RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: SDS-R02

Building the Roots of the Quantum-Safe World

Avesta Hojjati, PhD (in progress)
Head of R&D
DigiCert Inc.

Alexander Truskovsky, MBA, MCompSc, CISSP
Director, Technical Strategy
ISARA Corporation

Avesta Hojjati, PhD (in progress)

Avesta is the head of R&D at DigiCert where he manages advanced development of cybersecurity products. Prior to DigiCert, Avesta was part of the Symantec and Yahoo security teams. Avesta focuses on applied cryptography, post-quantum cryptography, blockchain, and IoT. Avesta earned his Master's in Computer Science from University of Illinois at Urbana Champaign and is currently completing his PhD.

Alexander Truskovsky, MBA, MCompSc, CISSP

Alexander is responsible for technical strategy at ISARA. Previous to ISARA, he provided technical leadership in the development of core security protocols and features at BlackBerry and designed and built enterprise software at Oracle. He has a Master of Computer Science focusing on applied cryptography, an MBA, and holds a CISSP designation. He holds 20 patents in areas of security protocols.

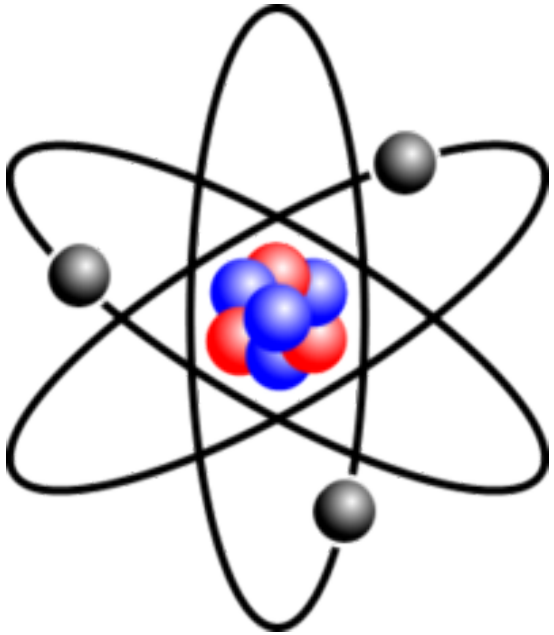
Agenda

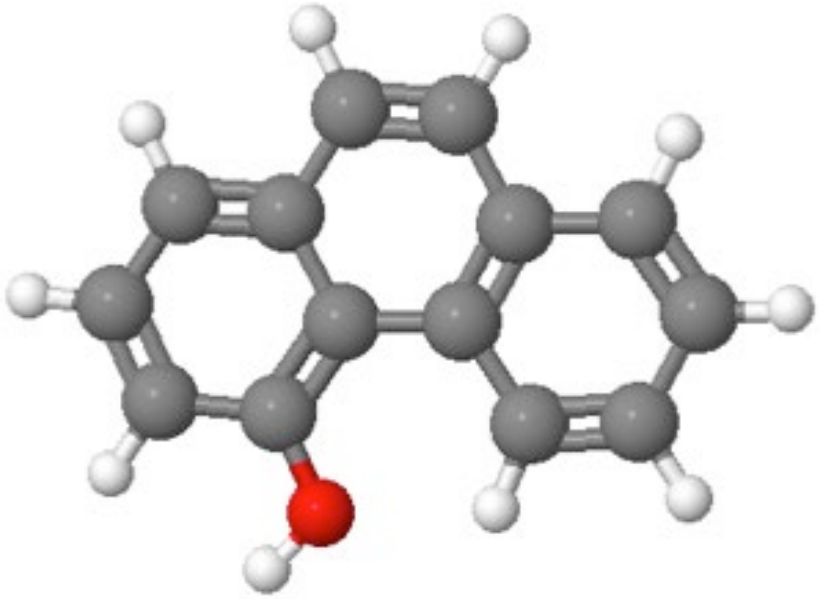
- Quantum Computing
- Threat & Mitigation
- Migration Challenges & Crypto Agility
- Quantum-safe Roots of Trust and Code Signing
- Conclusions

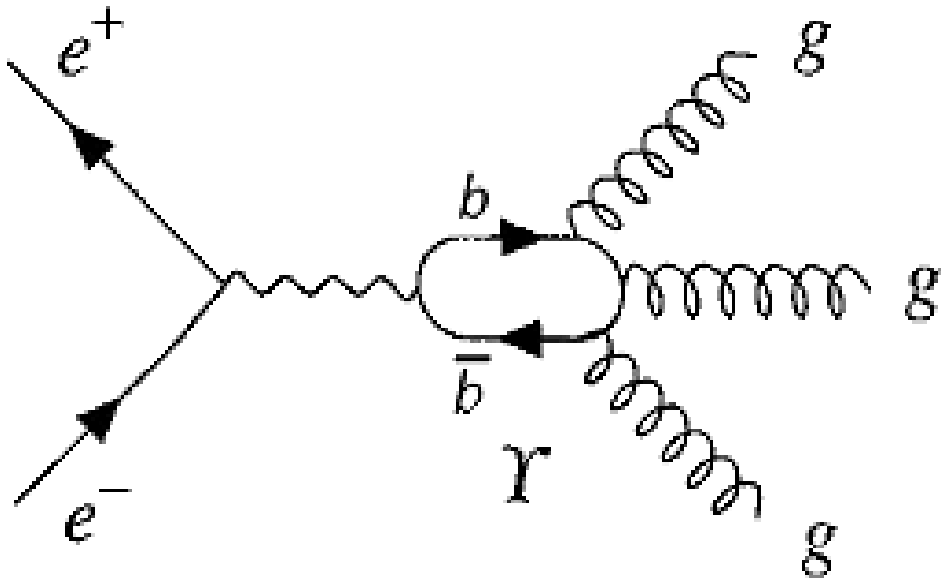
RSAConference2019
Asia Pacific & Japan

Quantum Computing

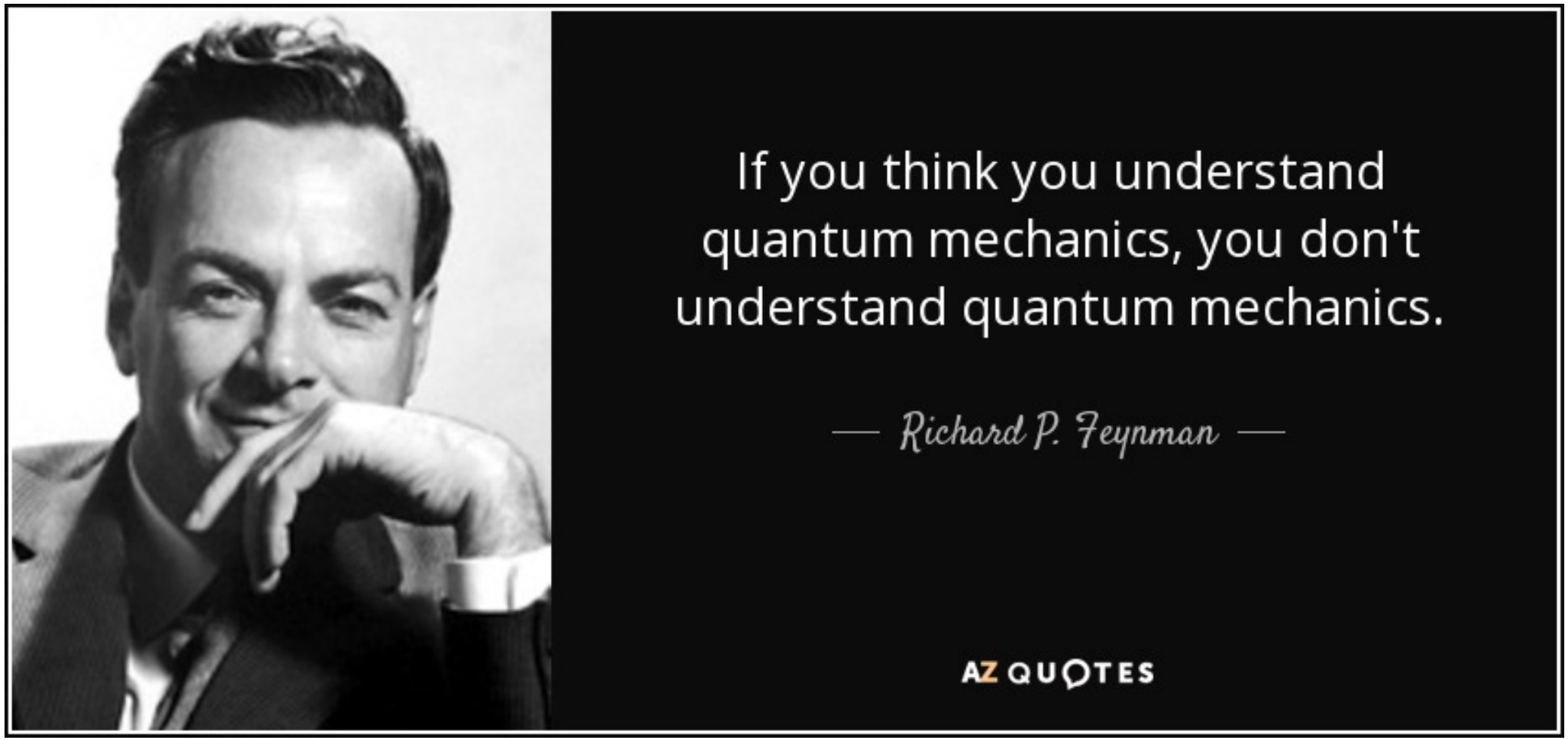
QUANTUM MECHANICS



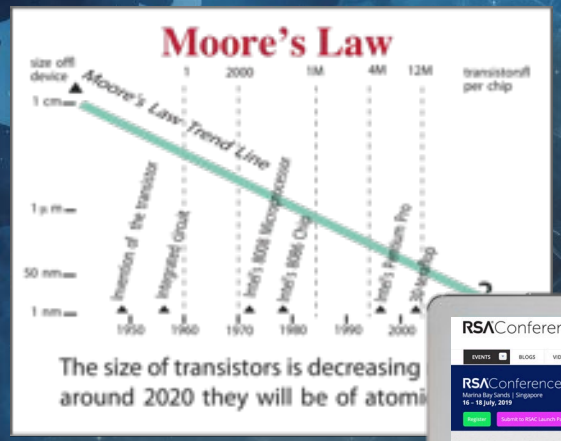


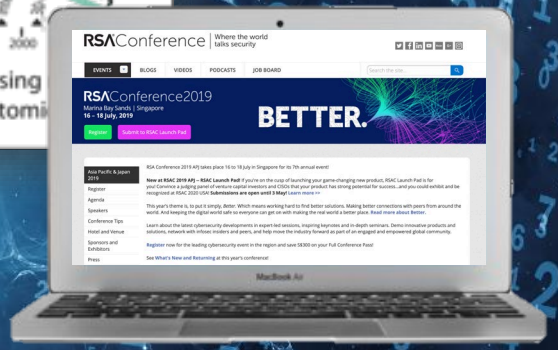


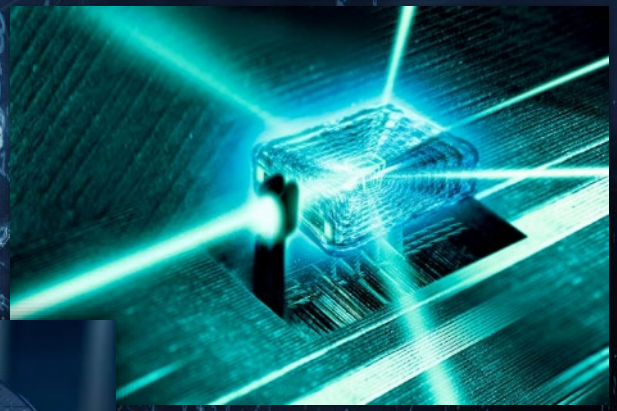
THE WORLD IS NOT WHAT IT SEEMS

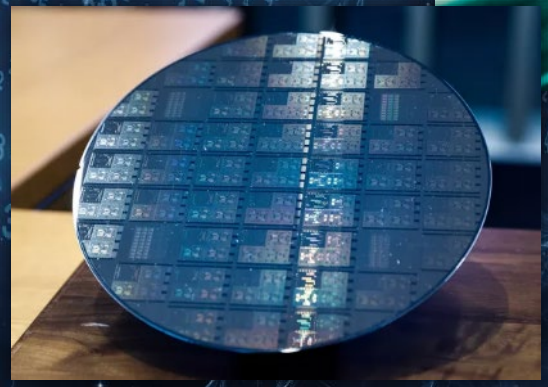

If you think you understand quantum mechanics, you don't understand quantum mechanics.
— Richard P. Feynman —
AZ QUOTES

QUANTUM COMPUTING IS THE MARRIAGE OF...









