QUANTUM THREAT, INTERNET TRUST

Planning the DNSSEC and RPKI Transition to PQC over the Next Decade

João Moreno Falcão - IS3C

March 11, 2026

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

Roadmap

1. Why now
2. Why us
3. Research findings
4. What comes next

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

PQC: today’s challenge

1

We don’t know when a capable quantum computer will appear

2

Transition time is really long

3

The DNSSEC transition taught us about how hard it is

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

Center for Assurance Research and Engineering

HOME | DNSSEC STAGES | DNSSEC STATISTICS | CITATIONS | CONTACT US

The following maps provide a view into global DNSSEC deployment and break the deployment status of top-level domains (TLDs) out into six stages:

DNSSEC

Select Region
World

Animate

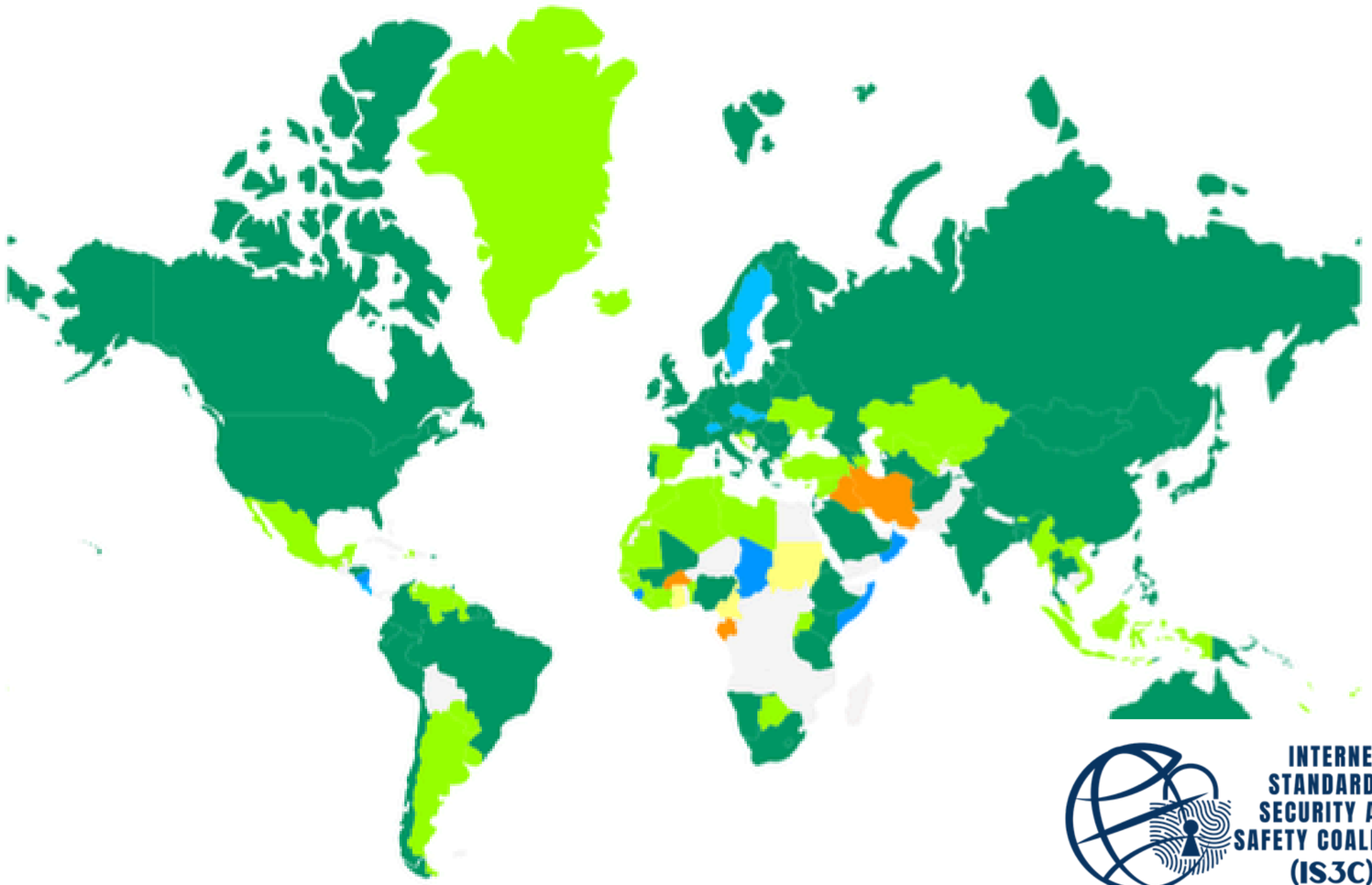
2005 — 2026

General Statistics

Total ccTLD's

183

Unsigned	2	1%
Experimental	9	5%
Announced	4	2%
Partial	9	5%
DS in Root	69	38%
Operational	83	45%
DS Automation	7	4%

