Future-proofing against quantum computing threats. Will you be ready?

Olivier

NORA

Chief of Open Innovation

IDEMIA

Teresa

WU

VP, Smart Credentials

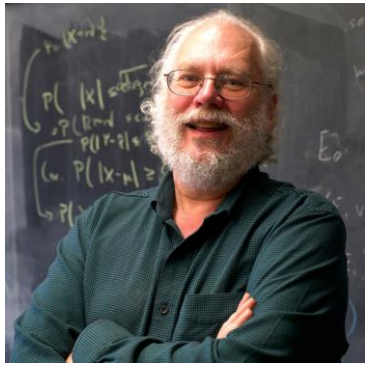
IDEMIA

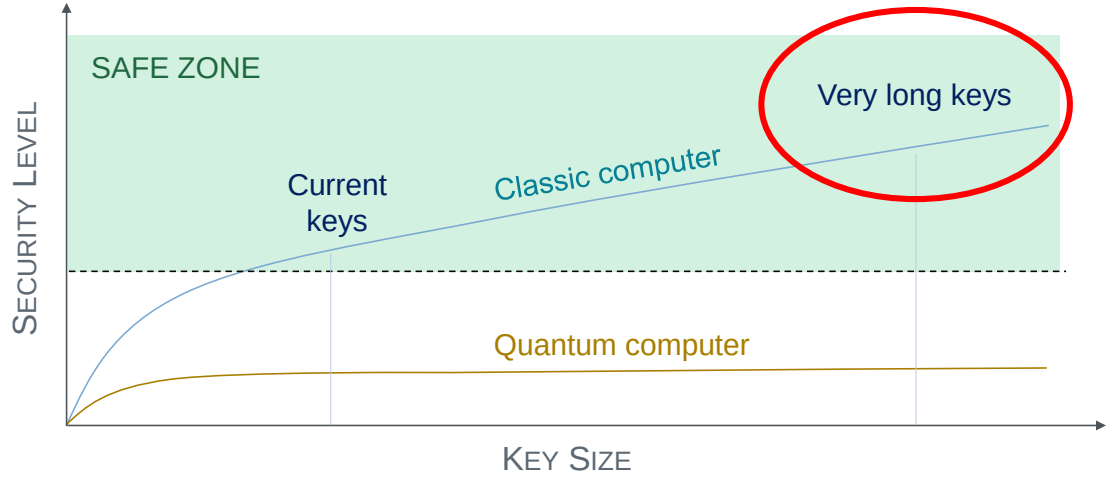
QUANTUM THREAT

- Quantum Computers are extremely efficient at solving specific problems
- Breaking cryptography is a topic at which Quantum Computers are very good
  - Symmetric cryptography (TDES, AES): they accelerate the search for keys
  - Asymmetric cryptography (RSA, ECC, DH): they solve the cryptographic problem

SHOR Algorithm allows quantum computers to break currently used asymmetric algorithms