INFORMATION THEORY

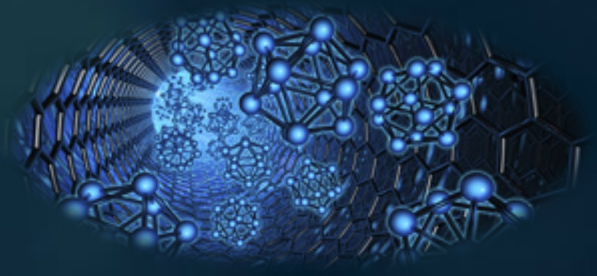
QUANTUM MECHANICS

QUANTUM vs CLASSICAL

Horsepower
December 17, 1903

1st Flight of Wright Flyer I
December 17, 1903

POSITIVE DISRUPTIONS



MATERIAL DESIGN

CHEMICAL DISCOVERY

DRUG DESIGN

OPTIMIZATION

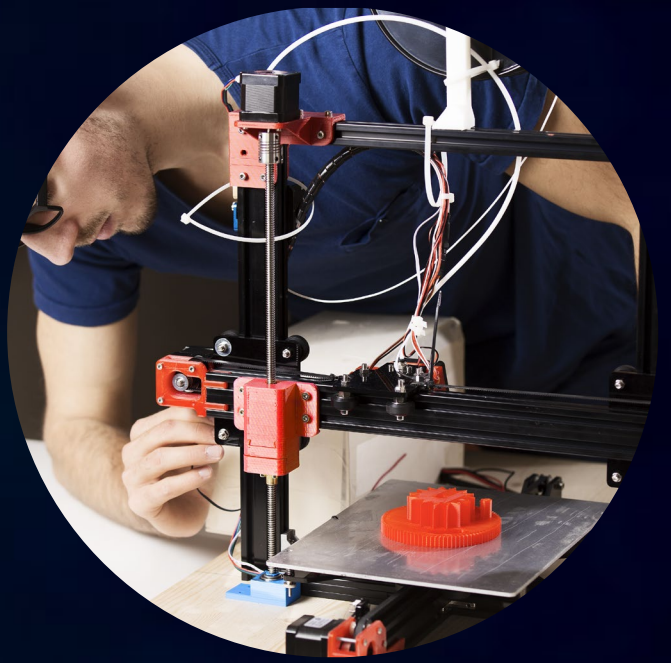
SEARCH/BIG DATA

MACHINE LEARNING

TIMELINE TO QUANTUM

ANALOG QC

NOISY QC



UNIVERSAL QC

The Quantum Race is on






Microsoft

Google

rigetti

D:wave

The Quantum Computing Company™

IBM

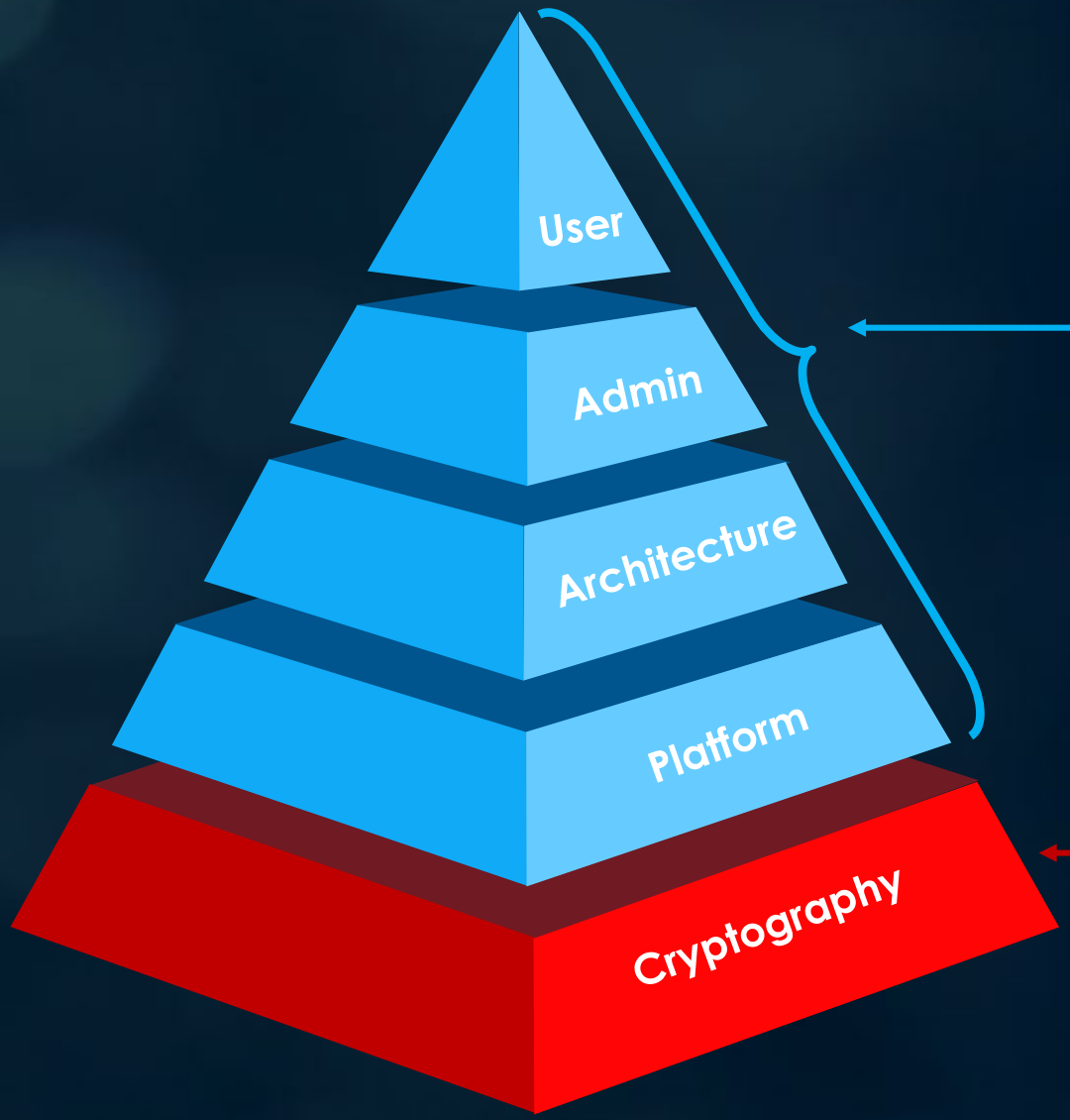
intel

RSAConference2019
Asia Pacific & Japan

Threat & Mitigation

The Quantum Effect on Today's Cryptography

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	



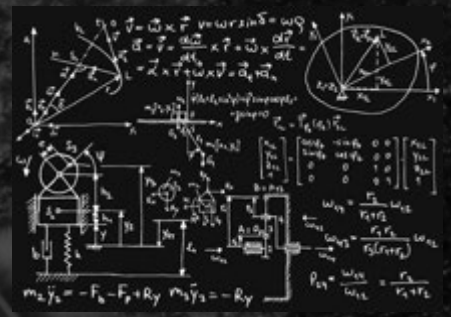
Cause of security breaches today

Quantum: an unprecedented threat looming


IBM
less than
20 years
ETSI
less than
10 years
NIST
less than
11 years
Future
Microsoft
less than
11 years
European
Commission
after 2025

PATHWAYS TO QUANTUM SAFETY

Quantum Key Distribution



Quantum-Safe Cryptography

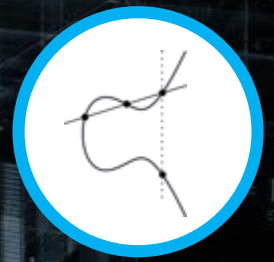
THE "NEW" MATH

Hash-based

Code-based

Lattice-based

Multivariate-based

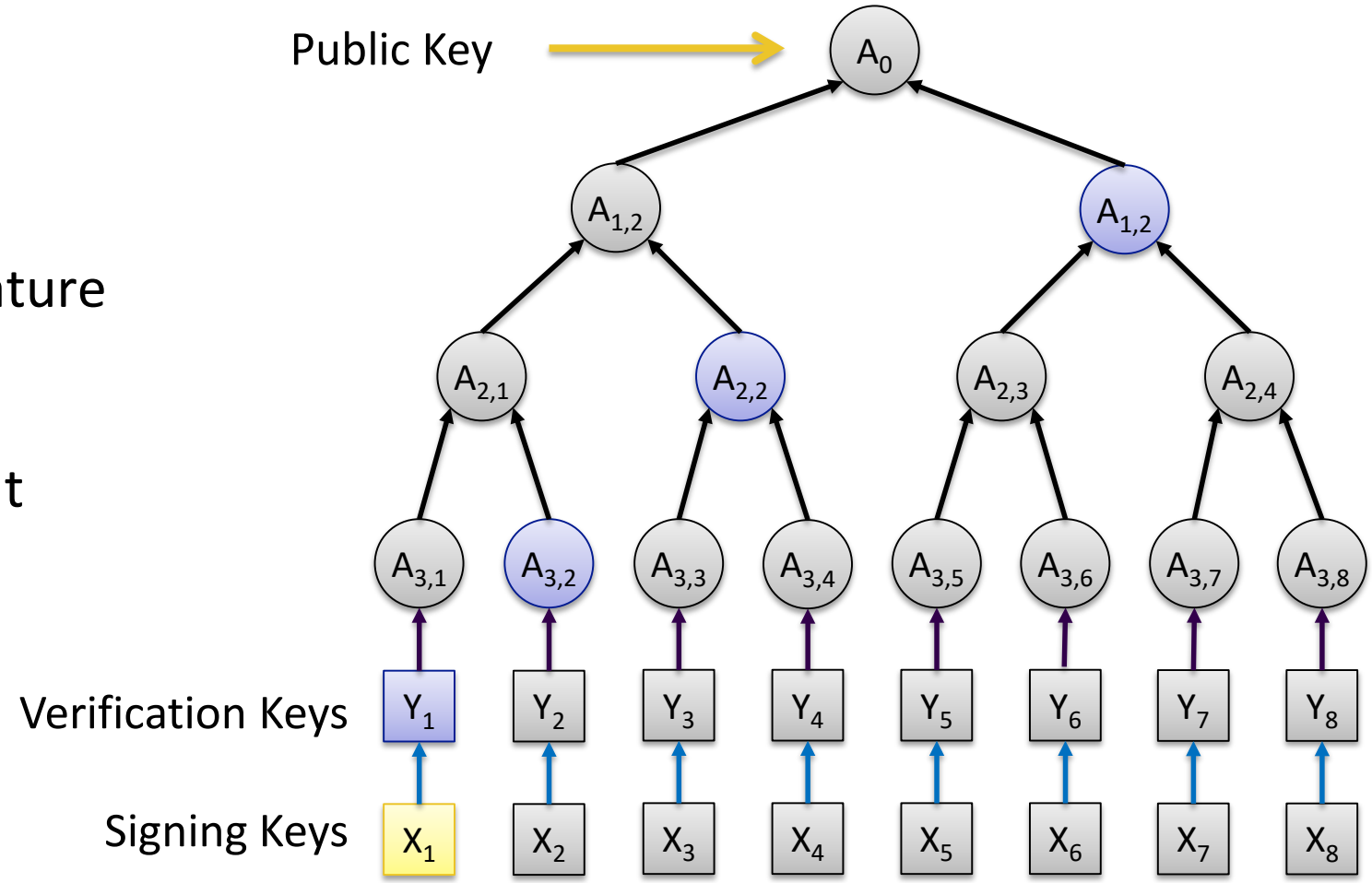


Isogeny-based

ISARA

Hash-Based Cryptography

- Introduced by Merkle in 1979
- Uses “one-time signatures”
- Small public key, medium signature size, very large private key
- Key generation can be slow, but signing & verification is fast
- Private key is stateful
- Can be used today