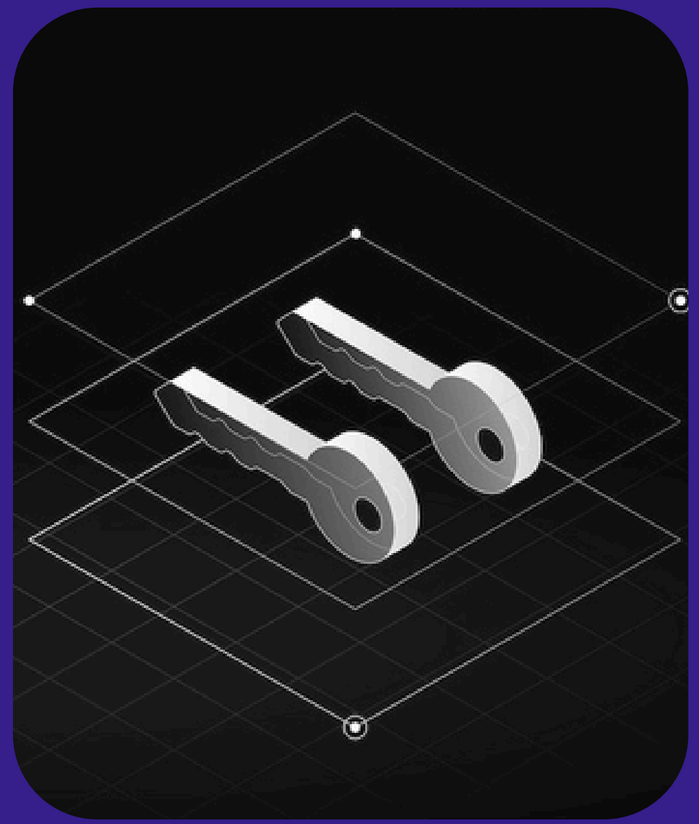


INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

What is quantum-unsafe

- Mandate secure-by-design & SBOM in procurement
- Harmonise global labelling & certification for consumer trust
- Invest in lightweight PQC R&D & secure OTA infrastructure
- Launch user education & automated patch programmes

