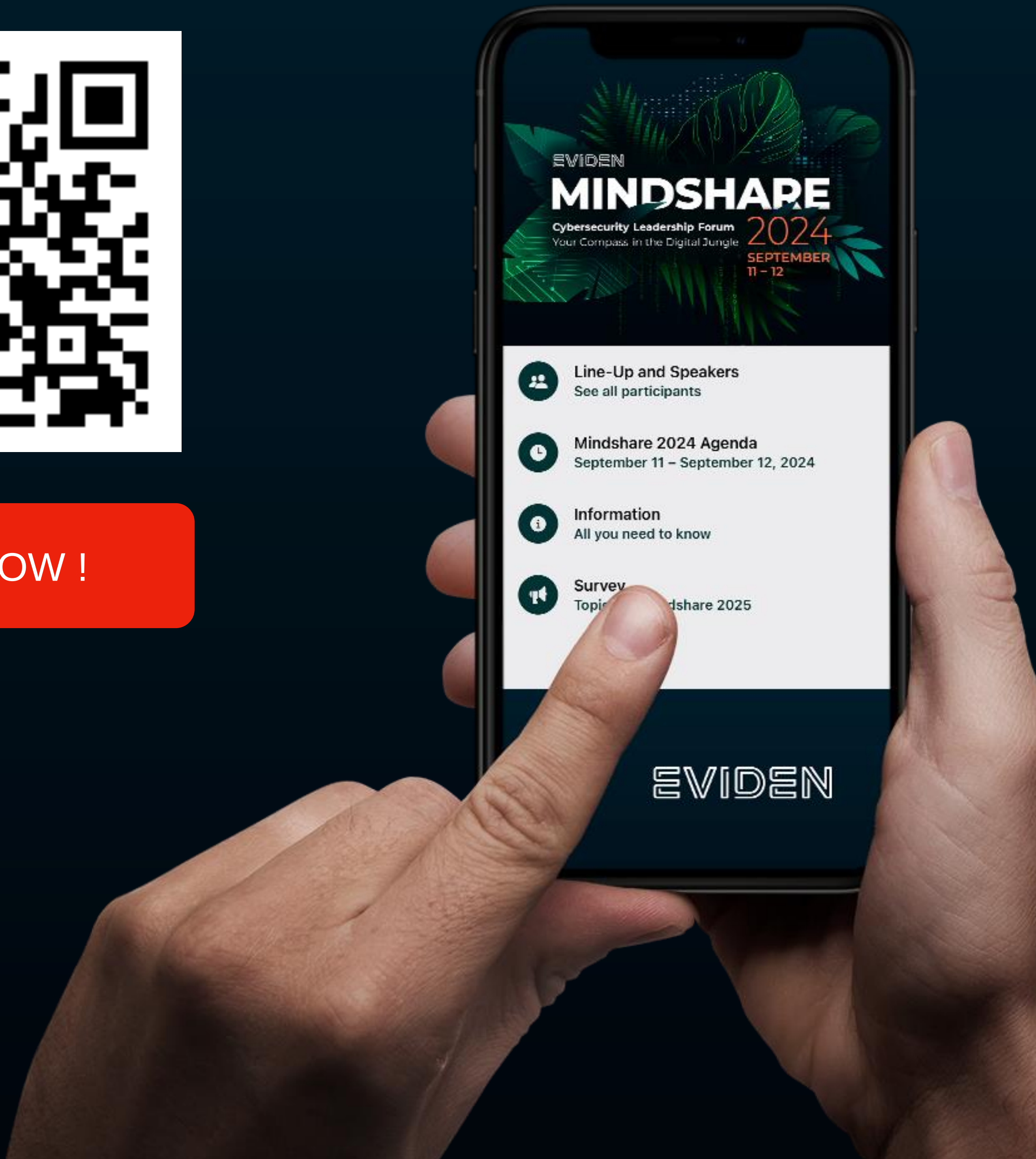
MINDSHARE 2024 AGENDA

SCAN NOW !



EVIDEN

MINDSHARE

Cybersecurity Leadership Forum
Your Compass in the Digital Jungle

2024
SEPTEMBER
11 – 12

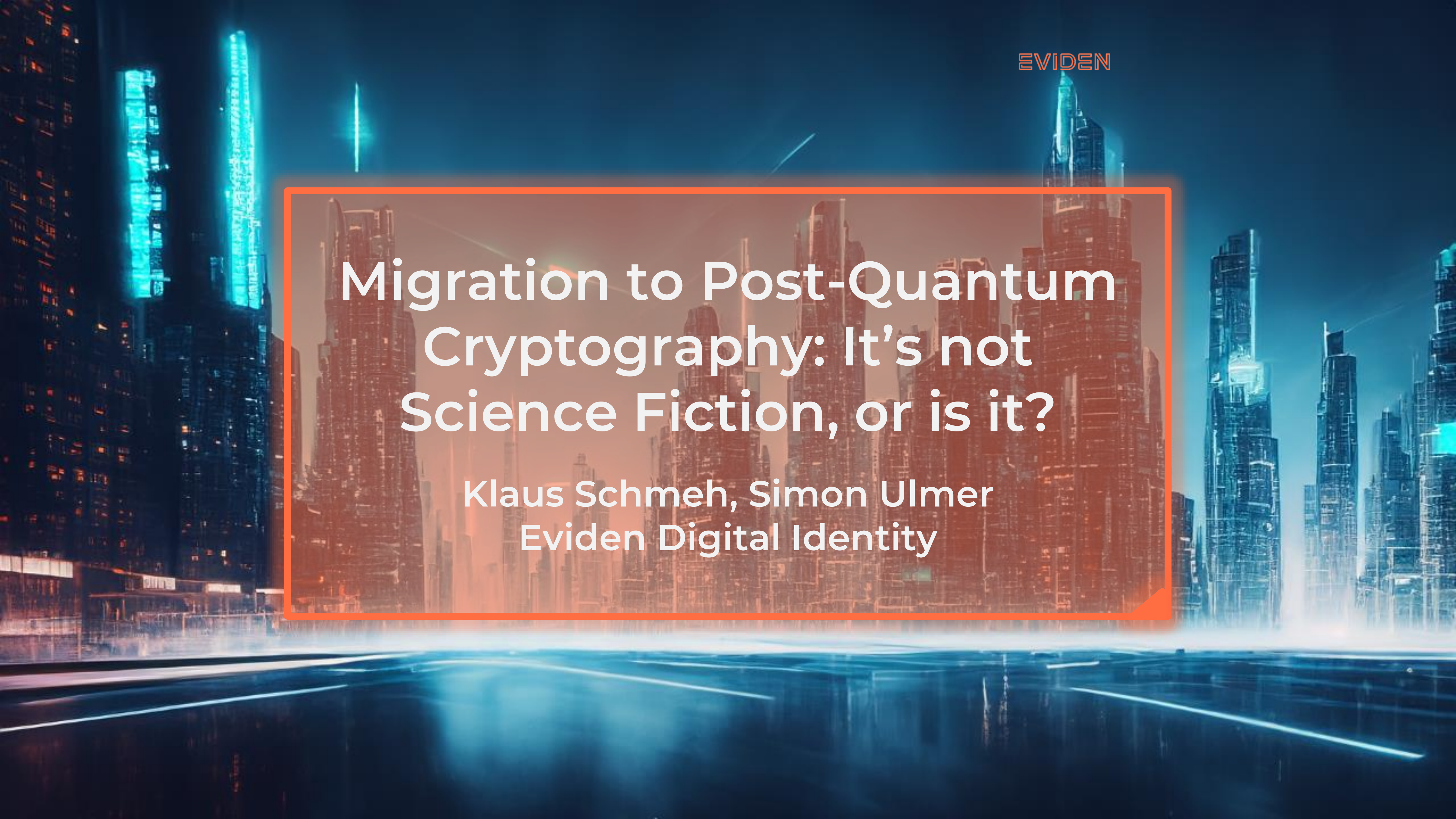
Line-Up and Speakers
See all participants

Mindshare 2024 Agenda
September 11 – September 12, 2024

Information
All you need to know

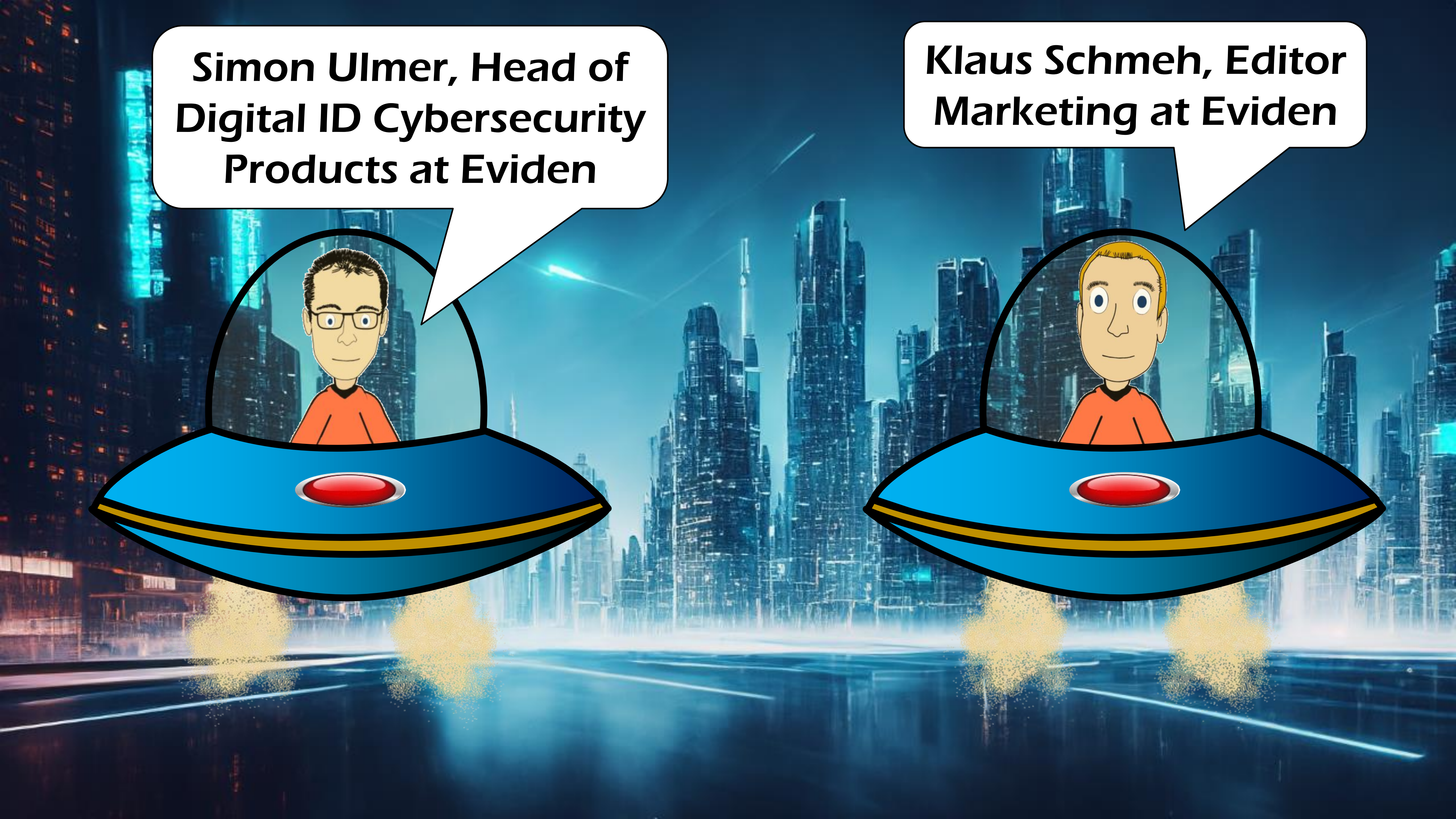
Survey
Topi dshare 2025

EVIDEN



Migration to Post-Quantum Cryptography: It's not Science Fiction, or is it?

Klaus Schmeh, Simon Ulmer
Eviden Digital Identity


Simon Ulmer, Head of Digital ID Cybersecurity Products at Eviden
Klaus Schmeh, Editor Marketing at Eviden

Eviden Digital Identity, Home of cryptovision and IDnomic
We protect electronic identities with cryptographic solutions.

Agenda

Q-Day

Post-Quantum Cryptography

Post-Quantum Migration

Crypto Inventory

Migration Execution

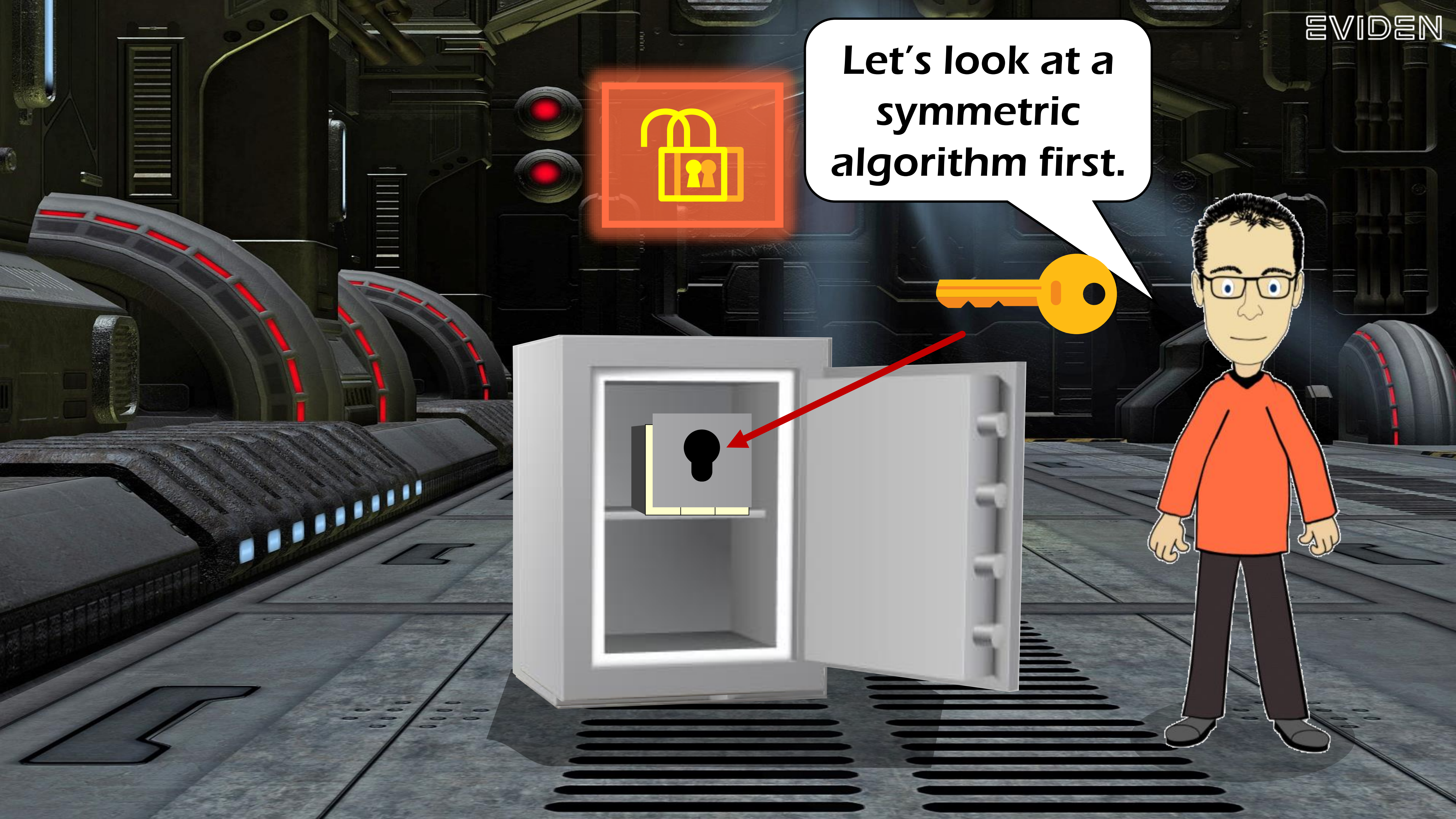
Conclusion

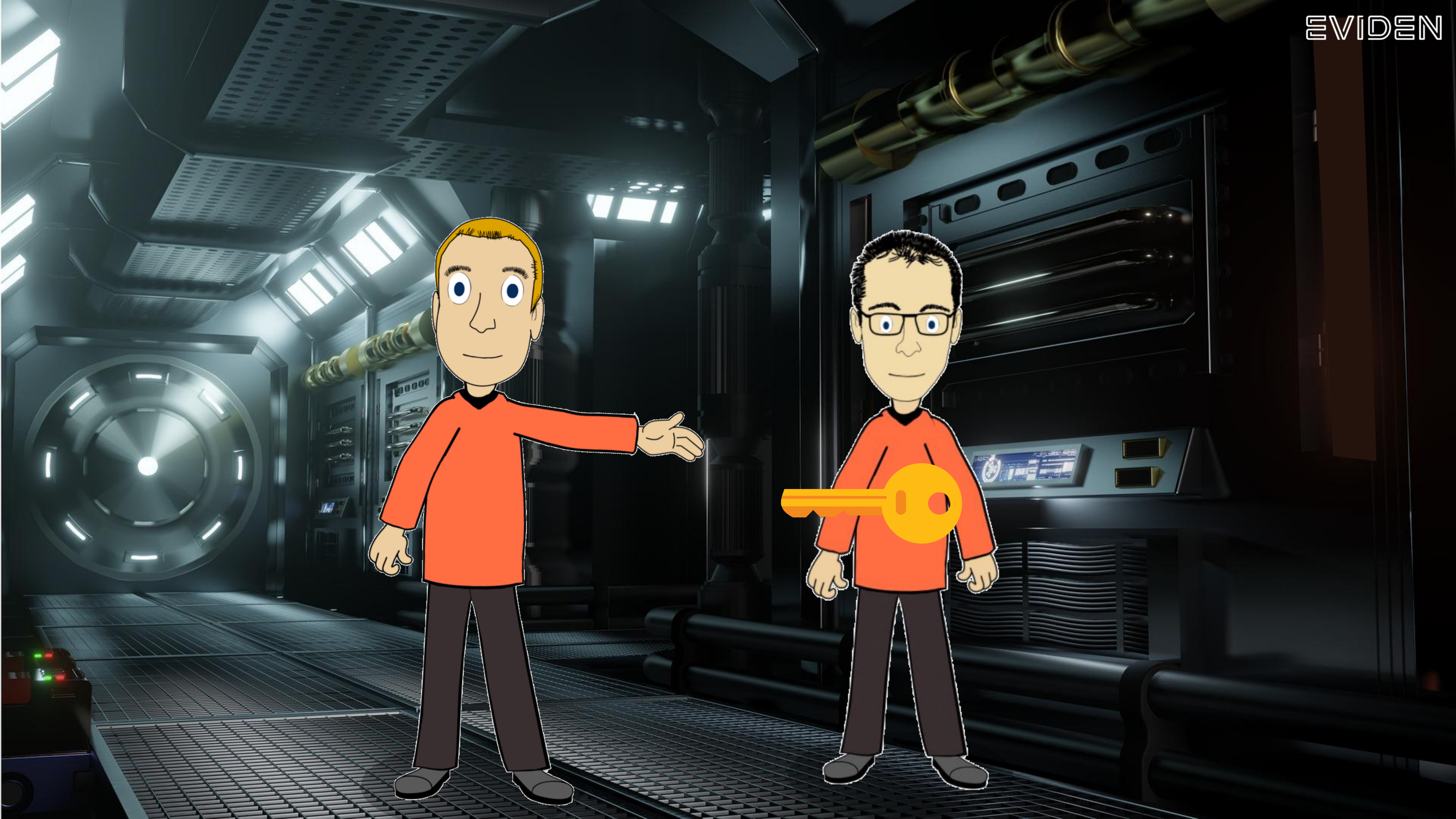
What do these systems have in common?

