NIST National Cybersecurity Center of Excellence
Overview

Cherilyn Pascoe, NCCoE Director

Who We Are

A **collaborative hub** convening experts from industry, government, and academia to solve organizations’ most pressing cybersecurity challenges

Our Applied Cybersecurity Work

- **Demonstrate standards-based, end-to-end solutions using off-the-shelf technology**
- **Publish usable guides to help U.S. organizations improve their cybersecurity**
- **Develop risk profiles to help communities prioritize their cybersecurity efforts**

Developed collaboratively through 170 agreements with collaborators across vendors, industry, government, and academia

Our Collaboration

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE staff work side-by-side with vendors, industry, academia, and government

- Our partners and collaborators help us identify projects to address industry's top challenges
- Together, we demonstrate and share guidelines for implementing real solutions—not just best practices

NCCoE By The Numbers

29 Active Projects

150 Active CRADAs

4 Interagency Agreements

38 NCEP MOUs

Stakeholder Feedback:

Our Value

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Stakeholder feedback gathered over the last year highlighted the NCCoE's value

Strengthen U.S. Cybersecurity

Provide practical guides to help organizations implement standards-based, repeatable, and scalable solutions

Drive Standards Adoption & Innovation

Reveal opportunities to improve standards to better address real-world challenges

Improve Technology

Help vendors strengthen products' security and interoperability by building actual demonstrations

Foster Public-Private Innovation

Convene cybersecurity experts from industry, academia, and government to develop integrated solutions

Stakeholder Feedback:
What We Heard

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Stakeholder feedback identified opportunities to increase our impact

Focus on Priority Challenges

NCCoE projects address important cybersecurity challenges

- Increase focus on national, broadly applicable cybersecurity challenges, informed by cybersecurity trends, national and NIST priorities, and input from partners
- Increase focus on Cyber/AI, intersection of IT/OT, application of cryptography and identity

Improve Communications and Transparency

NCCoE projects communicate effectively with project-level collaborators

- Increase visibility into current projects and priorities
- Provide more communications at the NCCoE level to highlight broader value and impact

Increase Project Agility and Innovation

NCCoE projects provide extremely detailed implementation resources—but they take time

- Release shorter, accessible resources (guides, tools, etc.)
- Adopt more agile practices and project management tools
- Pilot the use of AI/LLM tools to accelerate and streamline the NCCoE's work

Enhance Collaboration and Partnerships

The NCCoE enables technical collaboration between vendors, government and industry

- Expand engagement with industry and end users
- Increase participation in collaborator events
- Emphasize role as a neutral convener between vendors and industry

Our Pillars

To better communicate our work, we aligned our projects to four pillars

DATA PROTECTION
Cryptography, Identity, and Privacy

TRUSTED ENTERPRISE
Foundational Infrastructure & Hardware Roots of Trust

ARTIFICIAL INTELLIGENCE
Cybersecurity of AI Tools & AI for Cybersecurity

RESILIENT EMBEDDED SYSTEMS SECURITY
Cybersecurity of OT/ICS & IoT

NIST NCCoE Roadmap

Project Portfolio as of July 2025

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Data Protection

- Automation of the NIST Cryptographic Module Validation Program (CMVP) **ENDING**
- Cybersecurity and Privacy of Genomic Data **ENDING**
- Digital Identity Lab **NEW**
- Mobile Driver's Licenses (mDL)
- Genomics Privacy Enhancing Technologies (PETs)
- Post-Quantum Cryptography (PQC) Migration
- Multi-Factor Authentication (MFA) for Public Safety **ENDING**
- Ransomware CSF Profile

Trusted Enterprise

- 5G Cybersecurity
- Data Classification Practices
- Secure Software Development (DevSecOps) **NEW**
- TLS 1.3 Visibility **ENDING**
- Zero Trust Architecture (ZTA) Implementation **ENDING**

Artificial Intelligence

- Autonomous Vehicle Vision **NEW**
- Cyber AI Profile
- Dioptra*
- Natural Language Processing

Resilient Embedded Systems Security

- Healthcare Smart Home Integration **ENDING**
- IoT Onboarding **ENDING**
- Manufacturing Response and Recovery
- Manufacturing Supply Chain Traceability
- Manufacturing Training
- Position, Navigation, and Timing CSF Profile
- Semiconductor CSF Profile **ENDING**
- Transit CSF Profile
- Water and Wastewater

LEGEND

Highlight	Formal Collaboration (CRADA)	**NEW**	Forming / seeking collaborators
No Highlight	Informal Collaboration (no CRADA)	**ENDING**	Finalizing publications

*Interagency project; other interagency projects are not included in this diagram

Project Overview:
Migration to Post-Quantum Cryptography

Bill Newhouse, NIST

Migration to Post-Quantum Cryptography

Demonstrating practices to ease migration to post-quantum cryptography

Collaborators

Federal Agencies
- Cybersecurity and Infrastructure Security Agency (CISA)
- National Security Agency (NSA)
- U.S. Army DEVCOM C5ISR Center

Communication
- Cisco Systems, Inc.
- Cloudflare
- Comcast
- Palo Alto Networks
- Samsung SDS Co., Ltd.
- Society for Worldwide Interbank Financial Telecommunication (SWIFT)
- SSH Communications Security Corp
- Verizon
- wolfSSL

Cloud Providers
- Amazon Web Services, Inc. (AWS)
- Google
- Microsoft

Financial Institutions
- HSBC
- JPMorgan Chase Bank, N.A.
- M&T Bank
- Santander
- Wells Fargo

Software
- ATIS
- CryptoNext Security
- Data-Warehouse GbmH
- General Dynamics Information Technology (GDIT)
- Gutsy
- InfoSec Global
- ISARA Corporation
- Post-Quantum Solutions Ltd.
- QuantumXchange
- SafeLogic, Inc.
- SandboxAQ
- Tychon

Cryptography
- DigiCert
- Entrust
- Information Security Corporation
- Keyfactor

Hardware
- Crypto4A Technologies, Inc.
- Dell Technologies
- HP, Inc.
- IBM
- IDEMIA Secure Transactions
- Kudelski IoT
- NXP Semiconductors
- PQShield
- SEALSQ
- Siemens
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- Utimaco

Our Workstreams

Discovery Workstream

Exploring the use of discovery tools to:

- Detect and report quantum-vulnerable cryptography in systems and services
- Use outputs from tools to inform risk analysis for prioritizing migration actions

Vulnerable Algorithm Discovery

- Code Development Pipeline
- Operational Network Services & Protocols
- Operational Systems and Applications

Interoperability and Performance Workstream

- Demonstrating interoperability between collaborators' software and hardware implementing the same PQC algorithm
- Documenting performance characteristics

Table 3 Profile 1 interoperability test results for PQC key exchange in TL collaborator components

Profile 1	Client	Server: OQS-OpenSSL	Server: wolfSSL	Server: AWS s2n-tls
P256+Kyber-512	OQS-OpenSSL	Success	Success	Success
P256+Kyber-512	wolfSSL	Success	Success	Pending
P256+Kyber-512	AWS s2n-tls	N/A	Success	Success
P256+Kyber-512	Samsung SDS PQC-TLS	Success	Success	Success

Project Overview:

Digital Identities: Mobile Driver's Licenses (mDL)

Ryan Galluzzo, NIST

Mobile Driver’s Licenses: mDL

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Addressing security, privacy, and interoperability challenges with mobile driver’s licenses (mDLs)

- Developed an end-to-end implementation of mDL that used ISO, OIDF, and W3C standards to verify identities online for a representative financial institution
- Enabled the first remote interoperability testing event with OIDF for their presentation standards and testing with multiple US and internationally based wallets leveraging both mDL and W3C Verifiable Credentials
- Identified and coordinated efforts to address gaps in standards and ecosystem capabilities
- Inspired several participating FIs to begin internal POCs in preparation for assessment and broader deployment
- Piloting the use of agile practices and shorter, more frequent publication outputs for NCCoE projects

Our Collaborators

22 CRADA Partners

2 Largest Wallet Providers

5 of 10 Largest US Banks

5 State Issuers

2 Federal & SDOs

Federal Agencies

- Department of Homeland Security (DHS), Science and Technology Directorate

Financial Institutions

- Capital One
- JP Morgan Chase
- PNC Bank
- Raymond James
- Synchrony
- US Bank
- Wells Fargo

State Issuers

- American Association of Motor Vehicle Administrators (AAMVA)
- California Department of Motor Vehicles
- Georgia Department of Driver Services
- Maryland Department of Transportation
- New York State Department of Motor Vehicle