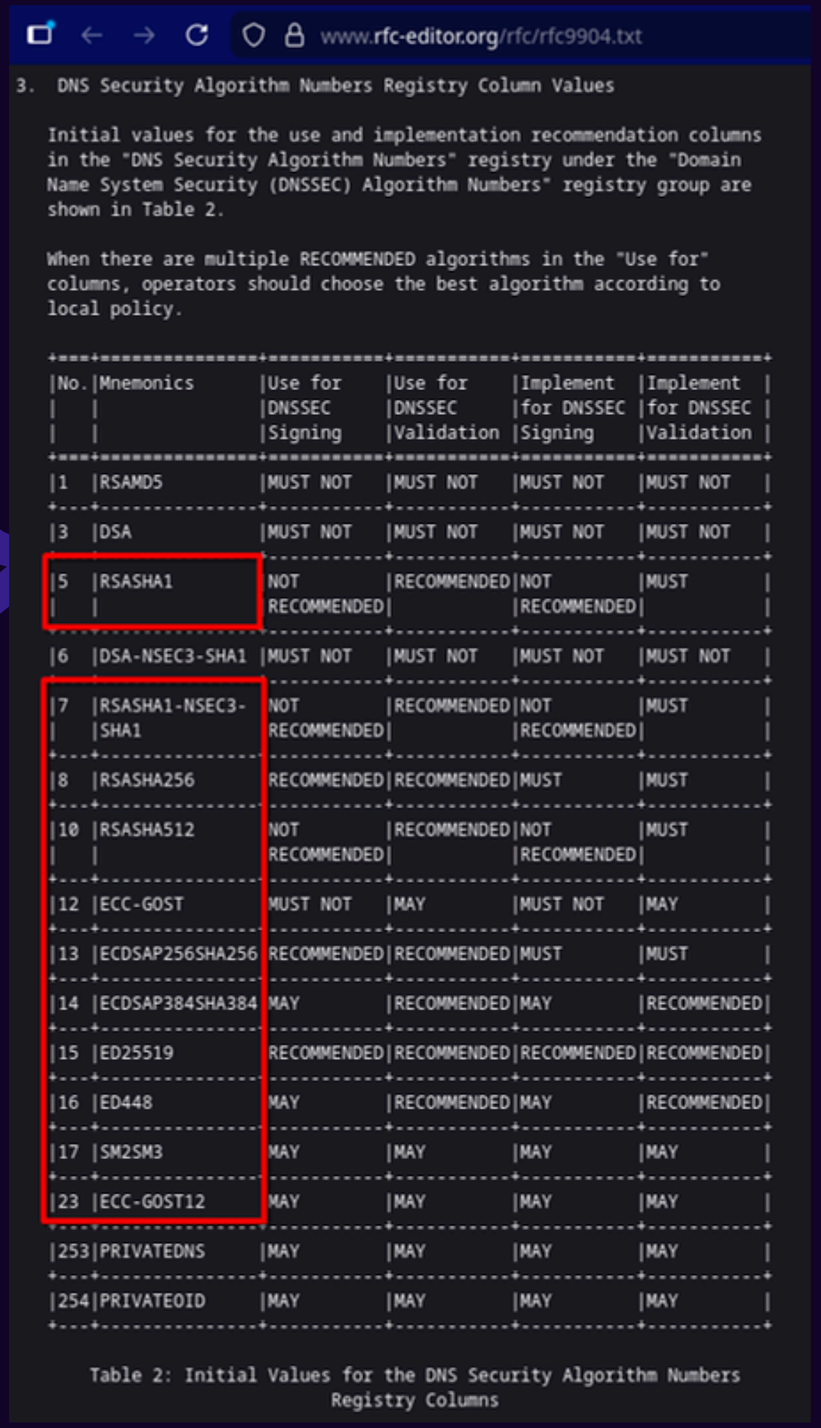
INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)



WHAT IS QUANTUM-UNSAFE?

public-key cryptography

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)



www.rfc-editor.org/rfc/rfc9904.txt

3. DNS Security Algorithm Numbers Registry Column Values

Initial values for the use and implementation recommendation columns in the "DNS Security Algorithm Numbers" registry under the "Domain Name System Security (DNSSEC) Algorithm Numbers" registry group are shown in Table 2.

When there are multiple RECOMMENDED algorithms in the "Use for" columns, operators should choose the best algorithm according to local policy.