Quantum-safe Asymmetric Algorithms (Table 1 of 2)

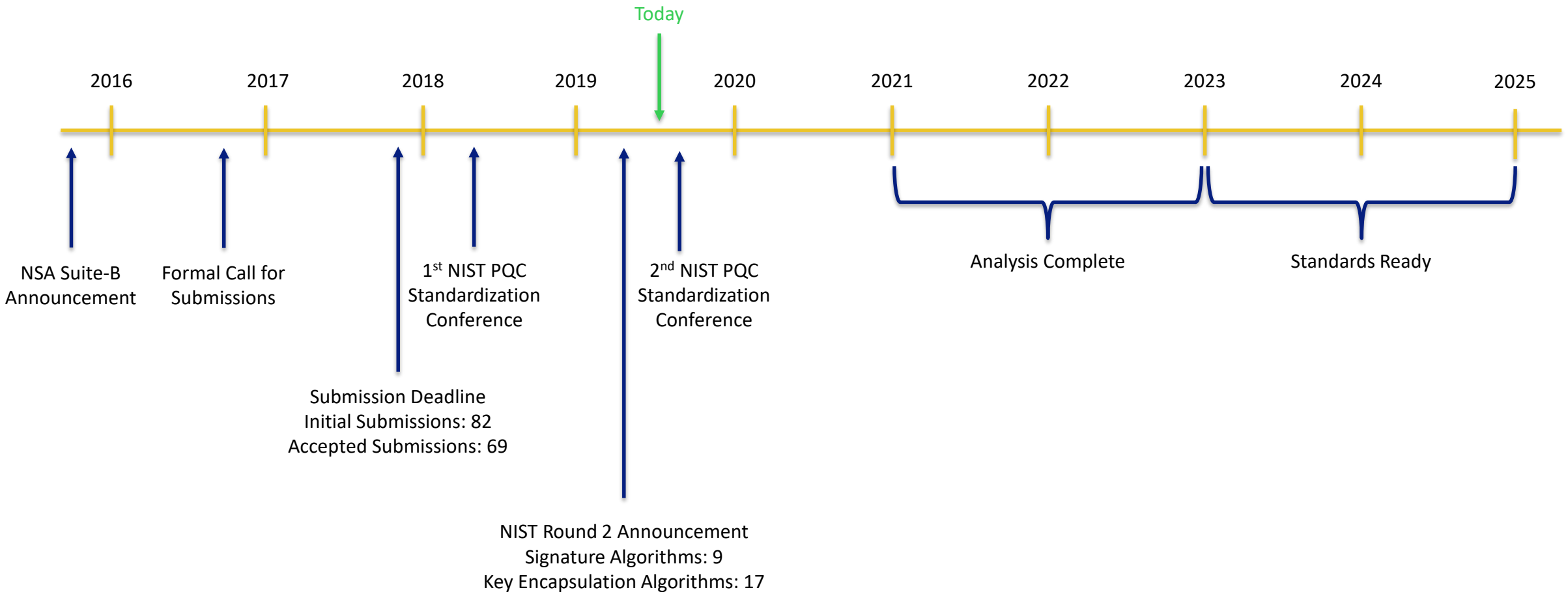
Scheme	Family	Type	Secret Key (Octets)	Public Key (Octets)	Signature (Octets)	Ciphertext (Octets)	Shared Secret (Octets)
LMS	Stateful Hash-based	Signature	56 + (2,064 - 2,147,483,664)	32	1,296 - 9,328	–	–
XMSS	Stateful Hash-based	Signature	104 + (65,568 - 67,108,896)	32	2,500 – 2,820	–	–
SPHINCS	Stateless Hash-based	Signature	64 - 128	32 - 64	8,080 - 49,216		
BIKE	Code-based	KEM	3,194 - 11,749	1,478 - 11,217	–	1,478 - 11,217	32
Classic McEliece	Code-based	KEM	6,452 - 14,080	261,120 - 1,357,824	–	128 - 240	32
HQC	Code-based	KEM	40	3,125 - 8,897	–	6,234 - 17,777	64
LEDAcrypt	Code-based	KEM	24 - 40	1,872 - 8,520	–	1,872 - 4,616	32 - 64
NTS-KEM	Code-based	KEM	9,248 - 19,922	319,488 - 1,419,704	–	128 - 253	32
ROLO	Code-based	KEM	40	465 - 2,493	–	465 - 2,621	40 - 64
RQC	Code-based	KEM	40	853 - 2,284	–	1,690 - 4,552	64
Kyber	Lattice-based	KEM	1,632 – 3,168	800 – 1,568	–	736 – 1,568	32
FrodoKEM	Lattice-based	KEM	19,888 - 43,088	9,616 - 21,520	–	9,720 - 21,623	16 - 32
LAC	Lattice-based	KEM	1,056 - 2,080	544 - 1,056	–	712 - 1,424	32
NewHope	Lattice-based	KEM	1,888 - 3,680	928 - 1,824	–	1,120 - 2,208	32

Quantum-safe Asymmetric Algorithms (Table 2 of 2)

Scheme	Family	Type	Secret Key (Octets)	Public Key (Octets)	Signature (Octets)	Ciphertext (Octets)	Shared Secret (Octets)
NTRU	Lattice-based	KEM	935 - 1,592	699 - 1,230	–	699 - 1,230	32
NTRUPrime	Lattice-based	KEM	1,125 - 1,999	897 - 1,322	–	897 - 1,184	32
Round5	Lattice-based	KEM	16 - 32	445 - 14,264	–	549 - 14,288	16 - 32
SABER	Lattice-based	KEM	1,568 - 3,040	672 - 1,312	–	736 - 1,472	32
Three Bears	Lattice-based	KEM	40	804 - 1,584	–	917 - 1,697	32
Dilithium	Lattice-based	Signature	96 - 2096	896 – 1,760	1,387 – 3,366	–	–
Falcon	Lattice-based	Signature	4,097 – 8,193	897 – 1,793	618 – 1,233	–	–
qTesla	Lattice-based	Signature	1,216 - 12,352	1,504 - 38,432	1,376 - 5,920	–	–
GeMSS	Multivariate-based	Signature	13,415 - 77,712	36,0643 - 3,210,845	33 - 75	–	–
LUOV	Multivariate-based	Signature	32	5,120 – 77,312	311 – 4,390	–	–
MQDSS	Multivariate-based	Signature	16 – 24	46 – 64	20,854 – 43,728	–	–
Rainbow	Multivariate-based	Signature	95,232 - 1,256,551	152,576 - 1,746,432	64 - 204	–	–
SIKE	Supersingular Isogeny-Based	KEM	374 - 644	330 - 564	–	346 - 596	16 - 32
Picnic	Zero-Knowledge Proof/MPC	Signature	16 - 32	32 - 64	13,802 - 209,506	–	–

POST-QUANTUM STANDARDS

NIST PQC Evaluation & Standardization Timeline



RSAConference2019
Asia Pacific & Japan

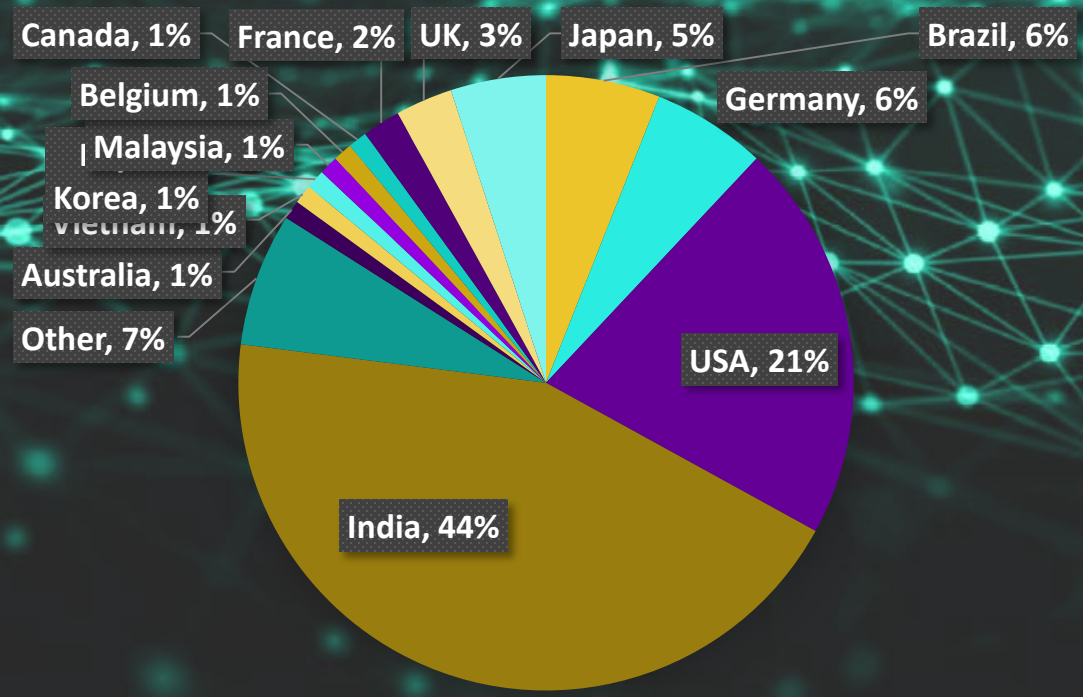
Migration Challenge & Crypto Agility

Hypothetical 15-year View For PQ Crypto

Slide based on Brian LaMacchia

Learning from the past

- Internet Protocol Version 4 (IPv4) has been around since **1981**
- In **1998**, IPv6 became a Draft Standard for the IETF
- **49 countries deliver more than 5% of traffic over IPv6,** with new countries joining all the time.
- Alexa Top Million Websites: **17% with working IPv6**

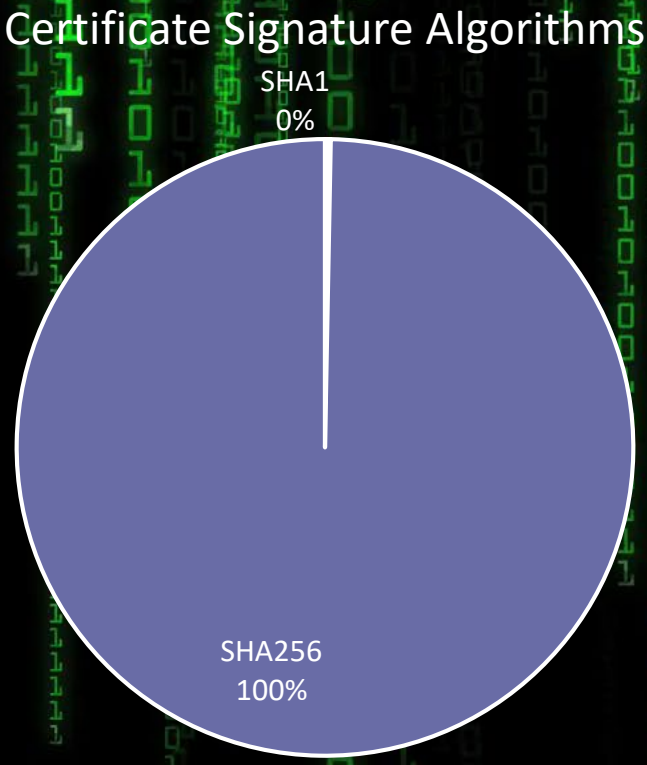


Lessons Learned

- Secure Hash Algorithm 1 (SHA1) was introduced in 1993
- In 2005, it was shown that SHA1 is not collision-resistant
- In 2017, Chrome announced SHA1 to be insecure
- 0% of public websites are using SHA1!