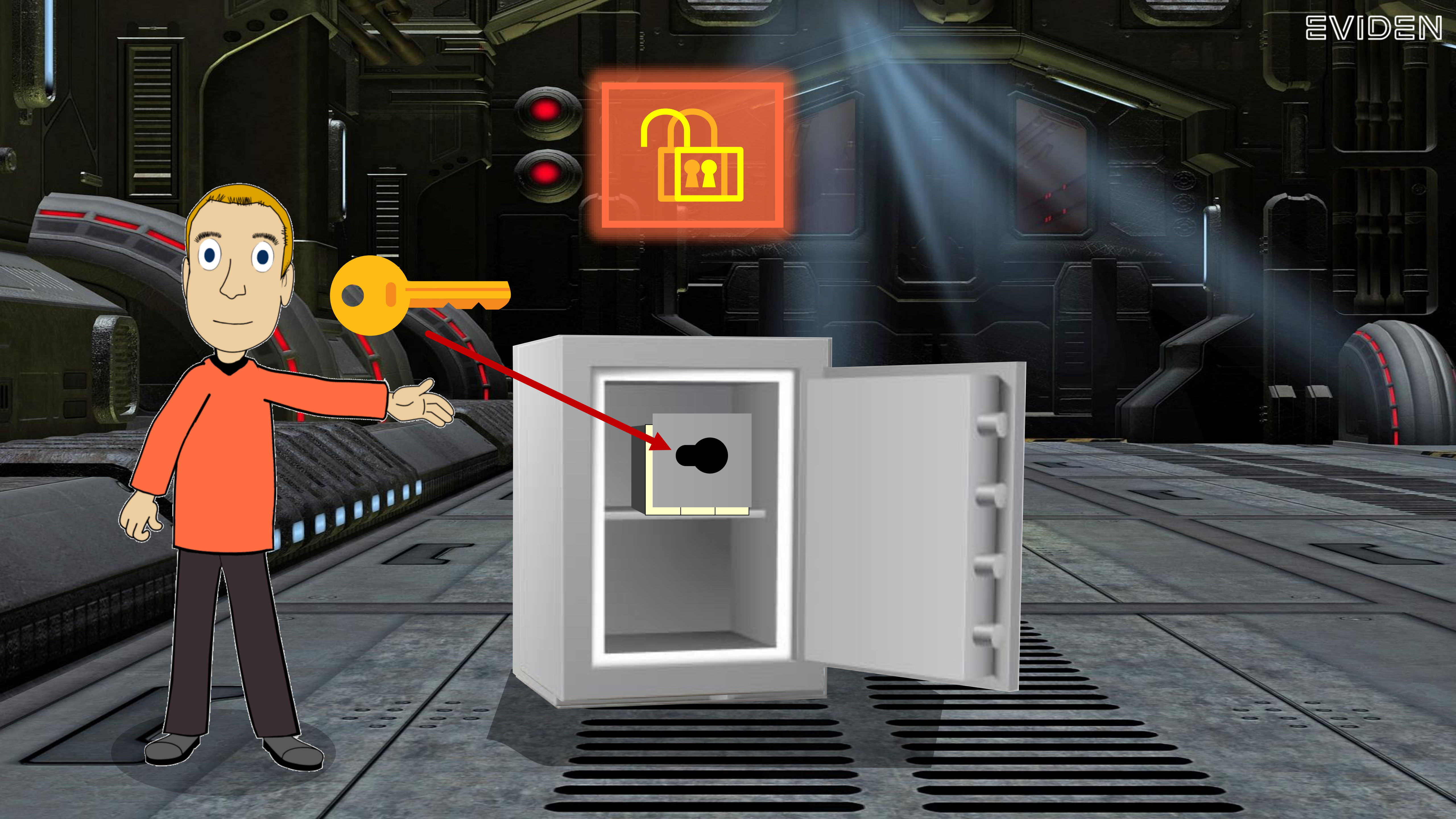
They use the RSA crypto algorithm.

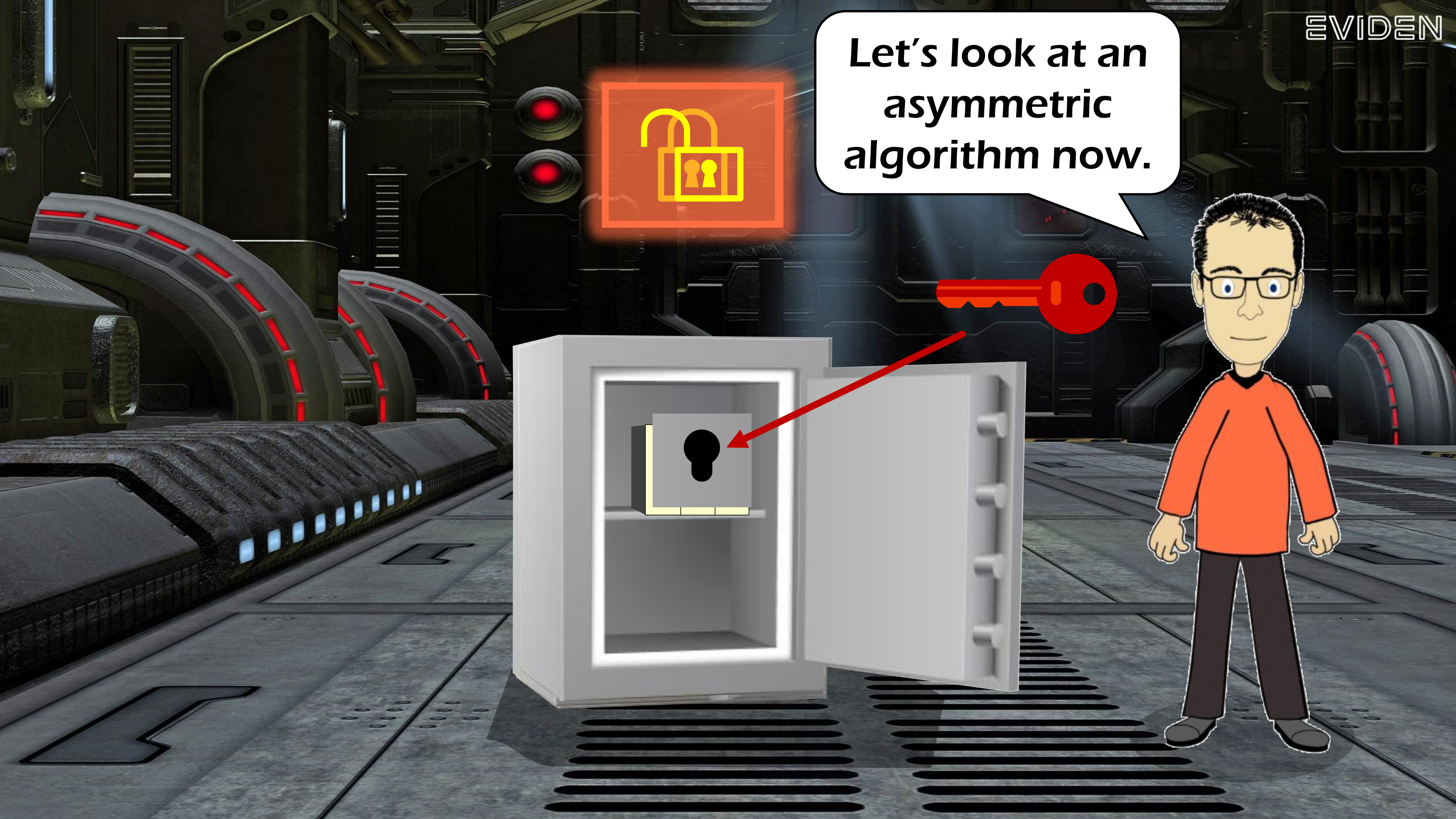
RSA is an asymmetric encryption algorithm.

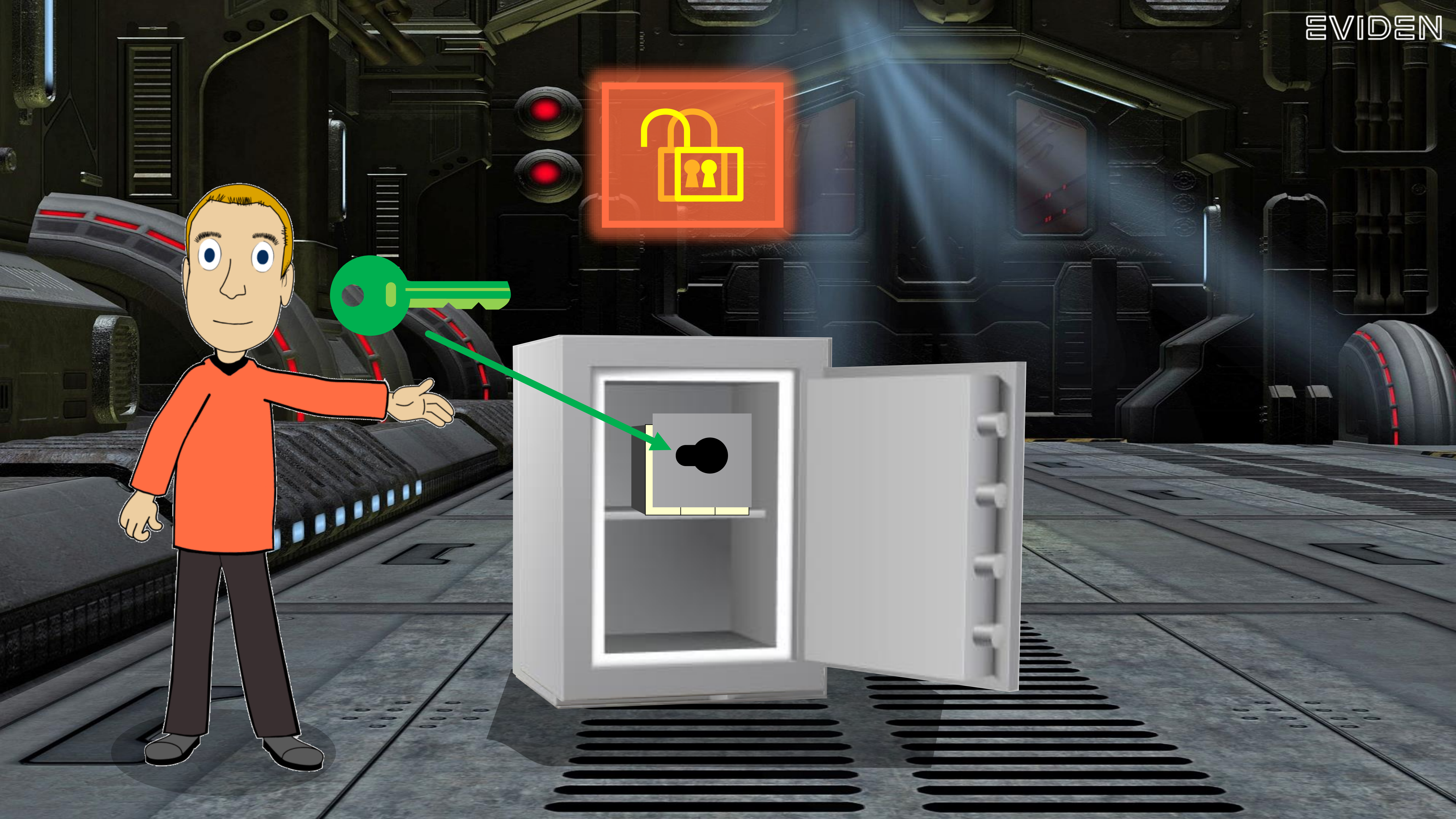
Smart-phone
Identity document
ATM
Web browser
Operating system
Email c


Let’s look at a symmetric algorithm first.






Let's look at an asymmetric algorithm now.



RSA Crypto System

Can be used for encryption
or digital signatures

$$\underset{\text{prime}}{17} \times \underset{\text{prime}}{23} = 291$$

Multiplication is easy,
factorization is difficult

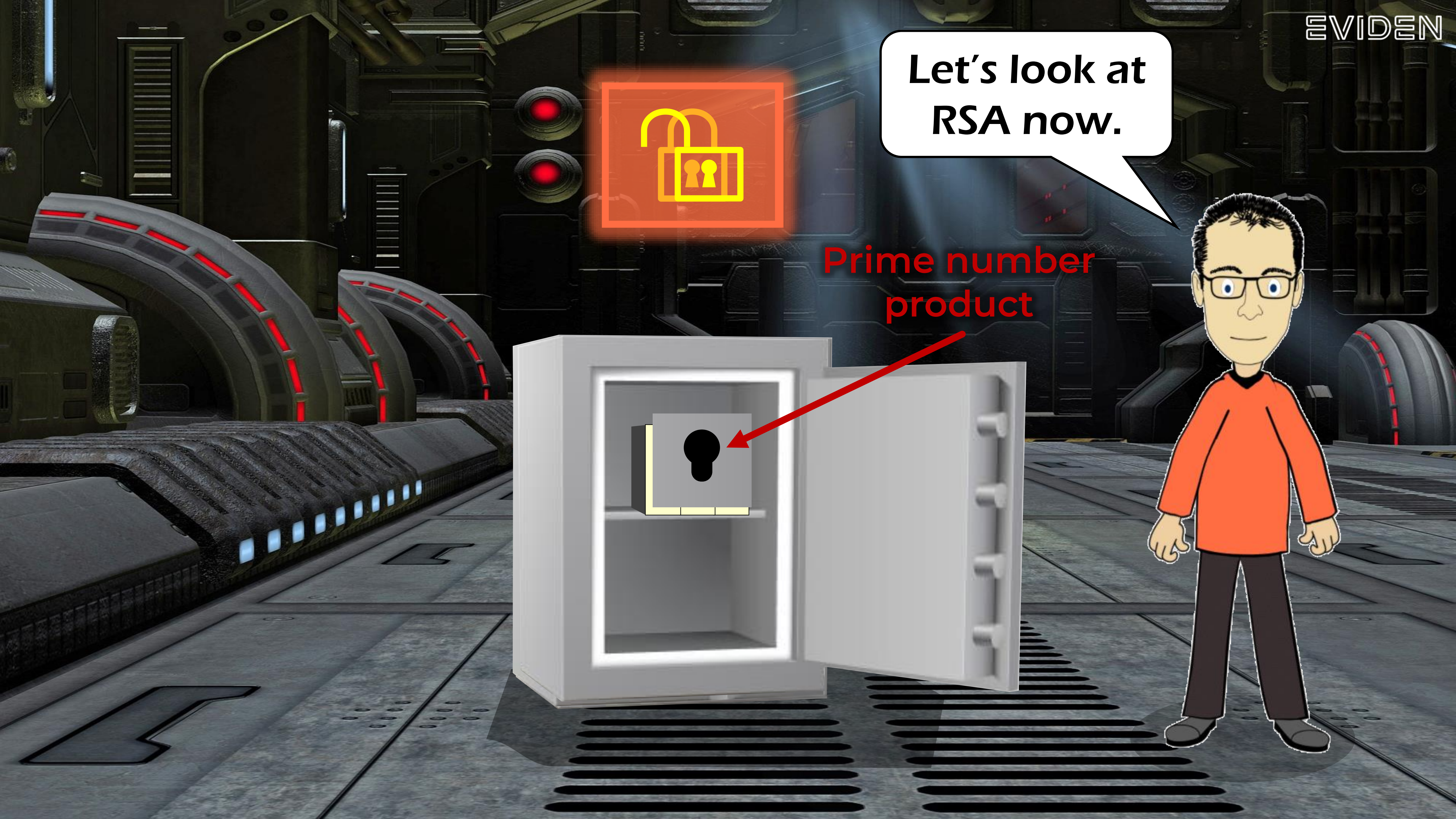
RSA Crypto System

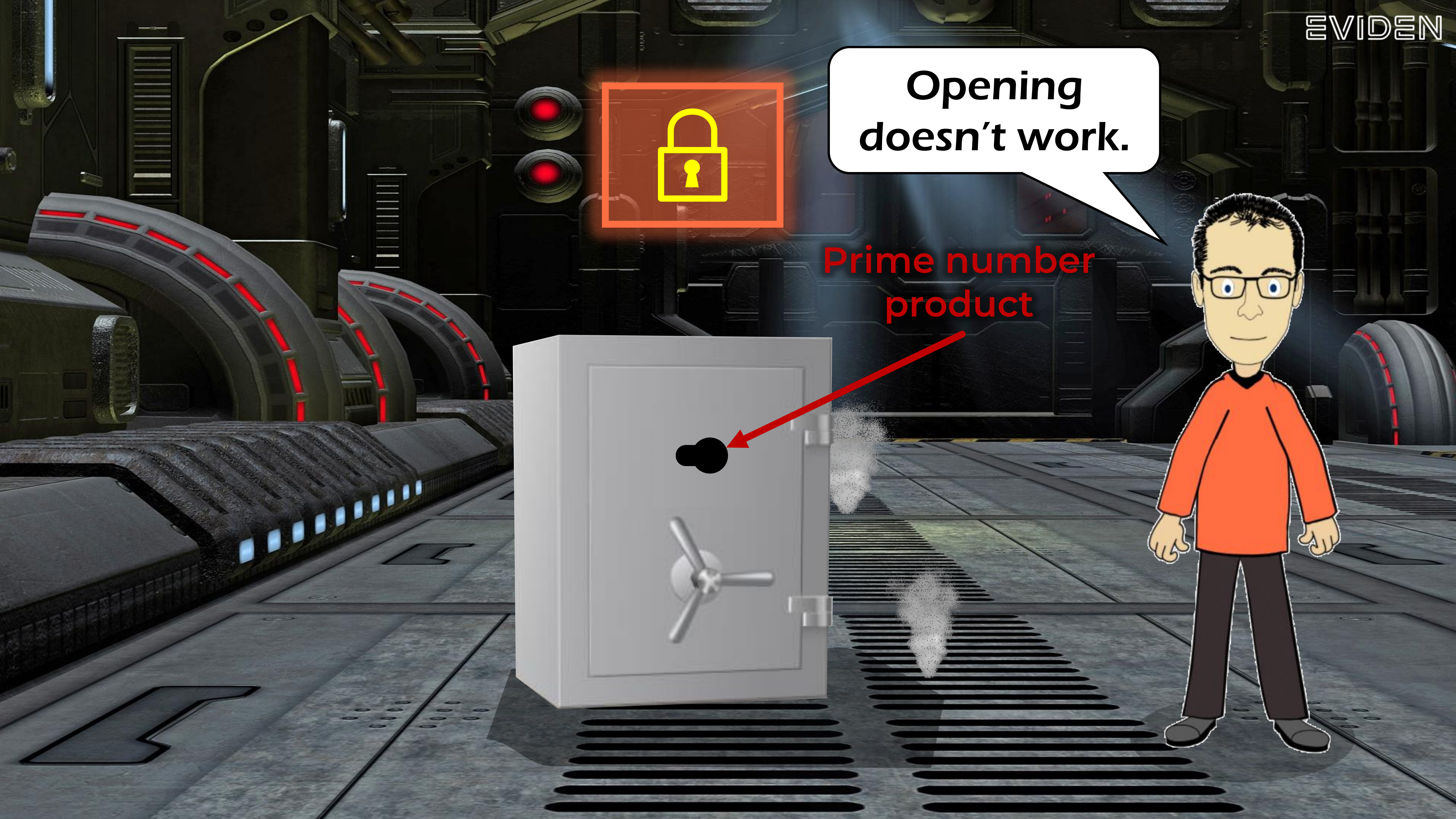
Private key
= key to open safe

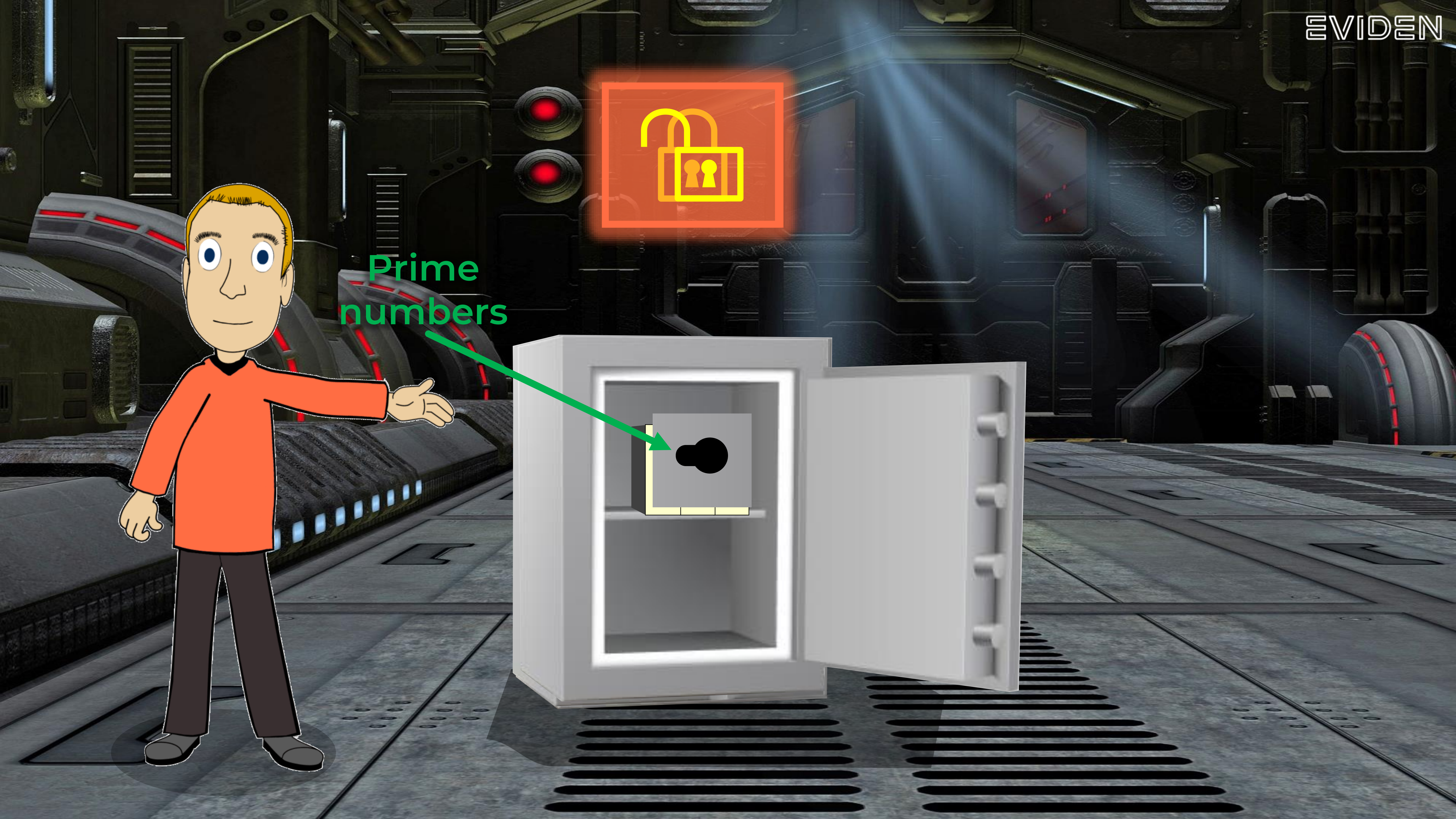
Public key
= safe

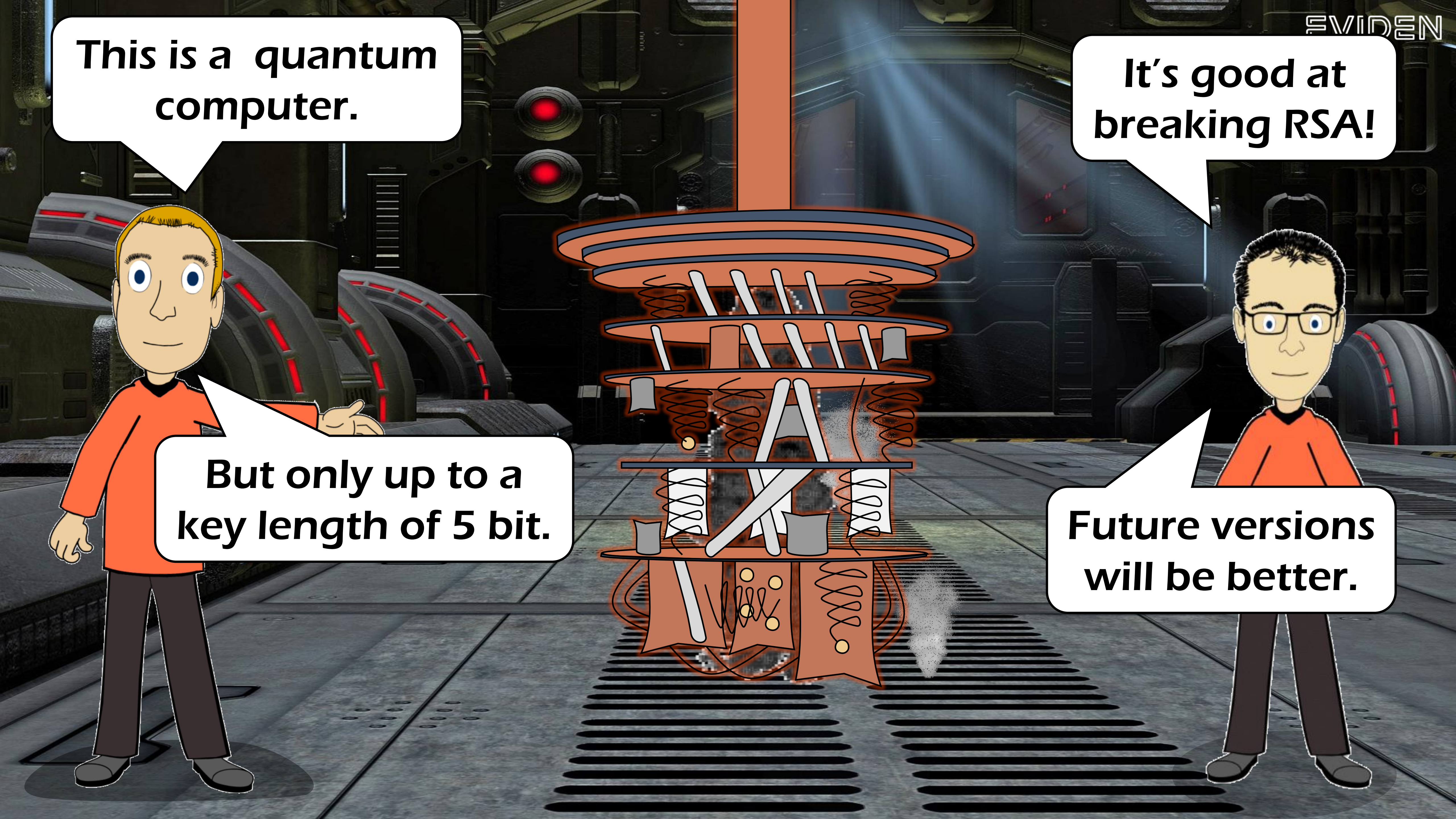
$$\underbrace{17}_{\text{prime}} \times \underbrace{23}_{\text{prime}} = 291$$

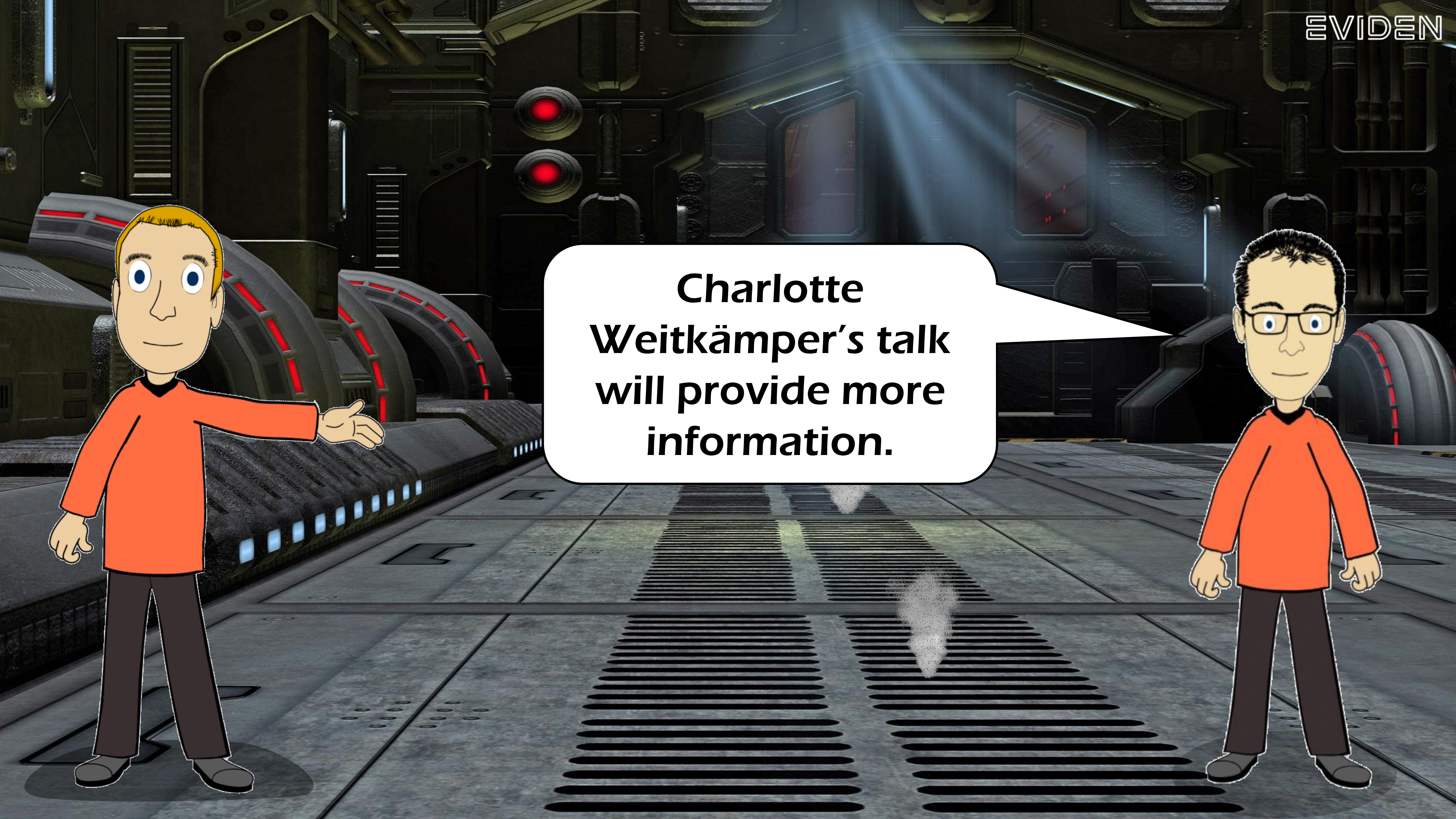
Typical public key length: 2048 bit

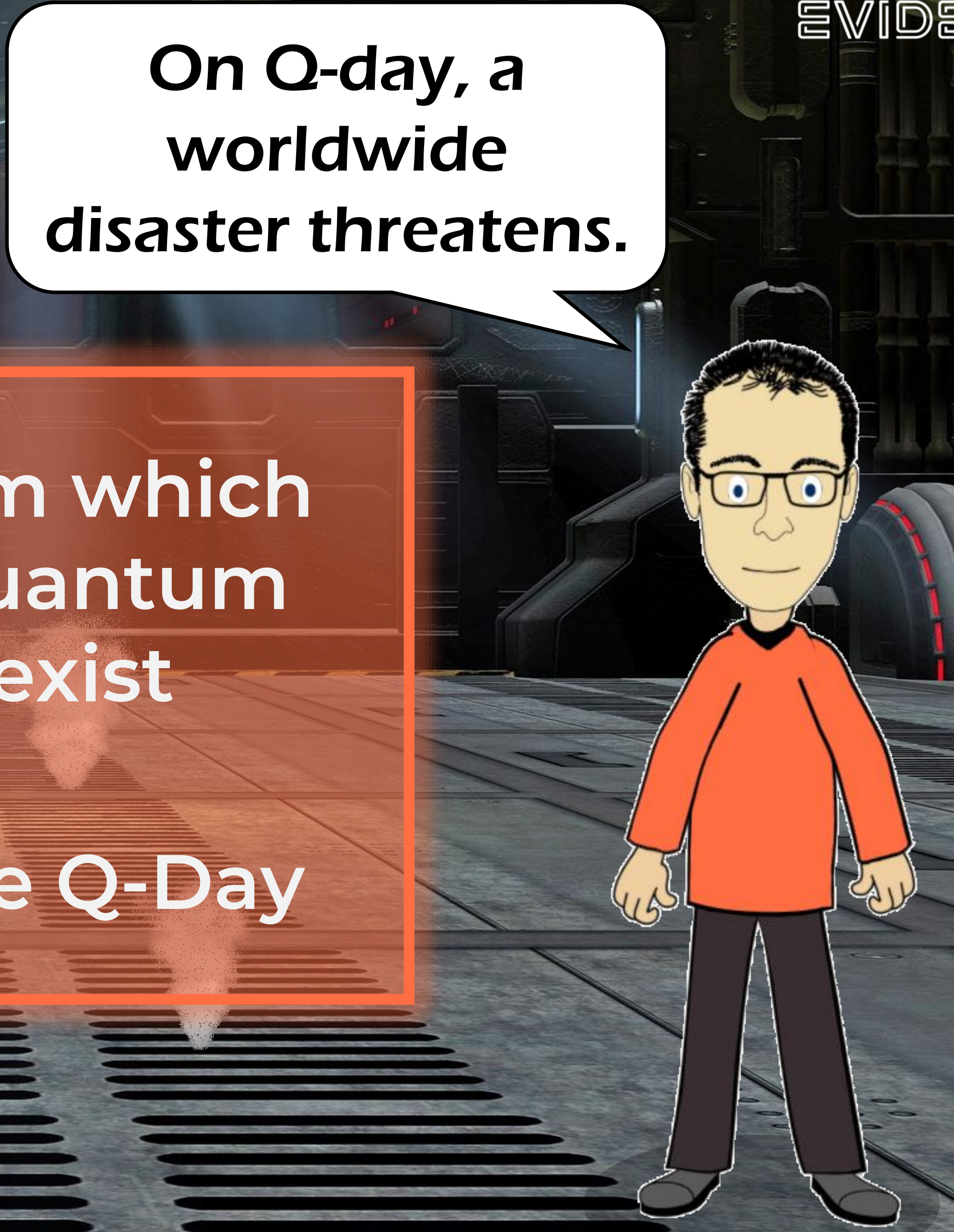

Let's look at RSA now.
Prime number product


Opening doesn't work.
Prime number product


Prime numbers


This is a quantum computer.
But only up to a key length of 5 bit.
It's good at breaking RSA!
Future versions will be better.


Charlotte Weitkämper's talk will provide more information.



Q-Day: Day from which on powerful quantum computers exist

Y2Q: Year of the Q-Day

BSI: Migration of security-critical IT until 2033

NSA: Migration of public IT 2035

Smartphone

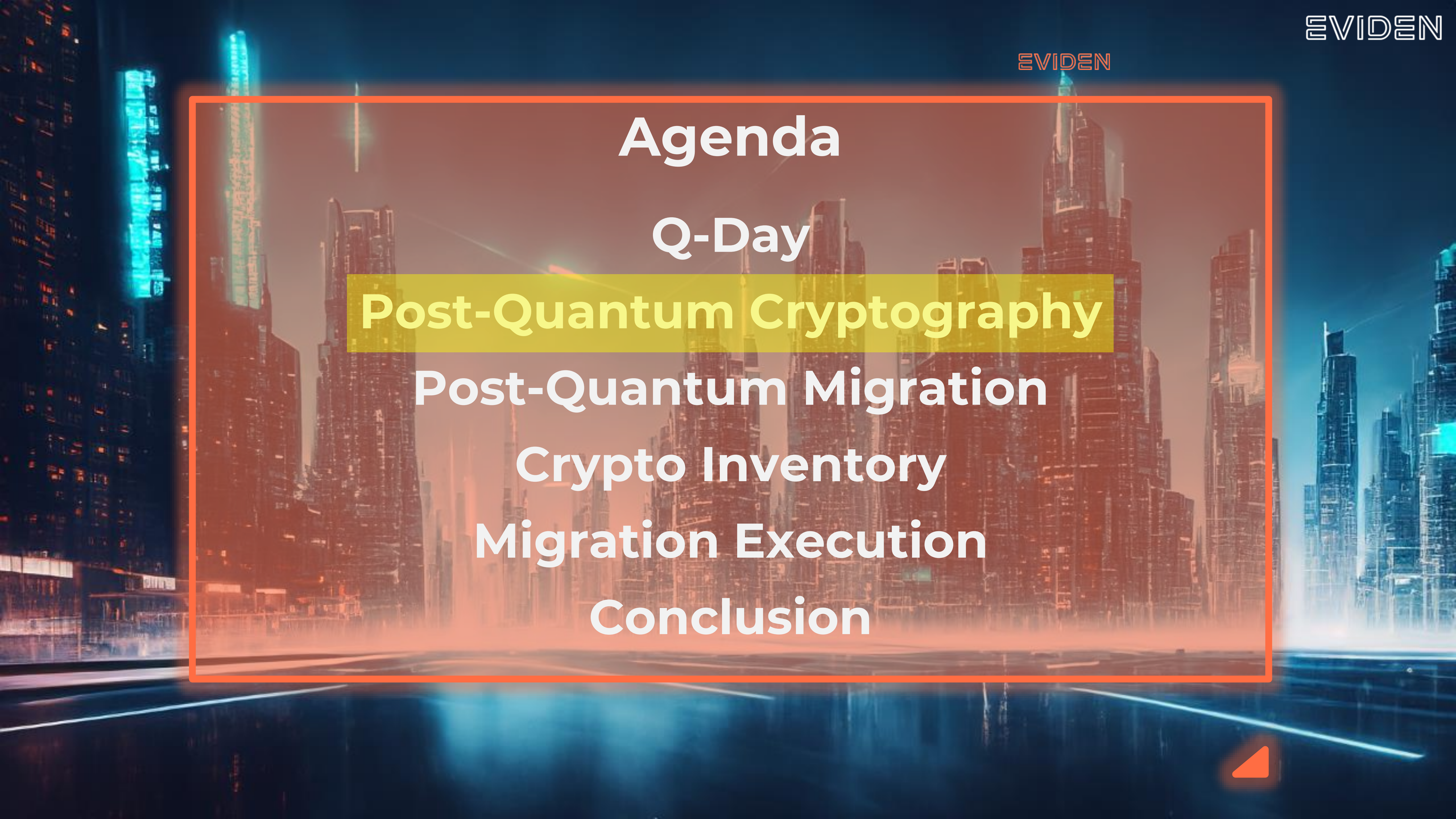
Web browser

Identity document

Operating system

ATM

Email client



Agenda

Q-Day

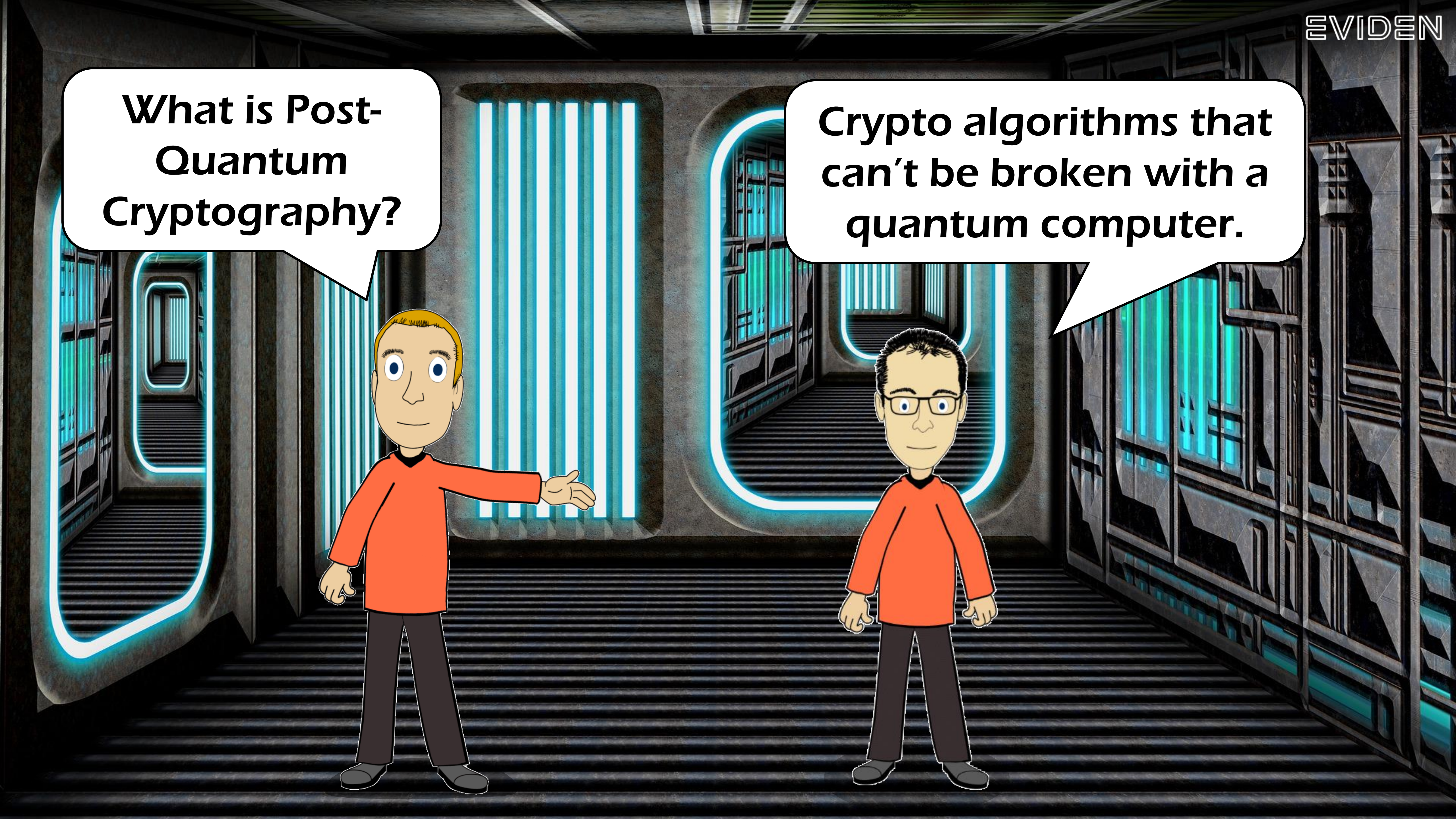
Post-Quantum Cryptography

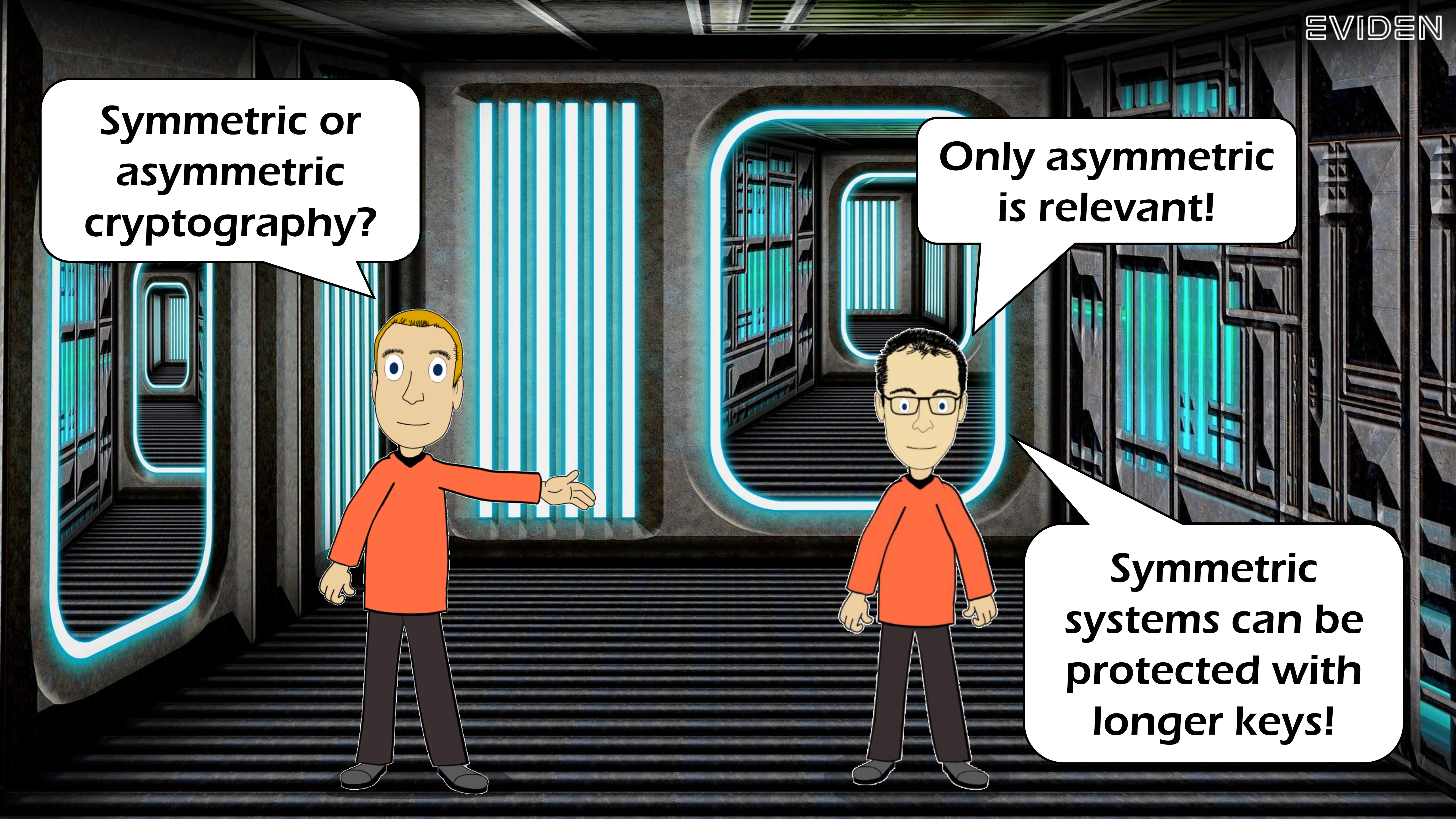
Post-Quantum Migration

Crypto Inventory

Migration Execution

Conclusion


What is Post-Quantum Cryptography?
Crypto algorithms that can’t be broken with a quantum computer.


Symmetric or asymmetric cryptography?
Only asymmetric is relevant!
Symmetric systems can be protected with longer keys!

Post-Quantum algorithms (asymmetric)

Current algorithms

CRYSTALS-Kyber

CRYSTALS-Dilithium

FALCON

SPHINCS+

FrodoKEM

XMSS

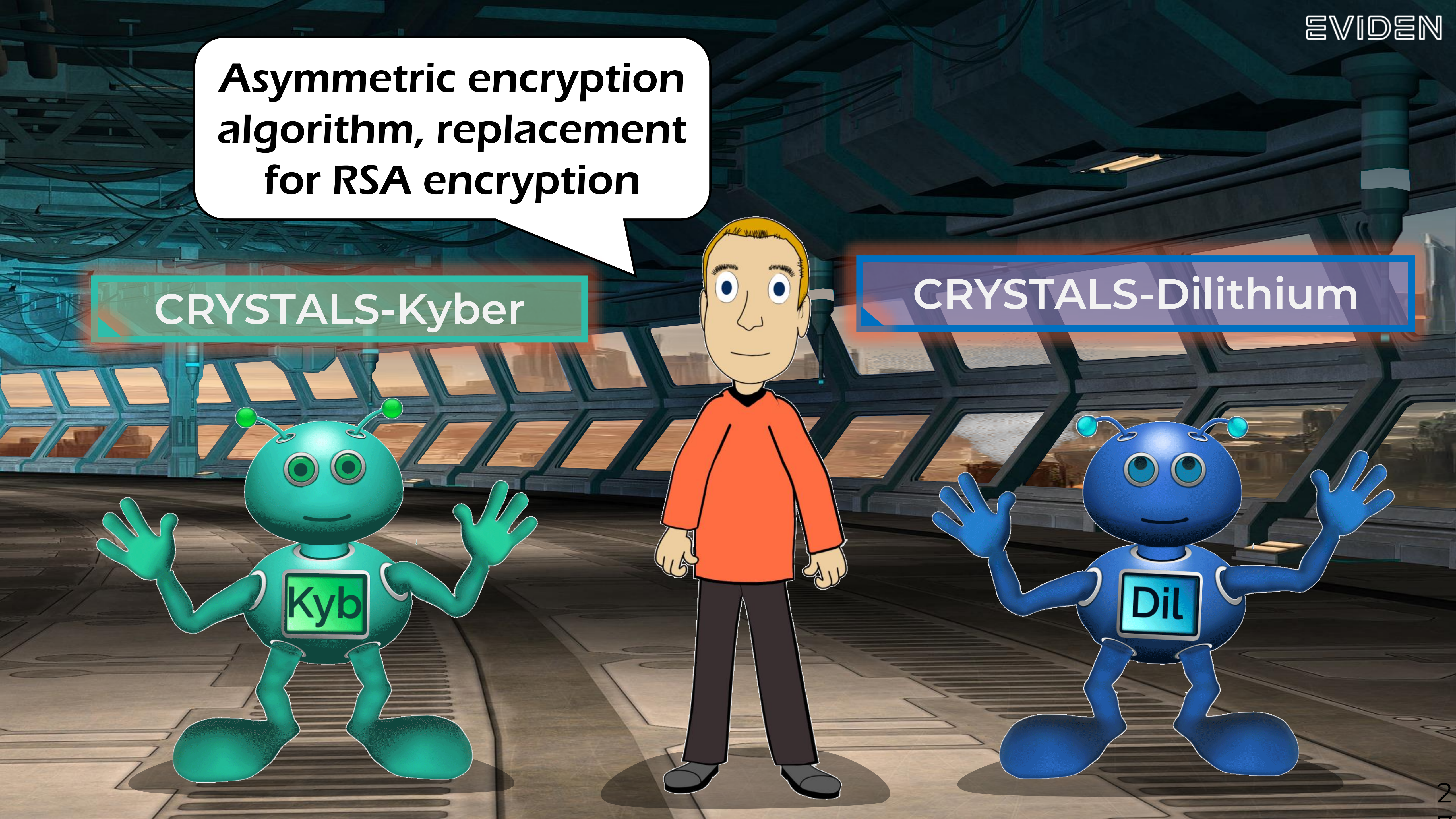
Leighton-Micali

Under evaluation

McEliece

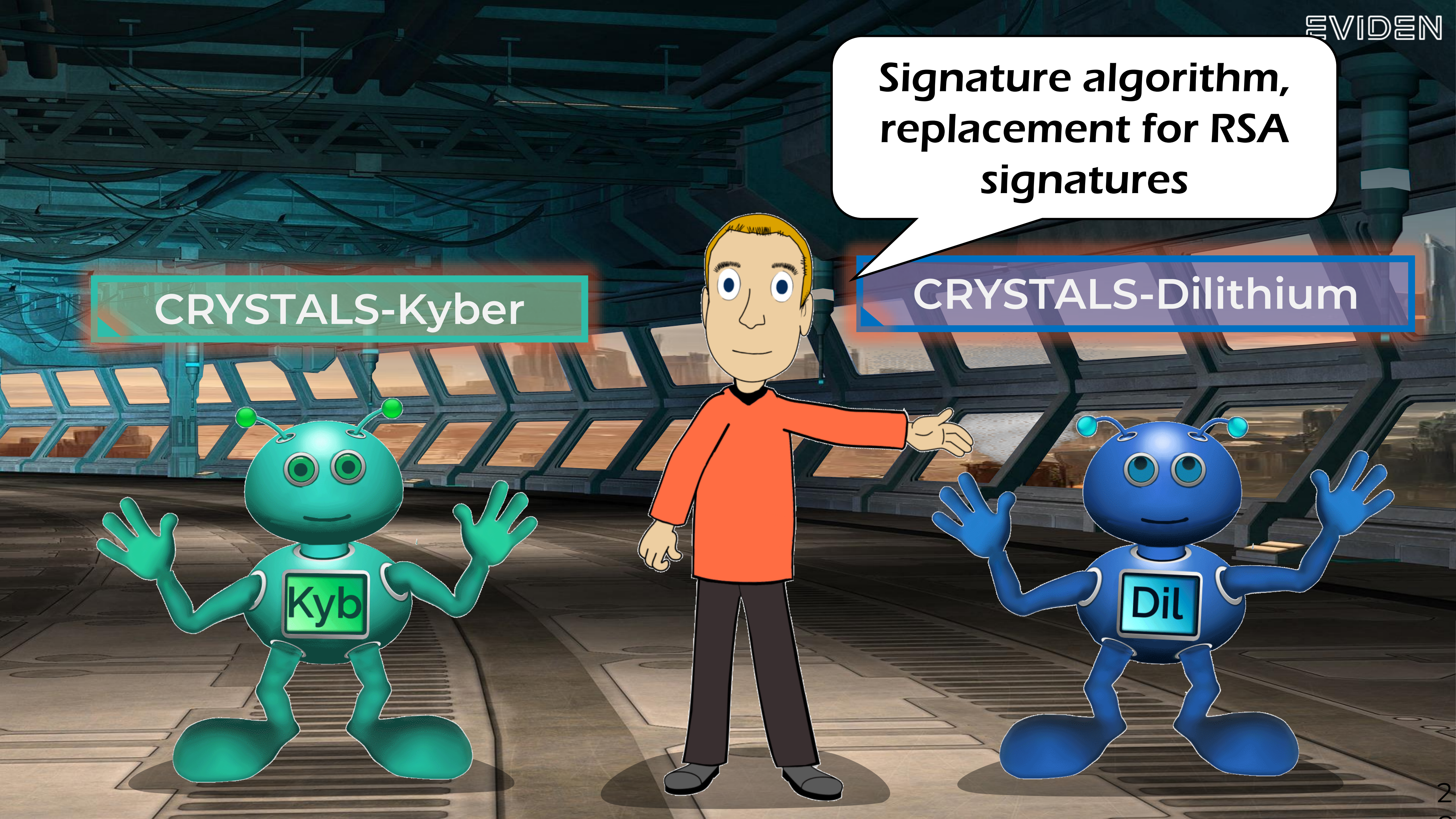
BIKE

HQC


Asymmetric encryption algorithm, replacement for RSA encryption
Kyb
Dil

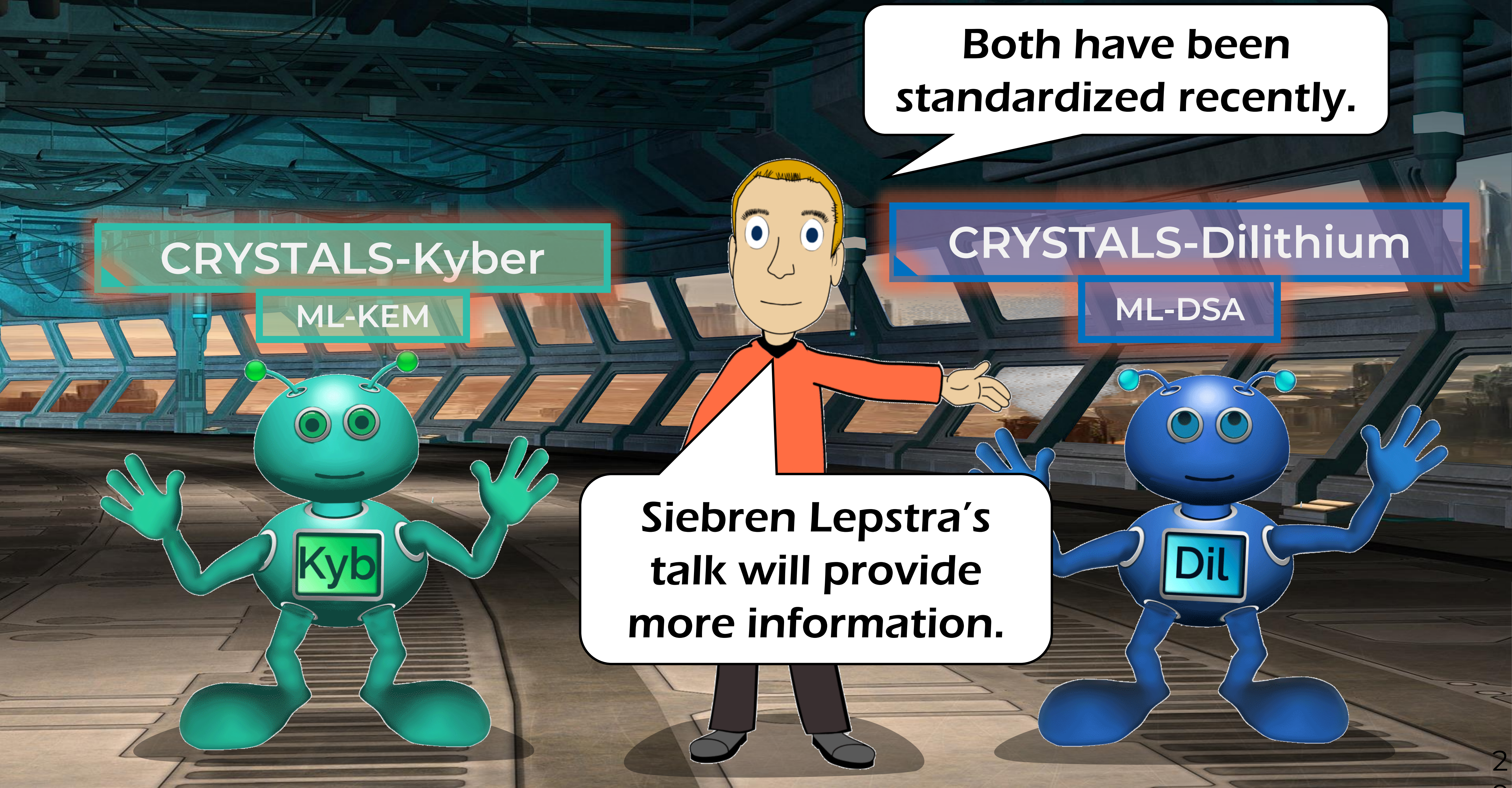
CRYSTALS-Kyber

CRYSTALS-Dilithium



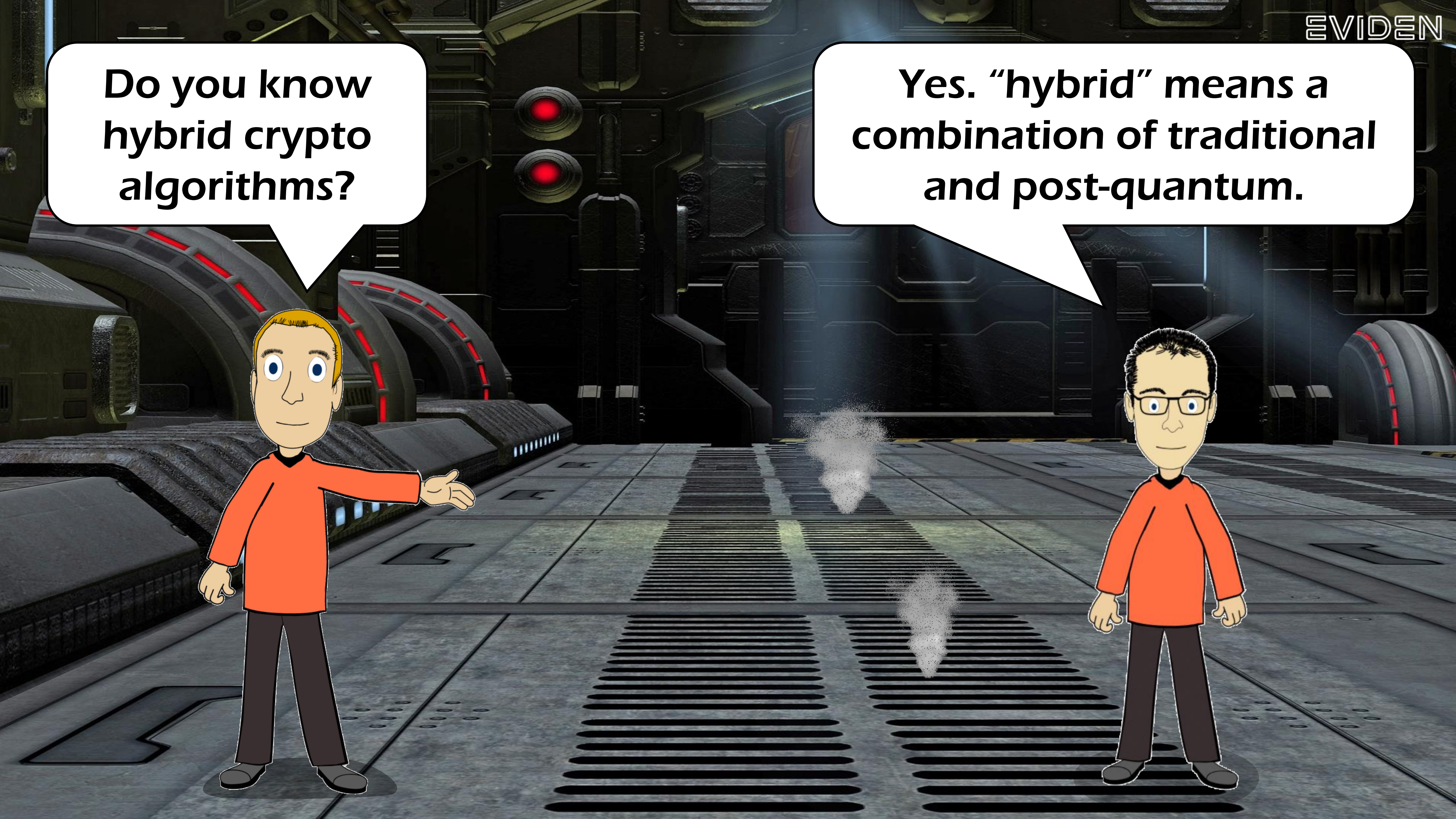
CRYSTALS-Kyber

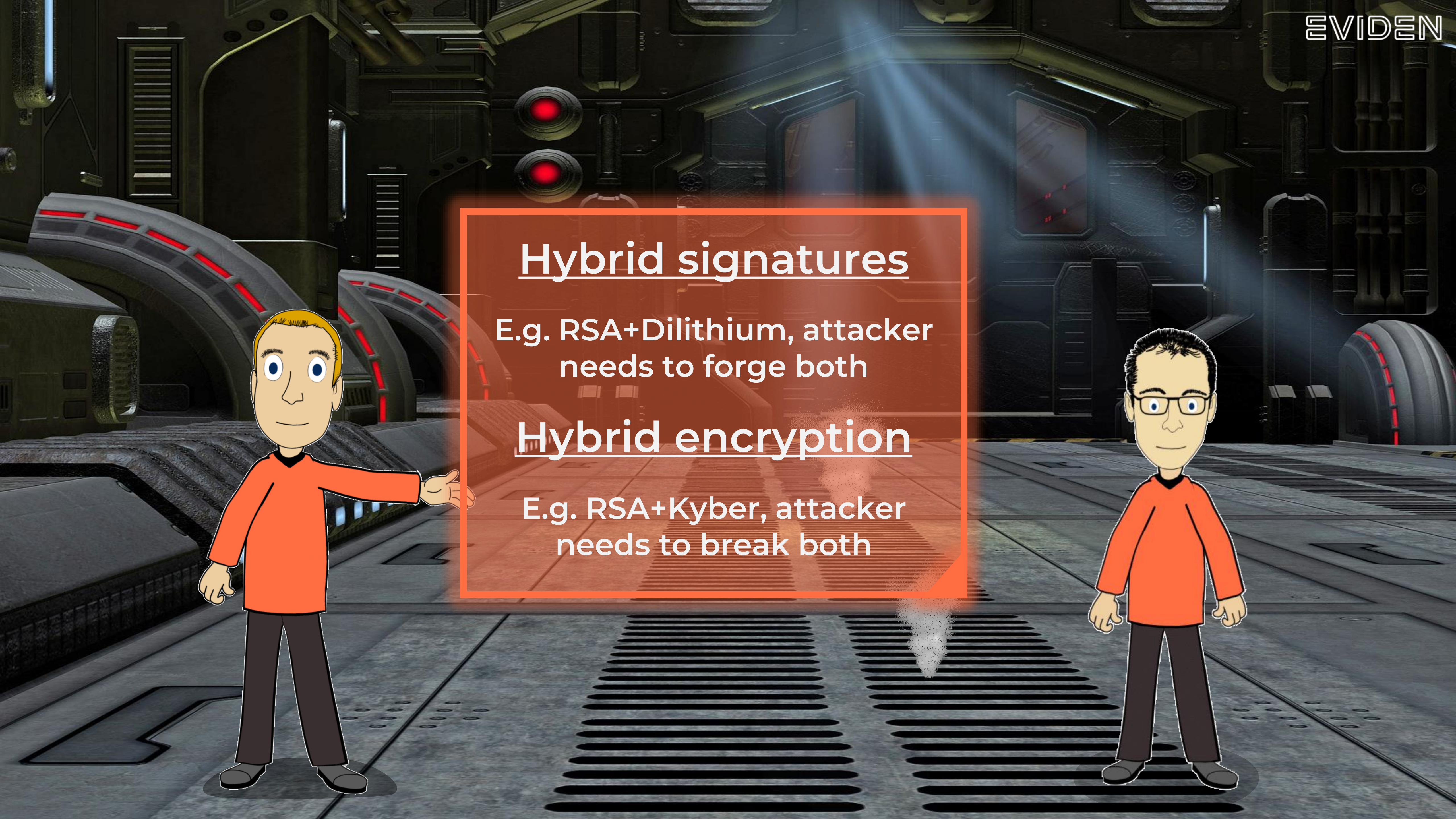
CRYSTALS-Dilithium



Both have been standardized recently.
CRYSTALS-Kyber
ML-KEM
CRYSTALS-Dilithium
ML-DSA
Siebren Lepstra's talk will provide more information.
Kyb
Dil

We need to put them into practice.
CRYSTALS-Kyber
ML-KEM
Kyb
CRYSTALS-Dilithium
ML-DSA
Dil


Do you know hybrid crypto algorithms?
Yes. “hybrid” means a combination of traditional and post-quantum.

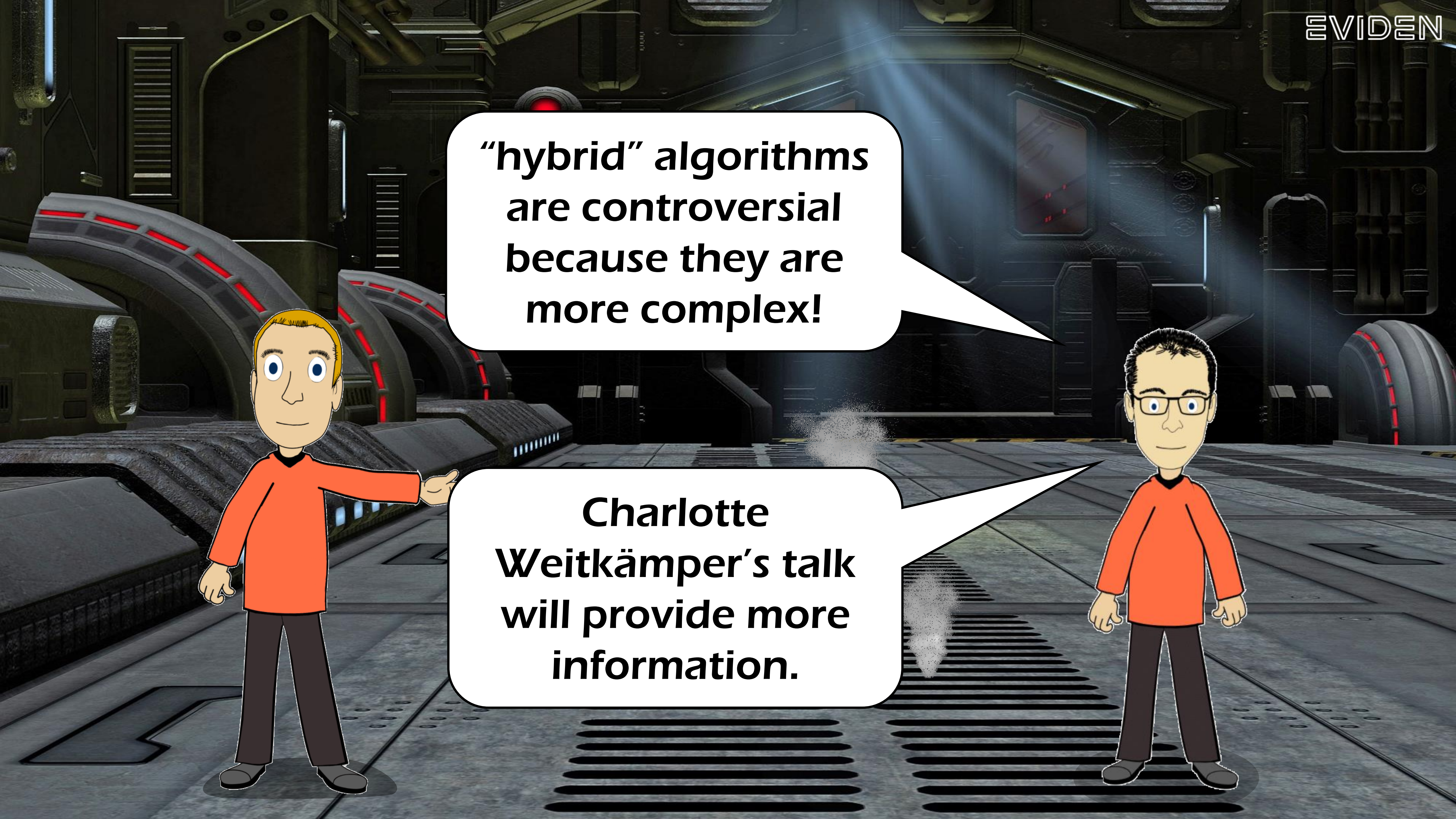


Hybrid signatures

E.g. RSA+Dilithium, attacker needs to forge both

Hybrid encryption

E.g. RSA+Kyber, attacker needs to break both


“hybrid” algorithms are controversial because they are more complex!
Charlotte Weitkämper’s talk will provide more information.

Agenda

Q-Day

Post-Quantum Cryptography

Post-Quantum Migration

Crypto Inventory

Migration Execution

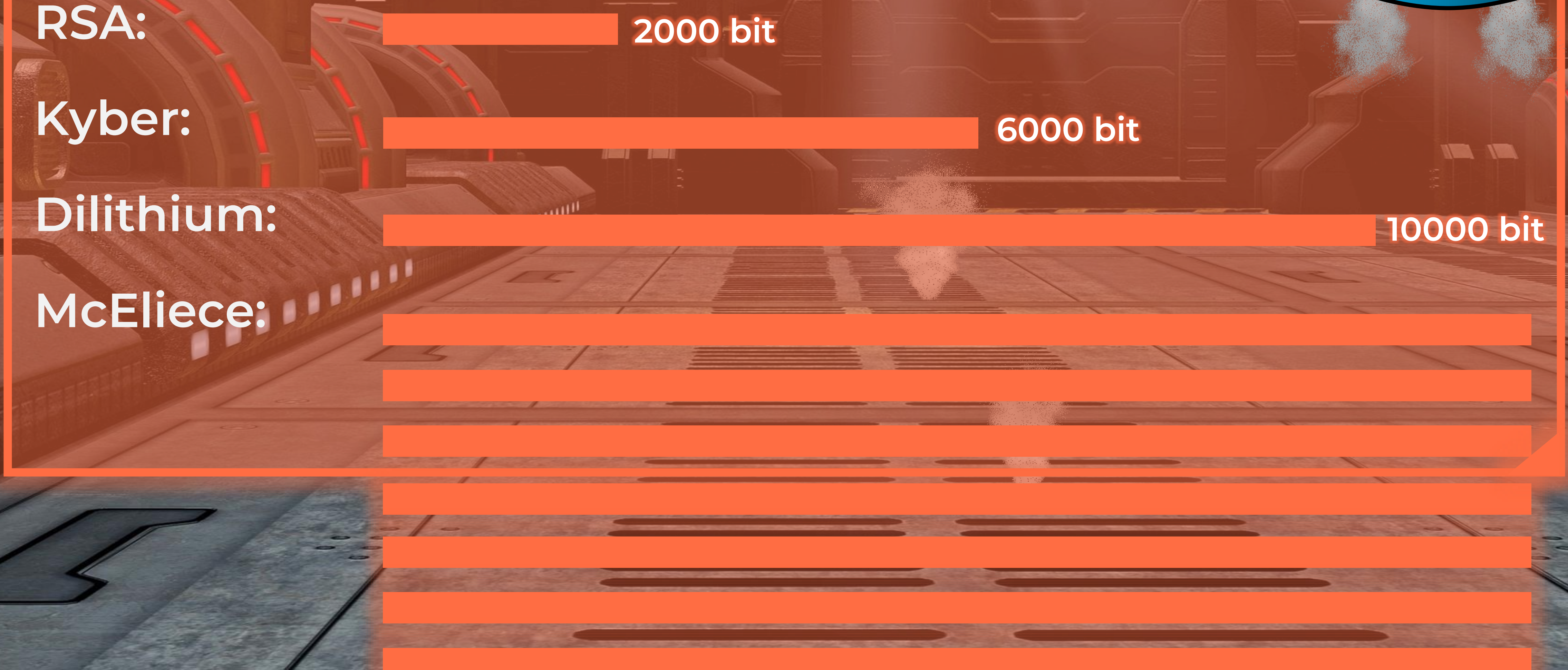
Conclusion

Crypto Agility

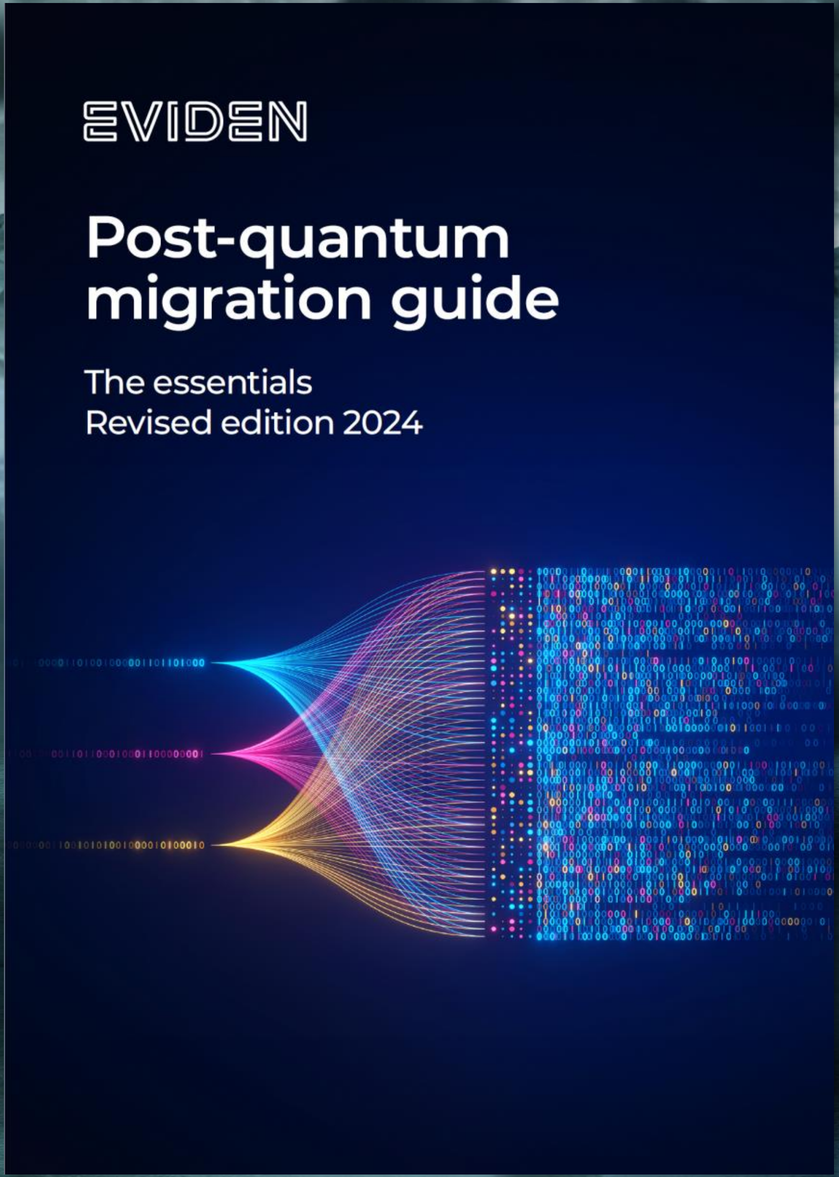
McEliece
Dilithium
Kyber
DH
RSA
Changing the crypto method shall be possible at mouseclick.
Long keys are a challenge.

Pul

In general, Post-quantum methods need more resources.


RSA:
2000 bit
Kyber:
6000 bit
Dilithium:
10000 bit
McEliece:

Crypto Agility

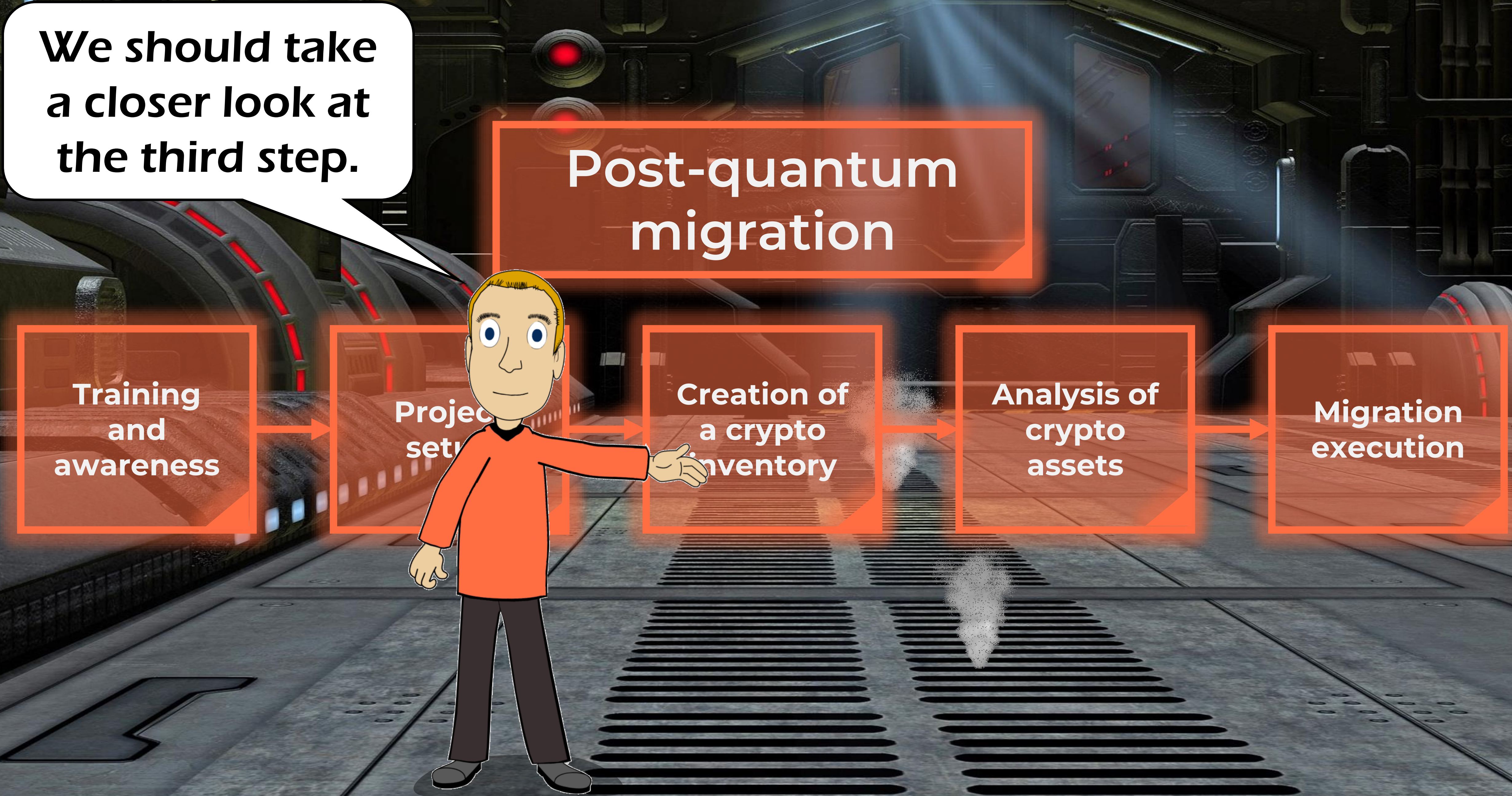


EVIDEN

Post-quantum migration guide

The essentials
Revised edition 2024

https://www.cryptovision.com/wp-content/uploads/2023/05/EVIDEN-PQC-Migration-Guide.pdf



Post-quantum migration

Training and awareness → Projec setu → Creation of a crypto inventory → Analysis of crypto assets → Migration execution

Agenda

Q-Day

Post-Quantum Cryptography

Post-Quantum Migration

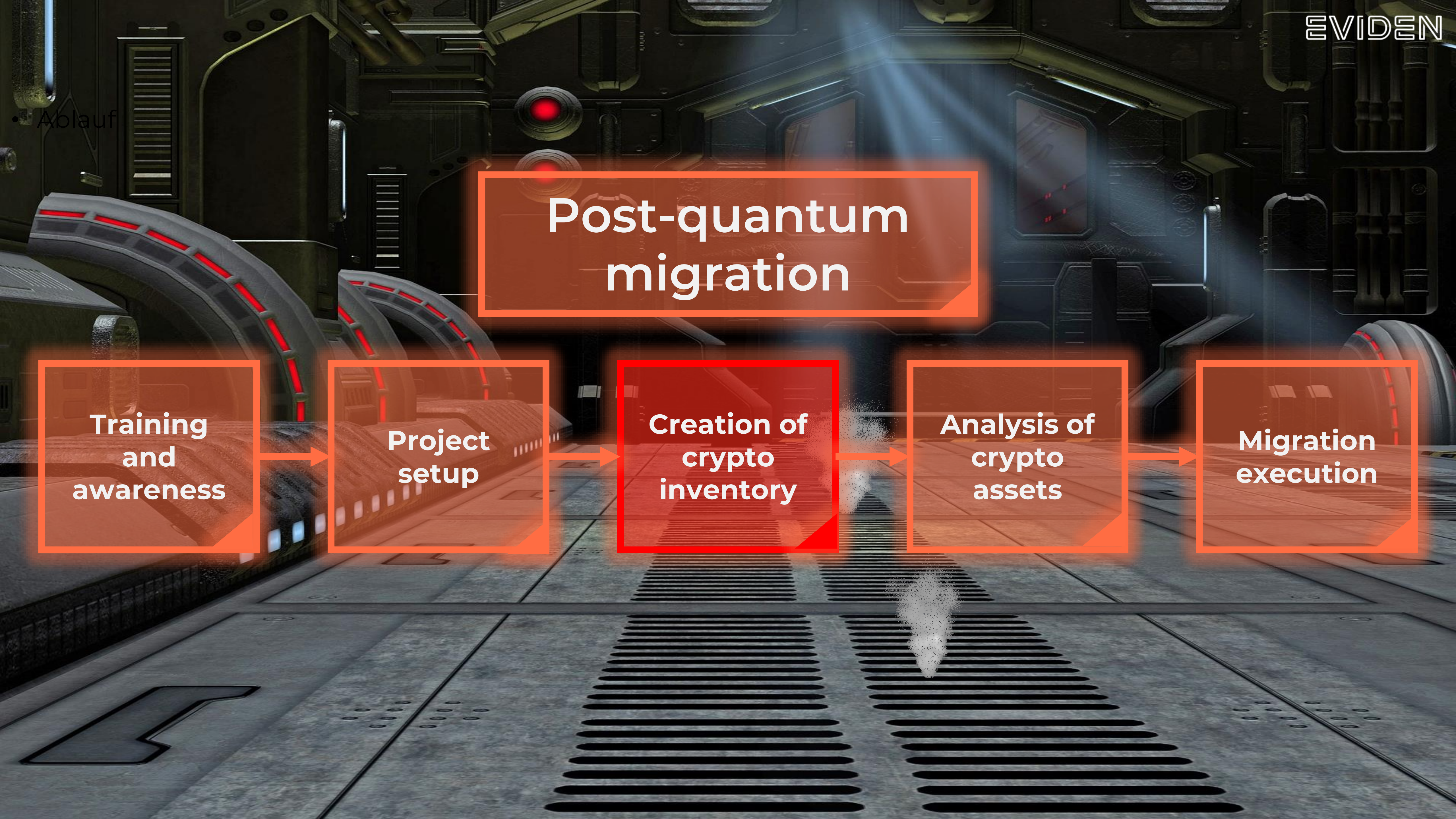
Crypto Inventory

Migration Execution

Conclusion

- Ablauf

Post-quantum migration



Training and awareness → Project setup → Creation of crypto inventory → Analysis of crypto assets → Migration execution

Crypto Inventory

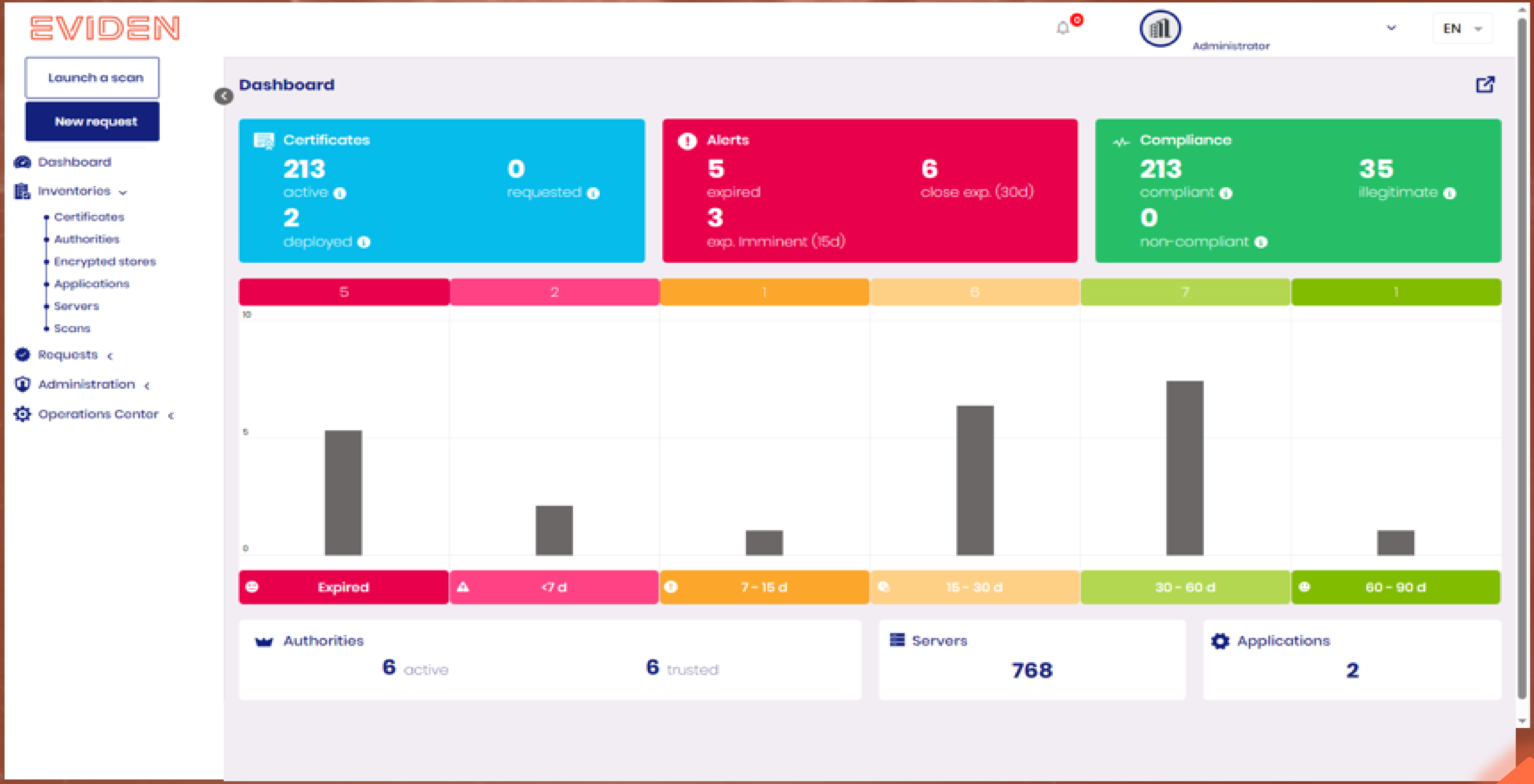
EVIDEN

ID	Field of application	Crypto solution	Crypto method	Status
259	Secure web access	Firefox TLS	AES-256 SHA-384 ECDH P-256	PQC-readiness plan
260	File encryption for USB drives	VeraCrypt	AES-256 SHA-512	PQC-ready
263	E-Mail encryption in controlling department	Outlook 2021 for Windows	AES-256 SHA-384 RSA-2048	PQC-readiness plan
264	E-Mail encryption in development department	Outlook 2021 for Windows	AES-256 SHA-384 RSA-2048	PQC-readiness plan
267	E-Mail crypto gateway	ABC Secure Mail Gate	AES-256 SHA-384 RSA-2048	PQC-readiness plan
269	VPN client	ABC VPN	AES-128 SHA-1 RSA-1024	PQC-option
270	E-mail signature	Mail-Sign	AES-256	PQC-readiness plan

Discover weak points

Increase visibility

Can this be automated?
Yes, there are tools.
EVIDEN
Launch a scan
New request
Dashboard
Inventories
Certificates
Authorities
Encrypted stores
Applications
Servers
Score
Requests
Administration
Operations Center
admin
Administrator
EN
Certificates
379 active
0 requested
0 deployed
Alerts
71 expired
18 close exp (30d)
18 exp imminent (5d)
Compliance
379 compliant
15 illegitimate
0 non-compliant
Expired
7 d
7 - 15 d
15 - 30 d
30 - 60 d
60 - 90 d
Authorities
0 active
20 trusted
Servers
726
Applications
0



Dashboard

Certificates
213 active
0 requested
2 deployed

Alerts
5 expired
6 close exp. (30d)
3 exp. imminent (15d)

Compliance
213 compliant
35 illegitimate
0 non-compliant

Expired	<7 d	7 - 15 d	15 - 30 d	30 - 60 d	60 - 90 d
5	2	1	6	7	1

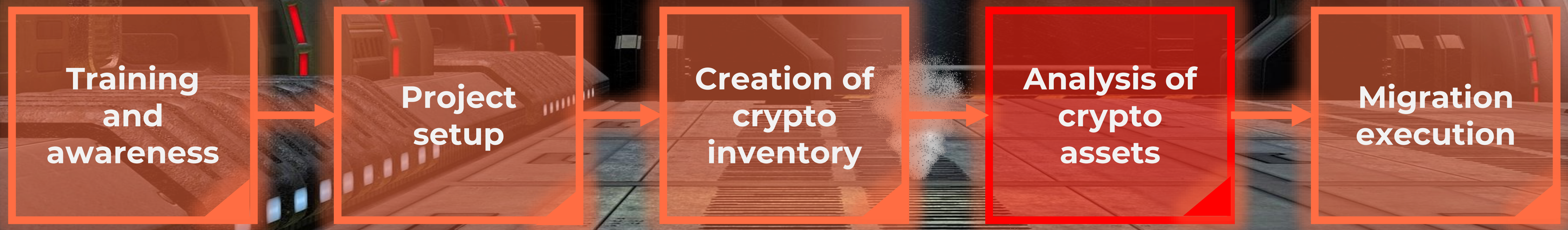
Authorities
6 active
6 trusted

Servers
768

Applications
2

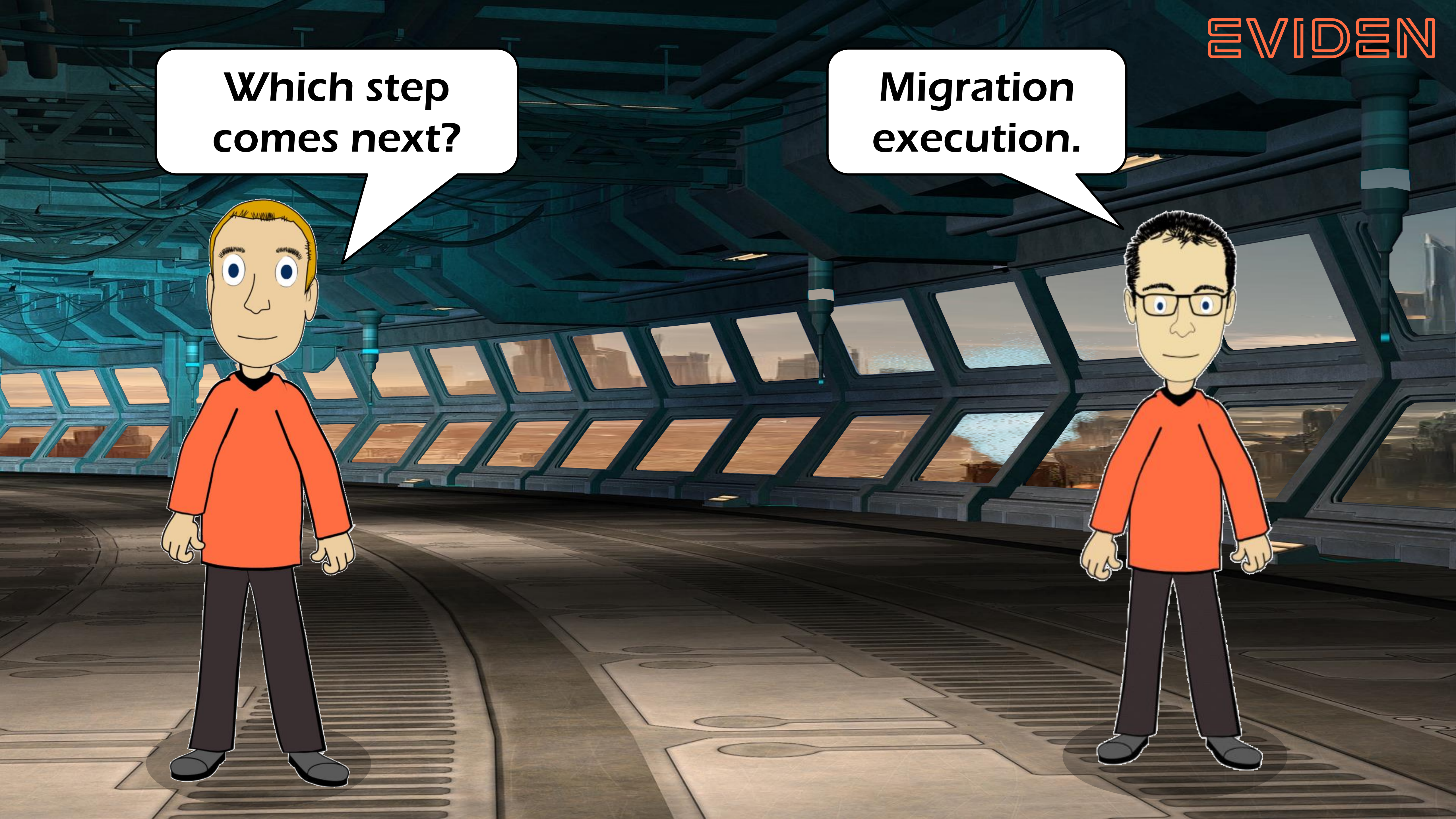
- Ablauf

Post-quantum migration



Training and awareness → Project setup → Creation of crypto inventory → Analysis of crypto assets → Migration execution

What do we do with an inventory?
Risk assessment and priorisation
Siebren's and Anastazija's talks will provide more information.


Which step comes next?
Migration execution.

Agenda

Q-Day

Post-Quantum Cryptography

Post-Quantum Migration

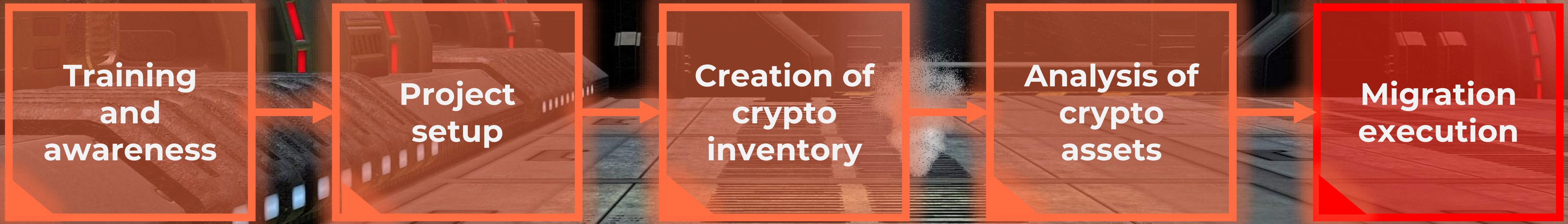
Crypto Inventory

Migration Execution

Conclusion

- Ablauf

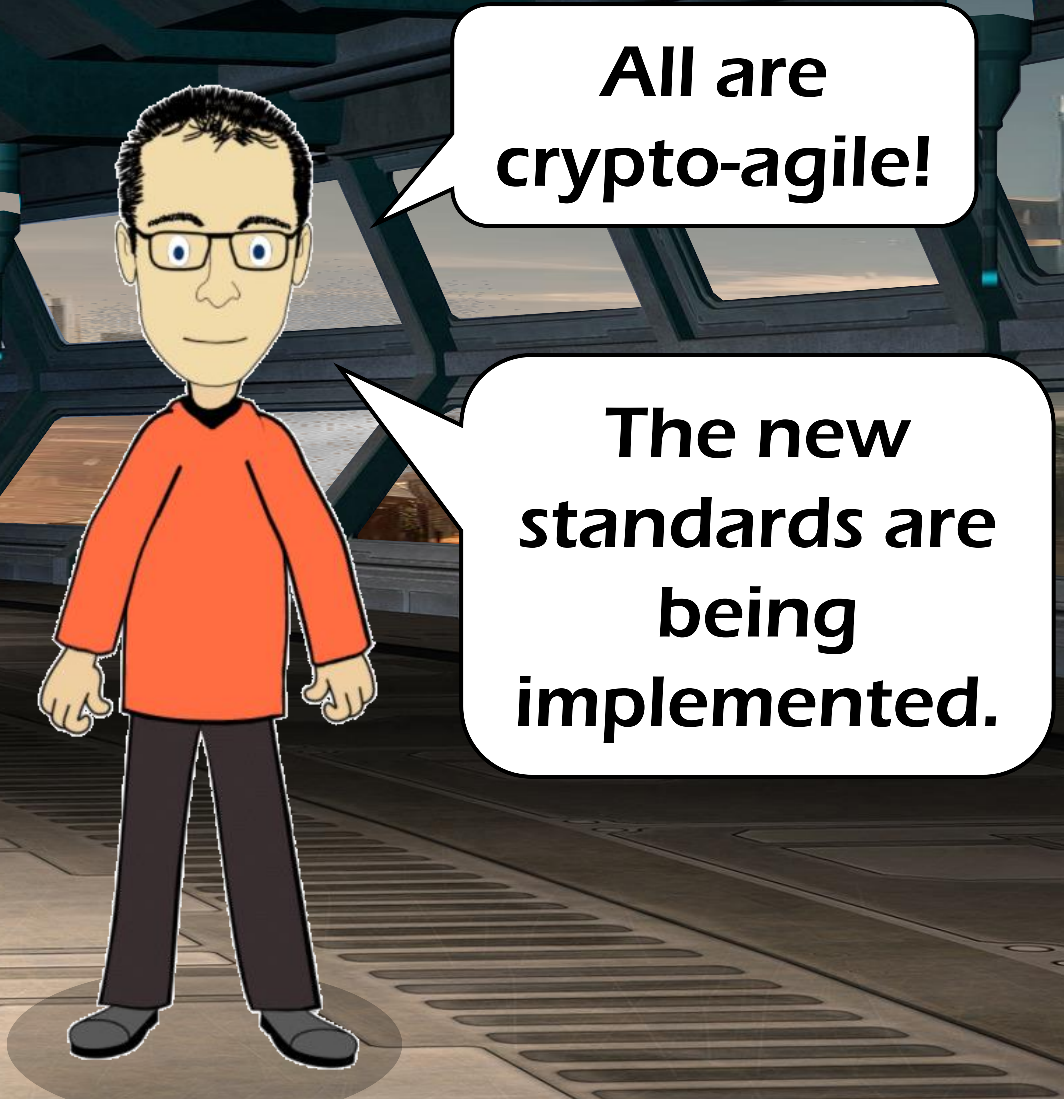
Post-quantum migration



Training and awareness → Project setup → Creation of crypto inventory → Analysis of crypto assets → Migration execution

Our products

- Mail/file encryption
- Digital signatures
- HSM crypto hardware
- Smart cards + tokens
- Credential Management System
- PKI + CLM



Our products

Mail/file encryption

Digital signatures

HSM crypto hardware

Smart cards + tokens

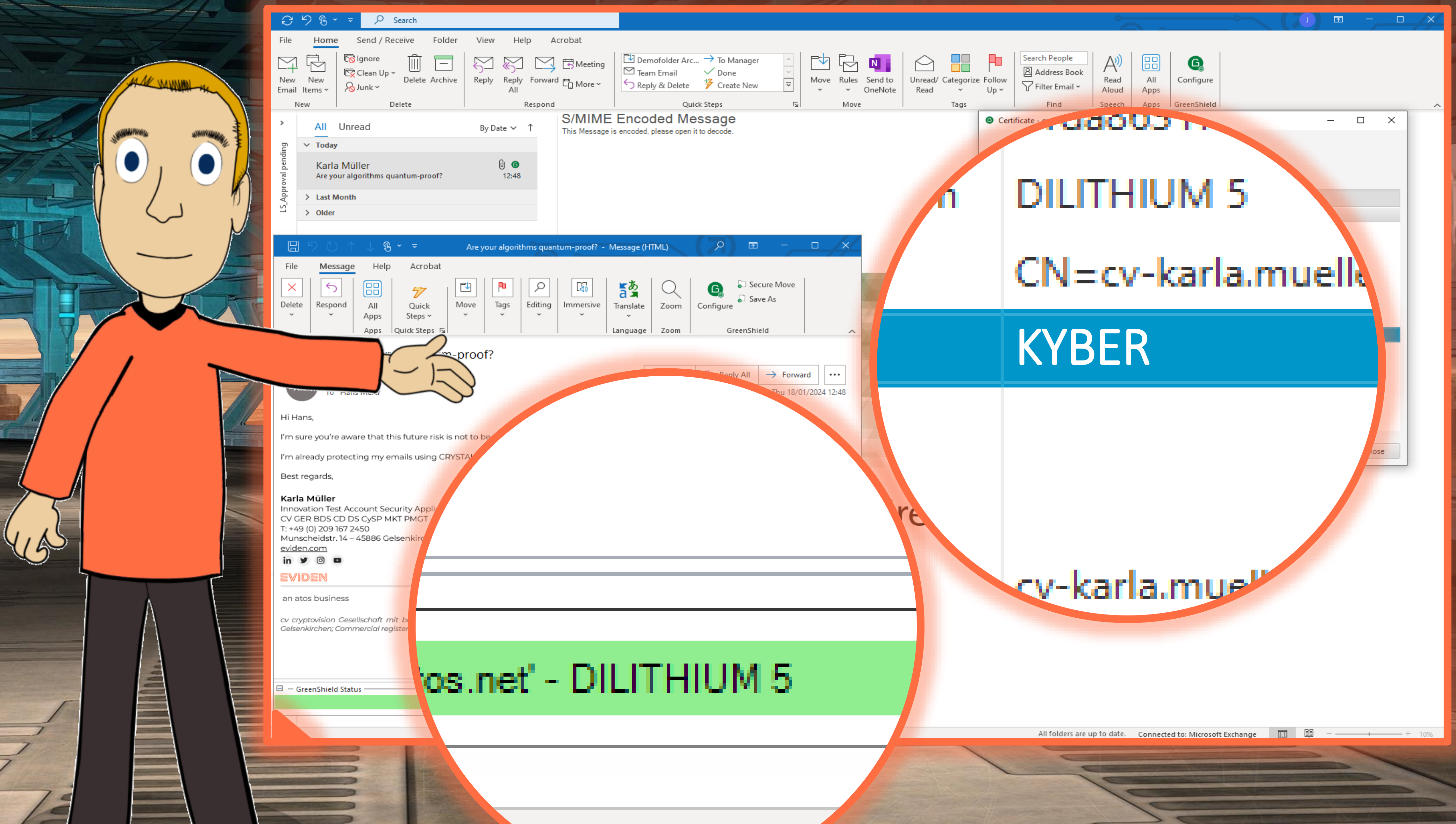
Credential Management System

PKI + CLM

cryptovision GreenShield

Mail/file encryption/ signature

EVIDEN



S/MIME Encoded Message

This Message is encoded, please open it to decode.

