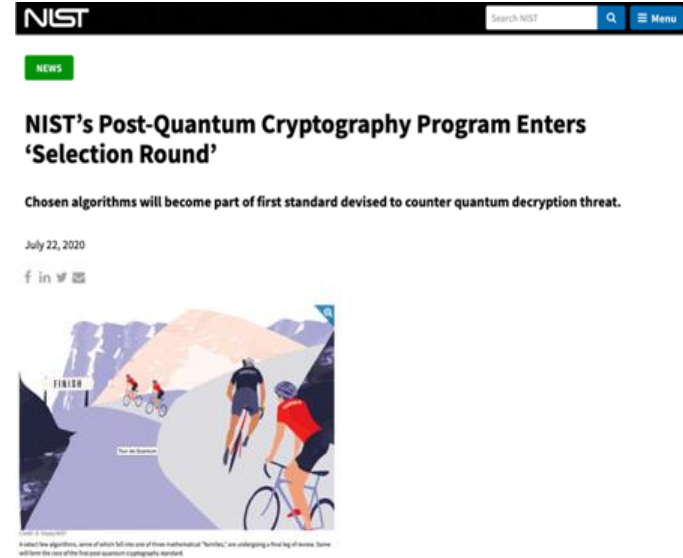
- Quantum Signature schemes
  - Dilithium, Falcon, Rainbow
- Key Encapsulation Mechanisms
  - SABRE, NTRU, Kyber, McEliece

## 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



# 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

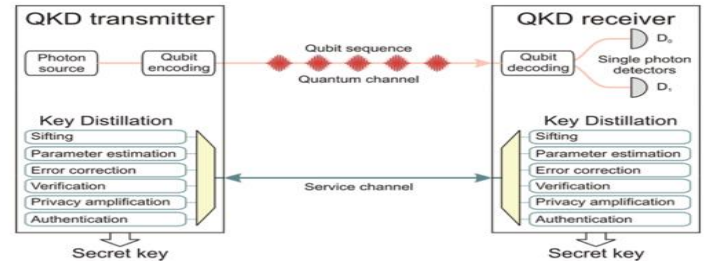
## #3 Quantum RNG

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

### NEW QUANTUM PROJECT AIMS FOR ULTRA-SECURE COMMUNICATION IN EUROPE

Today marks the launch of a pilot project, OPENQKD, that will install a test quantum communication infrastructure in several European countries. It will boost the security of critical applications in the fields of telecommunications, health care, electricity supply and government services.

Press release from European Commission  
September 3rd 2019 | 464 readers



# 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



# 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



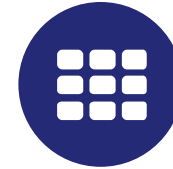
## Thales Luna HSM Customer Quantum Implementation



- 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



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!

Thank you

Gracias مكل اركش

धन्यवाद Merci

Danke 謝謝

ありがとうございました