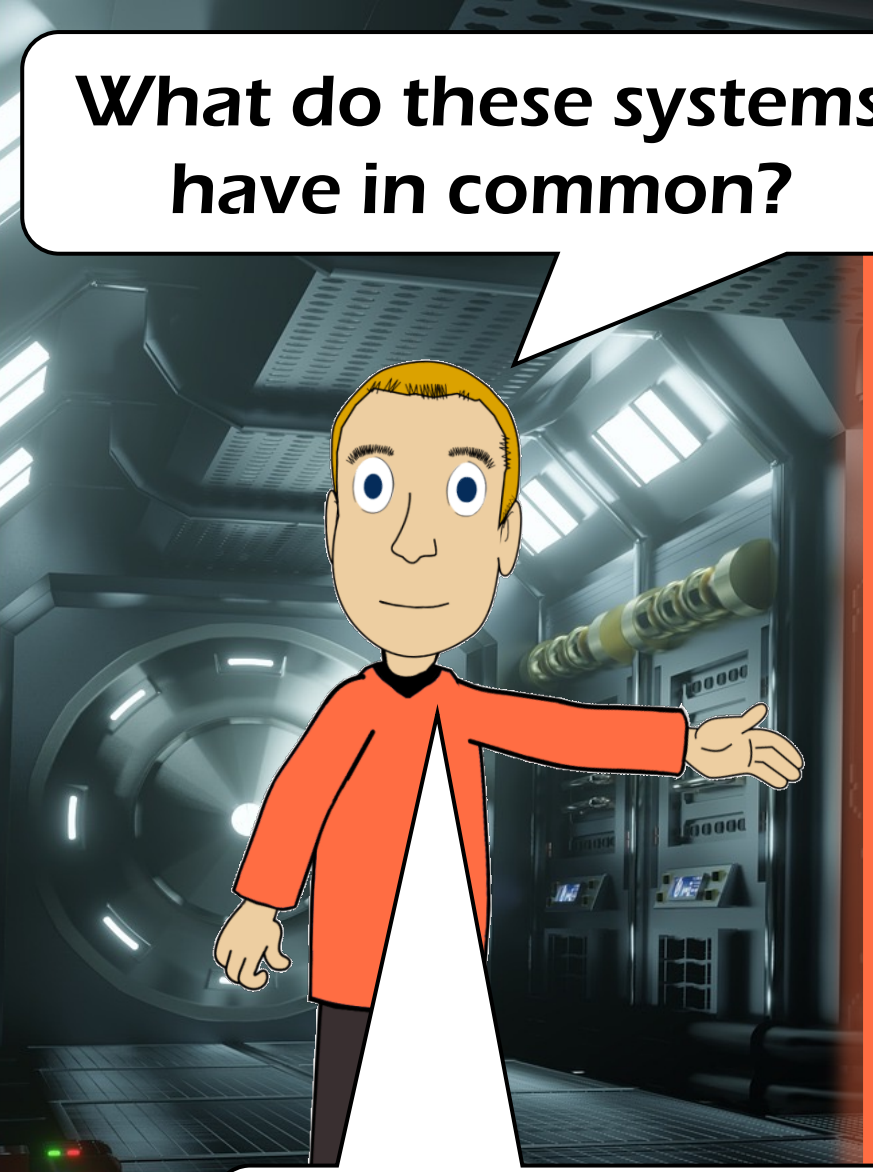
EVIDEN
an atos business

Implementing Post-Quantum Crypto Algorithms on Smart-Card Chips

Klaus Schmeh
Eviden Digital Identity

What do these systems have in common?



They use the RSA crypto system.

Smart-phone

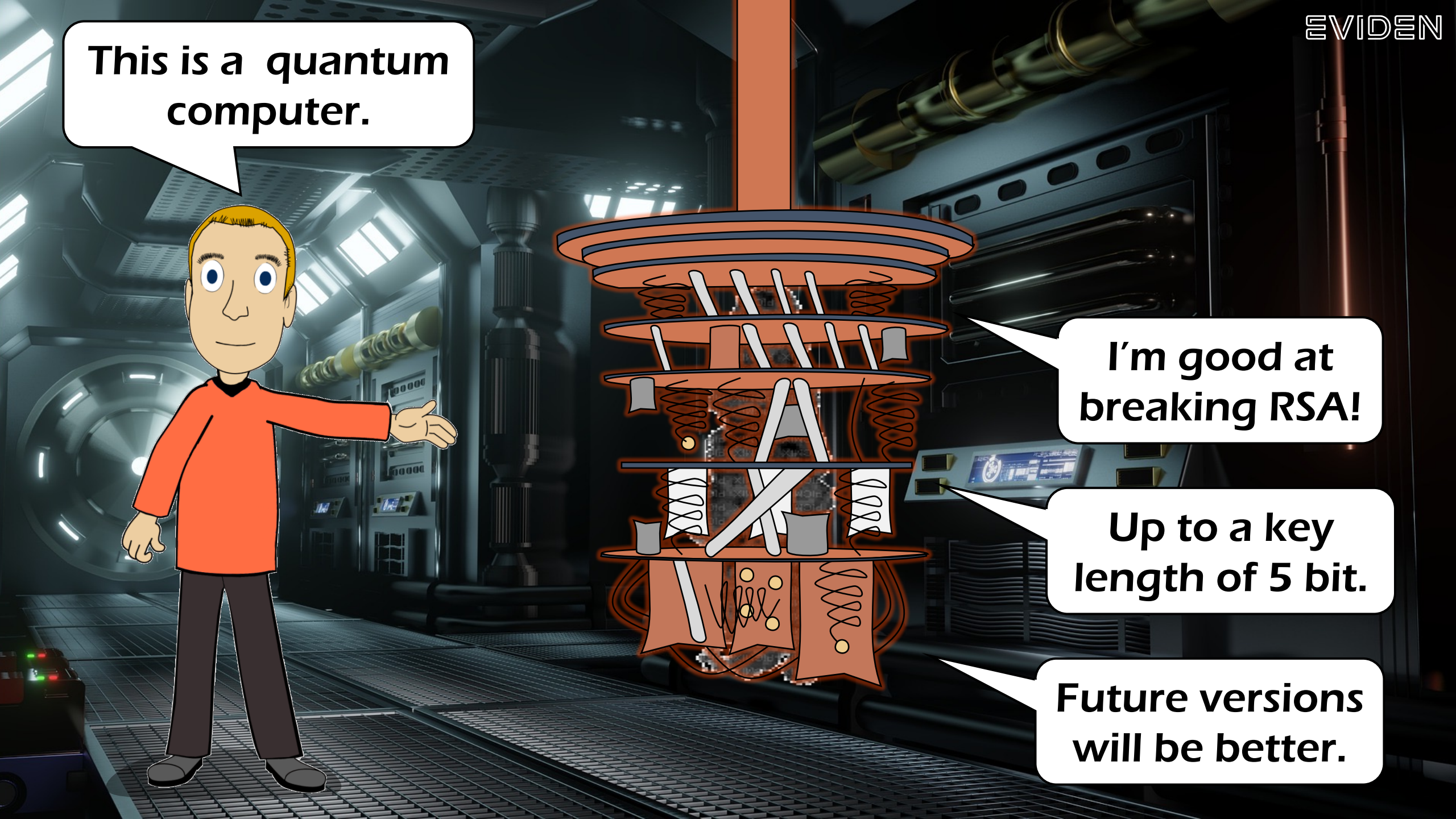
eID card

ATM

Web browser

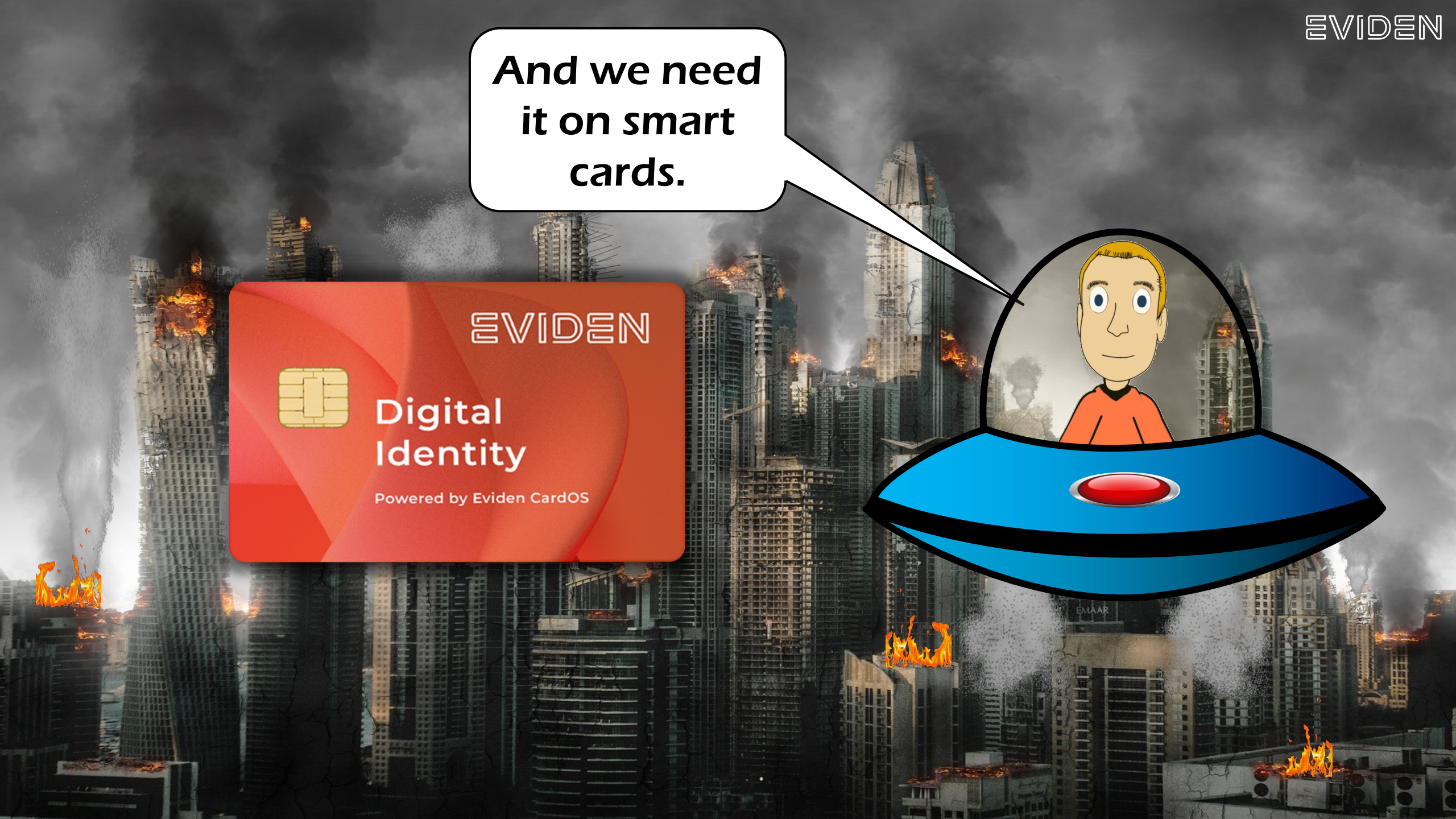
Operating system

Email client

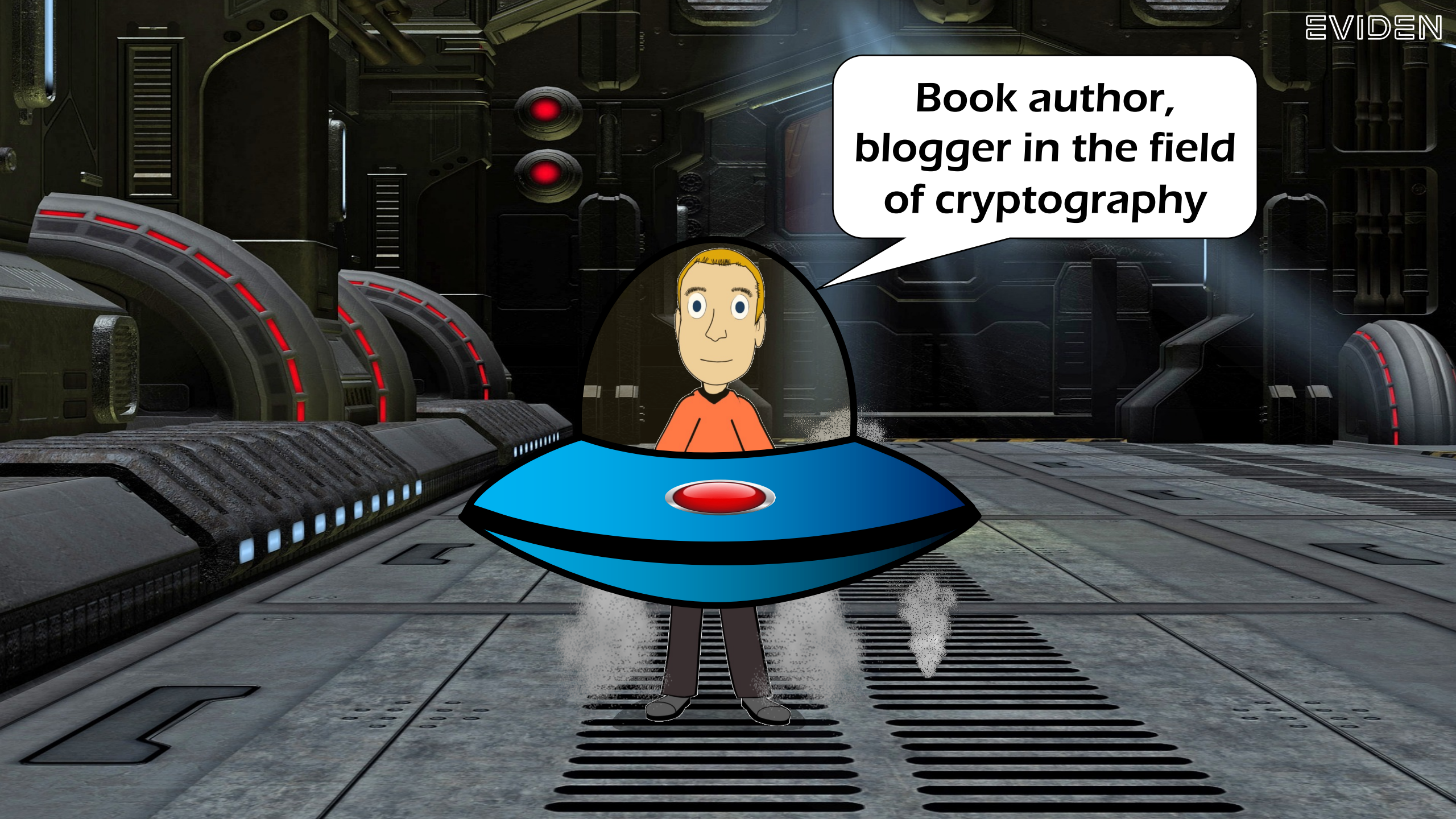

This is a quantum computer.
I'm good at breaking RSA!
Up to a key length of 5 bit.
Future versions will be better.

A disaster threatens!

We need post-quantum cryptography

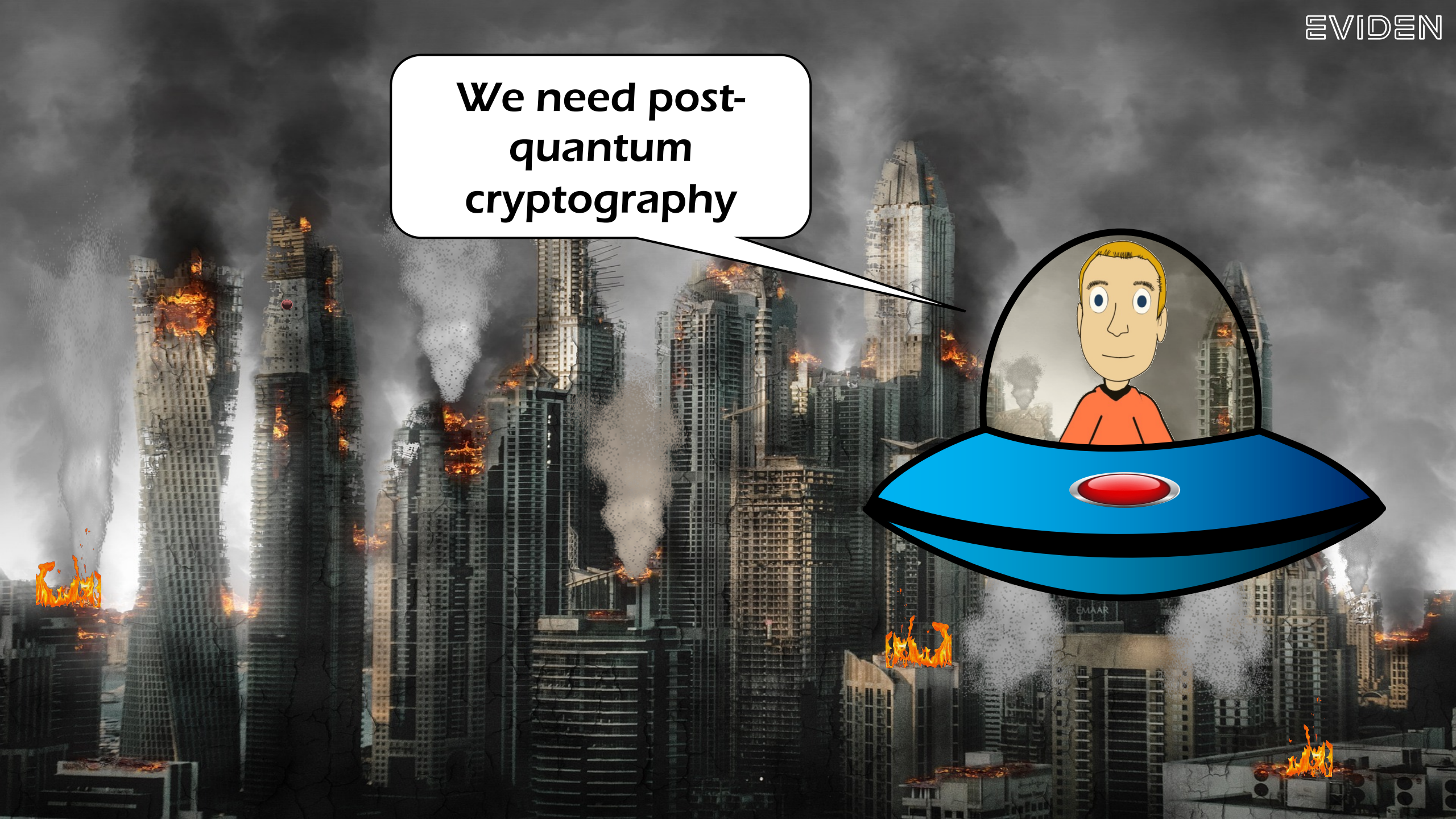

EVIDEN
And we need it on smart cards.
EVIDEN
Digital Identity
Powered by Eviden CardOS


Klaus Schmeh,
Marketing Editor at
Eviden Digital Identity.
EVIDEN


Book author, blogger in the field of cryptography


My books
Kryptografie
Klaus Schmeh
Codeknacker gegen Codemacher
Die faszinierende Geschichte der Verschlüsselung
3. Auflage
Kryptografie
Die Enigma
ELEKTRONISCHE AUSWEIS-DOKUMENTE
TELEPOLIS
Versteckte Botschaften
Die faszinierende Geschichte der Steganografie
Cryptography and Public Key Infrastructure on the Internet
Kryptografie
und Public-Key-Infrastrukturen im Internet
Safer Net
CODEBREAKING
A Practical Guide
ELONKA DUNIN & KLAUS SCHMEH
VERSUTUS
Das größte Genie seiner Zeit
Die Wahrheit wird überbewertet
Klaus Schmeh
NICHT ZU KNACKEN
Von ungelösten Enigma-Codes zu den Briefen des Zodiac-Killers
HANSER
Klaus Schmeh
Chief Security Officer
BISHER IST IMMER ALLES IRGENDWIE GUTGEGANGEN
Klaus Schmeh
Codeknacker gegen Codemacher
Die faszinierende Geschichte der Verschlüsselung
2. Auflage
Kryptografie
Klaus Schmeh
Codeknacker gegen Codemacher
Die faszinierende Geschichte der Verschlüsselung
CODEBREAKING
A PRACTICAL GUIDE
ELONKA DUNIN & KLAUS SCHMEH
Kryptografie
Klaus Schmeh
Die Welt der geheimen Zeichen
Die faszinierende Geschichte der Verschlüsselung
TELEPOLIS
Versteckte Botschafte
Die faszinierende Geschichte der Steganografie


EVIDEN
Eviden Digital Identity: Home of cryptovision and IDnomic solutions.
Secure electronic identities, user-friendly encryption.


We need post-quantum cryptography
EMAAR

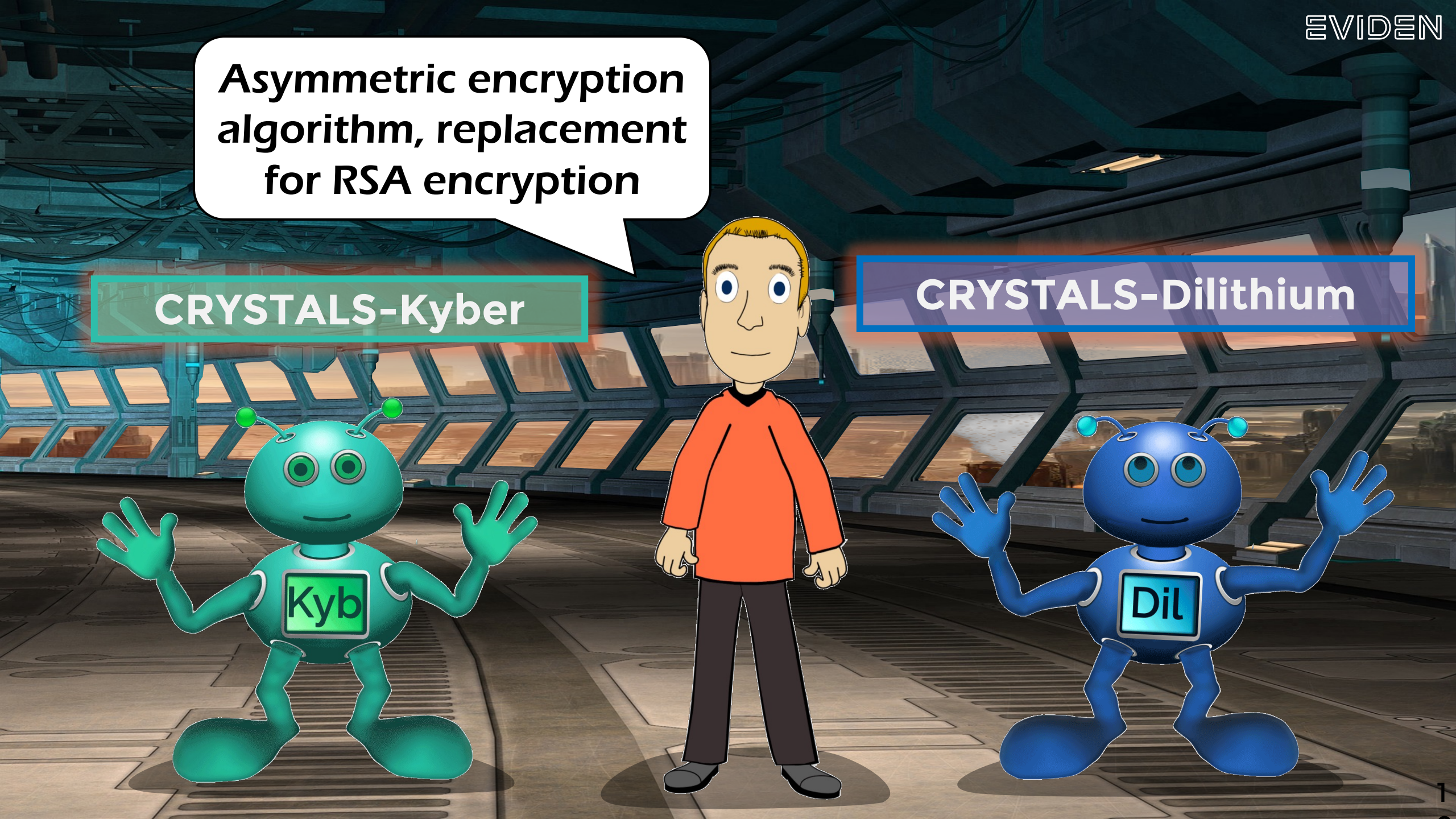
Post-Quantum algorithms

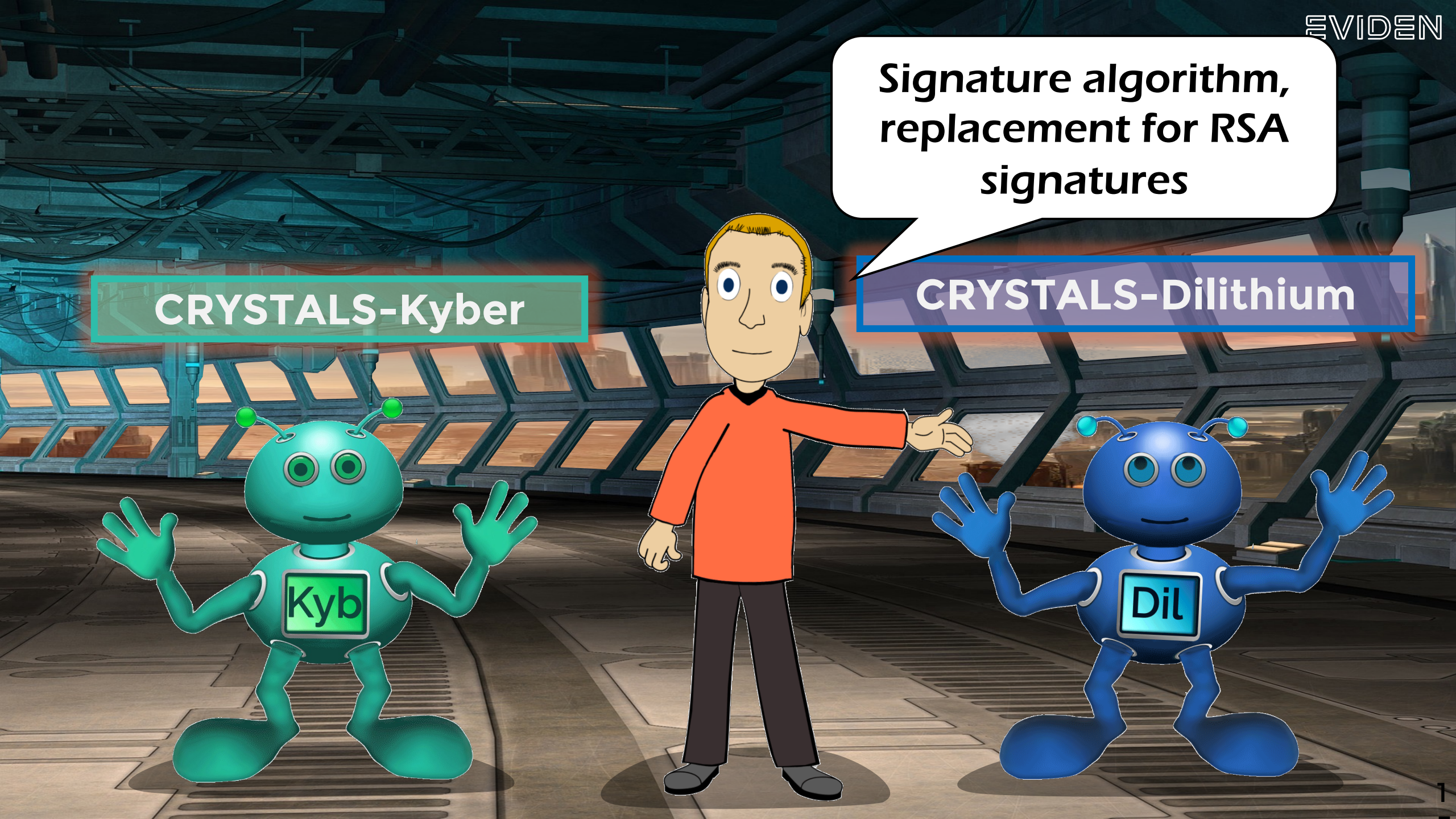
Current algorithms

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- FALCON
- SPHINCS+
- FrodoKEM
- XMSS
- Leighton-Micali

Under evaluation

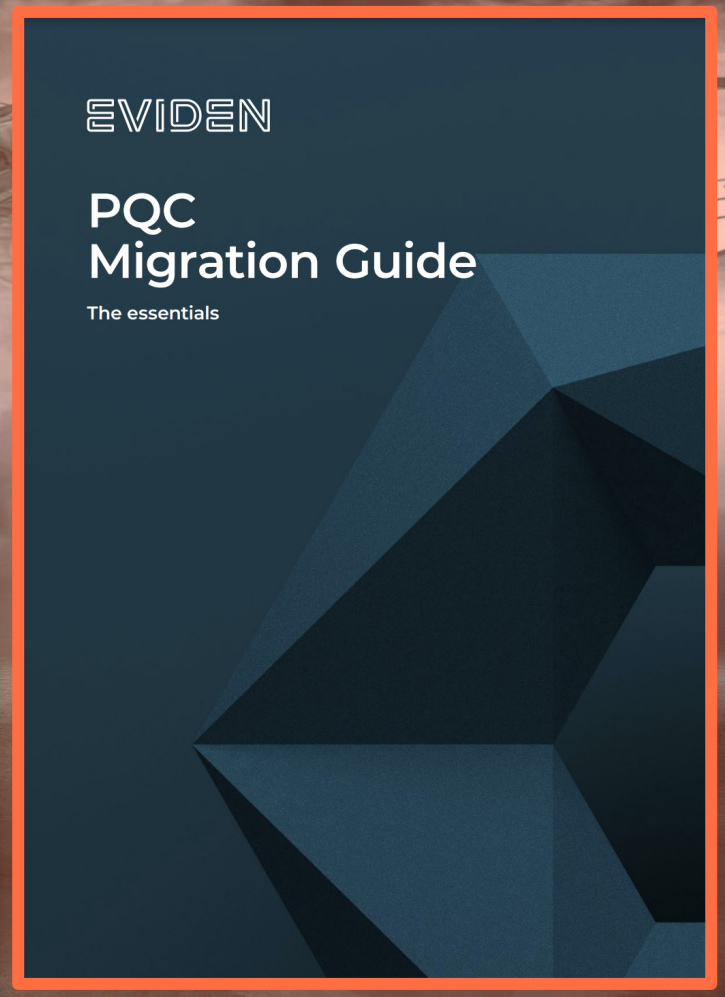
- McEliece
- BIKE
- HQC


Asymmetric encryption algorithm, replacement for RSA encryption
CRYSTALS-Kyber
CRYSTALS-Dilithium
Kyb
Dil


EVIDEN
Signature algorithm, replacement for RSA signatures
CRYSTALS-Kyber
CRYSTALS-Dilithium
Kyb
Dil

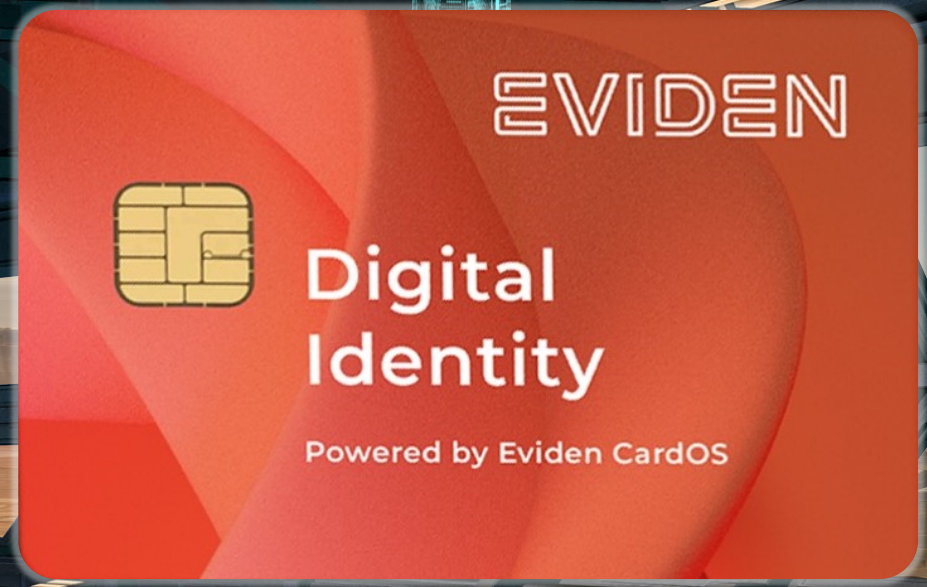

EVIDEN
We need to put them into practice.
CRYSTALS-Kyber
CRYSTALS-Dilithium
Kyb
Dil

EVIDEN



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

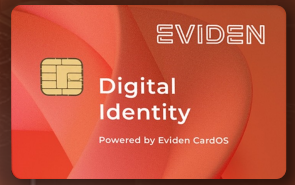
Let's look at smart cards ...



