Qubit® Conference

Impact of Agile Cryptography on Business

You can’t spell Cryptography without “cry” …

Jan Dušátko
jan.dusatko@cryptosession.cz

PRAGUE 18–20 MAY 2026

In security we trust ...

How this could be wrong?

"... Our IT environment leads in technology, leveraging **modern global platforms** for **seamless performance** and reliability. With **continuous innovation** and **strategic oversight**, we ensure our systems remain **resilient, adaptable**, and ready to **support ongoing digital growth**...„

Why is this important?

Why can crypto agility save you?

Qubit® Conference

Lifecycles as a security threat

Withdraw timescale in cryptography is usually about 10-15 years

Qubit® Conference

Algorithm / Protocol	Standard	Withdraw	Where you can find it
DES	1977	2005	TLS, IPSec
RC4	**1987**	**2015**	**Still in Kerberos (AD)**
3DES	1999	2019	TLS, IPSec
SkipJack	*1993*	*2010*	
MD4	**1990**	**2000**	**NTLMv1, Kerberos-RC4**
MD5	**1992**	**2008**	**NTLMv2**
SHA-1	1993	2017	Rare (TLS, IPSec)
DualEC DRBG	2006	2014	Backward compatibility only
IKEv1	**1994**	**2005**	**Still used**
SSLv2	**1994**	**2011**	**Old equipment**
SSLv3	**1996**	**2015**	**Old equipment**
TLSv1.0	**1999**	**2018**	**Still used**
TLSv1.1	**2006**	**2020**	**Still used**
DTLSv1.0	**2006**	**2020**	**Still used**

Lifecycles as a security threat

Withdraw timescale in cryptography is usually about 10-15 years

Qubit® Conference

Algorithm	Standard	Withdraw	Where you can find it
RC4	1987	2015	Still in Kerberos (AD)

- RC4 is a weak cipher
- But main problem is an architecture
- Microsoft released patch KB5074109 in January, enforced during April
- Attacks to RC4 (luckily others cannot be mounted)
  - Kerberoasting
  - AS-REP roasting
  - Pass the ticket
  - Golden ticket
  - Silver ticket
  - NTLM relay
  - Pass the hash

Lifecycles as a security threat

Withdraw timescale in cryptography is usually about 10-15 years

Qubit® Conference

Algorithm	Standard	Withdraw	Where you can find it
SSLv2	1994	2011	Old equipment
SSLv3	1996	2015	Old equipment
TLSv1.0	1999	2018	Still used
TLSv1.1	2006	2020	Still used
DTLSv1.0	2006	2020	Still used

Currently, depending on the version, more than 50 attack methods exist, and some versions have no available fixes.

How are your systems doing?

Most frequent issues: lack of certificate management

Qubit® Conference

Incident	Year	Problem	Mitigation
Debian RNG	2006–2008	Predictable key material	Months
Dual_EC_DRBG	**2007–2013**	**Decrypting of encrypted channels**	**Years**
DigiNotar	2011	Complete loss of trust provided by CA	Months
Heartbleed	2014	Key material could available (include private keys)	Months
SHA-1 migration	**2014–2017**	**Obsoleted algorithm**	**Years**
Logjam	2015	Weak DH parameters – Decrypting of encrypted channels	Months
DROWN	2016	Weak protocol – Private keys was computable	Months
ROCA	**2017**	**Weak RSA key generator - Private keys was computable**	**Months to years**
Twitter/X (TLS certificate)	*2020*	*Certificate management – Loss of trust*	*Hours*
Let's Encrypt root expiration	**2021**	**Trust chain expiration – Loss of trust**	**Years**
Twitter/X (TLS certificate)	*2022*	*Certificate management – Loss of trust*	*Hours*

How are your systems doing?

Example of worldwide impact

Qubit® Conference

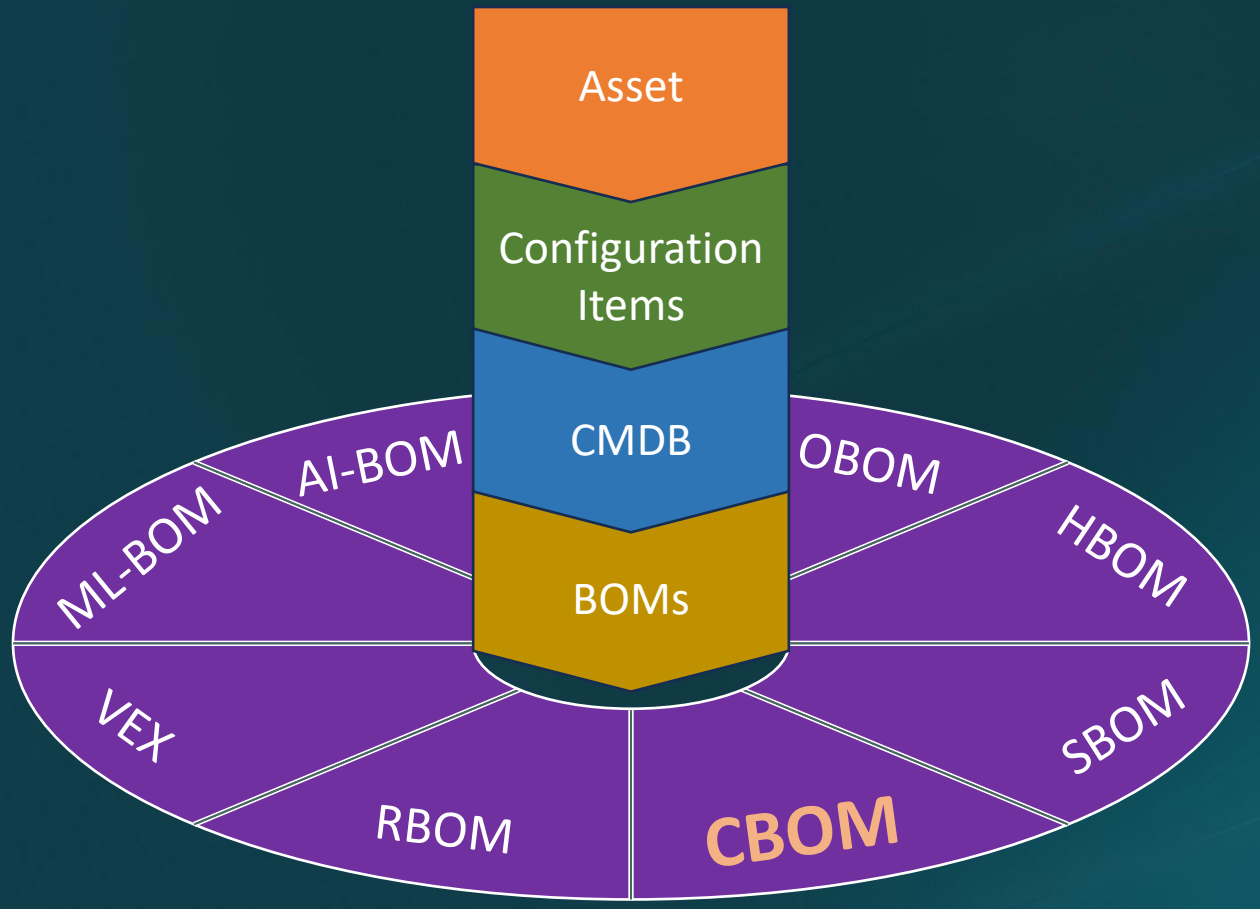
Incident	Year	Problem	Mitigation
ROCA	2017	Weak RSA key generator - Private keys was computable	Months to years

Details:

- Infineon TPM & encryption chips affected (smart cards, secure elements)
- Faulty library generated weak RSA keys
- ~760,000 keys found; estimated 50 millions
- Impacted systems: TPMs, smart cards, tokens, TLS/HTTPS certs, software signing keys
- Costs for key replacement estimated up to 1 billion Eur
- Costs for device replacement estimated up to 300 millions Eur
- Plus, prices of audits

How Crypto Agility Benefits You

Interesting relation: Asset management and Flexibility



CBOM (**C**ryptography **B**ill **o**f **M**aterials)

Consist:

- Libraries
- Protocols
- Algorithms
- Key materials

Scopes:

- Capability
- Dependencies
- Default configuration
- Used settings

Mosca's theorem

Not only quantum computer can endanger security of your data ...

Qubit® Conference

$$X + Y > Z$$

X Migration time 🛠️

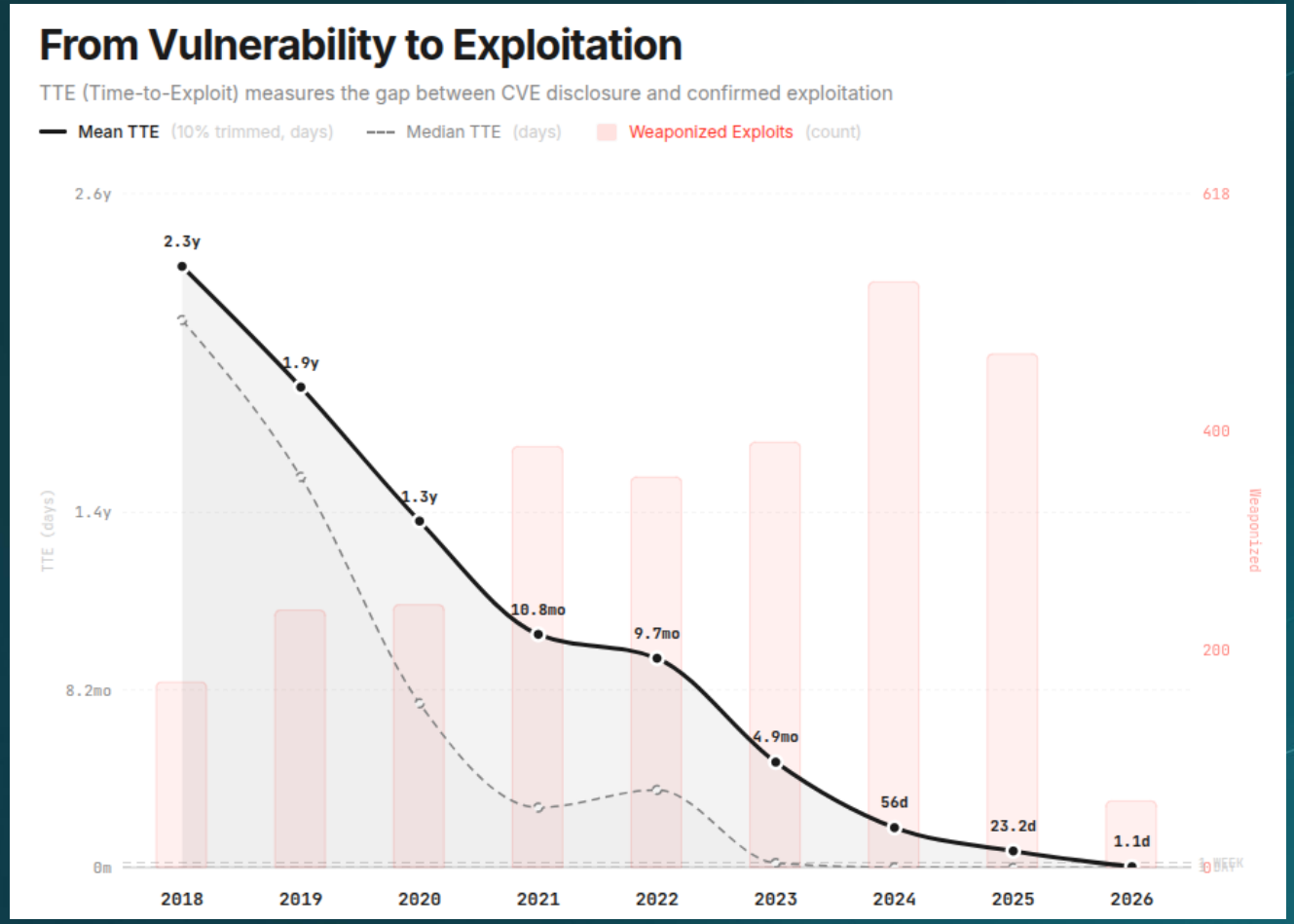
Y Security shelf life 🟩🟦

🕐 **Z** Time to compromise

☠️ Secret keys compromised

Time to exploit

Cybercrime and AI twist the game, this will affect cryptography also



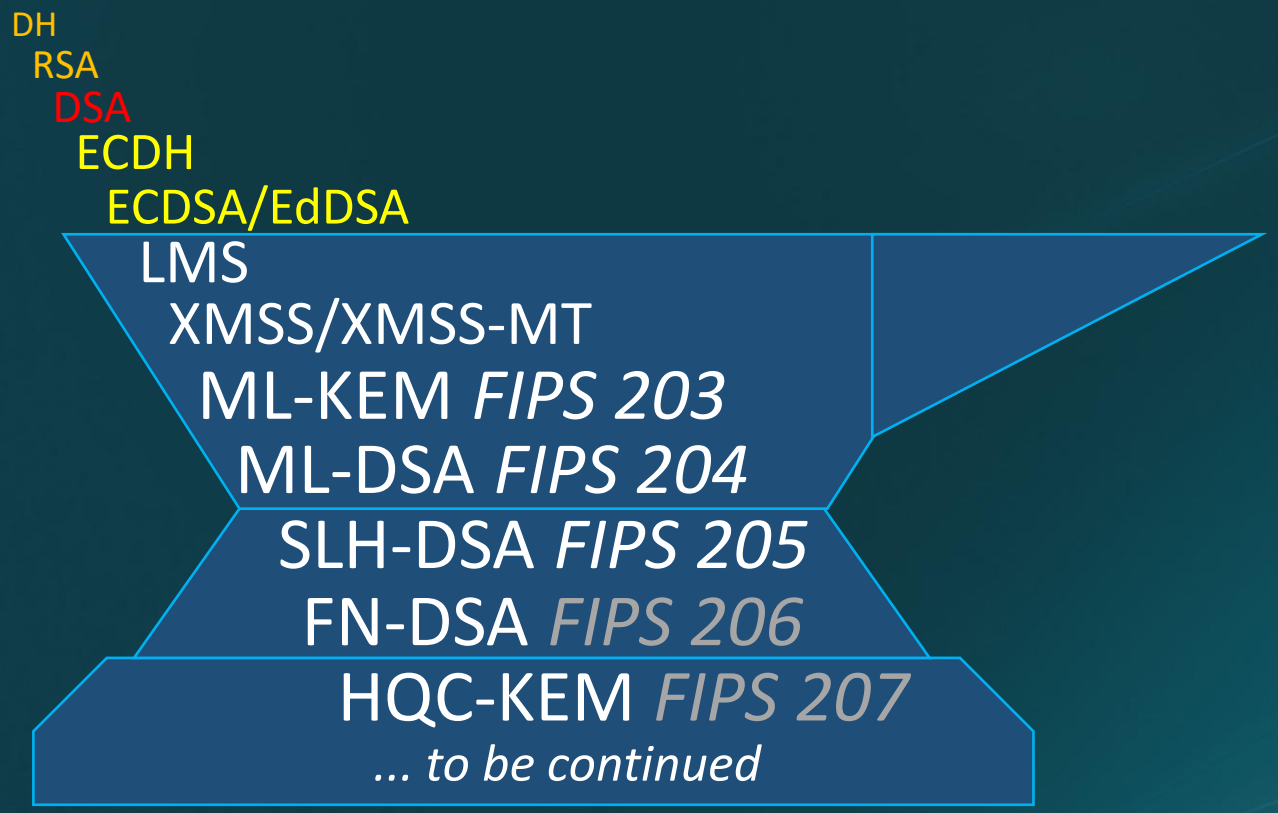
15 years versus prediction

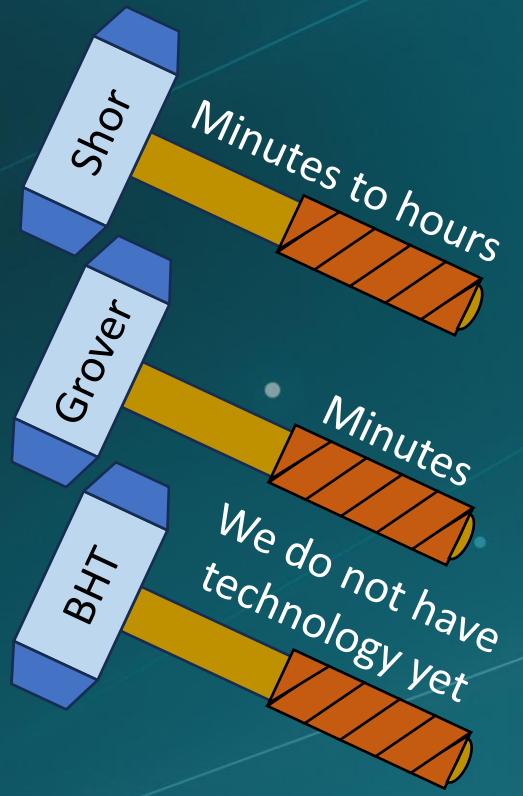
- 2026 - 1 day
- **2027 - 10 minutes**
- **2028 - 1 minute !!!**

Source: https://zerodayclock.com/

Quantum computer threat

Current cryptography will not be sufficient soon

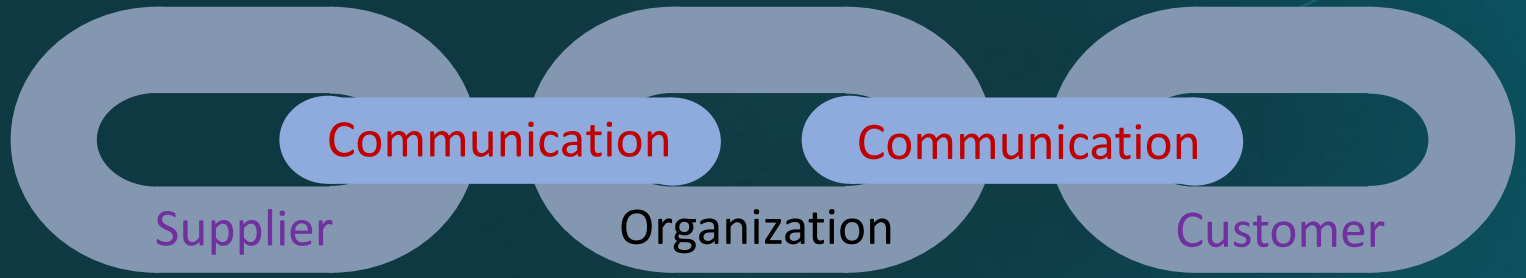




Quantum algorithms

Supply chain

Why you should be interested in enforcing strong protection



- Start with internal enforcement (*faster, cheaper, under your control*)
- Comply with laws, standards, and best practices (*avoid penalties, reduce risk, baseline of security*)
- Take partner audits seriously (*how much you can trust a partner*)
- Enforce accountability through contracts (*ensure partners take security obligations seriously*)
- Exchange basic CBOM information (*clarifies capabilities and flexible changes*)
- Disable fallback to weak security (*part of defence against attackers*)
- Define a minimum-security baseline (*ensures consistent quality across all partners*)

What is a requirements

Record, measure, evaluate, manage … and comply

Qubit® Conference

Minimum level of quality:

1) Ensure compliance - make rules legally binding
2) To reduce legal risk, align with key regulations (NIS2, CRA, DORA)
3) Adopt proven widely accepted standards (ISO 27001, 27002, 27005, 21827)
4) Maintain strong asset management, which give you full visibility and control
    - To improve transparency, require CBOM from external applications
    - Enable faster risk assessment by use complete security metadata (CBOM, SBOM, RBOM, VEX)

What is a goal?

How can you save costs and time? By policy driven management.

Qubit® Conference

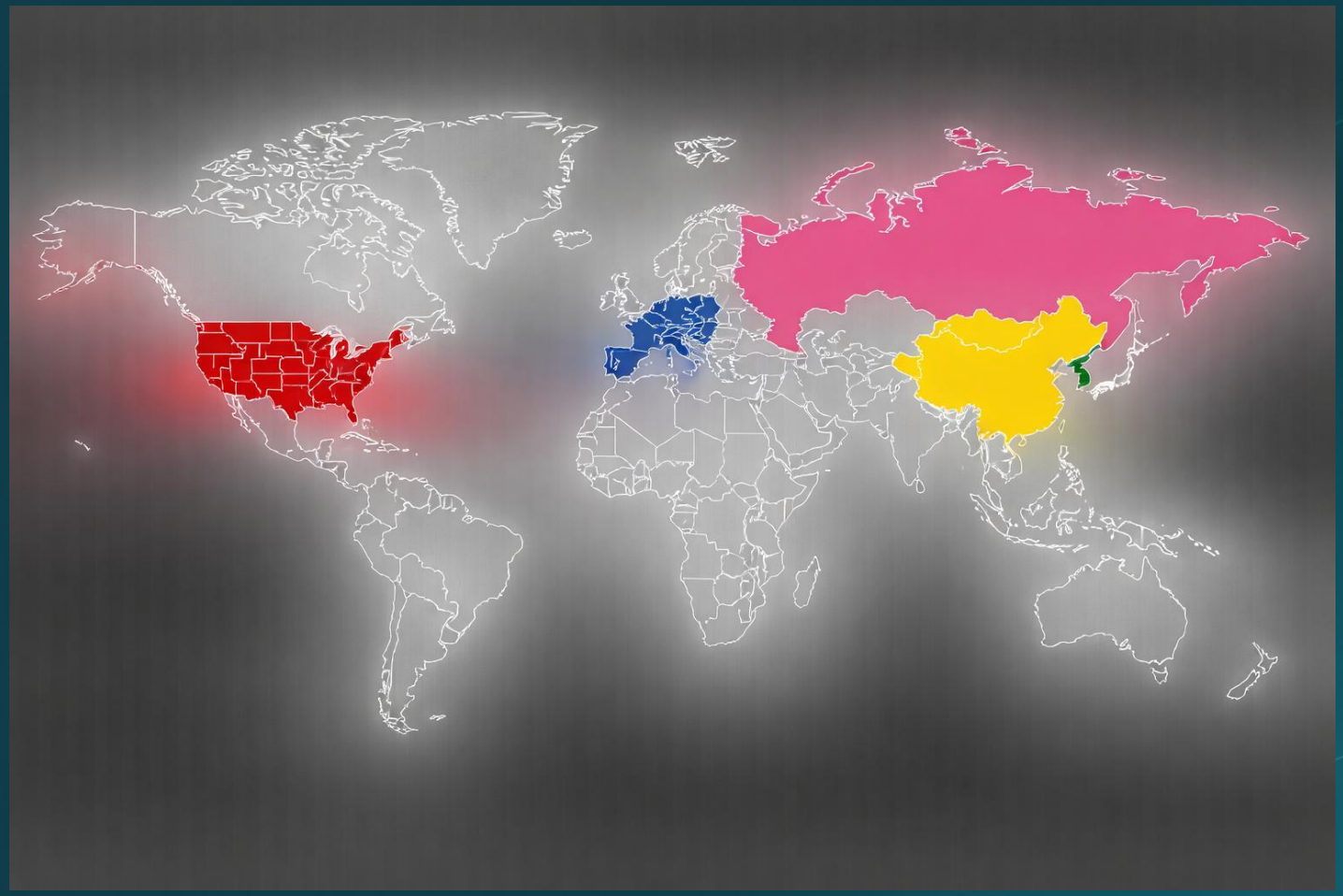
It is doable? Yes.

1) Asset management allow you to own knowledge about your systems
2) CBOM, SBOM, RBOM and similar will help you understand configuration and capability of systems
3) VEX allow you to know and understand actual threat and exploits
4) Appropriate measurement allows you to understand needs
5) Policy driven settings allow you to do changes in minutes, rather than months

Are you interested?

Dark side: Geopolitical context

Export of soft power and projecting power through standardization



Specific regulations:

- China (OSCCA)
- EU (ENISA, ETSI, ITU-T)
- Japan (CRYPTREC)
- Russian Federation (GOST)
- South Korea (NIS, NSR)
- USA (NIST)

Conclusion

Crypto agility is a difficult journey, but other paths are suicidal.

Qubit® Conference

Starring:

Cryptography
Compliance
Asset management
Monitoring
Evaluation of assets
Threat modelling
Risk analysis
Technology
Processes
Reporting
Policies

and many others …

Qubit® Conference

Thank you for attention

Jan Dušátko
jan.dusatko@cryptosession.cz