Lessons Learned

- Secure Hash Algorithm 1 (SHA1) was introduced in 1993
- In 2005, it was shown that SHA1 is not collision-resistant
- In 2017, Chrome announced SHA1 to be insecure
- 0% of the public websites are using SHA1!



NIST ON CRYPTO-AGILITY

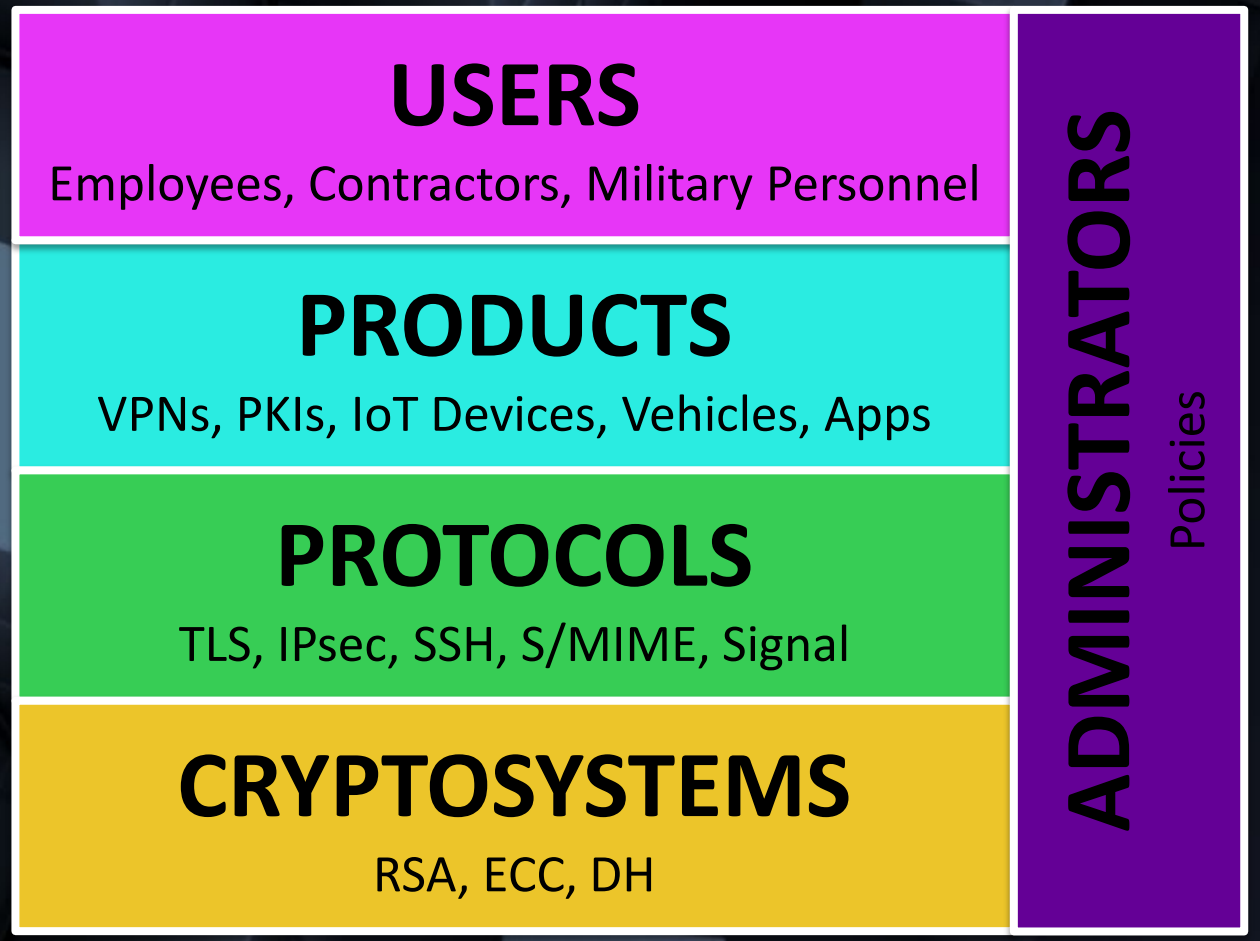
"As the replacements for currently standardized public key algorithms are not yet ready, a focus on **maintaining crypto agility is imperative**.

Until new quantum-resistant algorithms are standardized,
agencies should continue to use
the recommended algorithms currently specified in NIST standards."

- "Report on Post-Quantum Cryptography", NIST, April 2016

NIST
National Institute of
Standards and Technology

What is Crypto Agility?



BRIDGING THE GAP

HOW ARE SECURE COMMUNICATIONS VULNERABLE?

Secure Communication Protocol

Shor's Algorithm **breaks** current public-key algorithms

Key Establishment

Authentication

Grover's Algorithm **weakens** symmetric encryption (square root)

Encrypted Transmissions

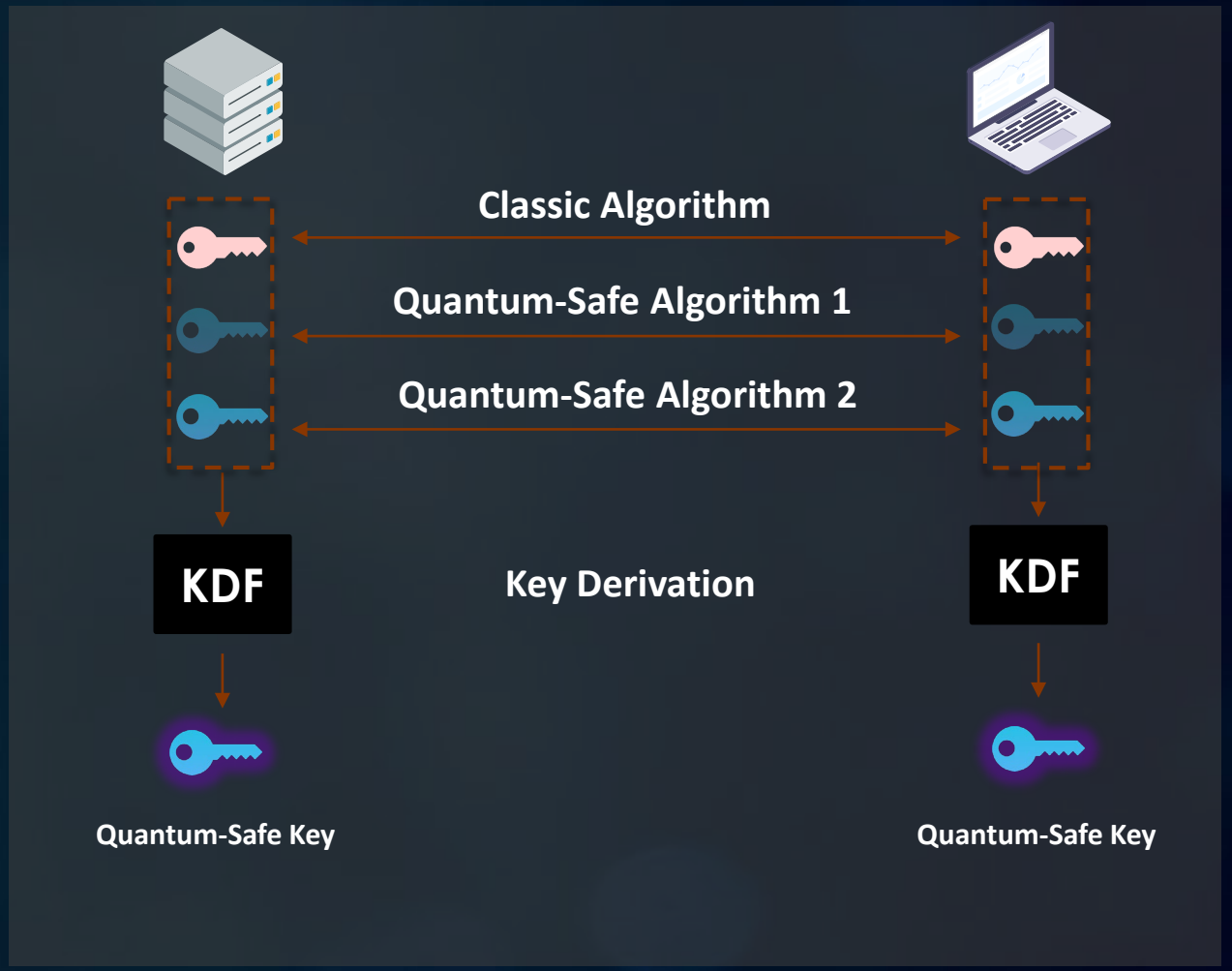
A HARVEST & DECRYPT ATTACK ON VPN

VPN Session

Handshake | **Data Exchange**

Quantum attack using Shor's algorithm → **Key Establishment** → Obtain private key → **Ciphertext** → Decrypt using extracted key → **Plaintext**

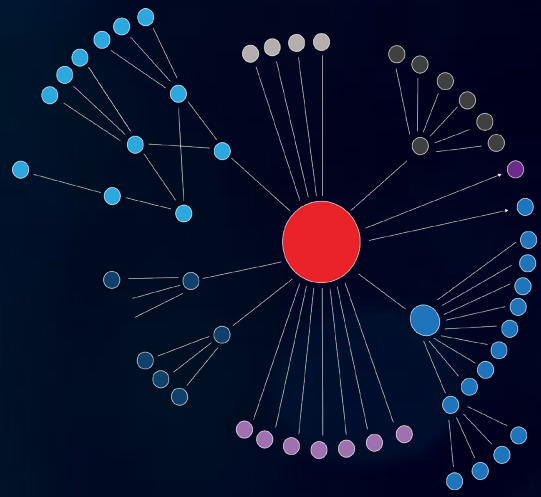
HYBRID KEY ESTABLISHMENT



THE MIGRATION CHALLENGE
KEY ESTABLISHMENT vs AUTHENTICATION

Key establishment can be **easily upgraded** because the client and server negotiate which algorithm to use.

1) Use quantum-safe **key transport** or **key agreement** algorithms
2) Use **hybrid keys**, a mix of both classic and quantum-safe algorithms



The complexity and interconnectivity of public key infrastructure demands action today in order to be ready for the quantum age, and difficult to do while maintaining backward compatibility.

DoD PKI MIGRATION

There's more than
4.5 million active users
in the DoD identity management system.

Creating a quantum-safe duplicate infrastructure is time-consuming and cost prohibitive.

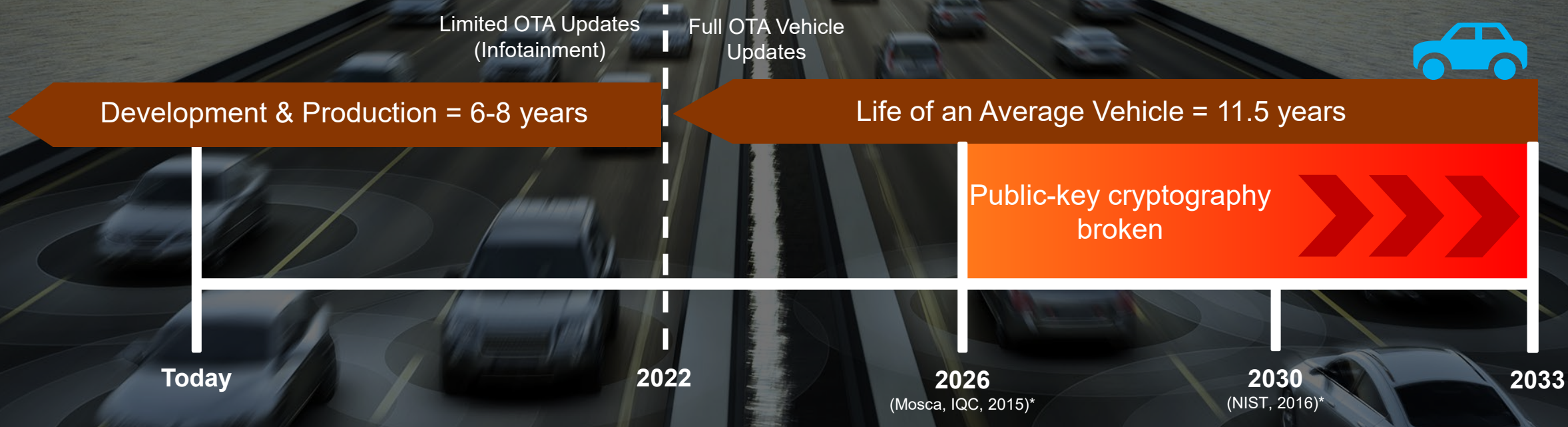
ISARA

Certificates Support a Single Algorithm

RSAConference2019
Asia Pacific & Japan

Quantum-safe Roots of Trust and Code Signing

PRIORITIZING THE FIX FOR TOMORROW'S THREAT



*Mosca, Michele., Institute for Quantum Computing. 2015. "Cybersecurity in an era with quantum computers: will we be ready?". https://eprint.iacr.org/2015/1075.pdf
*NIST. April 2016. "Report on Post-Quantum Cryptography". http://dx.doi.org/10.6028/NIST.IR.8105

AUTHENTICATED SOFTWARE UPDATES

What's at risk?

Durable connected devices (IoT) **with long in-field lives** (i.e. connected cars, medical devices, satellites).

What's the attack?

Forged software updates: quantum-enabled adversaries will be able to sign software updates that appear authentic, injecting malicious code onto the device to take it over.

How to protect against it?

Physically embed stateful hash-based roots of trust today to avoid costly, logistically challenging recalls in the future.

NIST on Stateful Hash-based Signatures (HBS)

- HBS schemes are good candidates for early standardization because they're trusted, mature, and well understood
- NIST is actively reviewing XMSS and LMS for early approval outside the Post-Quantum Standardization Process
- NIST is considering stateful HBS for specific use-cases, such as code-signing
- The security of an HBS scheme relies on the same basis as many current NIST-approved cryptographic algorithms and protocols, and no known quantum algorithms pose a practical threat

Stateful HBS Implementation Considerations in HSM

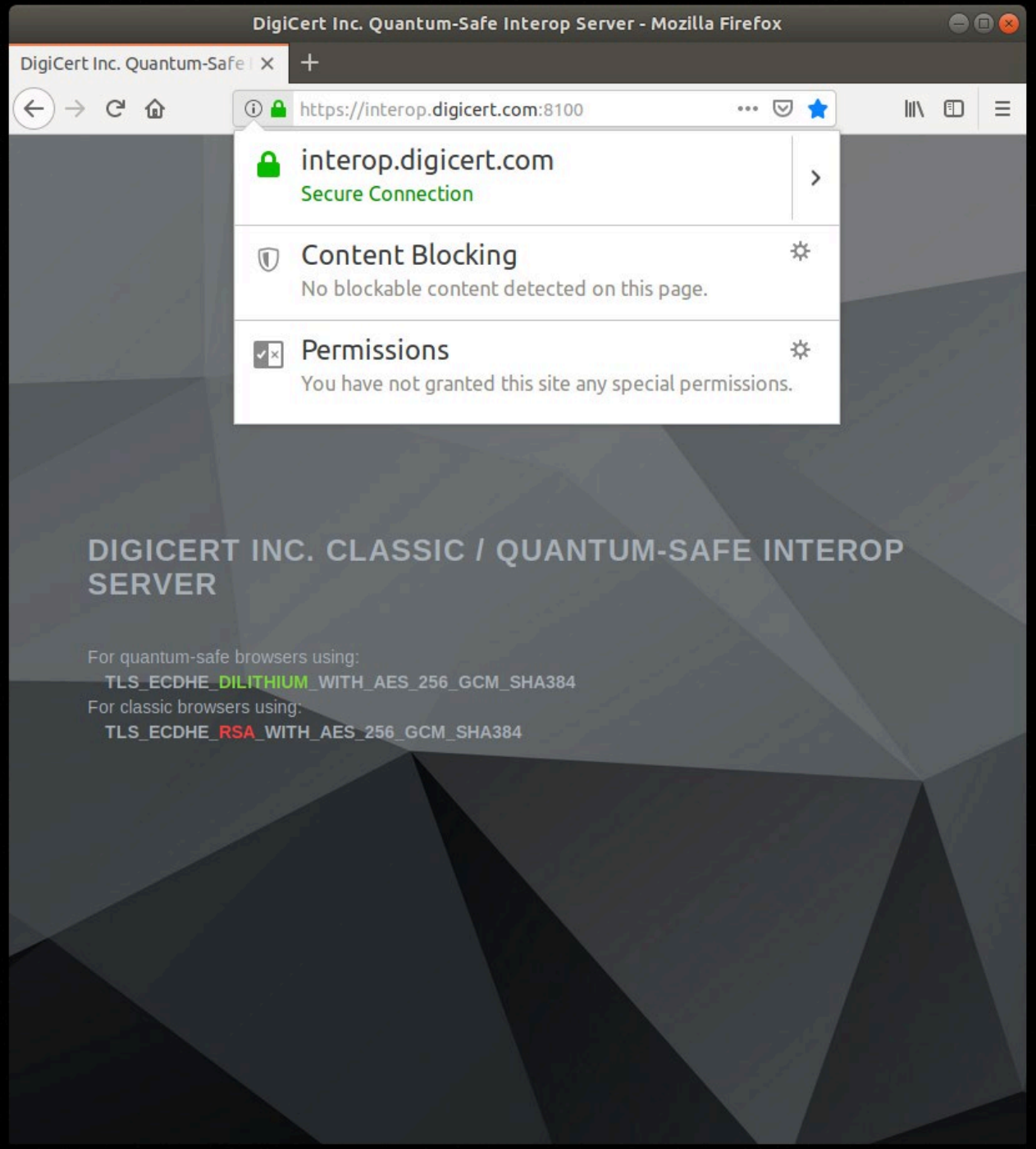
- If not implemented properly, stateful HBS are vulnerable to misuse
- Stateful HBS signing keys are strictly one time use only
- The full private key needs to be split up for 1) back up and 2) to reserve a part of it for revocation, all parts need to be managed completely independently
- The full tree, or a part of it, is often too large to fit in an HSM without using tree compression
- At run time a range of keys needs to be loaded but before any of them are used, they need to be marked as used up

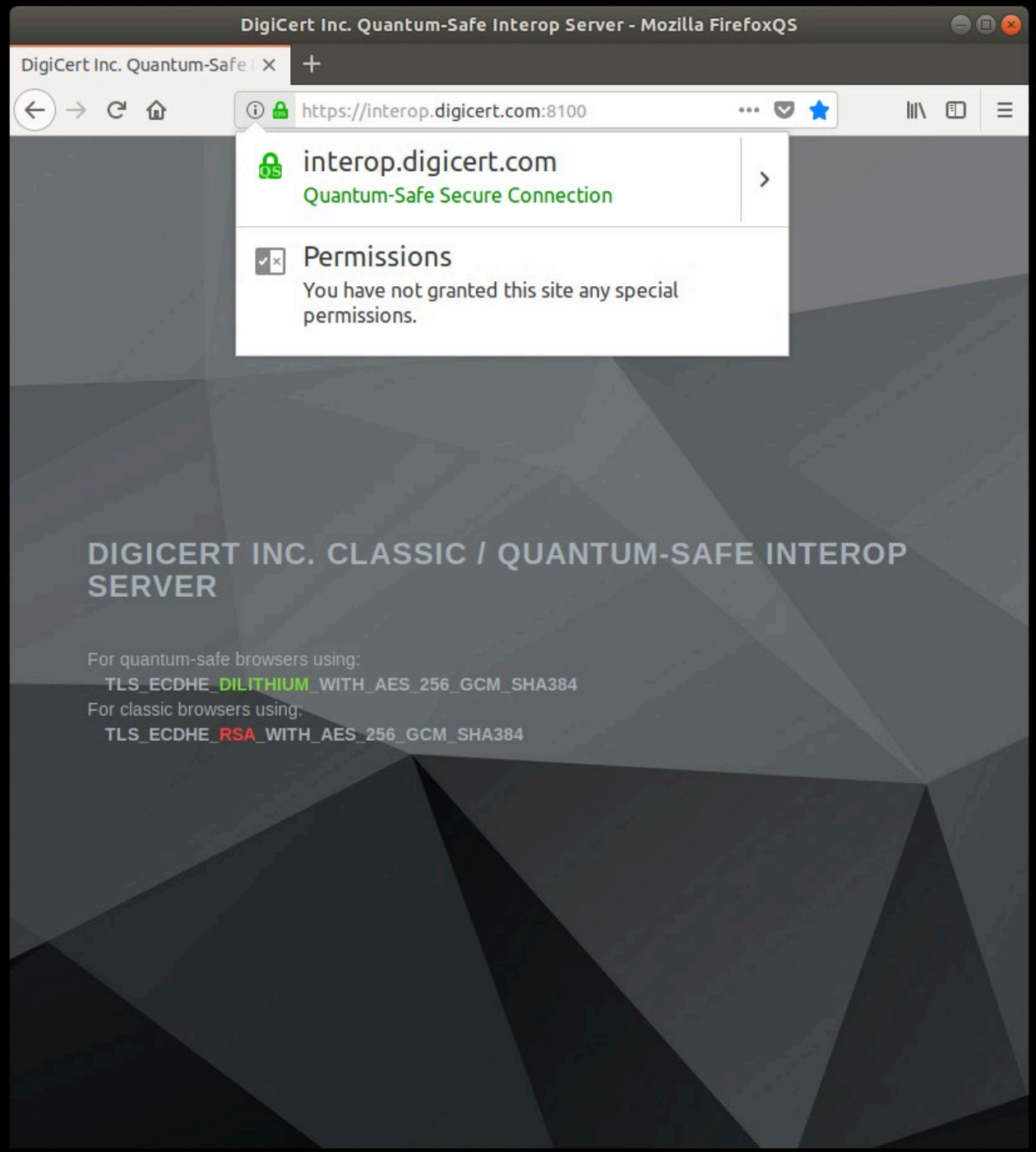
Operational Implications When Using HBS

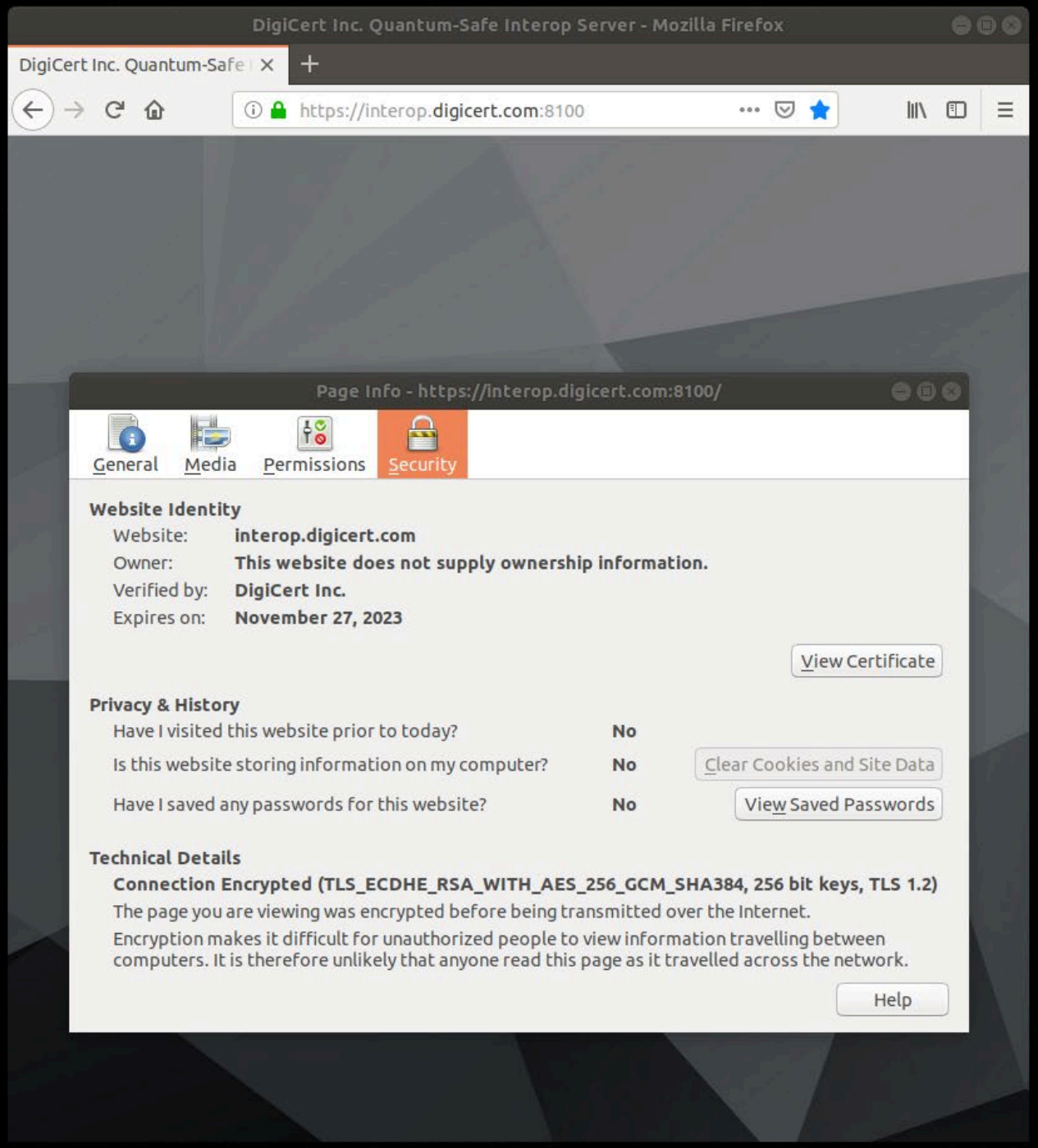
- The private key of a stateful HBS scheme is an “exhaustible” resource, so careful planning is required or you’ll run out of keys
- Signature size grows as the size of the private key grows
- Private key splitting and state management is not something the industry has had to deal with before
- For extremely high-value root keys that don’t produce many signatures during their validity a manual process for state management may be required

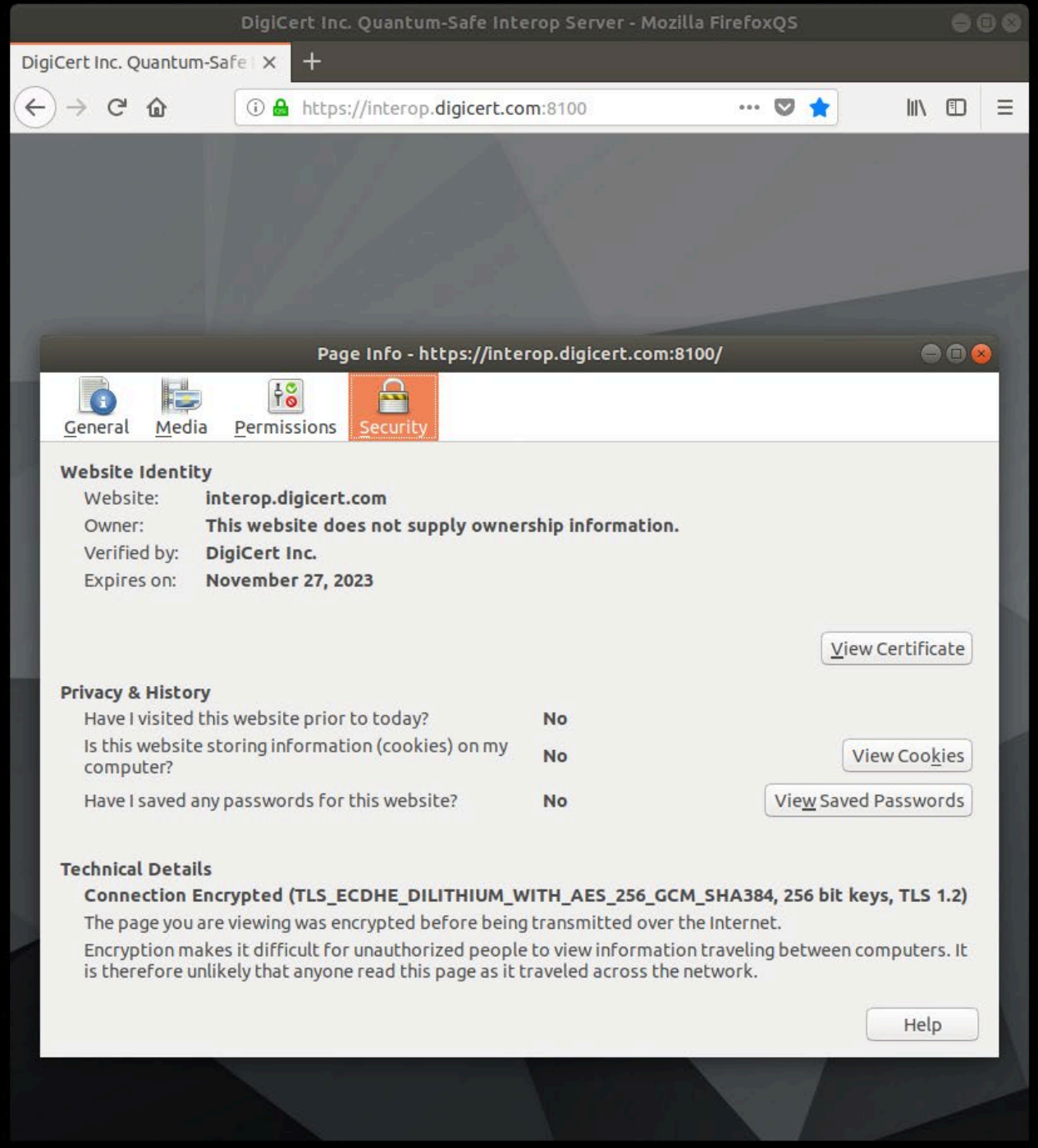
RSAConference2019
Asia Pacific & Japan

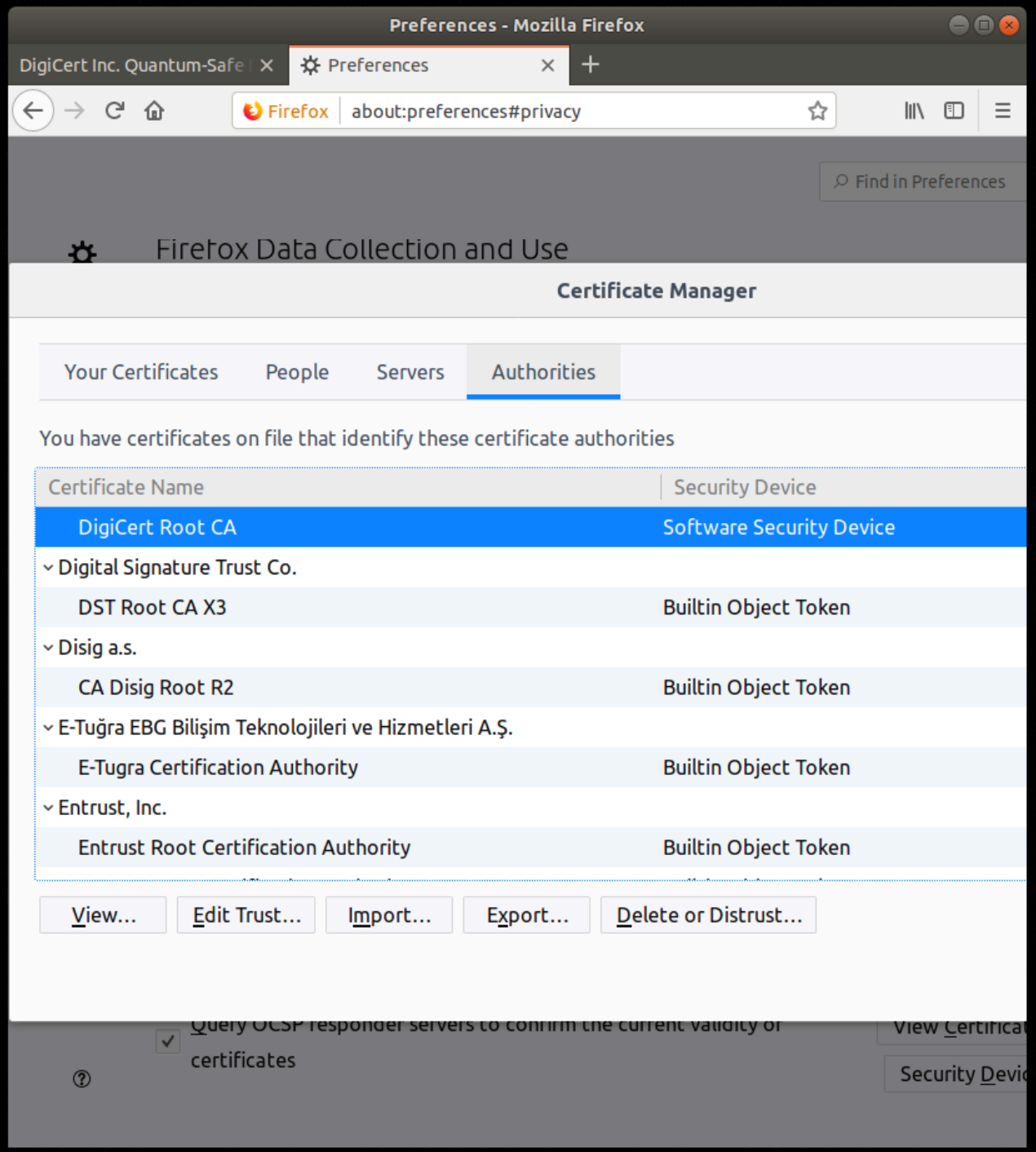
Demo

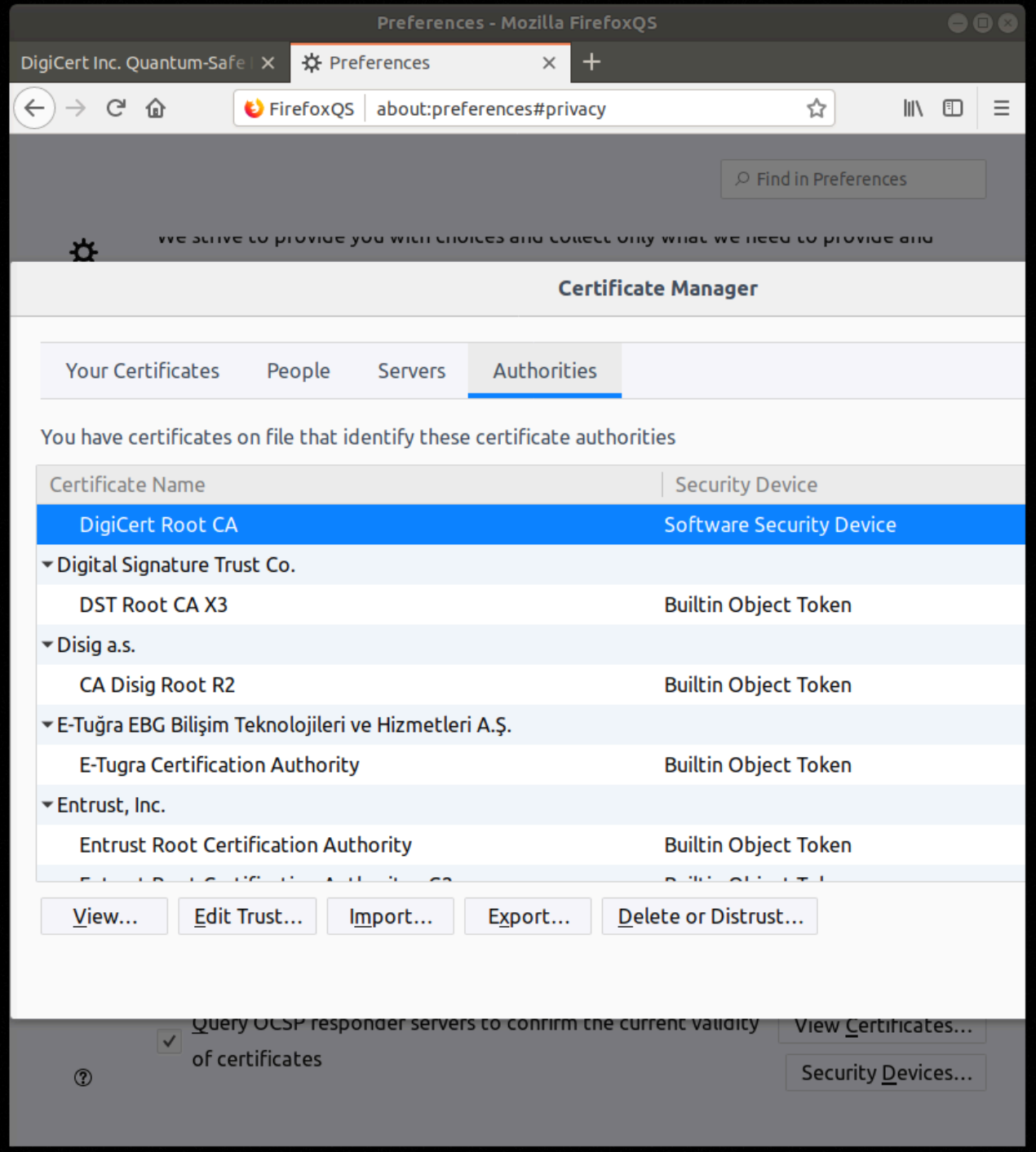

DigiCert Inc. Quantum-Safe Interop Server - Mozilla Firefox
DigiCert Inc. Quantum-Safe
https://interop.digicert.com:8100
interop.digicert.com
Secure Connection
Content Blocking
No blockable content detected on this page.
Permissions
You have not granted this site any special permissions.
DIGICERT INC. CLASSIC / QUANTUM-SAFE INTEROP SERVER
For quantum-safe browsers using:
TLS_ECDHE_DILITHIUM_WITH_AES_256_GCM_SHA384
For classic browsers using:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

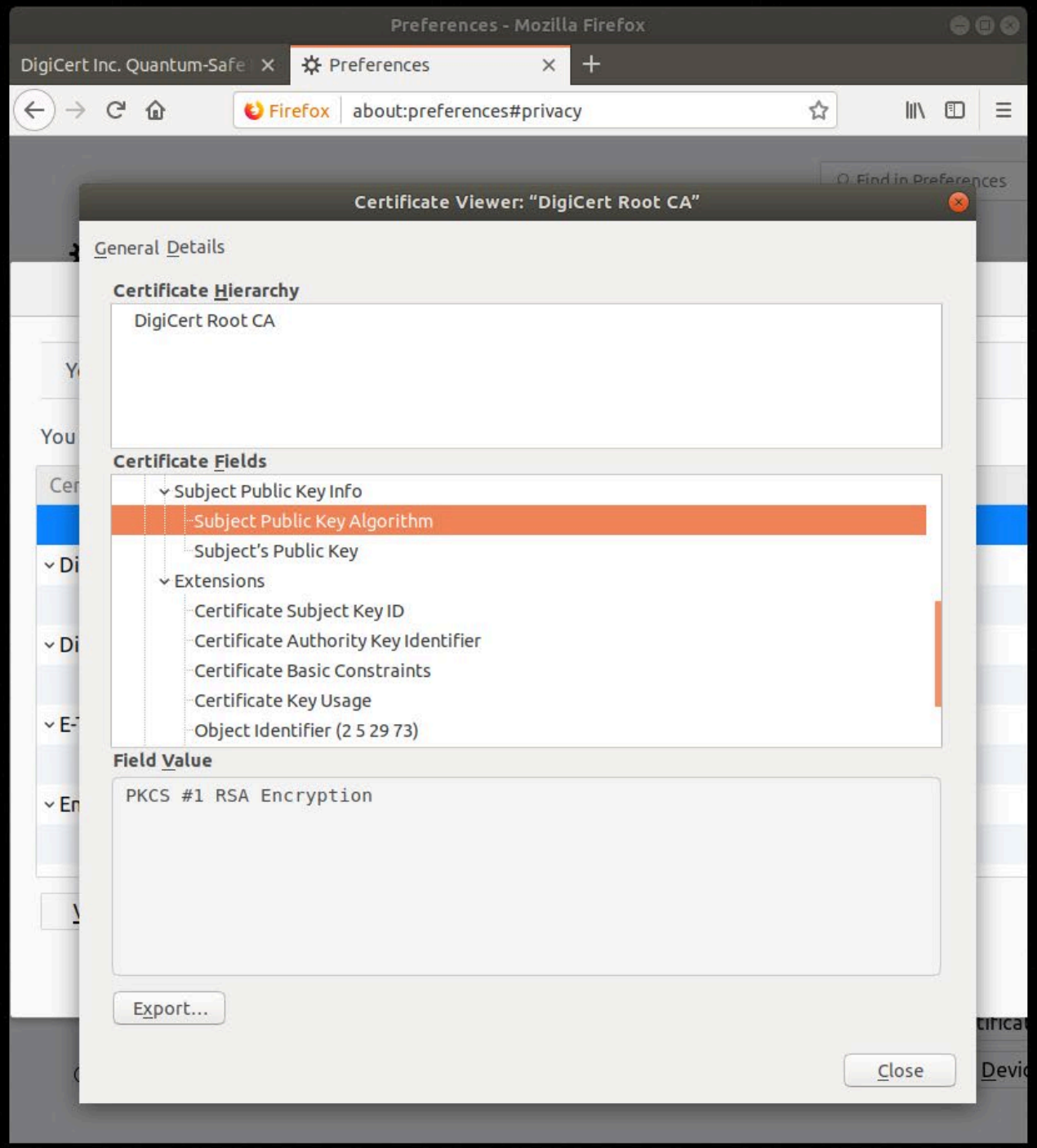

DigiCert Inc. Quantum-Safe Interop Server - Mozilla FirefoxQS
DigiCert Inc. Quantum-Safe
https://interop.digicert.com:8100
interop.digicert.com
Quantum-Safe Secure Connection
Permissions
You have not granted this site any special permissions.
DIGICERT INC. CLASSIC / QUANTUM-SAFE INTEROP SERVER
For quantum-safe browsers using:
TLS_ECDHE_DILITHIUM_WITH_AES_256_GCM_SHA384
For classic browsers using:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

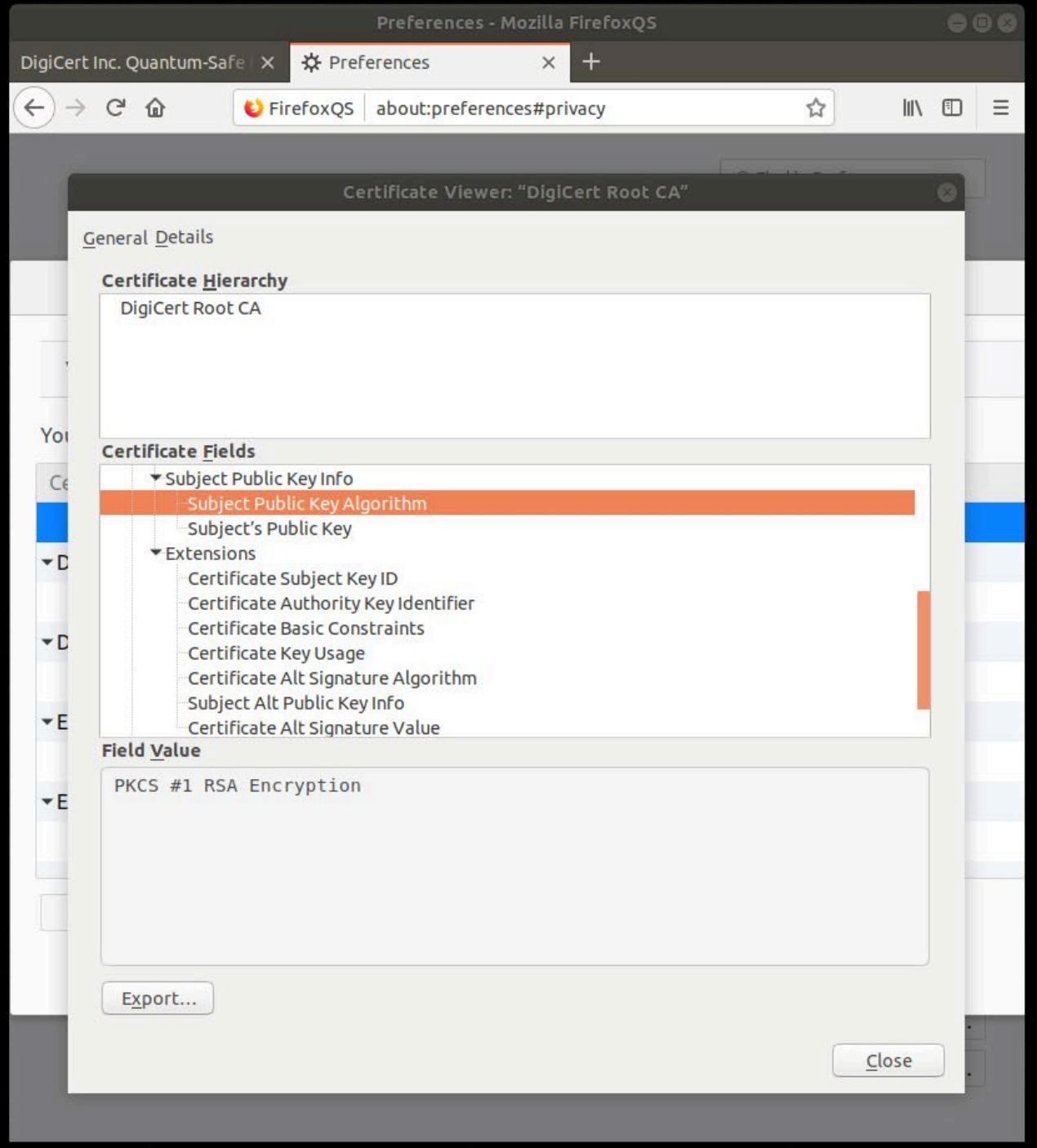

DigiCert Inc. Quantum-Safe Interop Server - Mozilla Firefox
DigiCert Inc. Quantum-Safe
https://interop.digicert.com:8100
Page Info - https://interop.digicert.com:8100/
General
Media
Permissions
Security
Website Identity
Website: interop.digicert.com
Owner: This website does not supply ownership information.
Verified by: DigiCert Inc.
Expires on: November 27, 2023
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? No
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.
Help

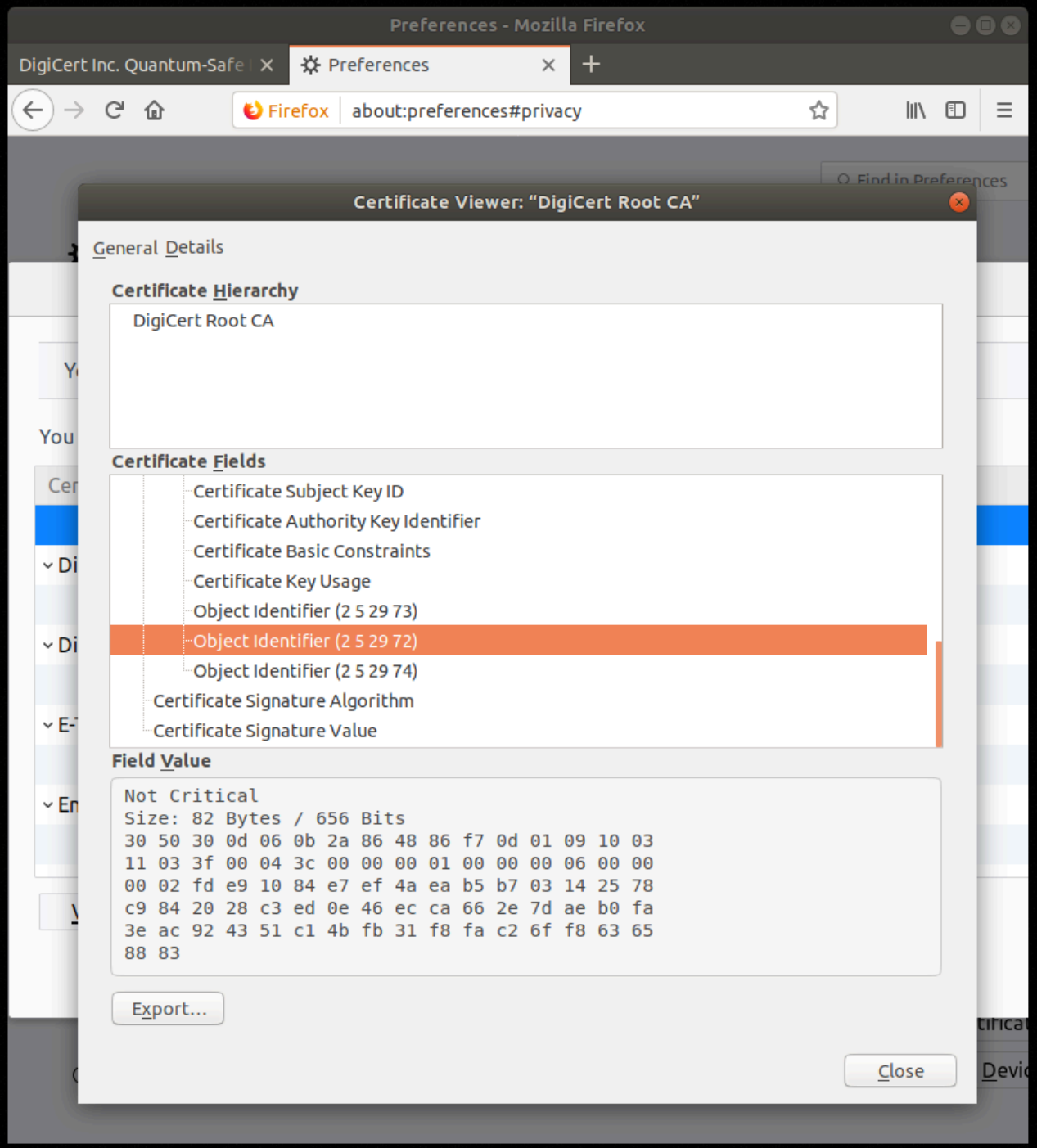

DigiCert Inc. Quantum-Safe Interop Server - Mozilla FirefoxQS
DigiCert Inc. Quantum-Safe
https://interop.digicert.com:8100
Page Info - https://interop.digicert.com:8100/
General
Media
Permissions
Security
Website Identity
Website: interop.digicert.com
Owner: This website does not supply ownership information.
Verified by: DigiCert Inc.
Expires on: November 27, 2023
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information (cookies) on my computer? No
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_DILITHIUM_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
Help

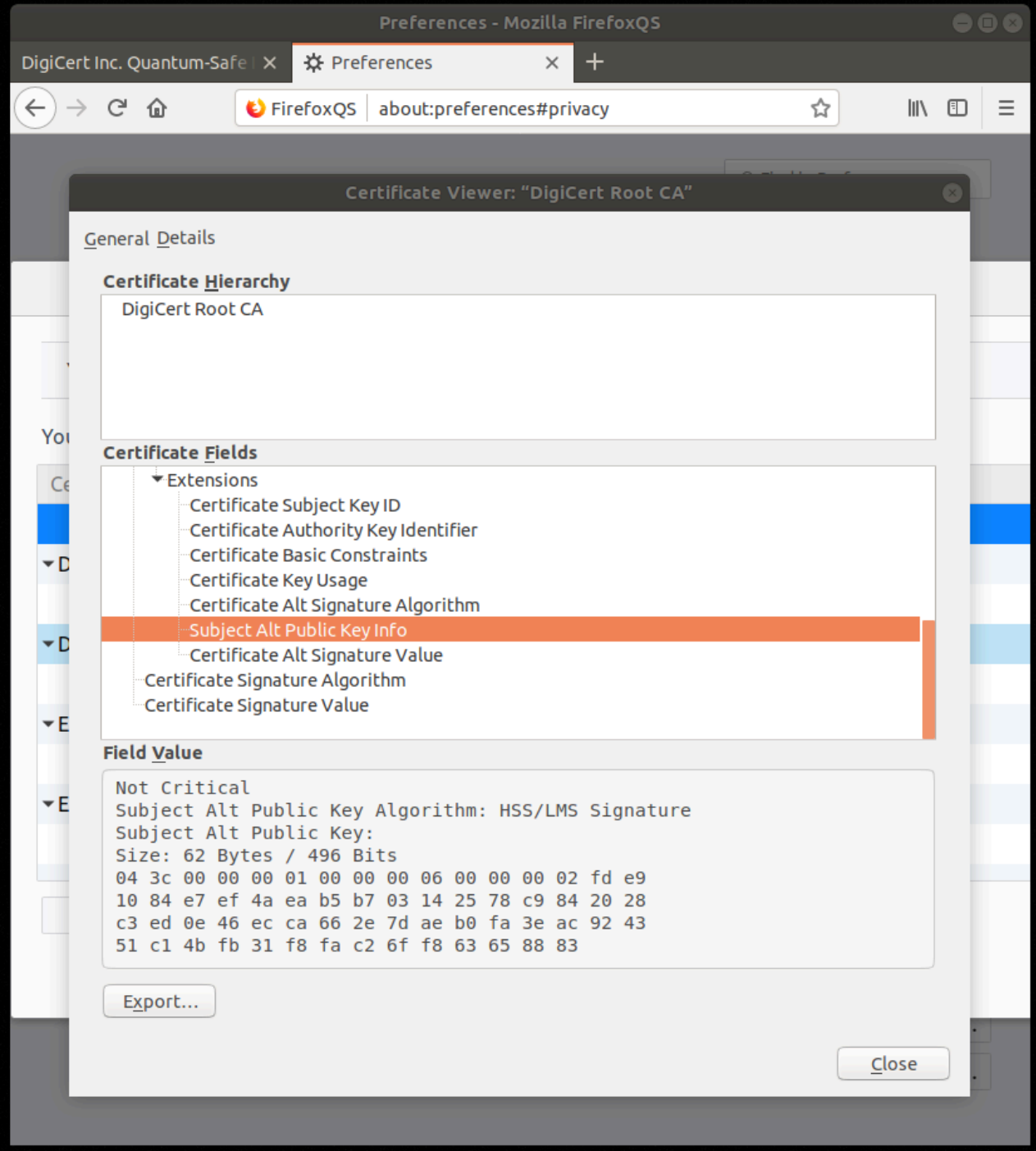

Preferences - Mozilla Firefox
DigiCert Inc. Quantum-Safe
Preferences
Firefox
about:preferences#privacy
Find in Preferences
Firefox Data Collection and Use
Certificate Manager
Your Certificates
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
DigiCert Root CA
Software Security Device
Digital Signature Trust Co.
DST Root CA X3
Builtin Object Token
Disig a.s.
CA Disig Root R2
Builtin Object Token
E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
E-Tugra Certification Authority
Builtin Object Token
Entrust, Inc.
Entrust Root Certification Authority
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
certificates


Preferences - Mozilla FirefoxQS
DigiCert Inc. Quantum-Safe
Preferences
FirefoxQS
about:preferences#privacy
Find in Preferences
Certificate Manager
Your Certificates
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
DigiCert Root CA
Software Security Device
Digital Signature Trust Co.
DST Root CA X3
Builtin Object Token
Disig a.s.
CA Disig Root R2
Builtin Object Token
E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
E-Tugra Certification Authority
Builtin Object Token
Entrust, Inc.
Entrust Root Certification Authority
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...


Preferences - Mozilla Firefox
DigiCert Inc. Quantum-Safe
Preferences
Firefox
about:preferences#privacy
Certificate Viewer: "DigiCert Root CA"
General Details
Certificate Hierarchy
DigiCert Root CA
Certificate Fields
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Subject Key ID
Certificate Authority Key Identifier
Certificate Basic Constraints
Certificate Key Usage
Object Identifier (2 5 29 73)
Field Value
PKCS #1 RSA Encryption
Export...
Close


Preferences - Mozilla FirefoxQS
DigiCert Inc. Quantum-Safe
Preferences
FirefoxQS
about:preferences#privacy
Certificate Viewer: "DigiCert Root CA"
General Details
Certificate Hierarchy
DigiCert Root CA
Certificate Fields
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Subject Key ID
Certificate Authority Key Identifier
Certificate Basic Constraints
Certificate Key Usage
Certificate Alt Signature Algorithm
Subject Alt Public Key Info
Certificate Alt Signature Value
Field Value
PKCS #1 RSA Encryption
Export...
Close


Preferences - Mozilla Firefox
DigiCert Inc. Quantum-Safe
Preferences
Firefox
about:preferences#privacy
Certificate Viewer: "DigiCert Root CA"
General Details
Certificate Hierarchy
DigiCert Root CA
Certificate Fields
Certificate Subject Key ID
Certificate Authority Key Identifier
Certificate Basic Constraints
Certificate Key Usage
Object Identifier (2 5 29 73)
Object Identifier (2 5 29 72)
Object Identifier (2 5 29 74)
Certificate Signature Algorithm
Certificate Signature Value
Field Value
Not Critical
Size: 82 Bytes / 656 Bits
30 50 30 0d 06 0b 2a 86 48 86 f7 0d 01 09 10 03
11 03 3f 00 04 3c 00 00 00 01 00 00 00 06 00 00
00 02 fd e9 10 84 e7 ef 4a ea b5 b7 03 14 25 78
c9 84 20 28 c3 ed 0e 46 ec ca 66 2e 7d ae b0 fa
3e ac 92 43 51 c1 4b fb 31 f8 fa c2 6f f8 63 65
88 83
Export...
Close


Preferences - Mozilla FirefoxQS
DigiCert Inc. Quantum-Safe
Preferences
FirefoxQS
about:preferences#privacy
Certificate Viewer: "DigiCert Root CA"
General Details
Certificate Hierarchy
DigiCert Root CA
Certificate Fields
Extensions
Certificate Subject Key ID
Certificate Authority Key Identifier
Certificate Basic Constraints
Certificate Key Usage
Certificate Alt Signature Algorithm
Subject Alt Public Key Info
Certificate Alt Signature Value
Certificate Signature Algorithm
Certificate Signature Value
Field Value
Not Critical
Subject Alt Public Key Algorithm: HSS/LMS Signature
Subject Alt Public Key:
Size: 62 Bytes / 496 Bits
04 3c 00 00 00 01 00 00 00 06 00 00 00 02 fd e9
10 84 e7 ef 4a ea b5 b7 03 14 25 78 c9 84 20 28
c3 ed 0e 46 ec ca 66 2e 7d ae b0 fa 3e ac 92 43
51 c1 4b fb 31 f8 fa c2 6f f8 63 65 88 83
Export...
Close

RSAConference2019
Asia Pacific & Japan

Conclusions

THE CHALLENGE

With increased connectivity, the scale of what needs to be updated also increases.

Maintain Interoperability

Migrate Critical Systems Faster

Reduce Switching Costs

Summary of the Journey

- Identified long-lived devices as critical assets we need to protect today
- Selected a mature post-quantum algorithm suitable for this purpose
- Worked with Gemalto to implement HSS and XMSS on Luna7 HSM, including tree splitting, tree compression, and other state management strategies
- Updated operational procedures to include planning for exhaustible private key resource and private key state management across multiple key instances

Apply What You Have Learned Today

- Next week you should:
  - Conduct your own research on how large-scale quantum computing will impact public-key cryptography and how it will affect your business
- In the first three months following this presentation you should:
  - Perform an archeological expedition to understand how cryptography is used in your organization
  - Identify and prioritize high-value assets for migration
- Within six months you should:
  - Collaborate with your internal team to create a migration plan
  - Share your needs with key vendors to ensure their roadmap aligns

RSAConference2019
Asia Pacific & Japan

Thank You

avesta.hojjati@digicert.com

alex@isara.com