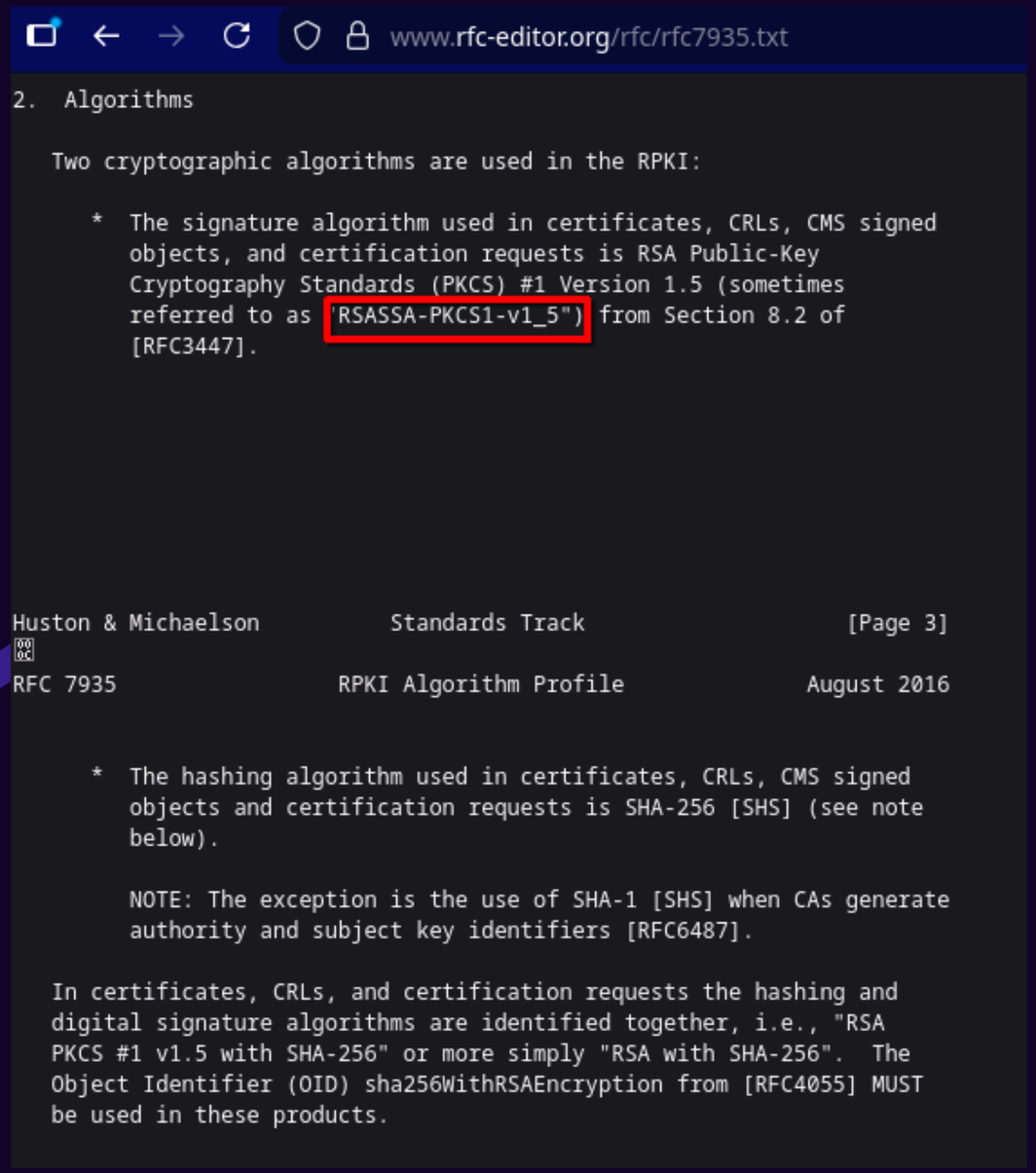
No.	Mnemonics	Use for DNSSEC Signing	Use for DNSSEC Validation	Implement for DNSSEC Signing	Implement for DNSSEC Validation
1	RSAMD5	MUST NOT	MUST NOT	MUST NOT	MUST NOT
3	DSA	MUST NOT	MUST NOT	MUST NOT	MUST NOT
5	RSASHA1	NOT RECOMMENDED	RECOMMENDED	NOT RECOMMENDED	MUST
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	RECOMMENDED	NOT RECOMMENDED	MUST
8	RSASHA256	RECOMMENDED	RECOMMENDED	MUST	MUST
10	RSASHA512	NOT RECOMMENDED	RECOMMENDED	NOT RECOMMENDED	MUST
12	ECC-GOST	MUST NOT	MAY	MUST NOT	MAY
13	ECDSAP256SHA256	RECOMMENDED	RECOMMENDED	MUST	MUST
14	ECDSAP384SHA384	MAY	RECOMMENDED	MAY	RECOMMENDED
15	ED25519	RECOMMENDED	RECOMMENDED	RECOMMENDED	RECOMMENDED
16	ED448	MAY	RECOMMENDED	MAY	RECOMMENDED
17	SM2SM3	MAY	MAY	MAY	MAY
23	ECC-GOST12	MAY	MAY	MAY	MAY
253	PRIVATEDNS	MAY	MAY	MAY	MAY
254	PRIVATEOID	MAY	MAY	MAY	MAY

Table 2: Initial Values for the DNS Security Algorithm Numbers Registry Columns

DNSSEC needs to change all algorithms

1. zone signing
2. validation chain

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)



RPKI needs to change the sign algorithm

1. certificates
2. CRLs
3. ROAs
4. manifests

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

Challenges

Operational transition

1. Secure migration
2. Interoperable migration
3. Live environments
4. No trust breakage
5. CPU usage
5. Network usage

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

our report

IS3C/Afnic research: governance findings

US

- top-down
- mandate-driven
- NIST-led

EU

- coordination-driven
- member-state alignment
- hybrid emphasis

National innitiatives

- France
- Germany
- Netherlands

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

What comes next

Two working groups:

1. DNS
2. Routing

Join us as:

1. Expert
2. Sponsor

1. map dependencies
2. identify blockers
3. test assumptions
4. improve interoperability
5. connect standards + operations

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

Q&A

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER