

Identity and Payment in the Post-Quantum Era



Teresa Wu
IDEMIA



Mark Stafford
Infineon



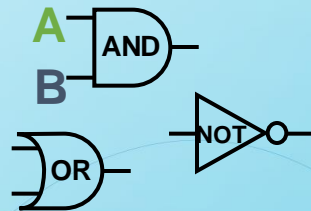
Classical vs. Quantum Computing

Classical Computing

Classical bit has
1 out of 2 possible states:
(using voltage in wire)



Logic gates perform
1 operation on n bits at a time

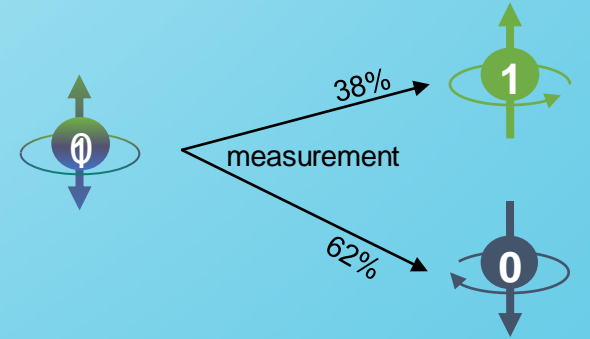


Good for:

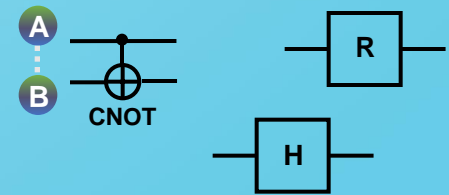
- › efficient and fast calculation of sequential tasks

Quantum Computing

Qubit can have a
superposition of both states
(if not observed)
(e.g. using
electron spin, photo polarization, etc...)



Quantum gates perform
**2ⁿ operations on n (entangled)
qubits at a time**



Good for:

- › speeding up certain mathematical problems, where multiple possible values have to be calculated in parallel (e.g. breaking asymmetric crypto ☹)

Quantum computing at a glance



Underlying principles

- Superposition
- Entanglement
- > Operating 1 qubit will affect multiple qubits and data



Good at

- Much faster problem solving such as
 - Finding an element in a large set
 - Finding an optimal solution

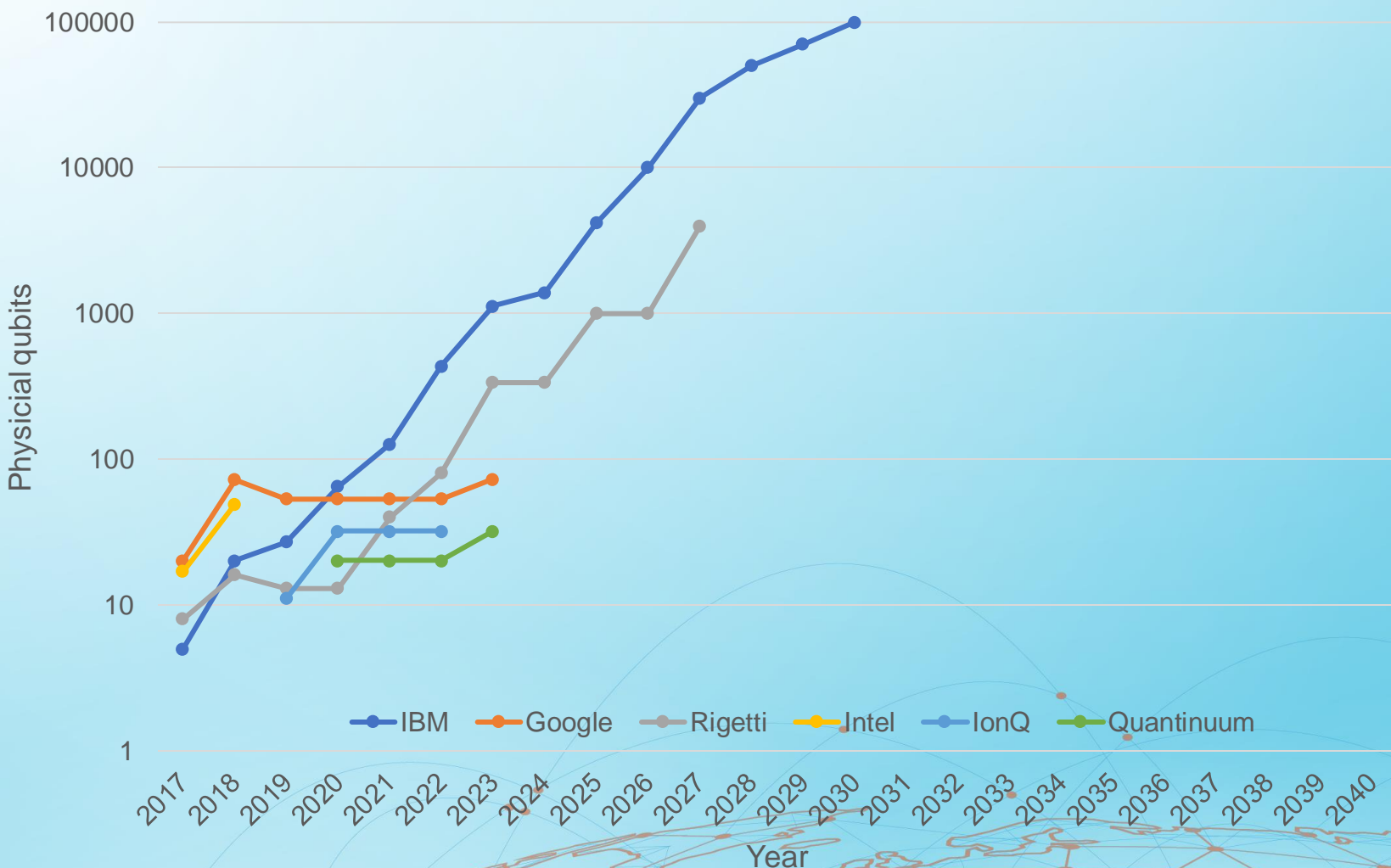


Particularly good at

- Prime factorization

$$851 = 23 \times 37$$

Quantum Computer Development



Funding and commercial landscape

- > EU: € 1 billion "Quantum Flagship" research initiative
- > Germany: € 3 billion action plan by federal ministry of education and reserach
- > Overall global quantum technology market will reach \$53.2 billion by 2028 (*)

(*) According to ResearchAndMarkets.com

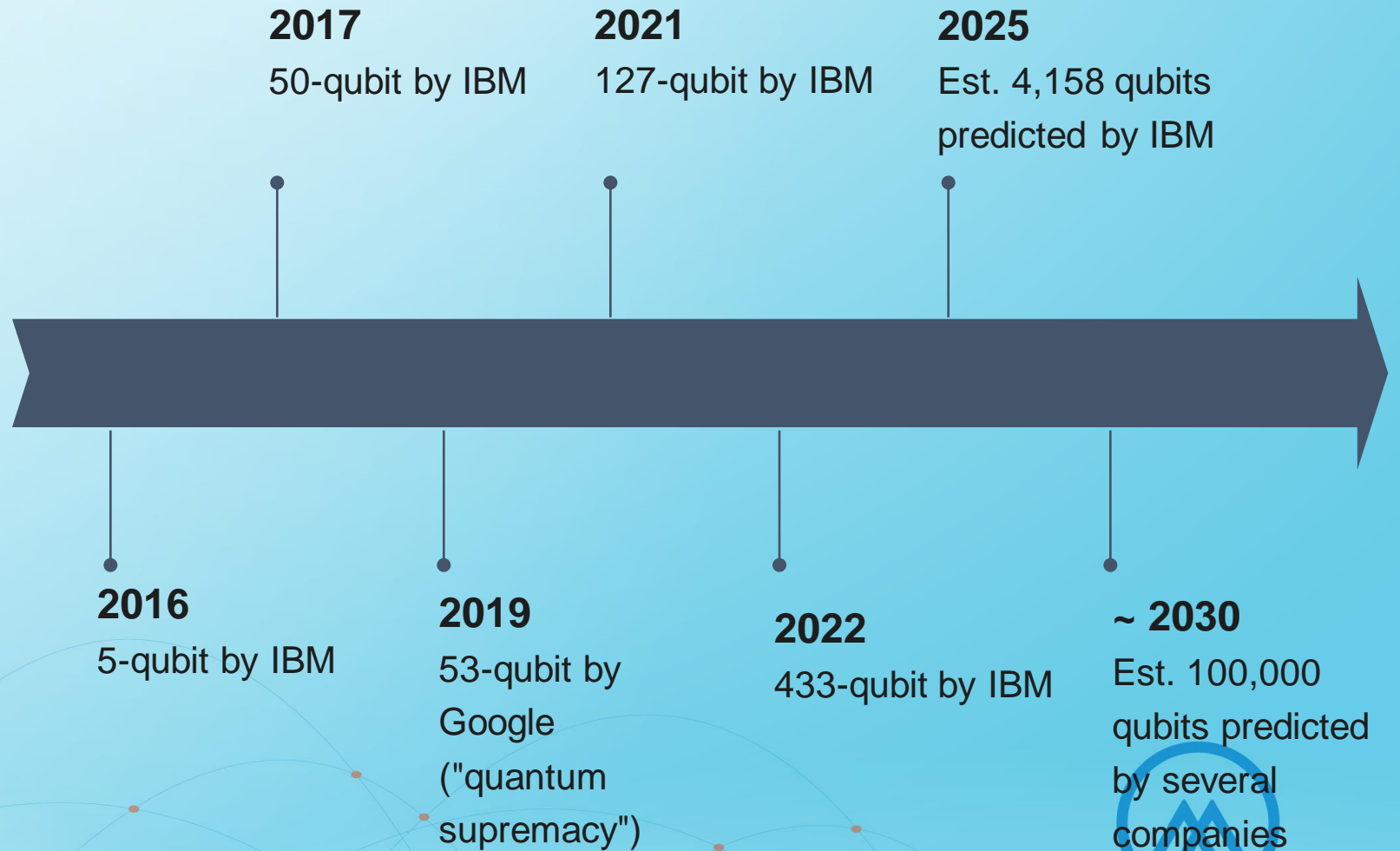


Challenges, achievements, and the road ahead



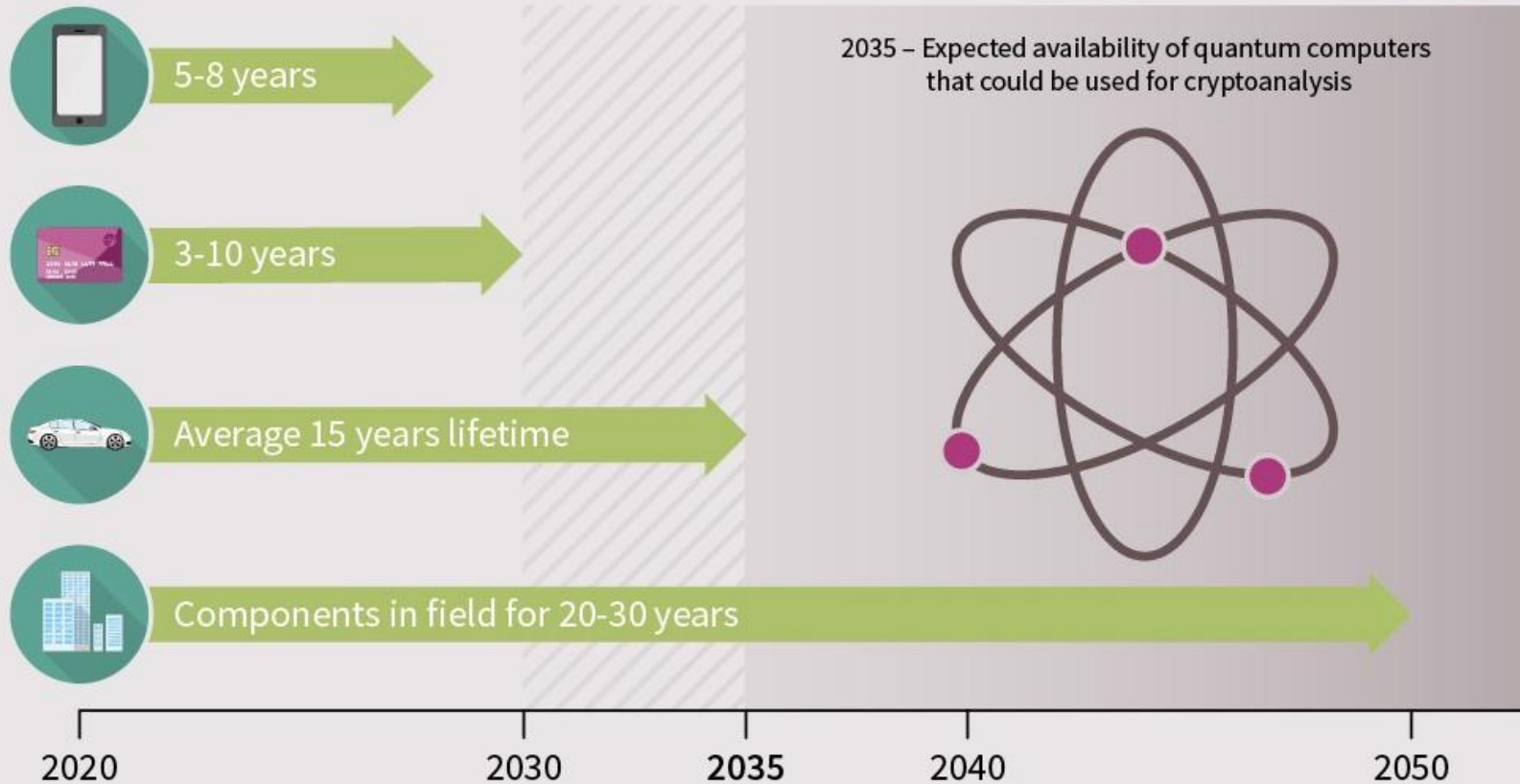
Challenges

- To have a **high number of stable** qubits (qubit decoherence)
- Scalability

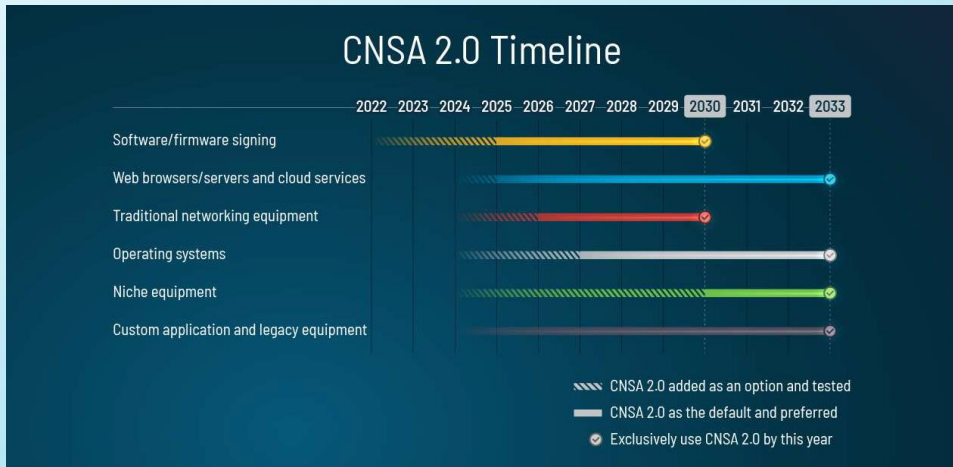
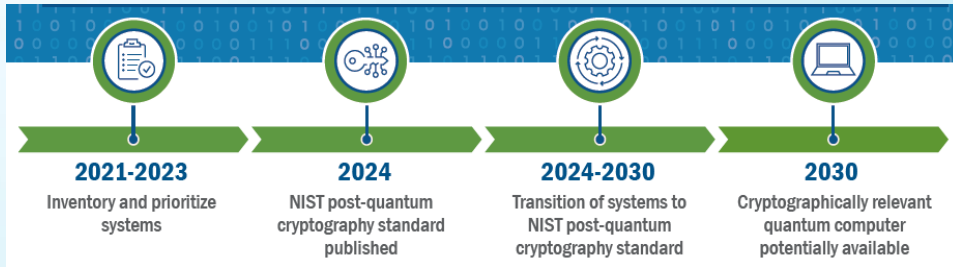


The future is near...

Devices with over 10 years of lifetime should be prepared for the quantum computing age **now**



WHEN WILL QUANTUM-SAFE CRYPTOGRAPHY BECOME MANDATORY?



NIST



- Security agencies set the timeline
- Quantum computer potentially available as soon as 2030
- Transition to Post Quantum Crypto to be finalized in **2030-2035**
- CISA sponsored study: Provide Identity Management and Associated Trust Support Services is #35 National Critical Function
- but it is a critical enabler of the PQC migration



QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

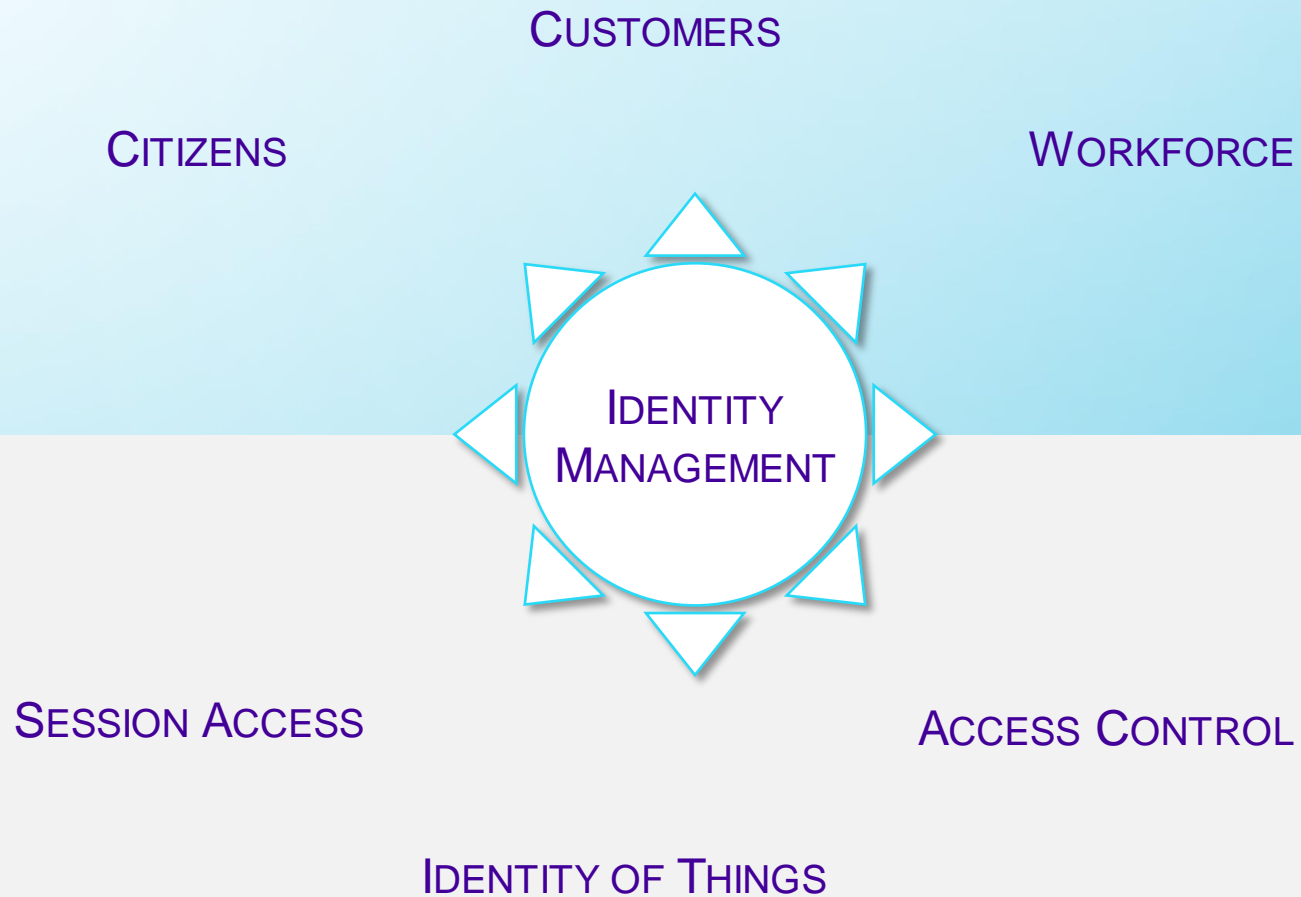


NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



- Establish a PQ Readiness Roadmap
- Prepare a Cryptographic Inventory
- Engage your Cryptography Vendors on PQC
- Supply Chain Quantum Readiness

WHAT DOES IT MEAN FOR IDENTITY MANAGEMENT?



COMPROMISED USER IDENTITY

- ✗ Identity proofing
- ✗ User authentication
- ✗ Account recovery
- ✗ Decentralized identity

BREACHED ACCESS MANAGEMENT

- ✗ Trusted authorities
- ✗ Session Authentication
- ✗ Equipment access control
- ✗ Equipment authentication
- ✗ Physical access control
- ✗ Digital signature

WHAT DOES IT MEAN FOR IDENTITY MANAGEMENT?

CUSTOMERS

COMPROMISED USER IDENTITY

CITIZENS

WORKFORCE

- ✗ Identity proofing
- ✗ Authentication
- ✗ Identity
- ✗ Identity

>>> Correlate cryptographic inventory with inventories available from existing programs, such as Asset Inventory, Identity, Credential, and Access Management, (ICAM), Identity & Access Management (IdAM), Endpoint Detection and Response (EDR), and Continuous Diagnostics and Mitigation (CDM)

ACCESS MANAGEMENT

DHS CISA

SESSION AC

- ✗ Authentication
- ✗ Access control
- ✗ Authentication

IDENTITY OF THINGS

- ✗ Physical access control
- ✗ Digital signature

HOW TO PROTECT FROM QUANTUM THREAT

Migrate to quantum-safe cryptographic algorithms


- Symmetric algorithms (TDES, AES) → move to AES 256
- Asymmetric (RSA, ECC, DH) → migrate to Post Quantum Algorithms

Implementing Post Quantum Algorithms is not plug-and-play, and needs to redefine all currently used protocols



- Communication protocols: TLS, HTTPS, VPN
- Certificates, Digital signature
- Session control: OpenID connect
- User authentication: FIDO, PIV

Standardization process is forthcoming

- Objective is to be ready for NIST/CISA/NSA timeline (Start of migration 2025)





SELECTED ALGORITHMS




FALCON **SPHINCS+**

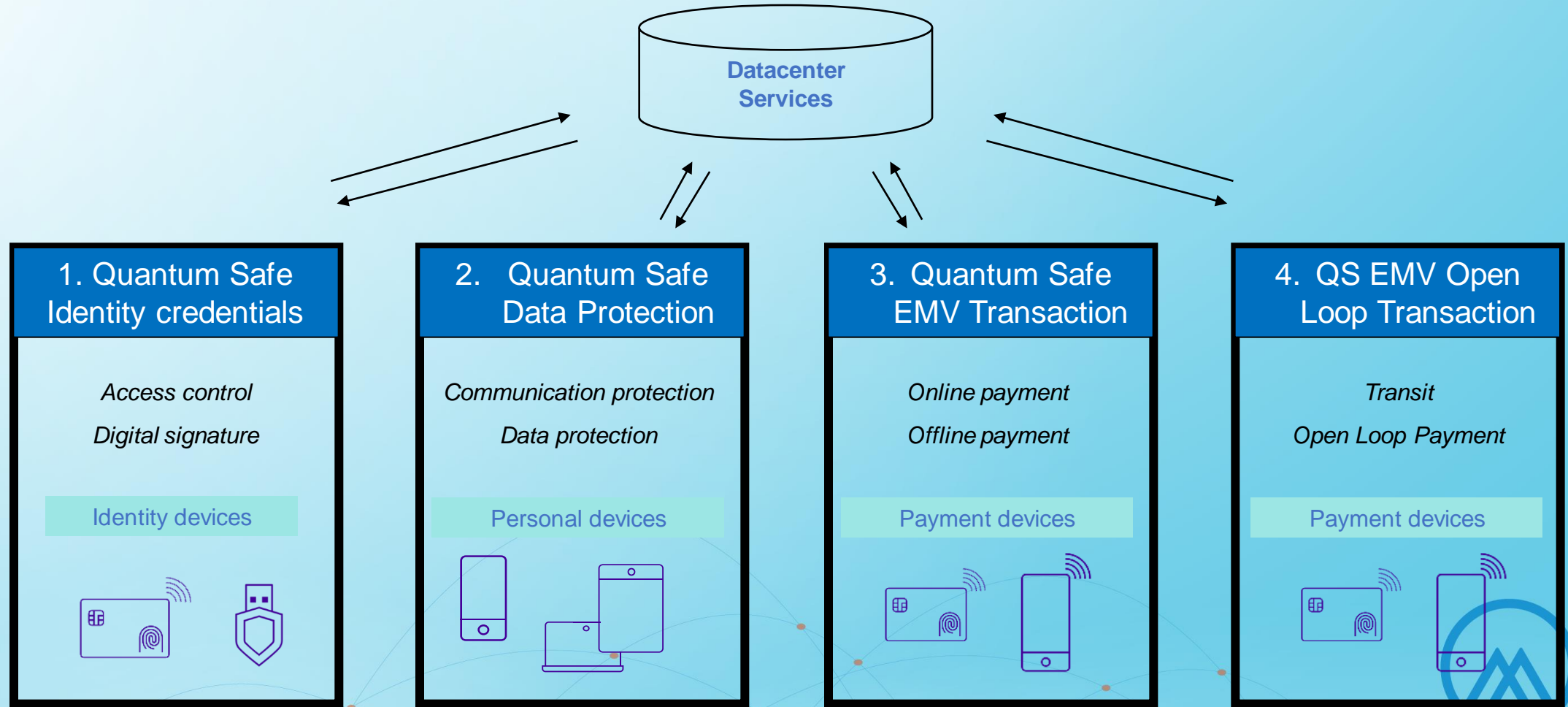
4TH ROUND ALGORITHMS



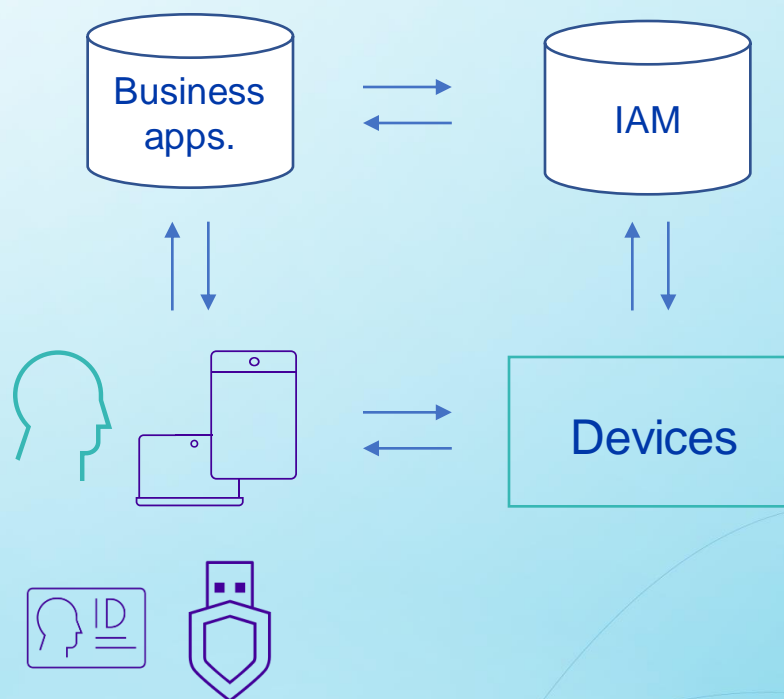
HQC **McEliece**



AREAS OF FOCUS



HOW TO PREPARE: SHORT TERM PRIORITIES FOR POC



1. Prepare digital world for crypto agility

- Impact on IAM architecture
- New required services
- Crypto agility implementation

2. Prepare the physical world for migration

- Deploy quantum-ready devices as soon as possible
- Remotely manage crypto agility

QUANTUM-SAFE PROOFS OF CONCEPTS

› PAYMENT TRANSACTION

- Quantum-safe EMV transaction

› 5G

- Quantum-safe SUCI encryption
- Quantum-safe Profile Download for eUICC

› IDENTITY

- Quantum-safe Passport Reading
- Quantum-safe Public Identity Verification (PIV) card

A NEW CHALLENGE: CRYPTOAGILITY



QUANTUM-SAFE ALGORITHMS ARE YOUNG

For the next 10-15 years,

- Vulnerabilities will be discovered
- Some algorithms can be “solved”
- Standards will be evolving

CRYPTOAGILITY IS CRITICAL FOR SECURITY

As soon as a vulnerability is discovered

- Algorithms must be updated
- Including physical credentials and devices

If there is a need to change algorithm

- Decouple encryption algorithms from workflows
- Protocols need to be changed everywhere at the same time
- Credentials must be reissued



Questions?



Identity and Payment in the Post-Quantum Era



Teresa Wu
IDEMIA

Teresa.Wu@us.idemia.com



Mark Stafford
Infineon

Mark.Stafford@infineon.com



THANK YOU!