Current typical cards have:
16 KB RAM
500 KB flash

EVIDEN

Private-key lengths



16 KB RAM
500 KB flash

RSA: 2000 bit

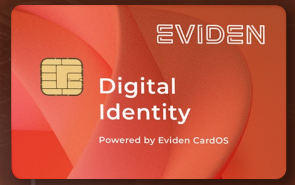
Kyber: 12000 bit

Dilithium: 20000 bit

McEliece: 100000 bit

EVIDEN

Public-key lengths



16 KB RAM
500 KB flash

RSA: 2000 bit

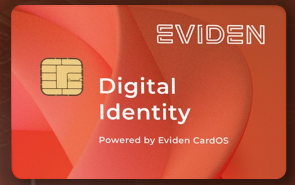
Kyber: 6000 bit

Dilithium: 10000 bit

McEliece:

EVIDEN

Signature/ciphertext lengths



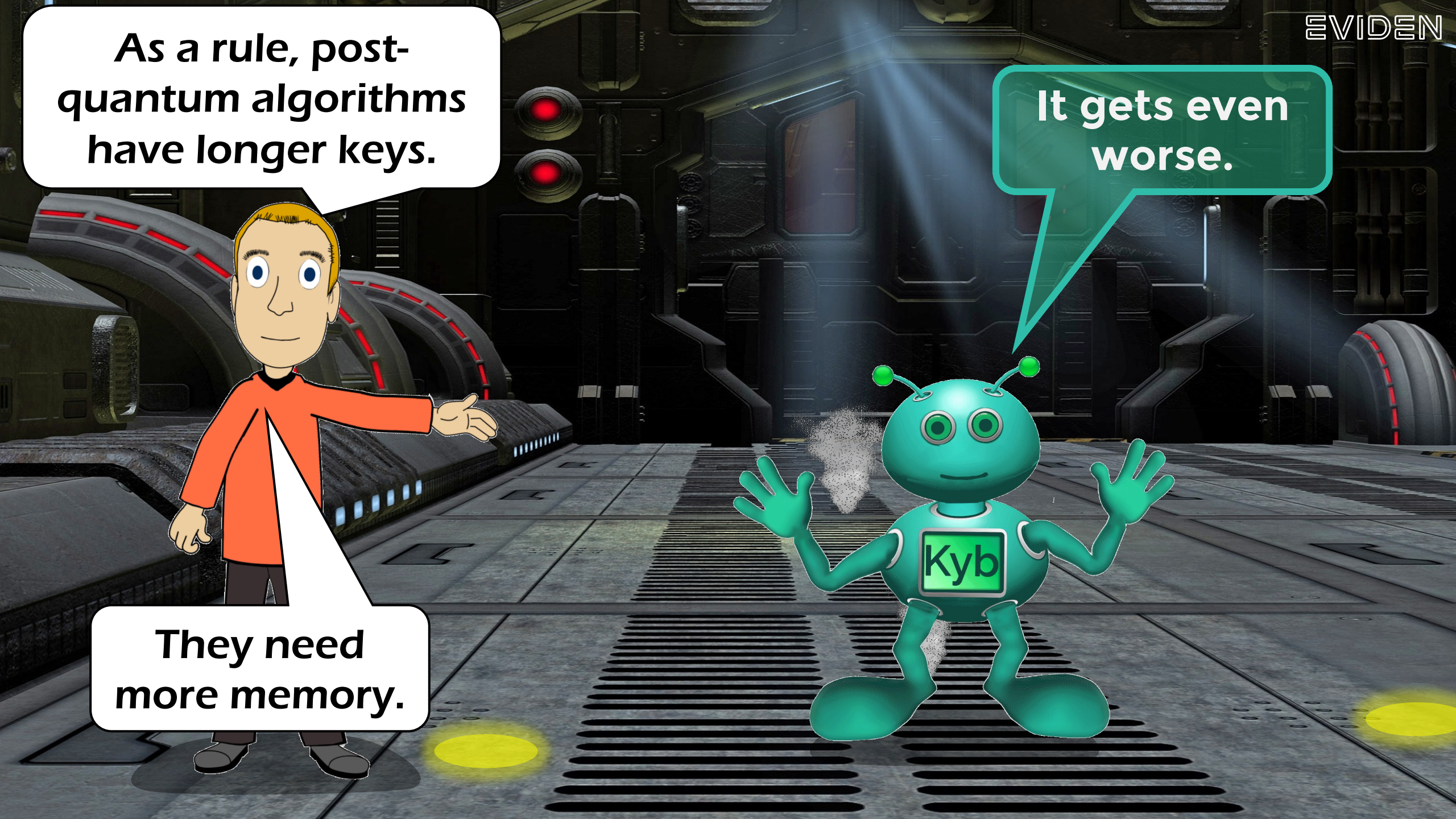
16 KB RAM
500 KB flash

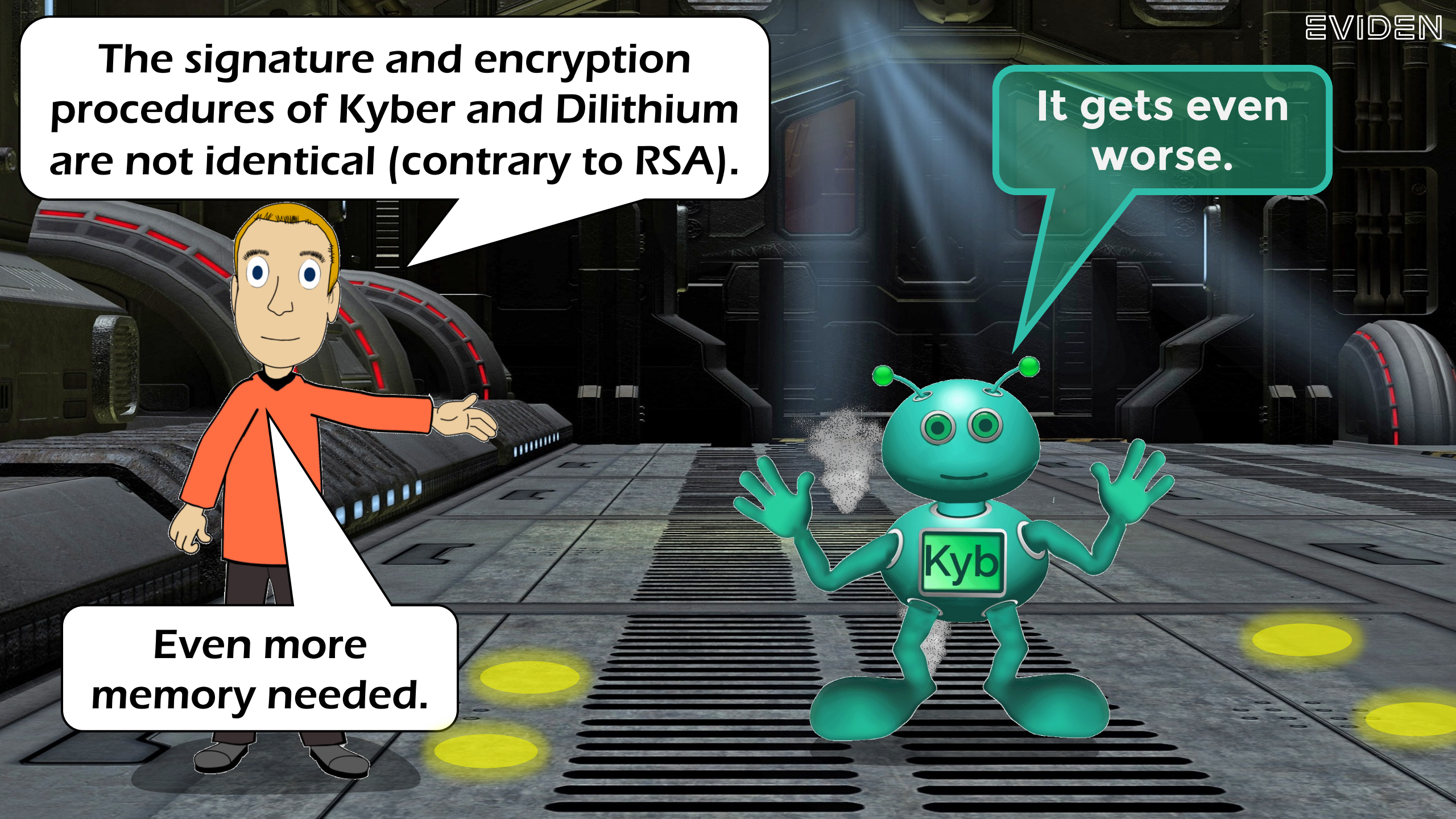
RSA: 2000 bit

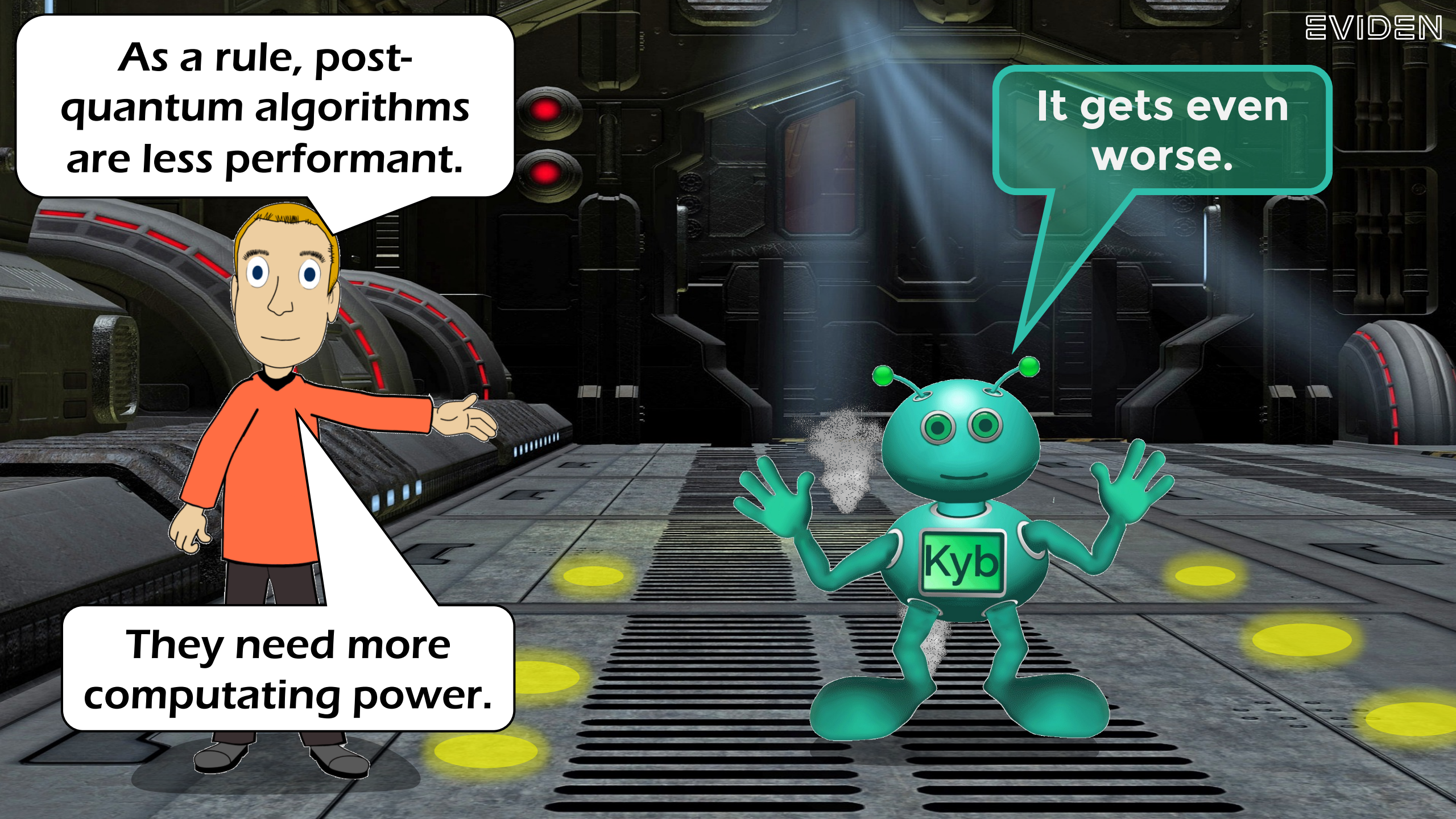
Kyber: 6000 bit

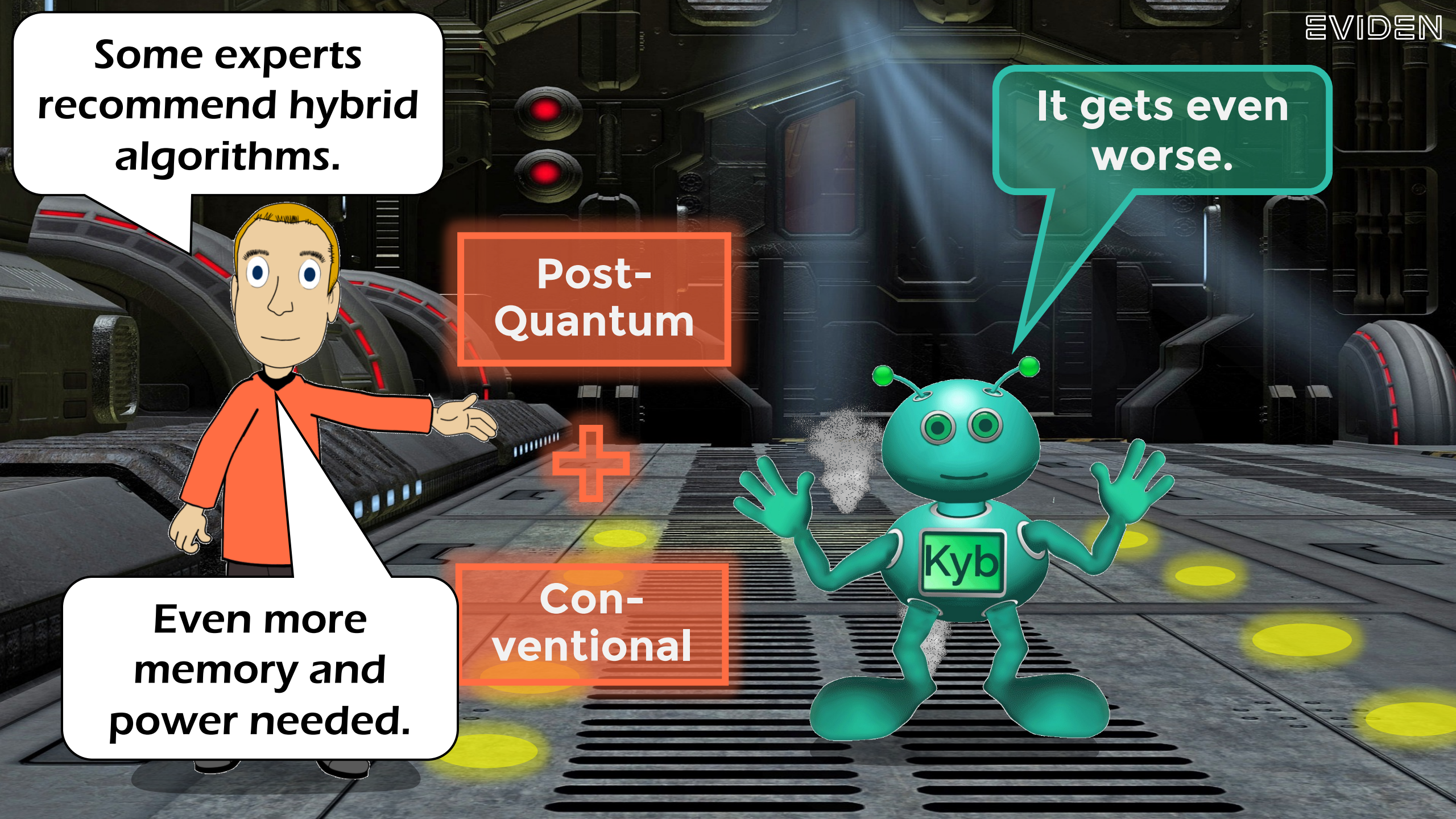
Dilithium: 20000 bit

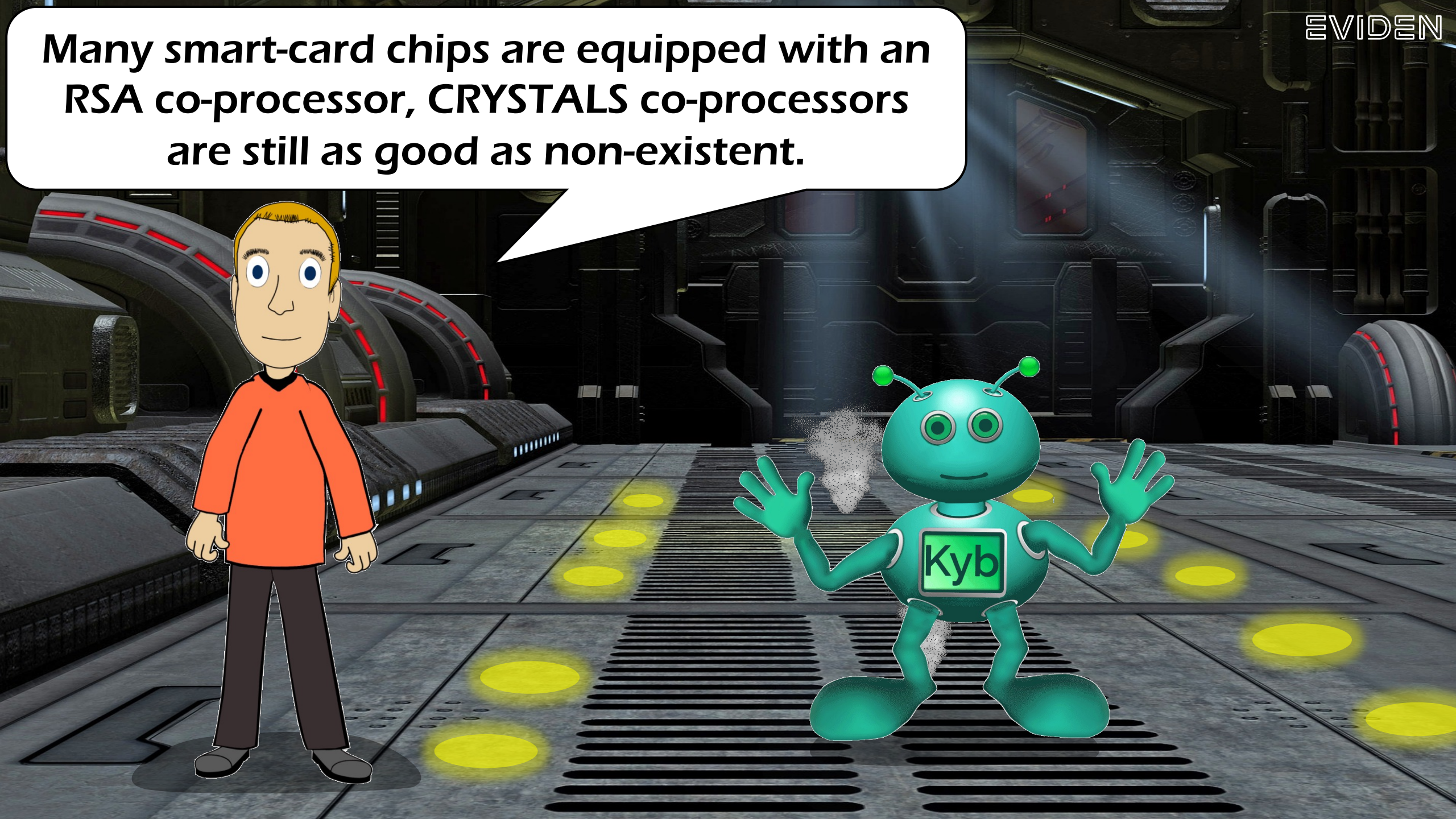
McEliece: 1700 bit

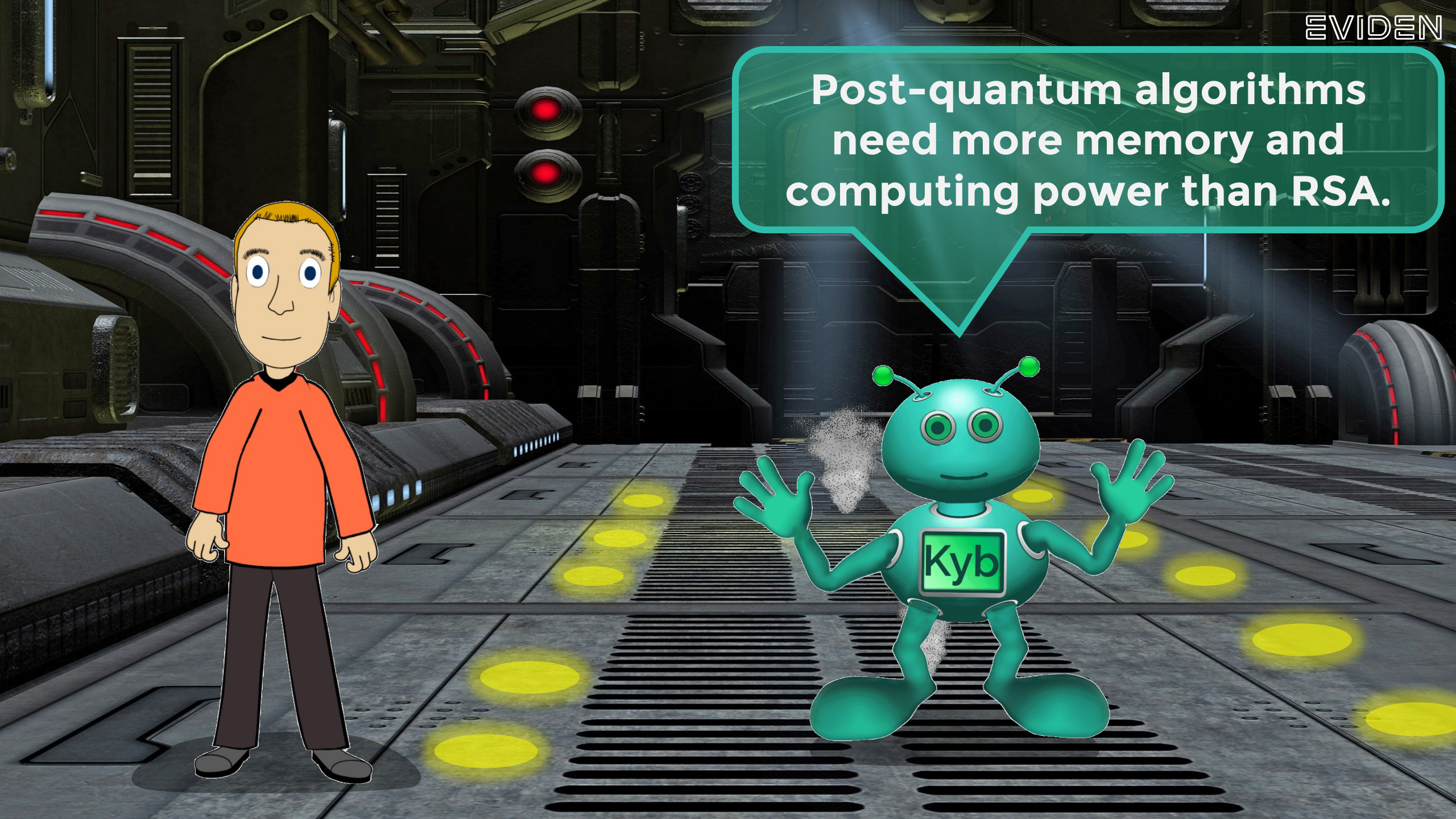

As a rule, post-quantum algorithms have longer keys.
They need more memory.
It gets even worse.
