Post-Quantum

Cryptography Conference

PQC Interoperability Project

The Post Quantum Crypto Interoperability project started as a hackathon project at the IETF in 2022. People interested in adding PQ algorithm support into existing X.509 keys, signatures and certificates brough their tools and started to collaborate using the proposed PQC algorithms. The project has continued to grow and includes an artifact repository anyone can use for interoperability testing, a list of prototype OIDS to facilitate interoperability, and a compatibility matrix to demonstrate interoperability between users. With the experience obtained by participating in the project, its collaborators also provide valuable feedback to the emerging standards that are in development for the support of PQC. This talk will give an overview of the project, how to use it for interoperability testing and will encourage you to become a participant in the project.

Corey Bonnell

Technology Strategist at DigiCert

SSL.com PQ SHIELD KEYFACTOR ENTRUST HID

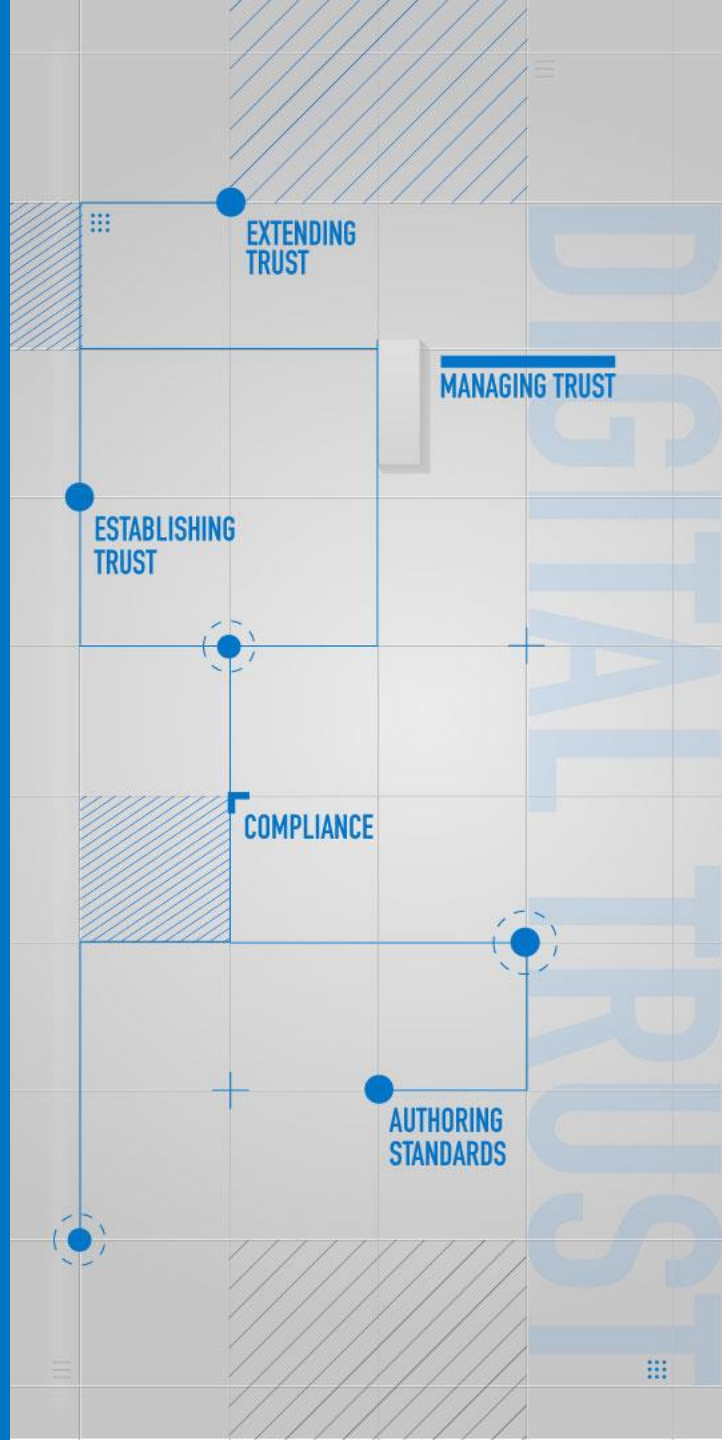
January 15 and 16, 2025 - Austin, TX (US) | Online

PQC INTEROPERABILITY AT THE IETF

3rd PKIC PQC Conference Update

January 16, 2025

digicert®



INTRODUCTION

Industry Standards team @ DigiCert

Over 15 years of software engineering and technical leadership experience, almost a decade in PKI

Active participant and contributor at several standards development organizations

Chair of validation sub-committee @ CA/Browser Forum

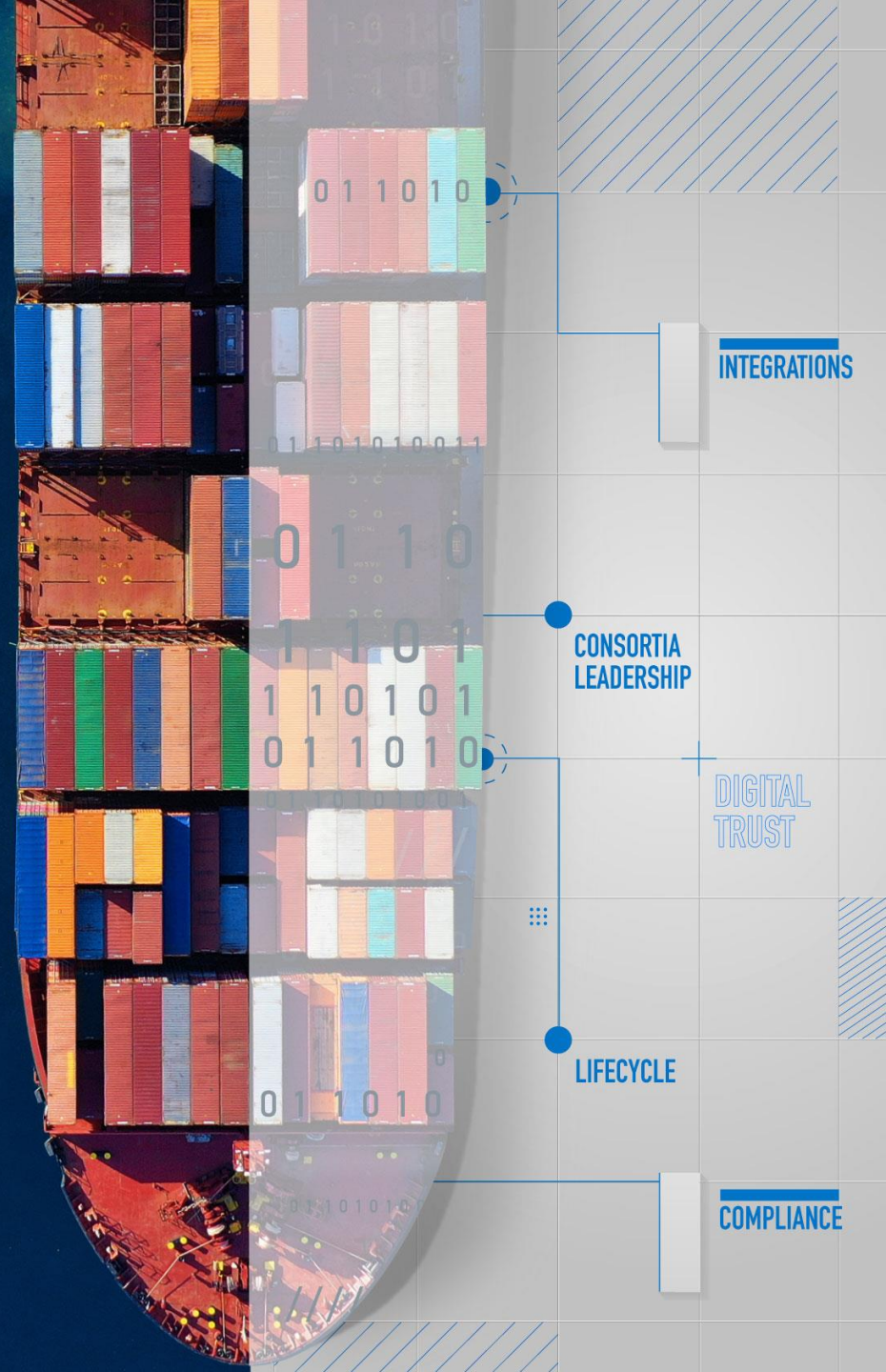
COREY BONNELL

Industry Technology Strategist

IETF HACKATHON OVERVIEW

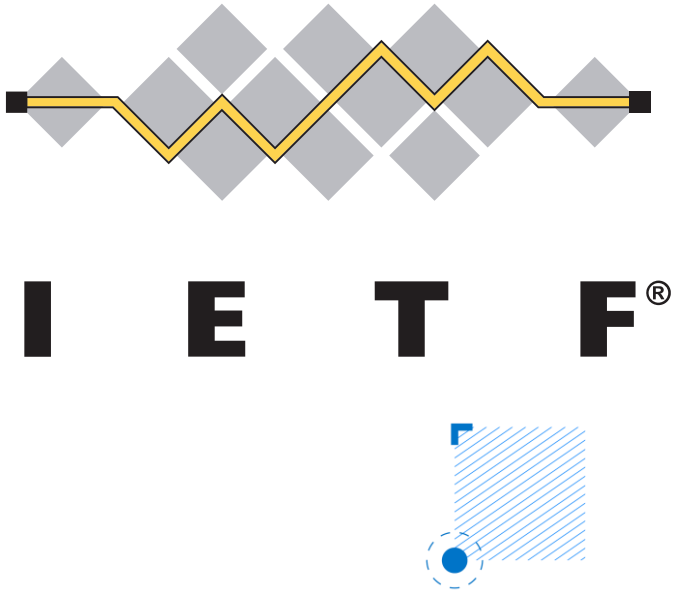
"WE REJECT: KINGS, PRESIDENTS, AND VOTING. WE BELIEVE IN: ROUGH CONSENSUS AND RUNNING CODE."

- David Clark



ROUGH CONSENSUS AND RUNNING CODE

The two guiding principles of the IETF process



“Rough consensus”: Overall – but not necessarily unanimous – agreement is sufficient

“Running code”: Actual implementation of the specification trumps theoretical design

IETF Hackathons help realize both principles:

- Produce concrete implementations of draft specifications
- Identify problematic areas in drafts

ROUGH CONSENSUS AND RUNNING CODE

The two guiding principles of the IETF process

IETF Hackathons help realize both principles:

- Produce concrete implementations of draft specifications
- Identify problematic areas in drafts

Name	Last commit message
..	
bc	update to latest composit...
botan	Manually converted core...
carl-redhound	rename zip file from v4 to...
cht	[CHT] add "Composite Si...
corey-digicert	Add r4 compatibility matr...
cryptonext-cnsprovider	Add cnsprovider resulrts ...
cryptonext	Add cnsprovider resulrts ...
entrust	Added artifacts in v4 for...
isi-wolfssl	Adjusted the artifacts_cer...
kris	[kris] Computes compat...
nist-acvts-test	Rename artifacts_r3_certs...
openca	Manually converted open...
oqs-gnutls	Merge pull request #69 fr...
oqs-openssl111	Rename Makefile to Mak...
oqs-provider	Fixed mgf1 to aling with -...
seventhsense.ai	Submit r4 dsa artifacts up...

A WEEKEND MEETING BEFORE THE MEETINGS

19 hours of hacking fun

Hackathons take place the Saturday and Sunday before the week of IETF meetings start

General schedule:

- 9 AM to 9 PM local time on Saturday
- 9 AM to 4 PM local time on Sunday
- On-site attendees are well fed and caffeinated

SEAMLESS HYBRID COLLABORATION

Remote participation is supported through Gather

- Regular “sync” meetings with on-site and remote participants throughout the event
- Messaging functionality for async communication
- Use of free tables to facilitate video-based “break-out” sessions
- Remote participants need to supply their own food and source of caffeine

PQC HACKATHON OVERVIEW

PROVING GROUND FOR X.509 INTEROPERABILITY

The “PQC keys and signatures in X.509” hackathon has met at the last 7 IETF hackathons and one virtual, “interim” hackathon

- First hackathon in November 2022 at IETF 115 with a small group
- Seventh IETF hackathon in November 2024 at IETF 121 with a very large, diverse group

Participants now include members from government agencies, open-source projects, and commercial providers

OPEN-SOURCE COLLABORATION

The group's work is published in a Github repository located at https://github.com/IETF-Hackathon/pqc-certificates

- Documentation of artifact archives for interoperability testing
- Automated test suites against popular open-source implementations
- HTML-based interoperability test results
- Specification of temporary Object Identifiers (OIDs)
- Minutes for monthly catch-up meetings

COMPREHENSIVE TEST RESULTS

https://ietf-hackathon.github.io/pqc-certificates/pqc_hackathon_results_certs_r4.html

IETF PQC Hackathon Certificate Interoperability Results

Generated: 2024-12-06 15:39 UTC

Algorithms Submitted

✅ = passing all verifiers
◒ = passing some verifiers
○ = not passing any verifiers
Columns represent producers who submitted artifacts. Verifiers are not listed in this table, but are listed in the broken-out tables below.

-	bc	carl-redhound	cht	corey-digicert	cryptonext	cryptonext-cnsprovider	entrust	kris	seventhsense.ai
Falcon-1024	◒				◒	◒	○	◒	
ML-DSA-44	✅	✅	✅	✅	✅	✅		✅	✅
ML-DSA-65	✅	✅	✅	✅	✅	✅		✅	✅
ML-DSA-87	✅	✅	✅	✅	✅	✅		✅	✅
SLH-DSA-SHA2-128s	✅	✅	✅		✅	✅			✅
SLH-DSA-SHA2-128f	✅	✅	✅		✅	✅			✅
SLH-DSA-SHA2-192s	✅	✅	✅		✅	✅			✅
SLH-DSA-SHA2-192f	✅	✅	✅		✅	✅			✅
SLH-DSA-SHA2-256s	✅	✅	✅		✅	✅			✅
SLH-DSA-SHA2-256f	✅	✅	✅		✅	✅			✅
SLH-DSA-SHAKE-128s	✅	✅	✅		✅	✅			✅
SLH-DSA-SHAKE-128f	✅	✅	✅		✅	✅			✅
SLH-DSA-SHAKE-192s	✅	✅	✅		✅	✅			✅
SLH-DSA-SHAKE-192f	✅	✅	✅		✅	✅			✅
SLH-DSA-SHAKE-256s	✅	✅	✅		✅	✅			✅
SLH-DSA-SHAKE-256f	✅	✅	✅		✅	✅			✅
HASH-ML-DSA-44	◒	✅		✅	◒				✅
HASH-ML-DSA-65	◒	✅		✅	◒				✅
HASH-ML-DSA-87	◒	✅		✅	◒				✅
HASH-SLH-DSA-SHA2-128s	◒				✅				✅
HASH-SLH-DSA-SHA2-128f	◒				✅				✅

PQC HACKATHON STANDARDS COVERAGE

AN EVOLVING SET OF STANDARDS

At the first hackathons, interoperability testing was limited to Dilithium (now ML-DSA), SPHINCS+ (now SLH-DSA), and “generic composite” signatures in X.509 certificates and CRLs

- This initial testing was immensely valuable in resolving issues in the draft standards

Current hackathons cover much more, such as:

https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/
https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/
https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/
https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/
https://datatracker.ietf.org/doc/rfc9629/
https://datatracker.ietf.org/doc/draft-ietf-lamps-rfc4210bis/
https://datatracker.ietf.org/doc/draft-ietf-lamps-cert-binding-for-multi-auth/01/
https://www.ietf.org/id/draft-lamps-okubo-certdiscovery-00.html
https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/
https://datatracker.ietf.org/doc/draft-gazdag-x509-hash-sigs/

HOW TO GET INVOLVED

HOW TO GET INVOLVED

There are two ways to get started:

1. If you have an X.509 implementation that generates or verifies signatures, submit artifacts: https://github.com/IETF-Hackathon/pqc-certificates?tab=readme-ov-file#folder-structure-of-this-repo
2. Reach out to our Hackathon Leader, John Gray (john.gray@entrust.com) and ask for an invitation to our monthly meeting

QUESTIONS?

THANK YOU!