- ✖ RSA, ECC, DH





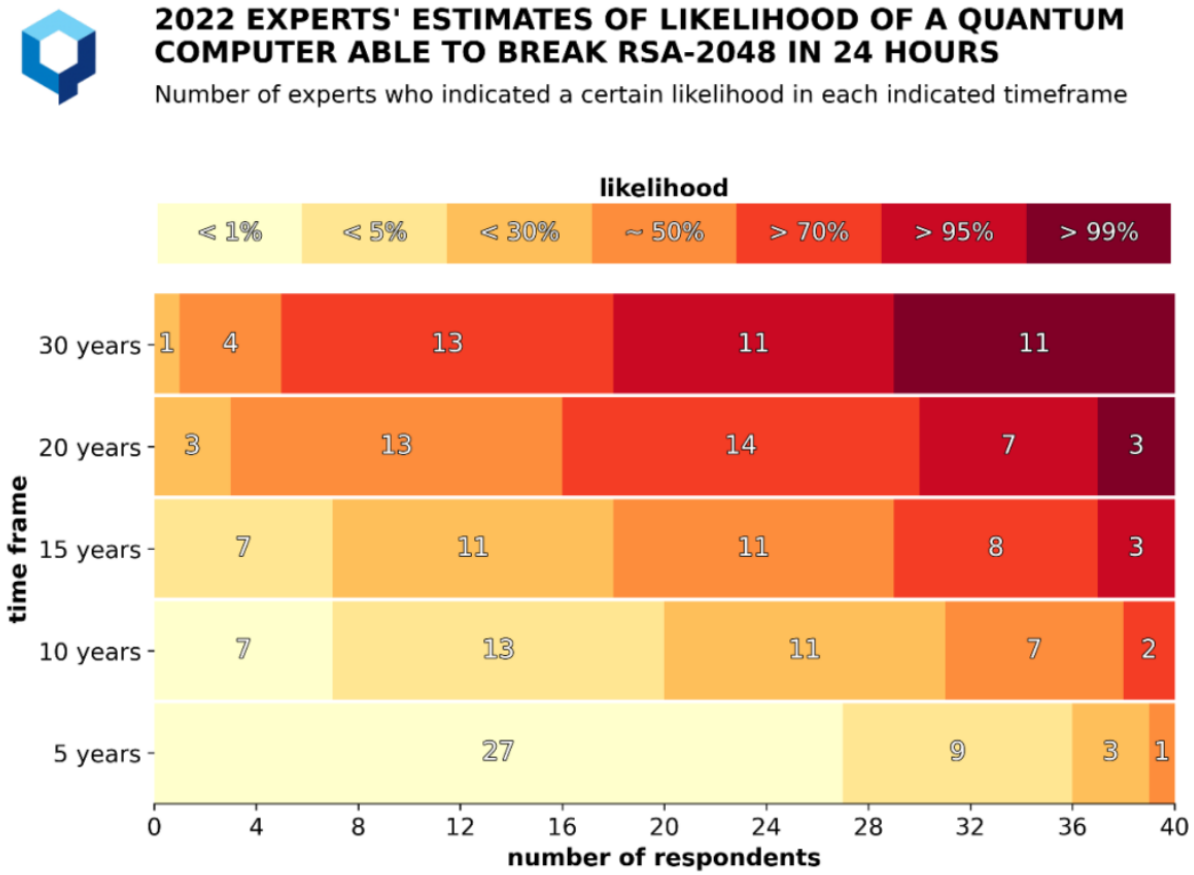
Time required to find RSA secret key depending on key size
Logarithmic scales

QUANTUM THREAT

When will Quantum Computer be able to break currently used cryptography?

50% experts assess that there is 50% chance that the answer is:

IN 2030-2035

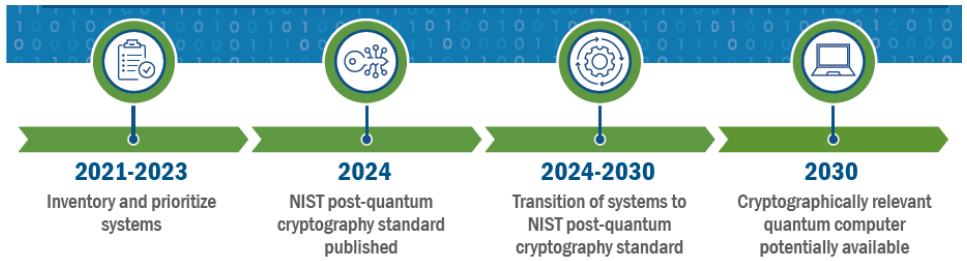


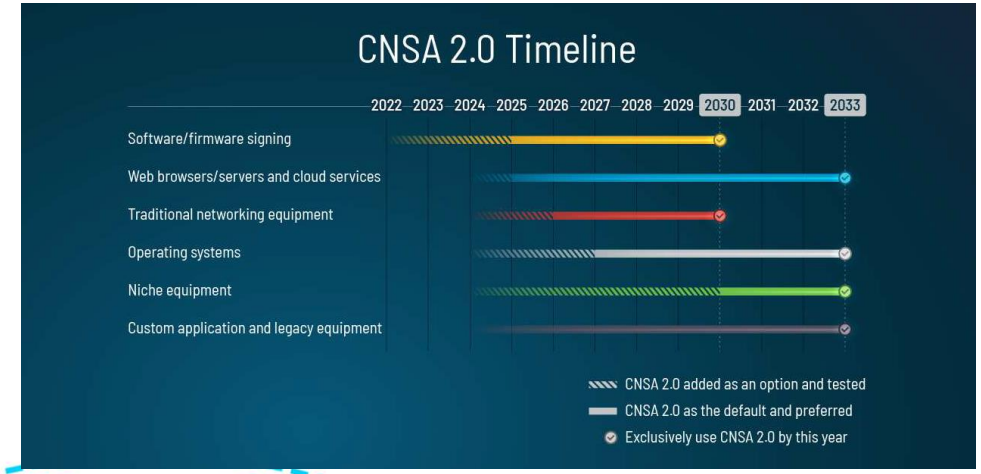
Global Risk Institute, Quantum Threat timeline report 2022

identiverse

#identiverse

WHEN WILL QUANTUM-SAFE CRYPTOGRAPHY BECOME MANDATORY?





- 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

WHAT DOES IT MEAN FOR IDENTITY MANAGEMENT?

CUSTOMERS

CITIZENS

WORKFORCE

SESSION ACCESS

ACCESS CONTROL

IDENTITY OF THINGS

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

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)

NIST

SELECTED ALGORITHMS

KYBER

DILITHIUM

FALCON

SPHINCS+

4TH ROUND ALGORITHMS

McEliece

HQC

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

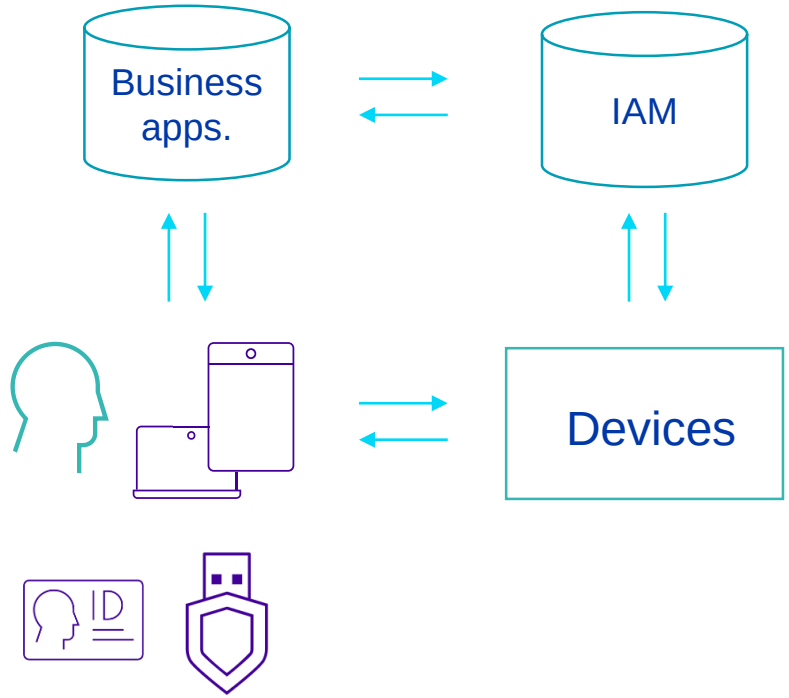
As soon as a vulnerability is discovered

- 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

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

Questions?

Olivier NORA

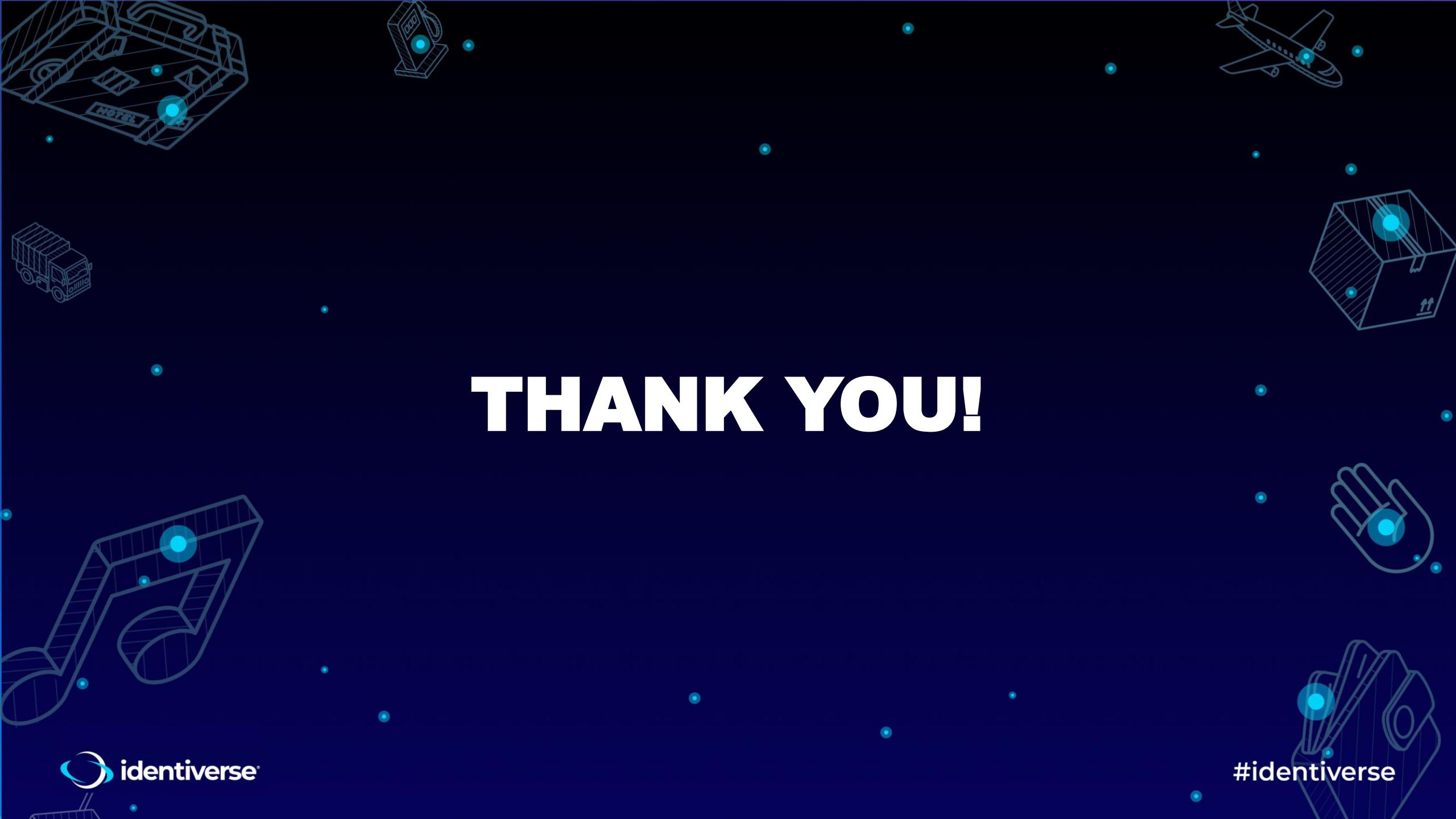
Olivier.Nora@idemia.com

IDEMIA

Teresa WU

Teresa.Wu@us.idemia.com

IDEMIA


THANK YOU!
identiverse
#identiverse