Kyb
EVIDEN

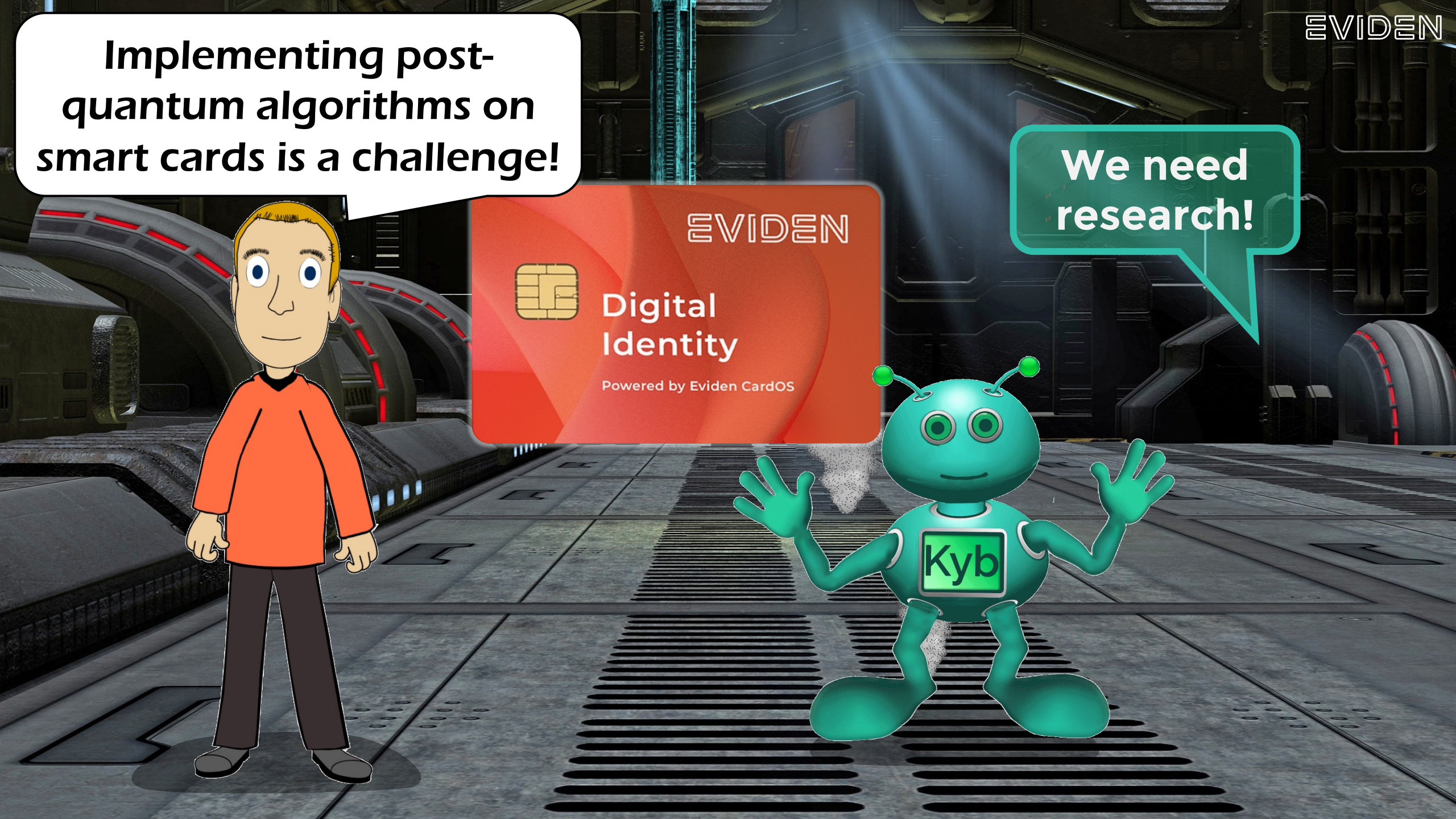

The signature and encryption procedures of Kyber and Dilithium are not identical (contrary to RSA).
It gets even worse.
Kyb
Even more memory needed.


As a rule, post-quantum algorithms are less performant.
They need more computating power.
It gets even worse.
Kyb
EVIDEN

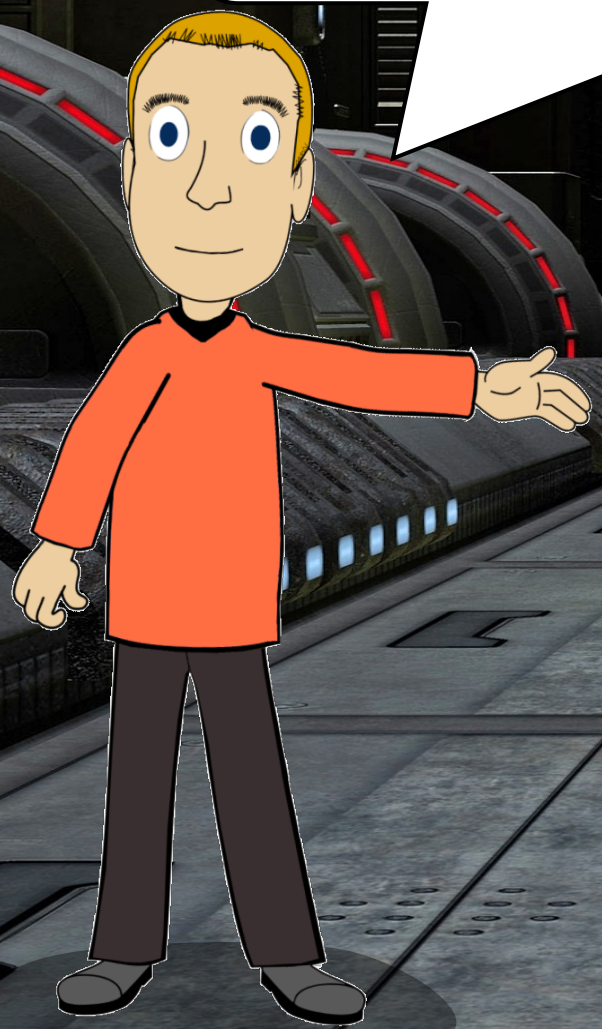

Some experts recommend hybrid algorithms.
Post-Quantum
+
Con-ventional
Even more memory and power needed.
It gets even worse.
Kyb
EVIDEN


Many smart-card chips are equipped with an RSA co-processor, CRYSTALS co-processors are still as good as non-existent.
EVIDEN
Kyb


Post-quantum algorithms need more memory and computing power than RSA.
Kyb


EVIDEN
Implementing post-quantum algorithms on smart cards is a challenge!
EVIDEN
Digital Identity
Powered by Eviden CardOS
We need research!
Kyb

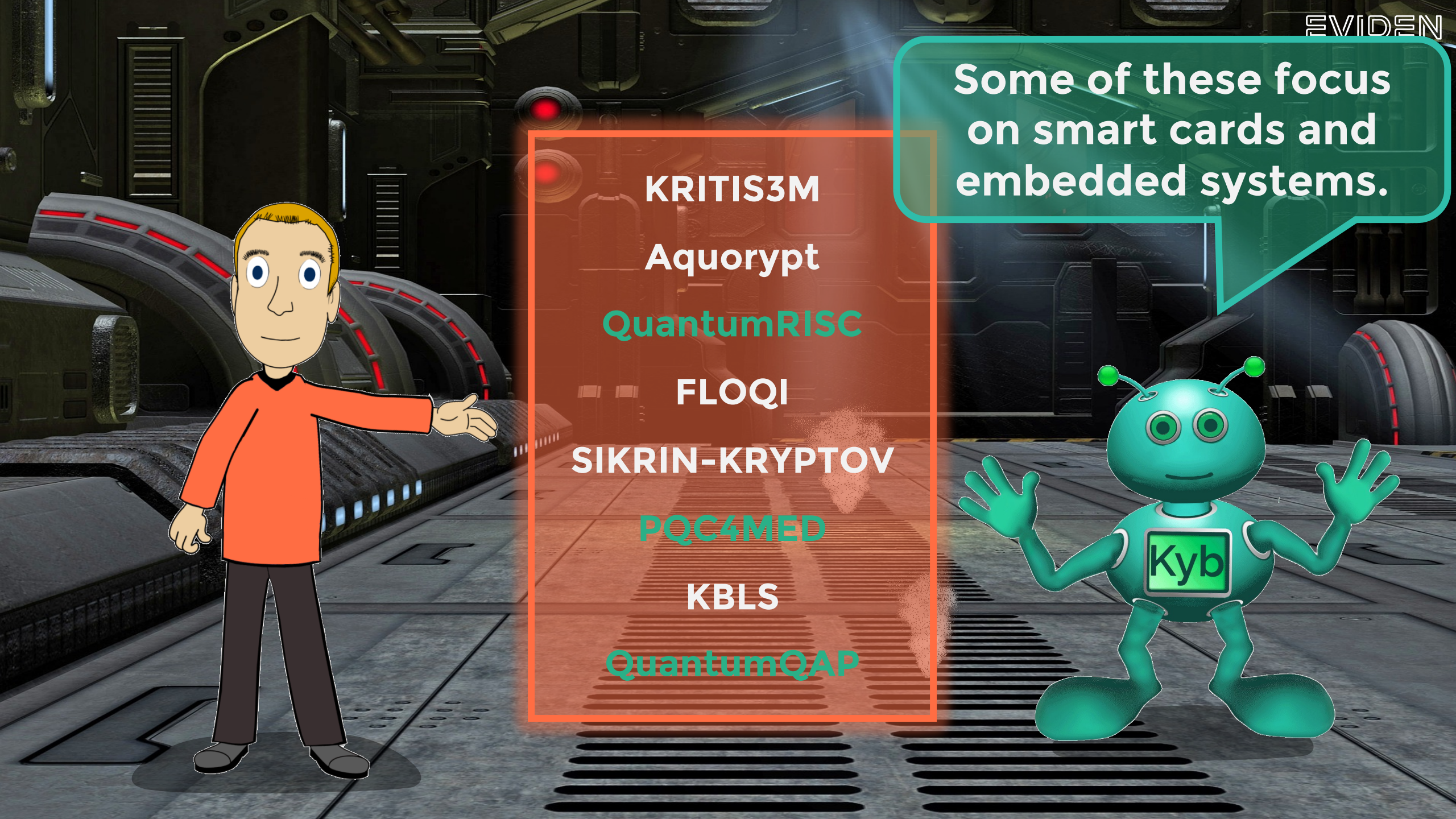
The German Federal Ministry of Education and Research is funding post-quantum projects.

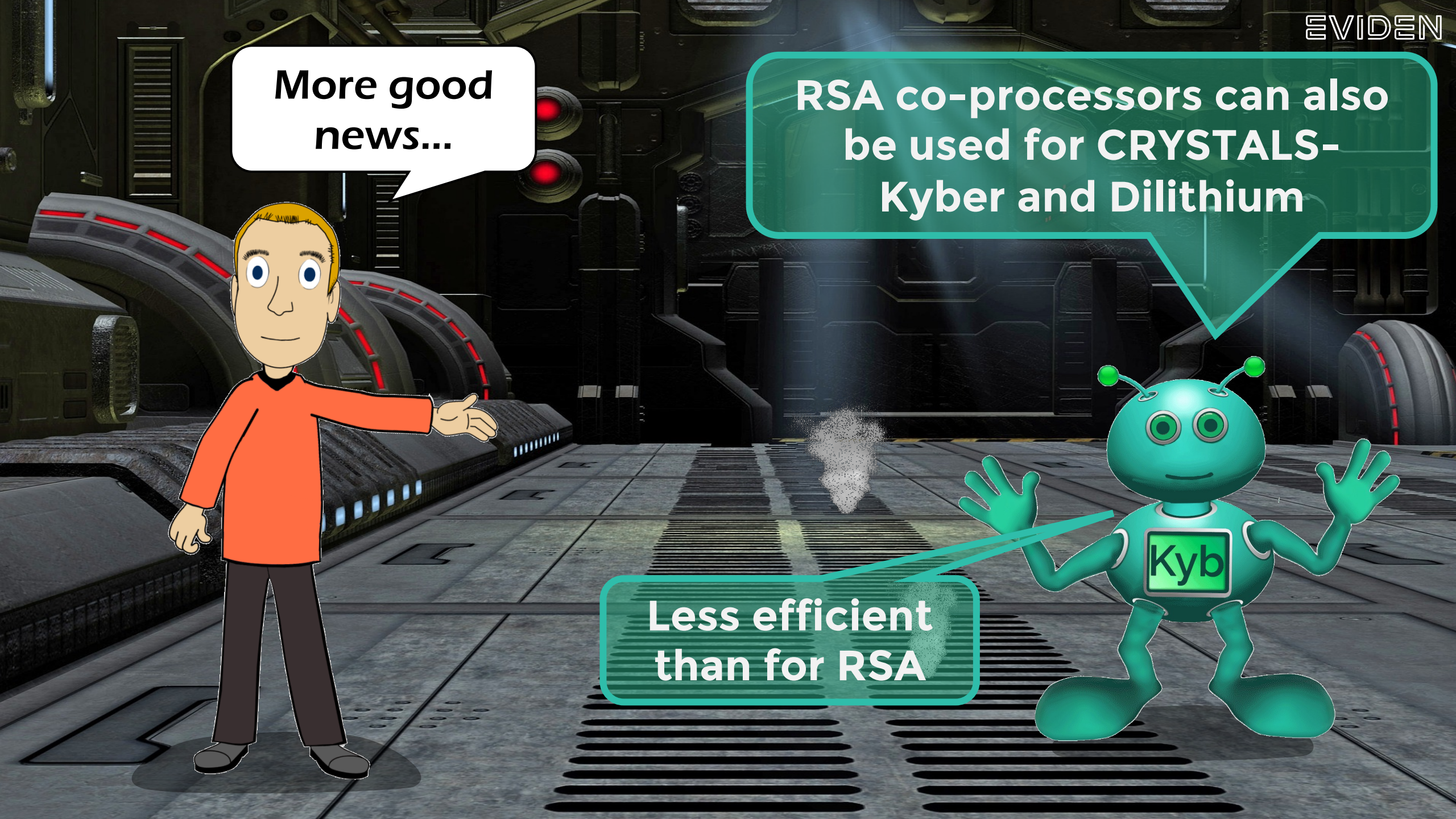


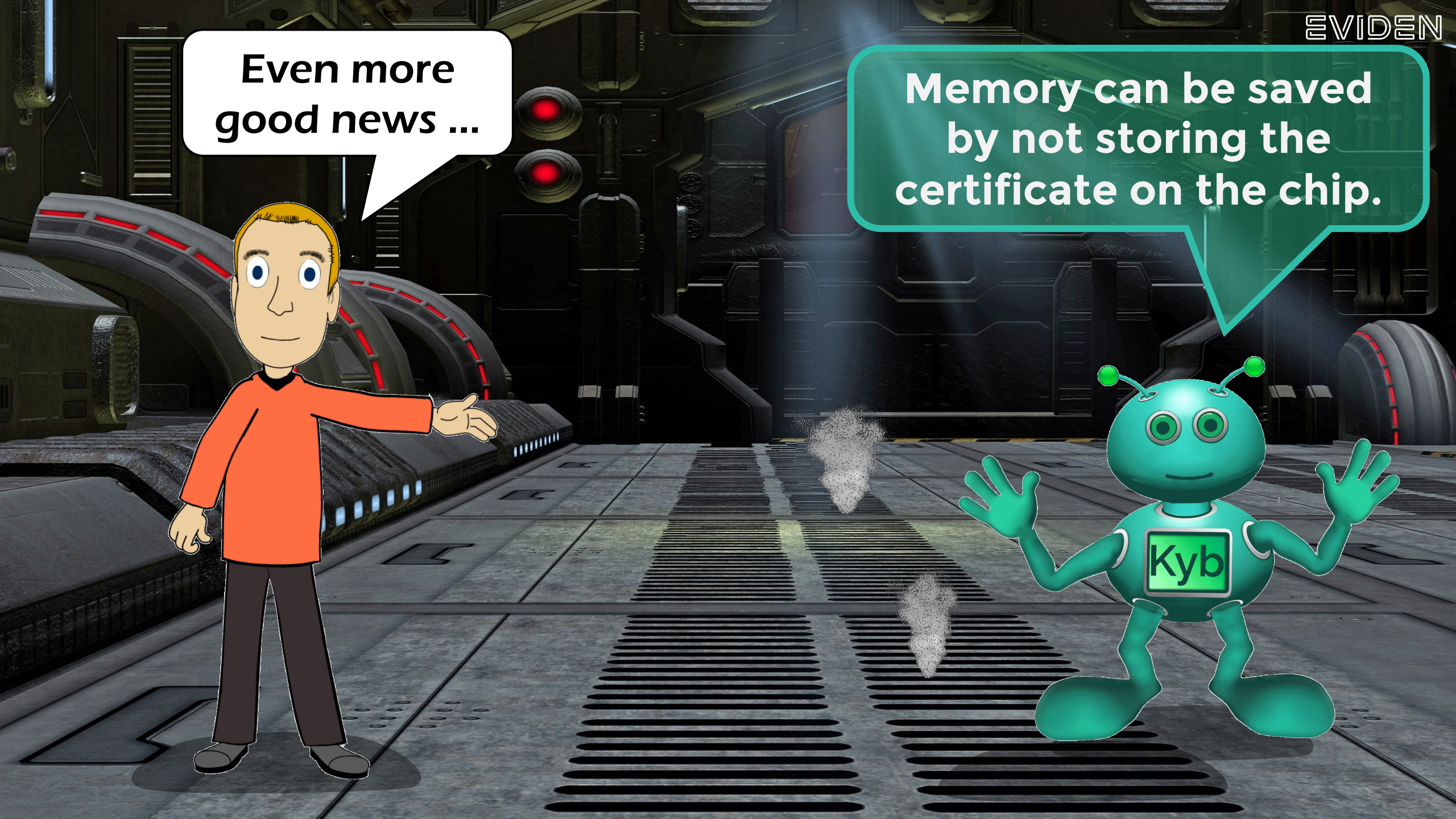
Directive for funding projects dedicated to "Bringing post-quantum cryptography to applications" 2022

Bundesministerium für Bildung und Forschung


Here are a few examples
KRITIS3M
Aquorypt
QuantumRISC
FLOQI
SIKRIN-KRYPTOV
PQC4MED
KBLS
QuantumQAP
Kyb


EVIDEN
Some of these focus on smart cards and embedded systems.
KRITIS3M
Aquorypt
QuantumRISC
FLOQI
SIKRIN-KRYPTOV
PQC4MED
KBLS
QuantumQAP
Kyb

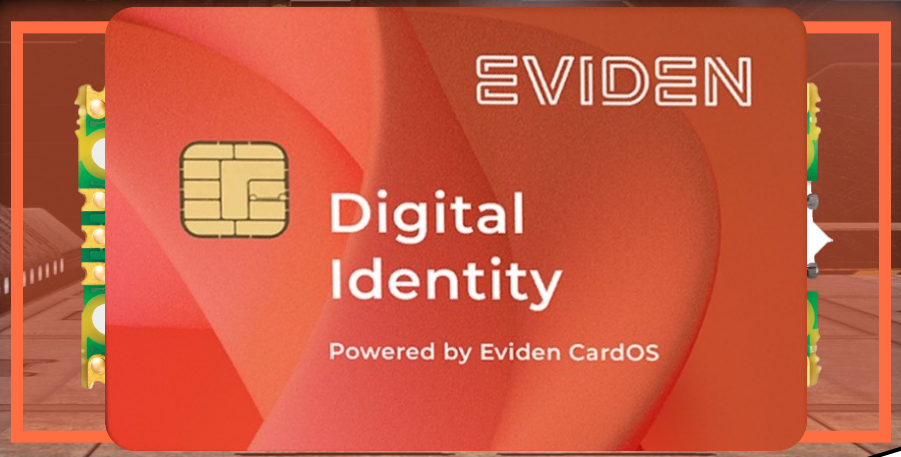

More good news...
RSA co-processors can also be used for CRYSTALS-Kyber and Dilithium
Kyb
Less efficient than for RSA


Even more good news ...
Memory can be saved by not storing the certificate on the chip.
Kyb