Karla Müller
Are your algorithms quantum-proof?
12:48

Are your algorithms quantum-proof? - Message (HTML)

Thu 18/01/2024 12:48

Hi Hans,

I'm sure you're aware that this future risk is not to be

I'm already protecting my emails using CRYSTA

Best regards,

Karla Müller
Innovation Test Account Security Appli
CV GER BDS CD DS CySP MKT PMGT
T: +49 (0) 209 167 2450
Munscheidstr. 14 – 45886 Gelsenkir
eviden.com

EVIDEN

an atos business

cv cryptovision Gesellschaft mit b
Gelsenkirchen; Commercial register

GreenShield Status

tos.net' - DILITHIUM 5

Certificate

DILITHIUM 5

CN=cv-karla.muell

KYBER

cv-karla.muell

All folders are up to date. Connected to: Microsoft Exchange

Agenda

Q-Day

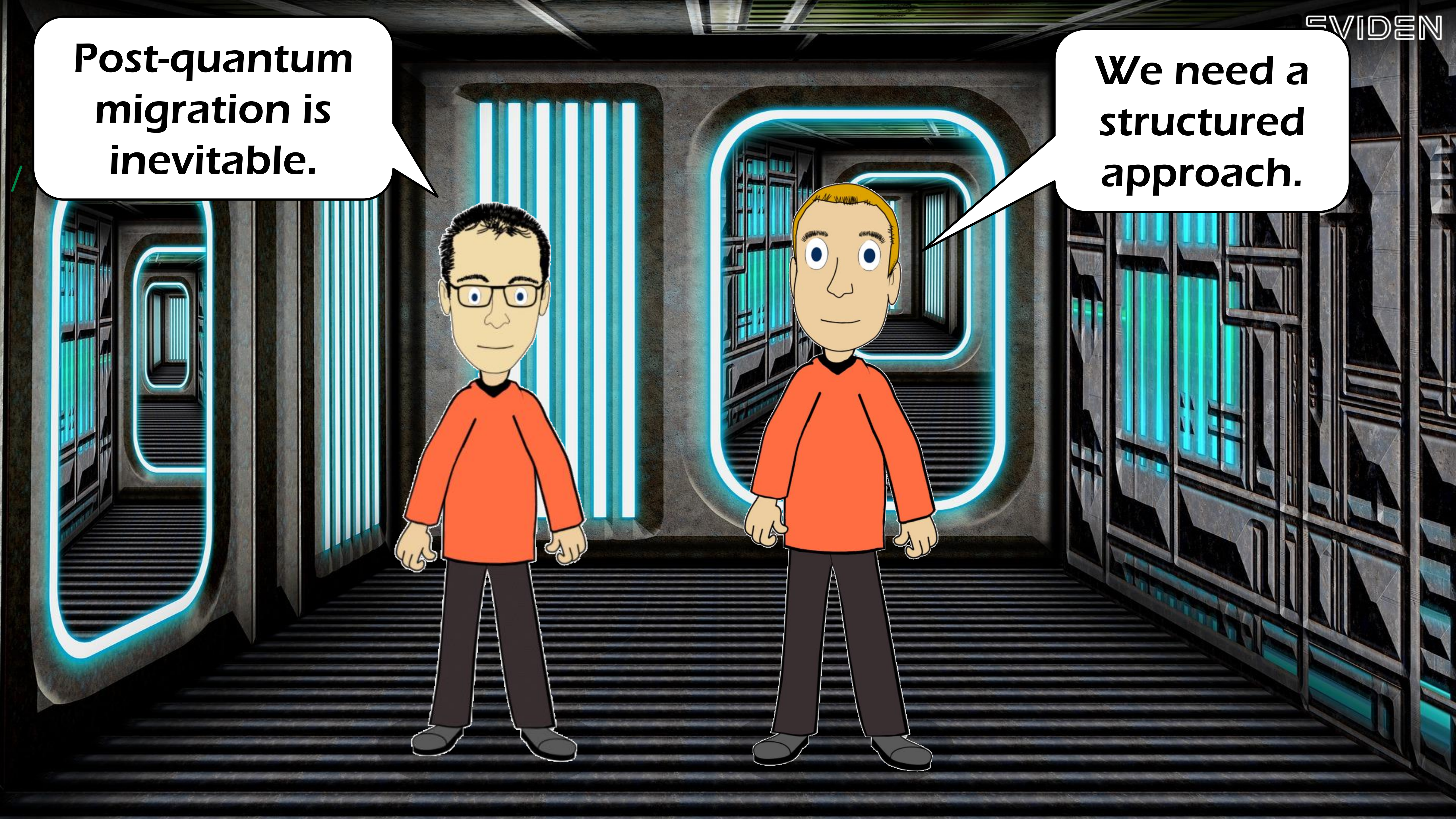
Post-Quantum Cryptography

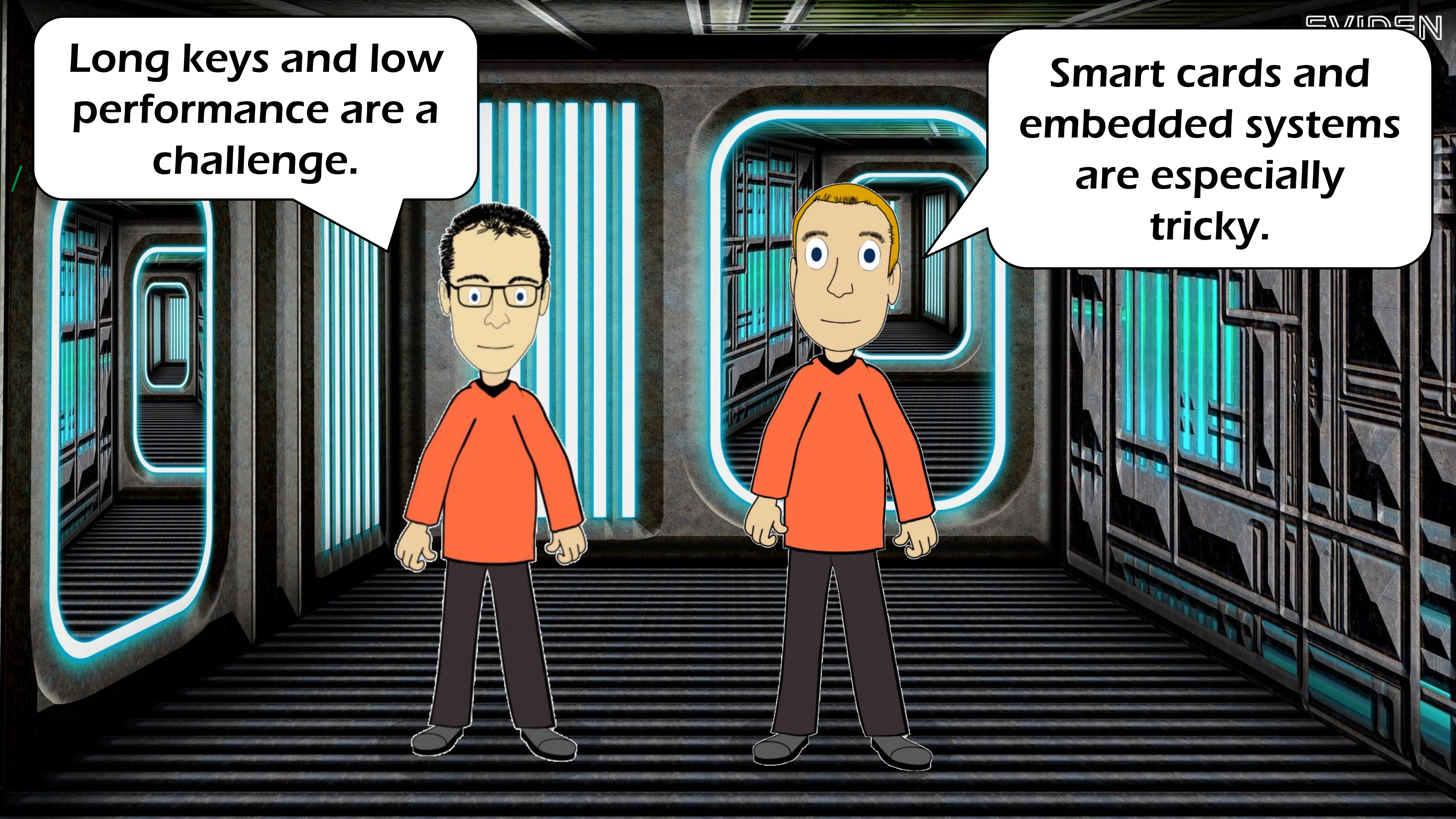
Post-Quantum Migration

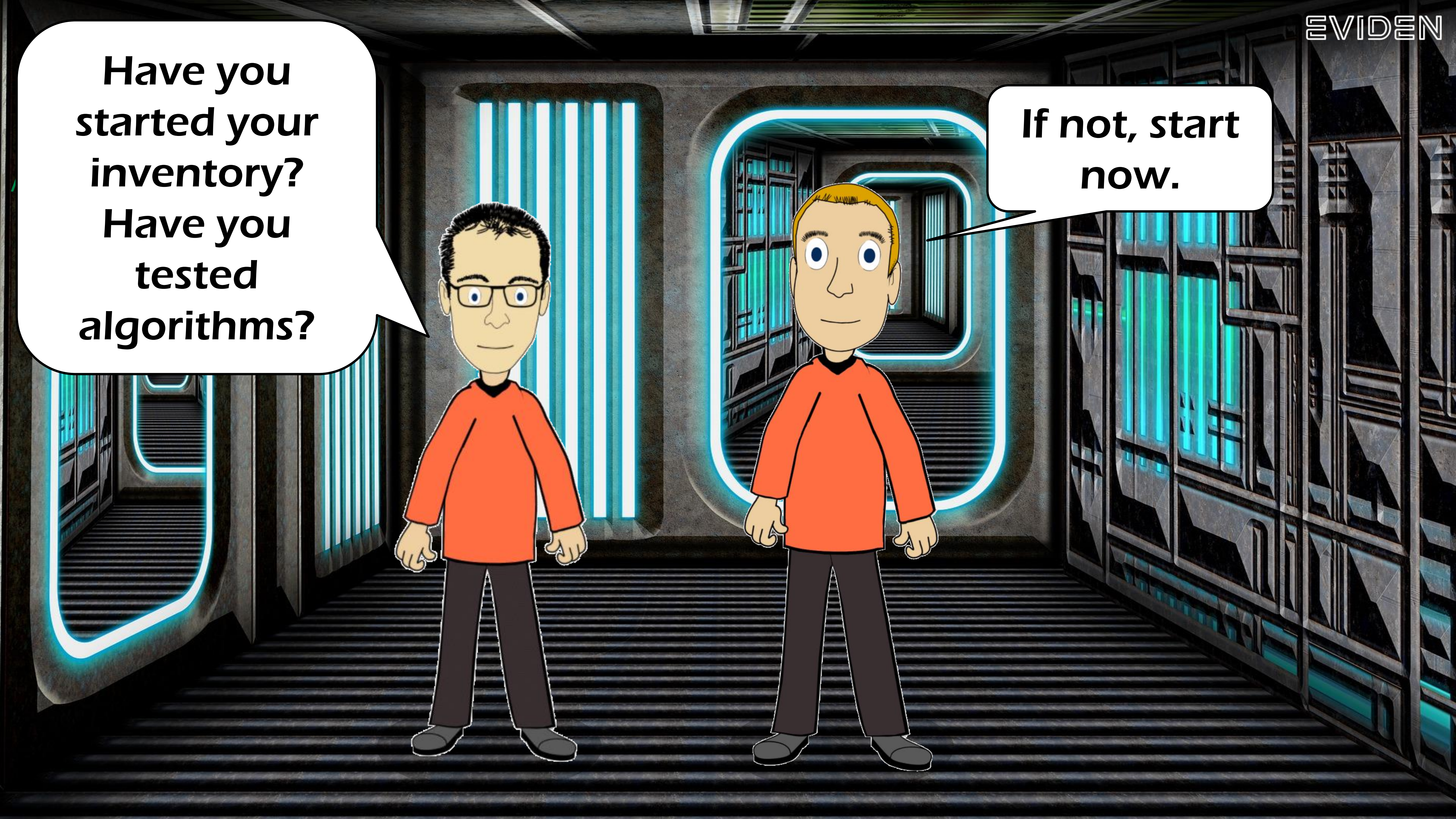
Crypto Inventory

Migration Execution

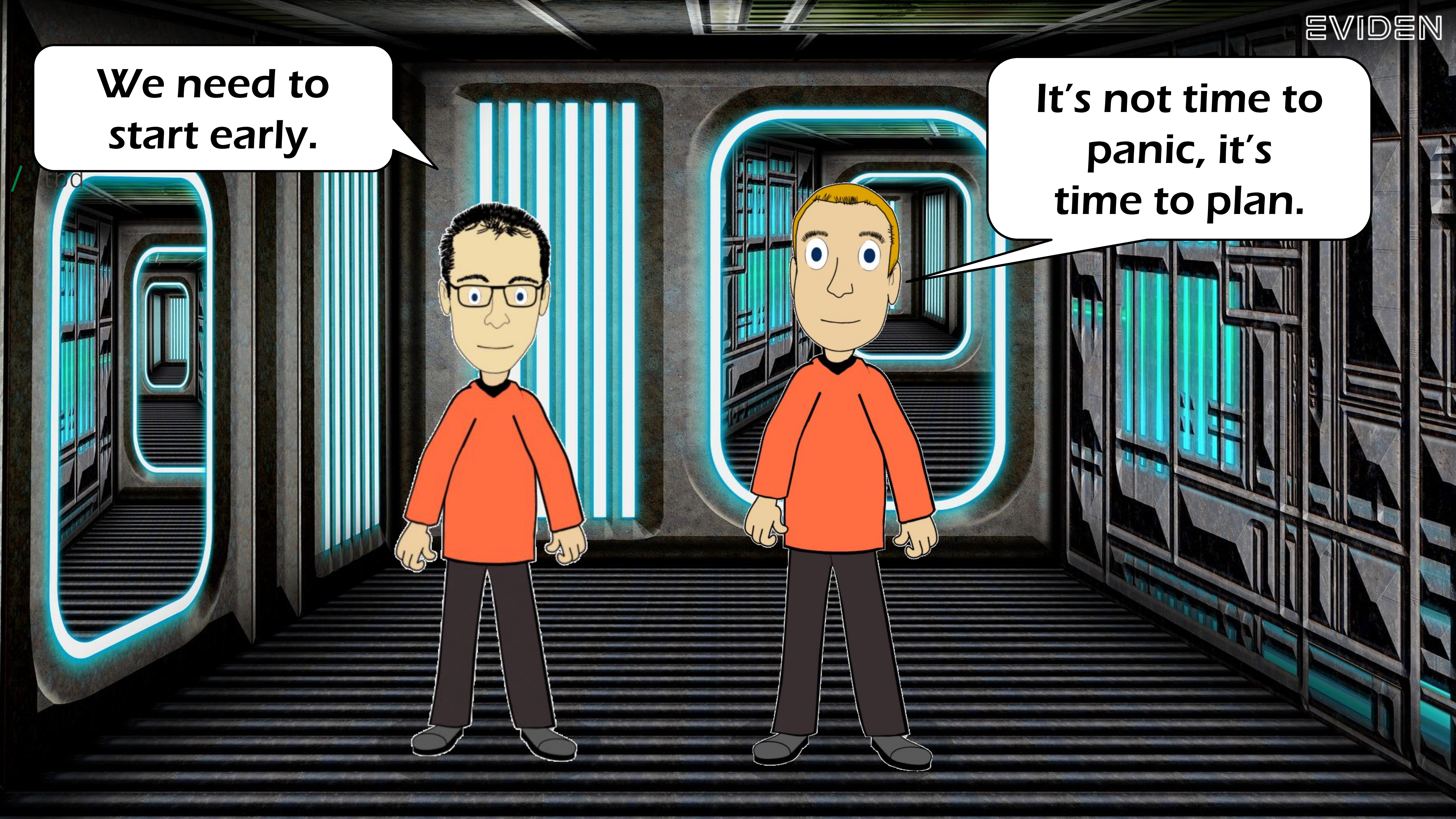
Conclusion


Post-quantum migration is inevitable.
We need a structured approach.


Long keys and low performance are a challenge.
Smart cards and embedded systems are especially tricky.


Have you started your inventory? Have you tested algorithms?
If not, start now.

/ tbd



END

TAKE A MINUTE AND GIVE US FEEDBACK ...

RATE NOW!

All Together

How to make a cat look like guacamole – Attacks on Artificial Intelligence

Ground Floor // Konferenzsaal - Pavillo...

Klaus Schmeh

● Speaker ● Host

Artificial Intelligence (AI) tools, such as ChatGPT or Bard, have become important aids for every IT user. However, there are powerful techniques to attack systems of this kind, including AI poisoning, adversarial patterns, AI jailbreaking, and image cloaking. This presentation gives an overview of these concepts in an entertaining wa