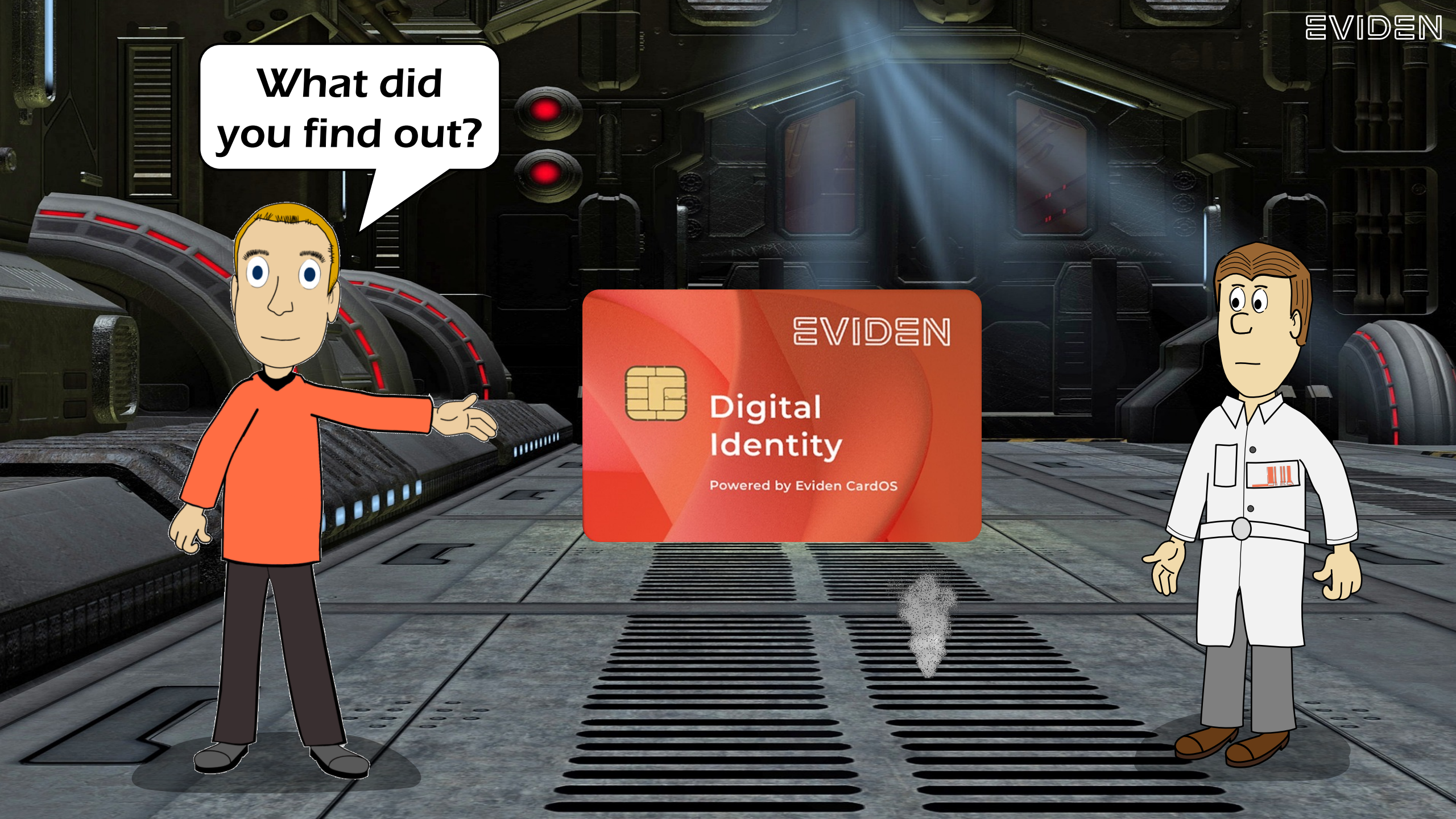

Even more good news ...
My employer is doing research, too!
EVIDEN
EVIDEN

EVIDEN

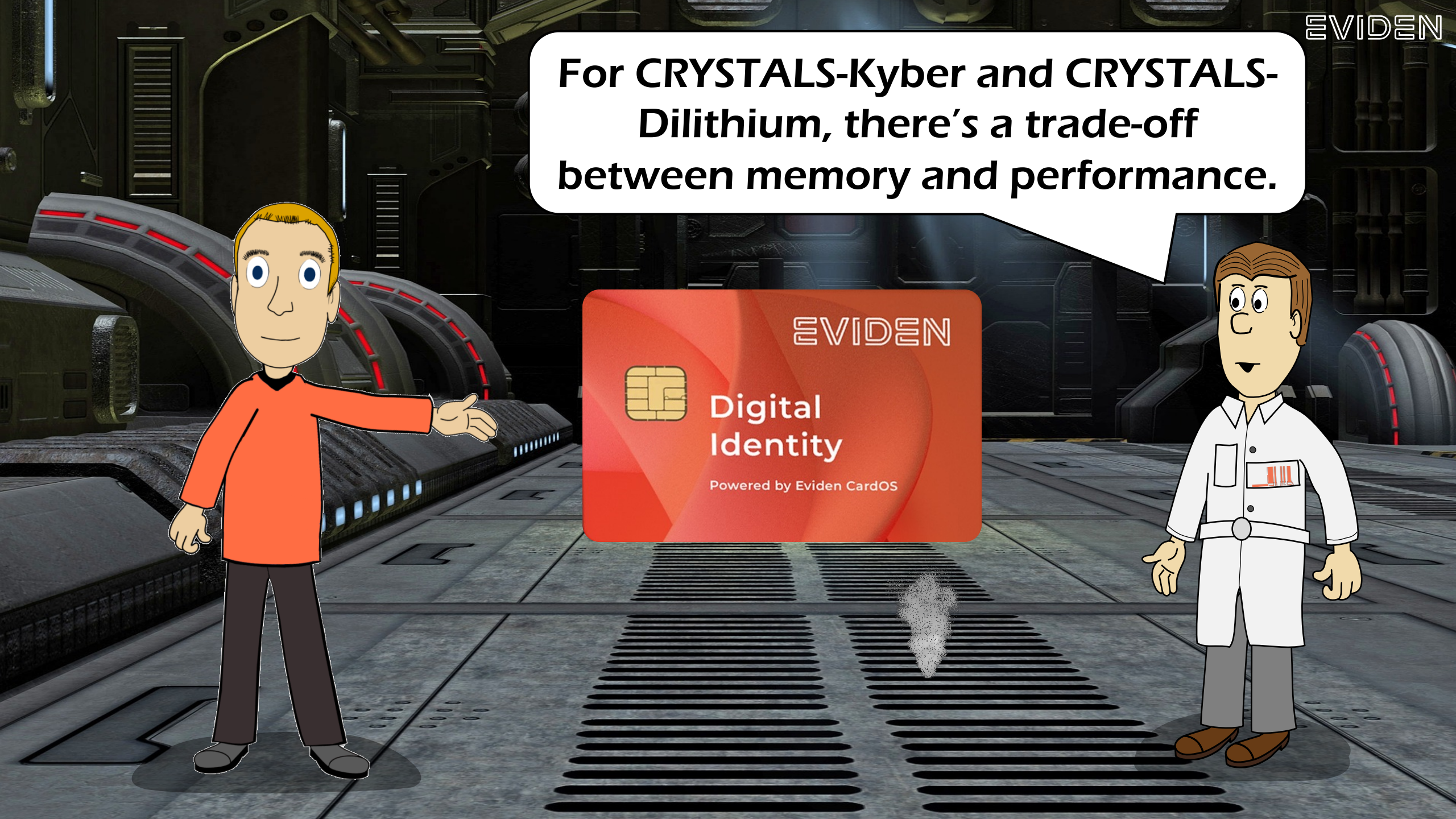
Eviden is testing post-quantum algorithms on a Raspberry-Pi Pico Microcontroller.



Several smart card architectures are simulated.


What did you find out?
EVIDEN
Digital Identity
Powered by Eviden CardOS
EVIDEN

For CRYSTALS-Kyber and CRYSTALS-Dilithium, there's a trade-off between memory and performance.

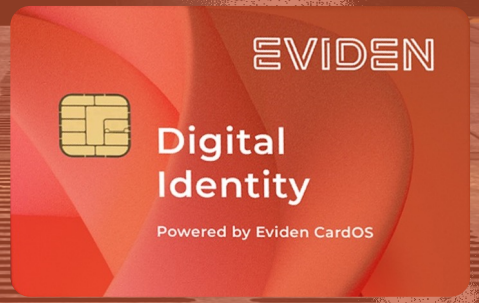


EVIDEN

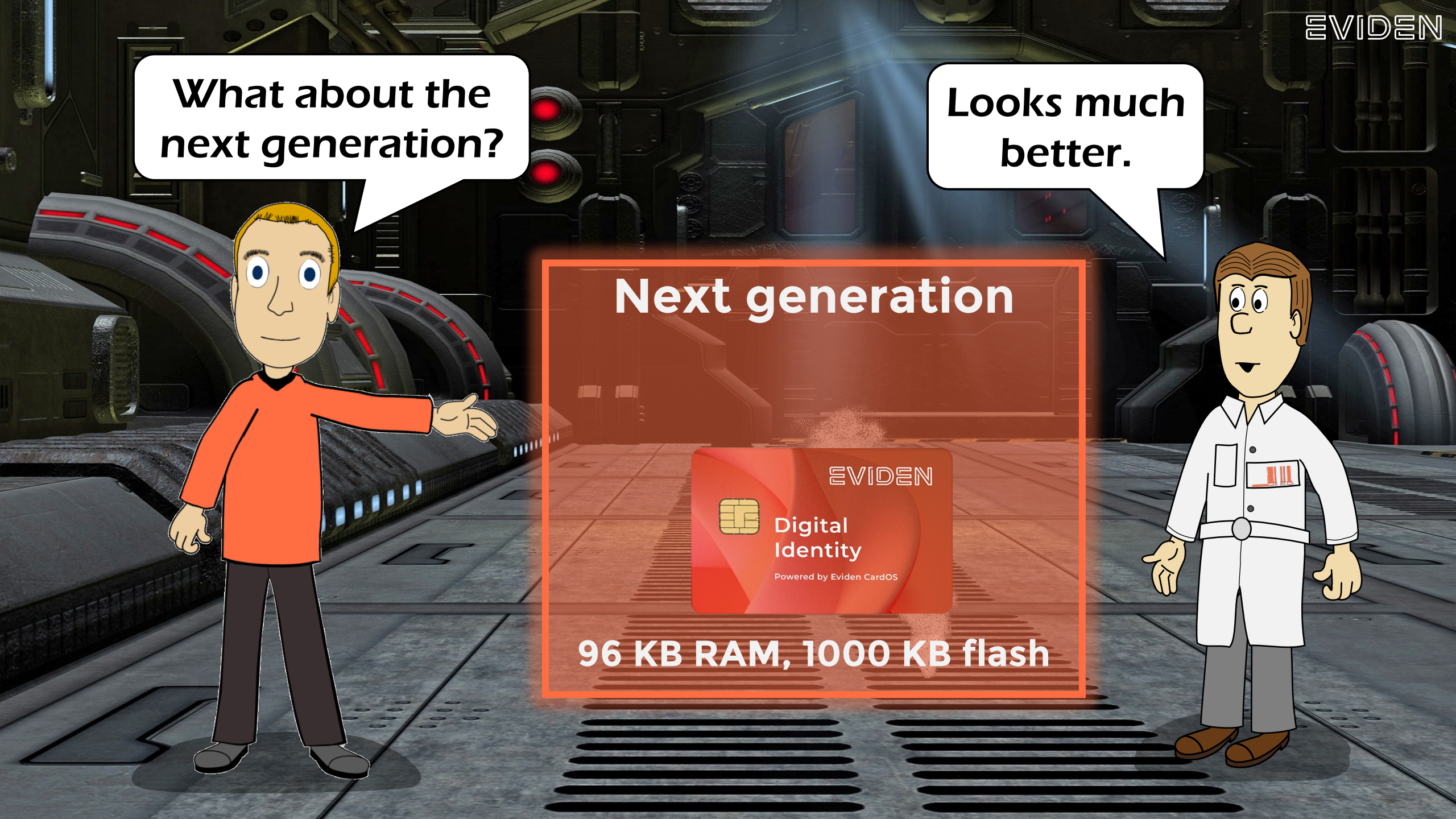
Is it possible to implement CRYSTALS-Kyber and CRYSTALS-Dilithium on such a card efficiently.

No.

Current mainstream smart-card architectures



16 KB RAM, 500 KB flash


What about the next generation?
Looks much better.
Next generation
EVIDEN
Digital Identity
Powered by Eviden CardOS
96 KB RAM, 1000 KB flash

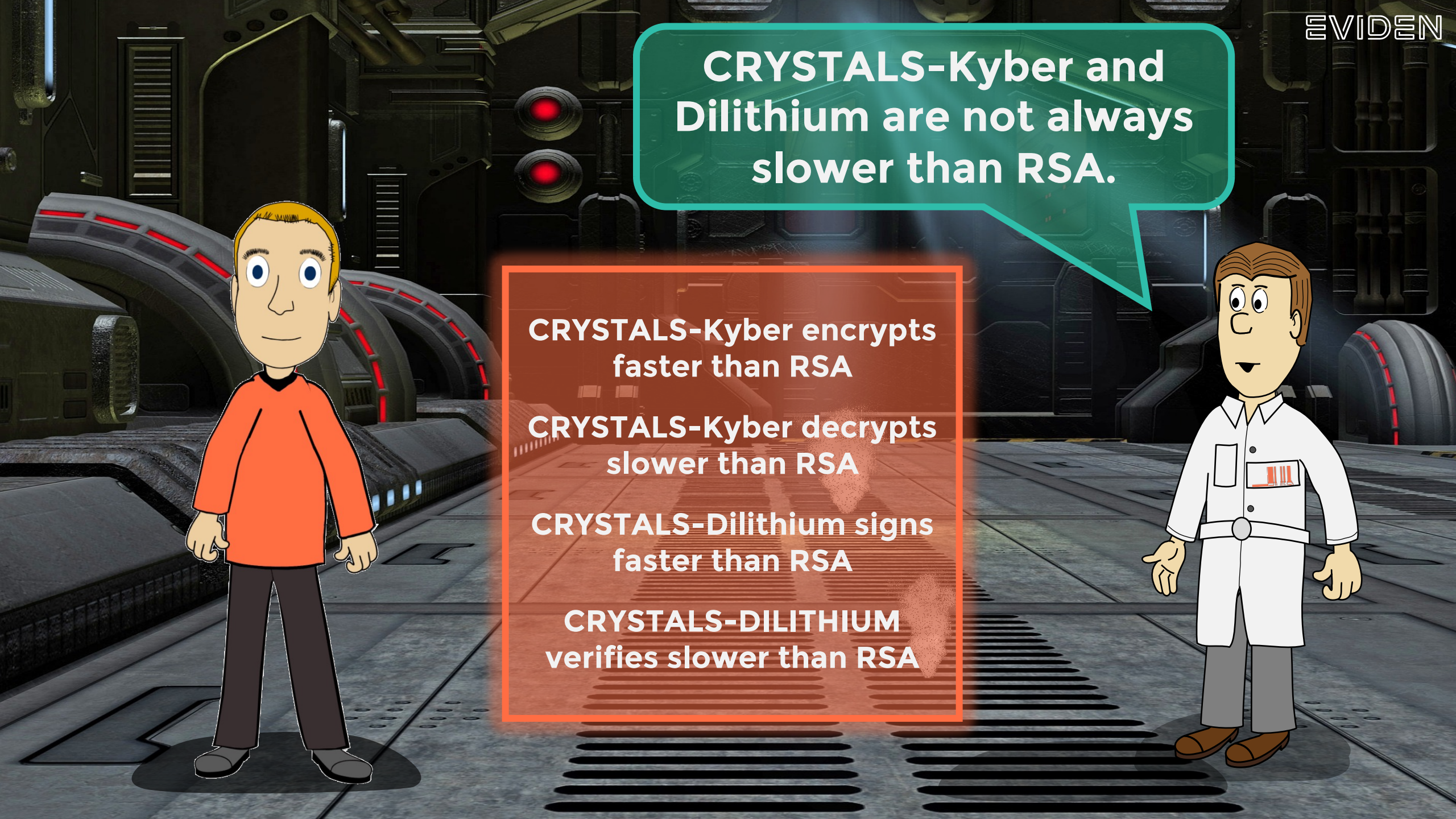
Eviden smartcard comparison tests

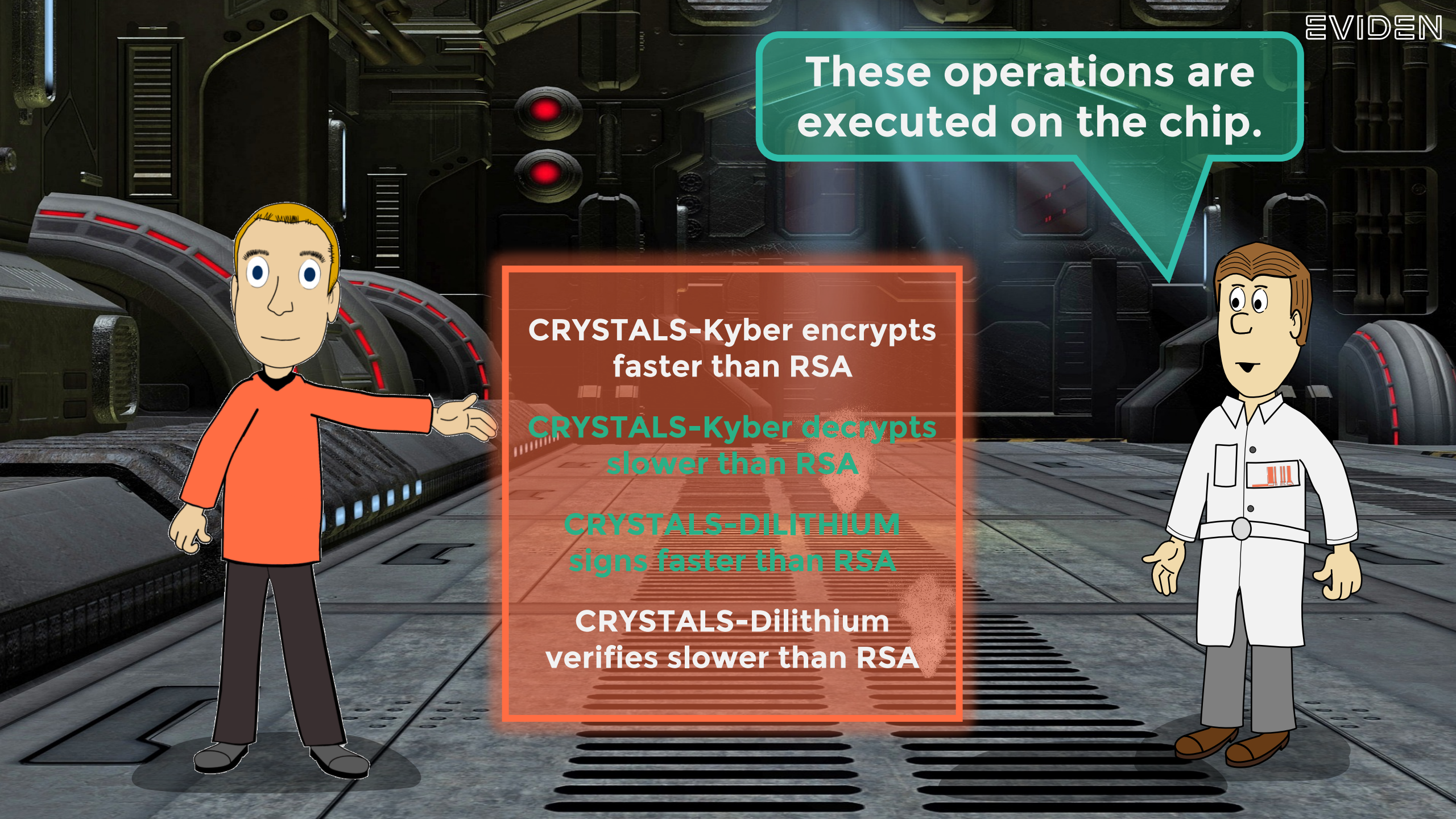
ALGORITHM	Security	SIGN ENCAPSULATE	VERIFY DECAPSULATE	KEY GENERATION
RSA 512		0,234 s	0,103 s	1,564 s
RSA 1024		0,717 s	0,119 s	13,306 s
RSA 2048	112	3,493 s	0,196 s	-
RSA 4096	140	21,067 s	0,477 s	-
ECC-192		0,771 s	1,466 s	0,758 s
ECC-224		1,057 s	2,028 s	1,036 s
ECC-256	128	1,189 s	2,298 s	1,170 s
ECC-384		3,120 s	6,150 s	3,091 s
ECC-521	256	6,686 s	13,313 s	6,646 s
Kyber	192	0,146 s	0,352 s	0,166 s
Dilithium	128	0,247 s	1,1176 s	0,150 s

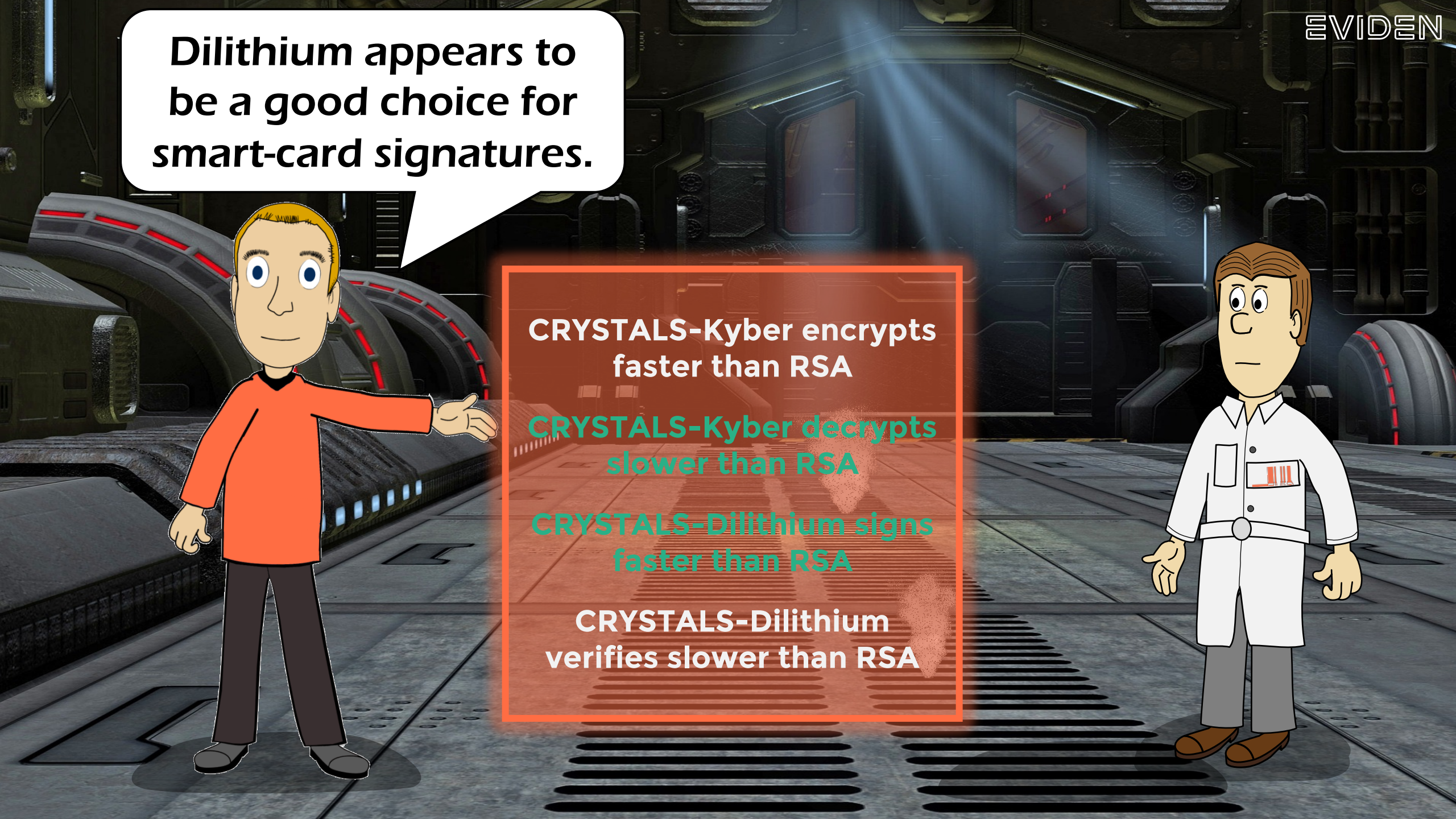
Eviden HSM comparison tests

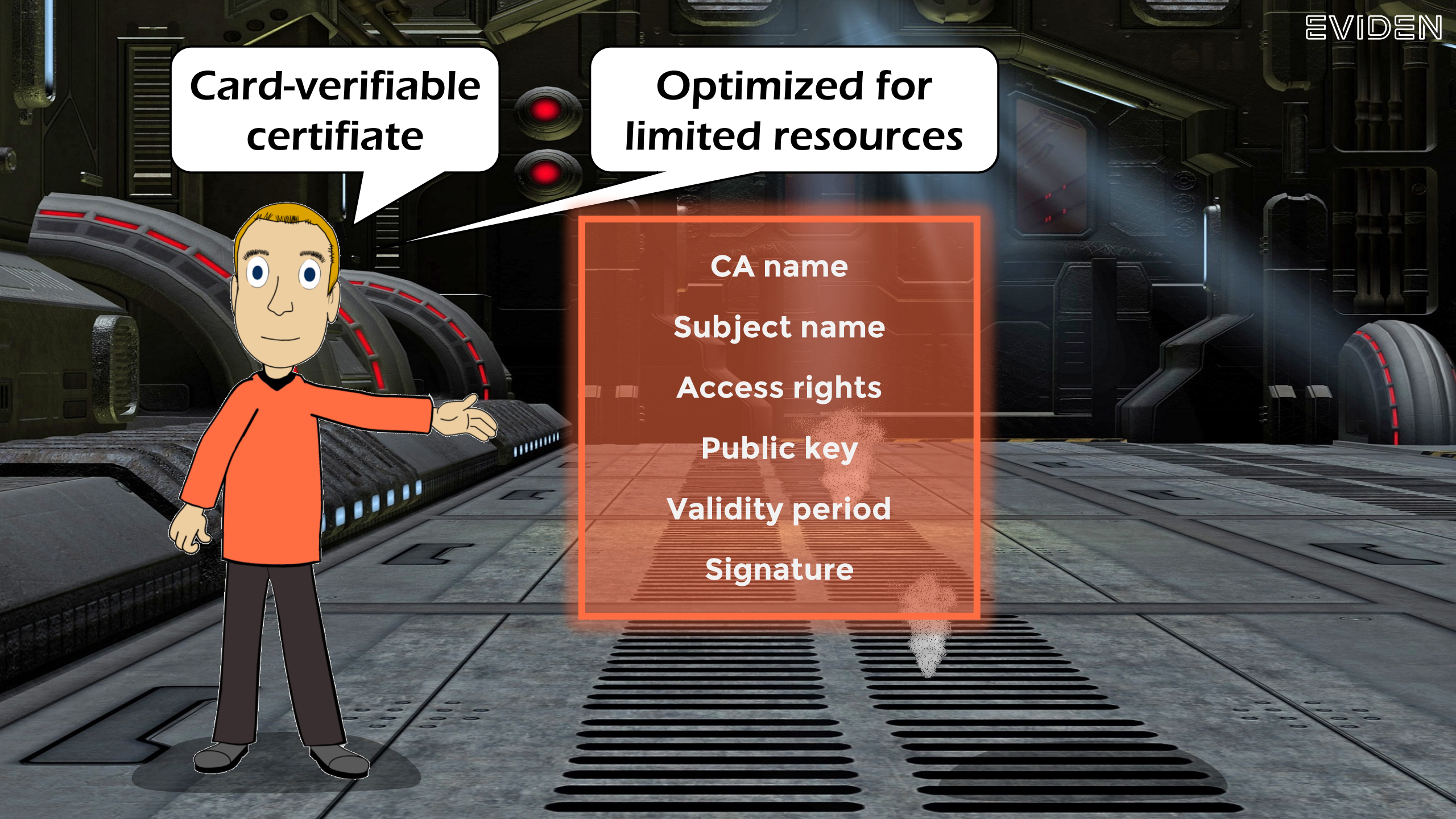
- Nb of operations per second - the bigger, the better

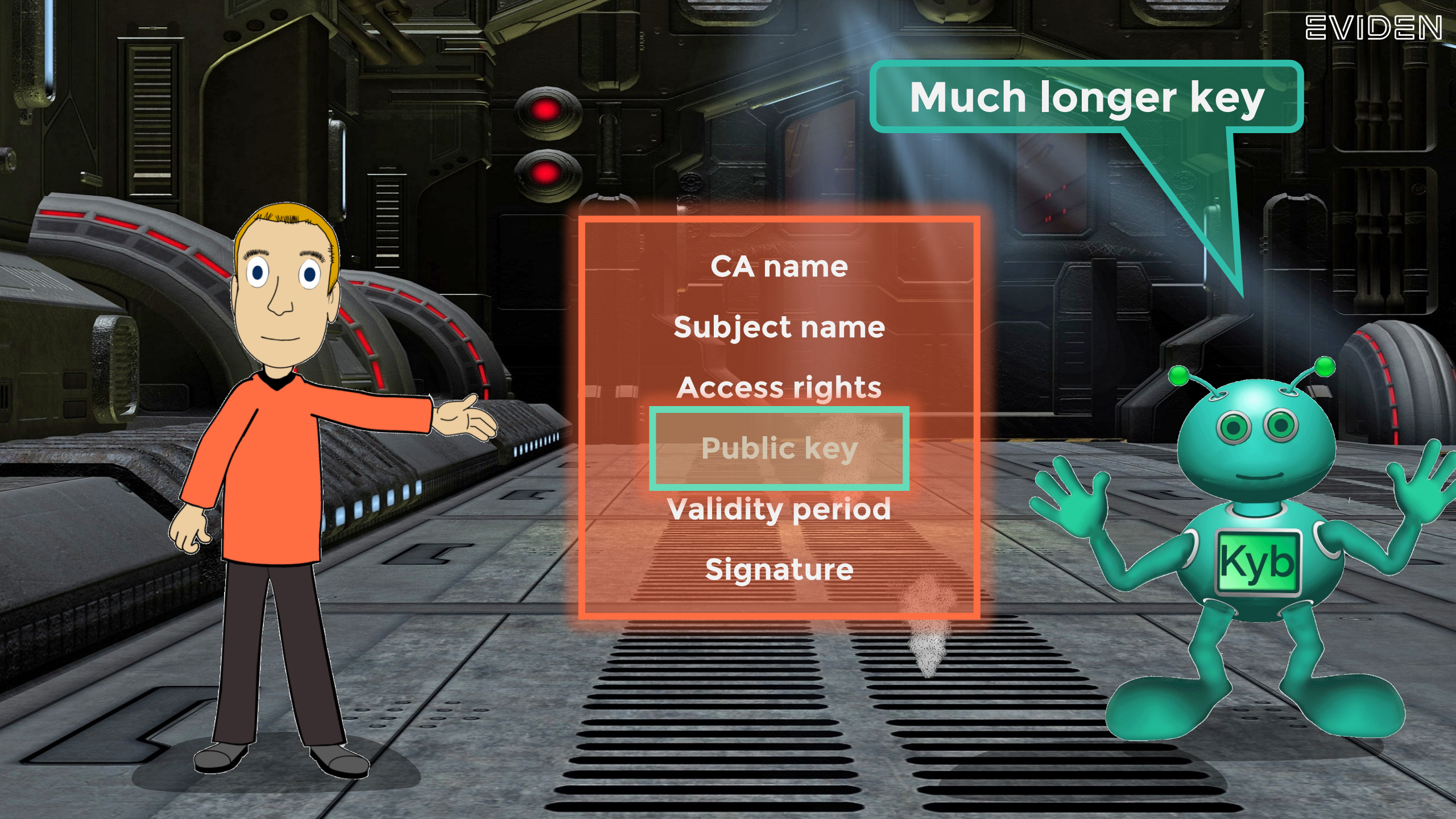
Algorithm	Security	Signatures	Verification	Encapsulation	Decapsulation
RSA-2048	112	1000 op/s	2100 op/s	-	-
RSA-4096	140	190 op/s	1200 op/s	-	-
ECC-256	128	2300 op/s	1100 op/s	-	-
ECC-521	256	880 op/s	430 op/s	-	-
Dilithium 44	128	820 op/s	1800 op/s	-	-
Dilithium 65	192	590 op/s	1300 op/s	-	-
Dilithium 87	256	420 op/s	670 op/s	-	-
Kyber 512	128	-	-	1100 op/s	1100 op/s
Kyber 768	192	-	-	1050 op/s	1000 op/s
Kyber 1024	256	-	-	1000 op/s	790 op/s

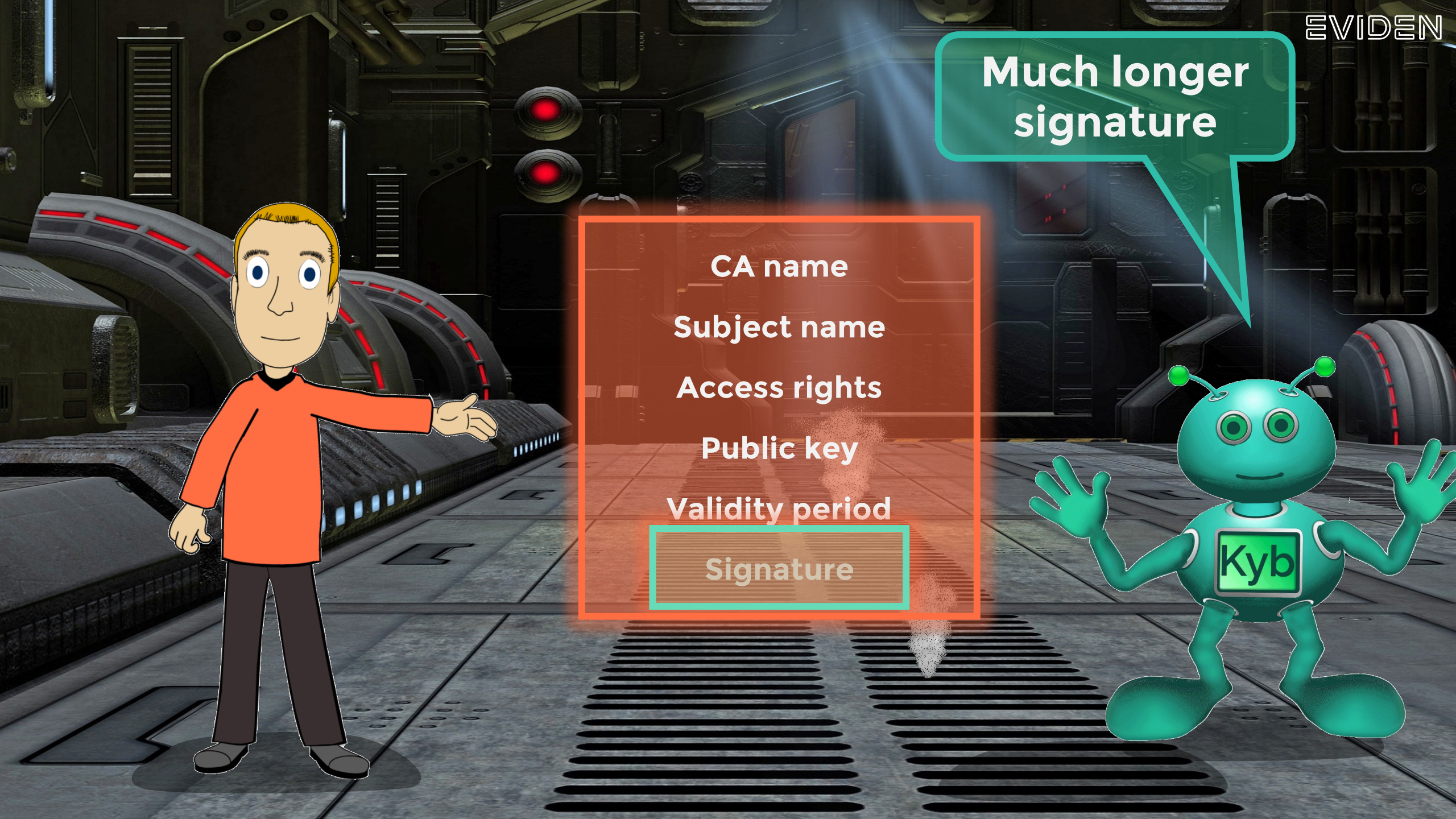

EVIDEN
CRYSTALS-Kyber and Dilithium are not always slower than RSA.
CRYSTALS-Kyber encrypts faster than RSA
CRYSTALS-Kyber decrypts slower than RSA
CRYSTALS-Dilithium signs faster than RSA
CRYSTALS-DILITHIUM verifies slower than RSA

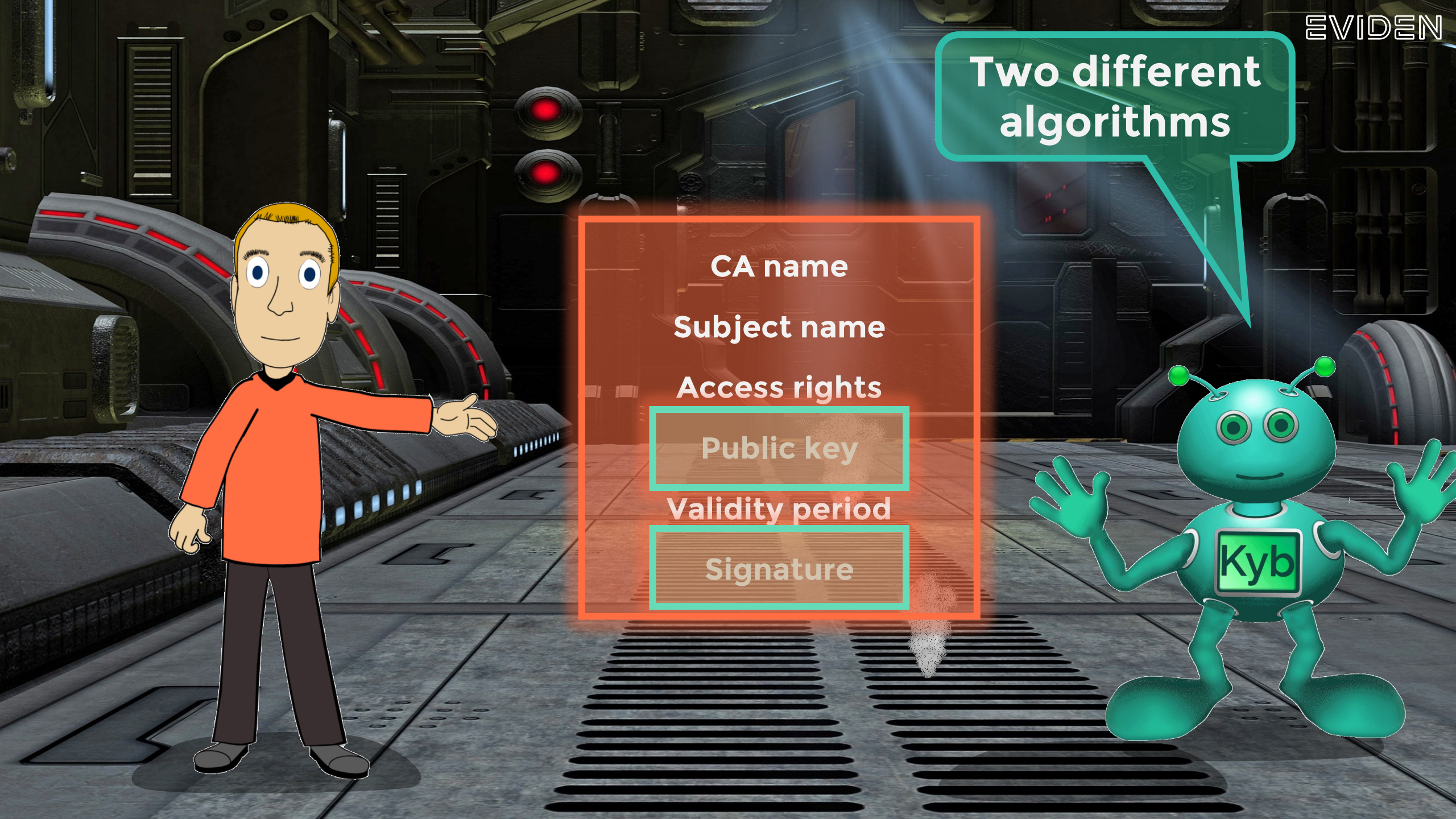

These operations are executed on the chip.
CRYSTALS-Kyber encrypts faster than RSA
CRYSTALS-Kyber decrypts slower than RSA
CRYSTALS-DILITHIUM signs faster than RSA
CRYSTALS-Dilithium verifies slower than RSA


Dilithium appears to be a good choice for smart-card signatures.
CRYSTALS-Kyber encrypts faster than RSA
CRYSTALS-Kyber decrypts slower than RSA
CRYSTALS-Dilithium signs faster than RSA
CRYSTALS-Dilithium verifies slower than RSA


Card-verifiable certifiate
Optimized for limited resources
CA name
Subject name
Access rights
Public key
Validity period
Signature

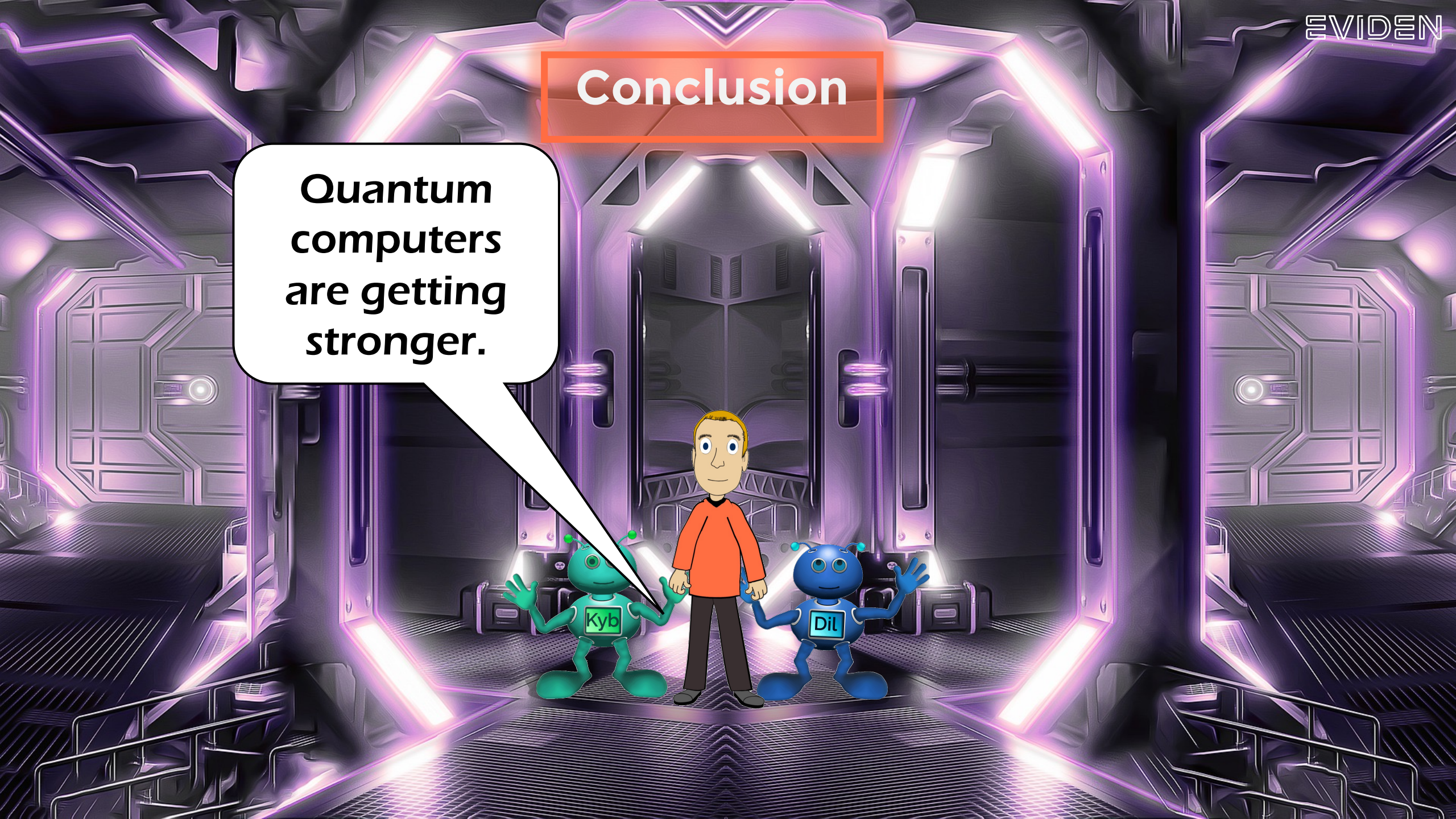

Much longer key
CA name
Subject name
Access rights
Public key
Validity period
Signature
Kyb


Much longer signature
CA name
Subject name
Access rights
Public key
Validity period
Signature
Kyb


Two different algorithms
CA name
Subject name
Access rights
Public key
Validity period
Signature
Kyb

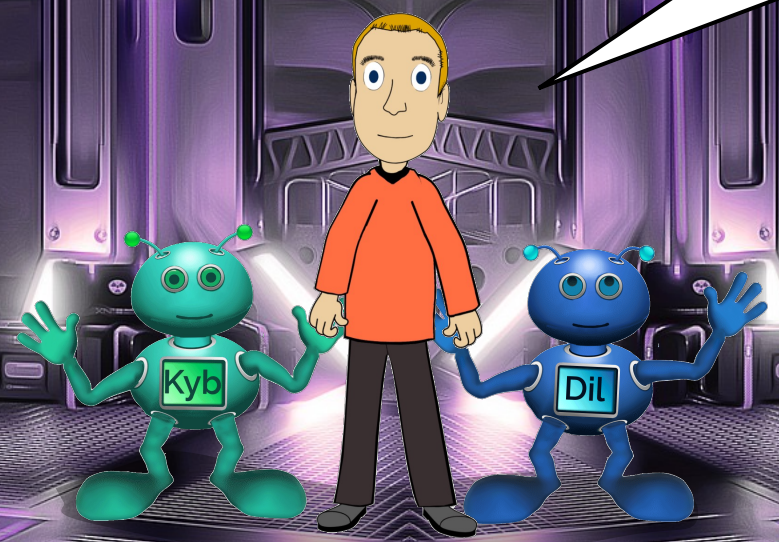

This is going to be a challenge!
CA name
Subject name
Access rights
Public key
Validity period
Signature
Kyb

Conclusion



Conclusion

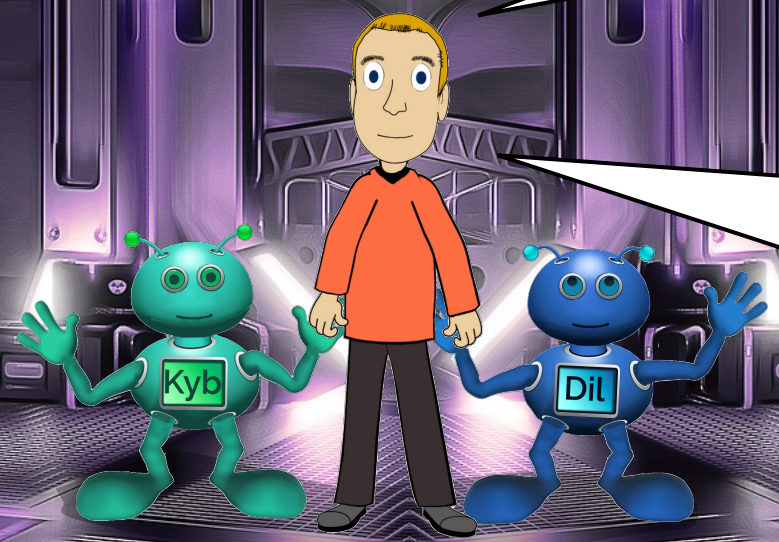
Smart cards need to support post-quantum crypto.



Conclusion

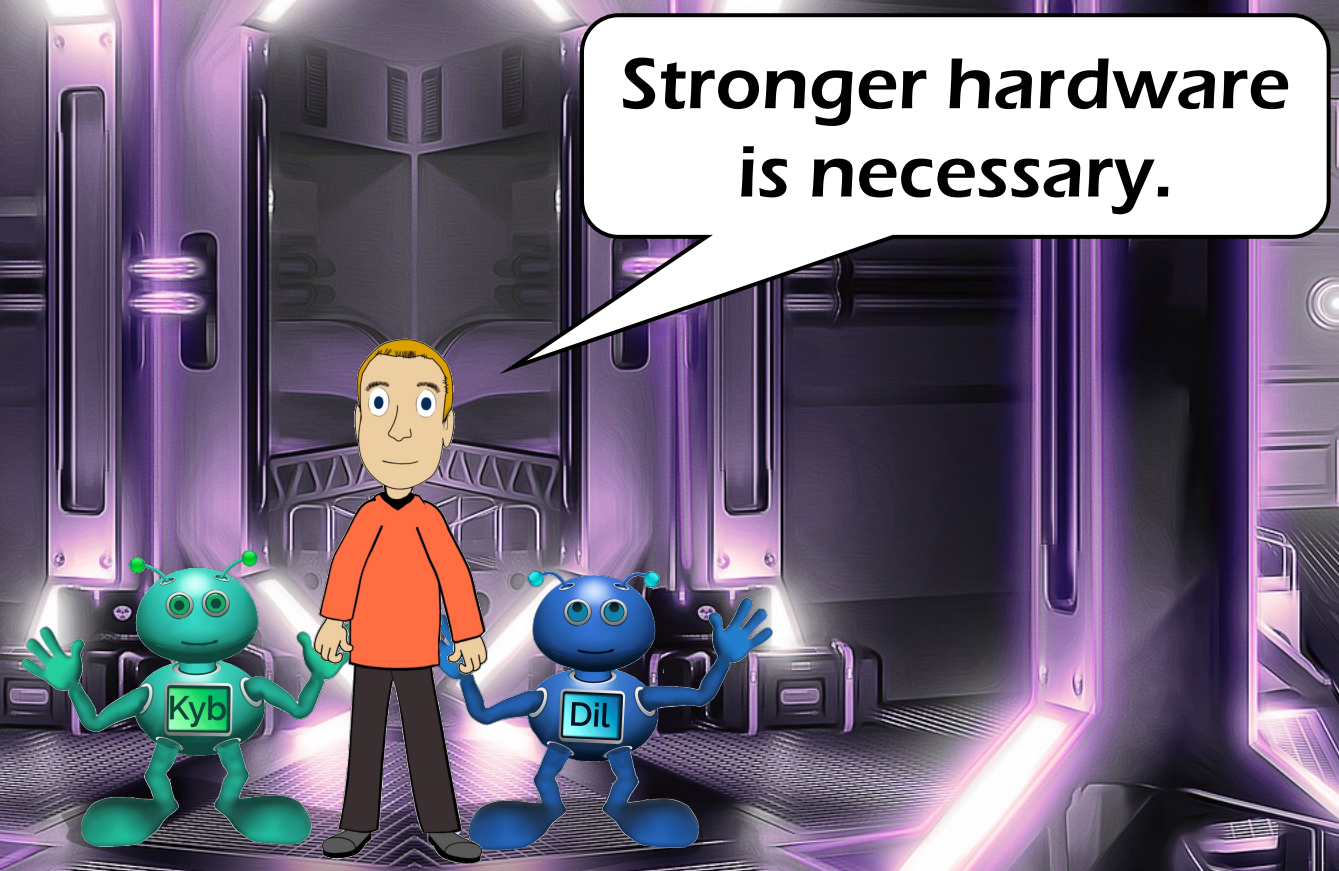
Implementing post-quantum crypto on smart cards is challenging.

Because of memory consumption and perfomance.



Conclusion


EVIDEN
Digital
Identity
Powered by Eviden CardOS


Stronger hardware is necessary.
Kyb
Dil

Conclusion


EVIDEN
Digital
Identity
Powered by Eviden CardOS


We need additional research.
Kyb
Dil


EVIDEN
END