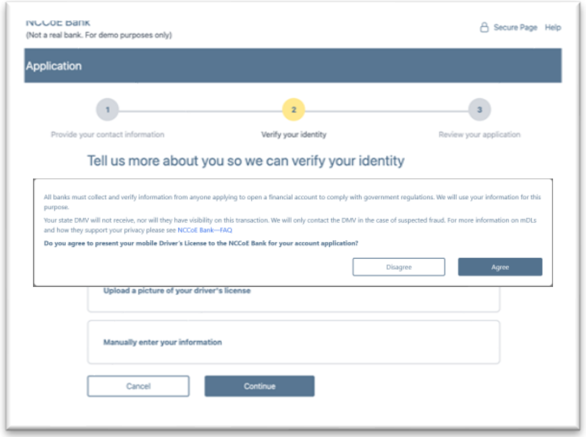
Standards Development Organizations

- OpenID Foundation

Vendors

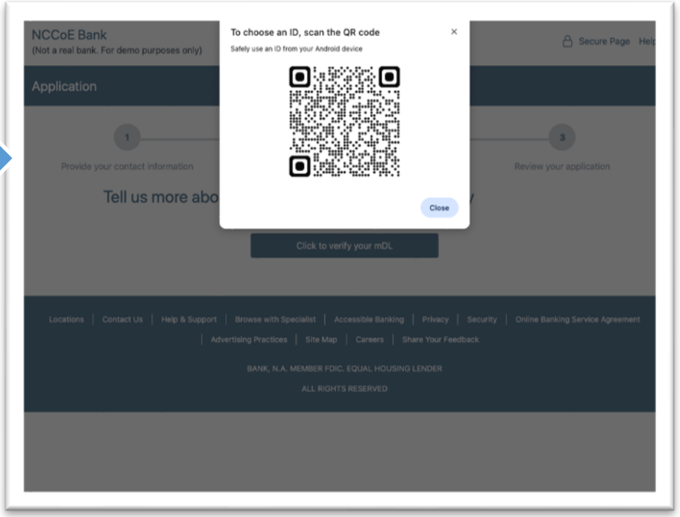
- 1Password
- Google
- Idemia
- iLabs
- MATTR Limited
- Microsoft Corporation
- SpruceID
- Yubico

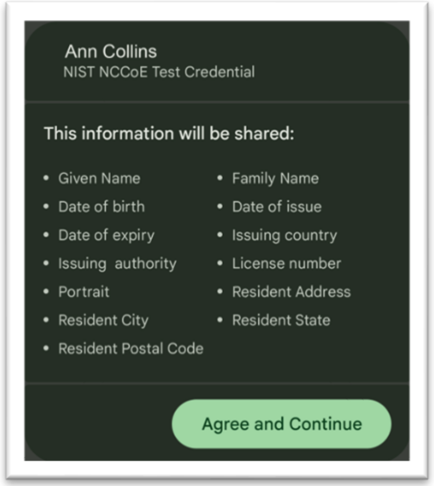
NCCoE Bank & mDL Integration
(Not a real bank)



Website

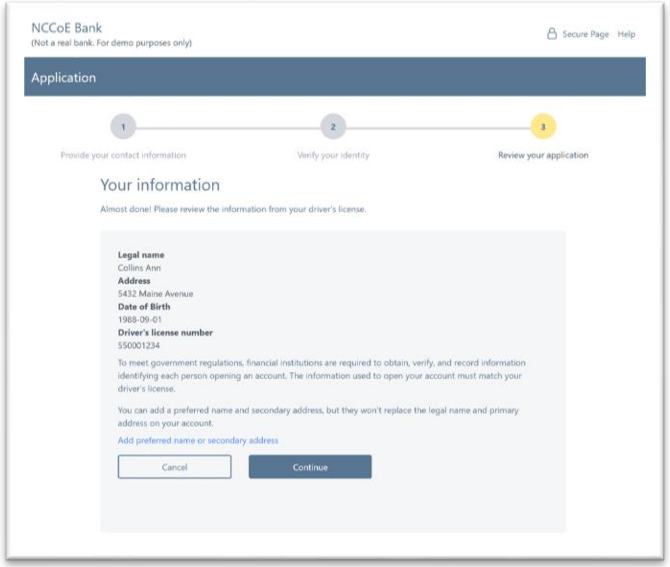
Browser





Device/Wallet

Website



All screen shots were captured from functional Bank of NCCoE demonstration environment and test devices with test credentials. *<u>No data are actual PII</u>*.

Iterative Deliverables

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Complete

- Build Criteria
- mDL Information Page
- Wireframes
- Architecture
- MVP Infrastructure
- Interop tests
- Functional Demonstration

Planned

- User Experience Testing
- Privacy Risk Assessment
- Threat Model
- Regulatory Mapping (CIP)
- 1800-42 Practice & Configuration Guides
- NIST SP 800-63 Profile

Discussion

Cherilyn Pascoe, NCCoE Director

Input Needed

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Where do you see opportunities for the NCCoE's collaborative technology demonstrations to help organizations strengthen their cybersecurity?

DATA PROTECTION
Cryptography, Identity, and Privacy

TRUSTED ENTERPRISE
Foundational Infrastructure & Hardware Roots of Trust

ARTIFICIAL INTELLIGENCE
Cybersecurity of AI Tools & AI for Cybersecurity

RESILIENT EMBEDDED SYSTEMS SECURITY
Cybersecurity of OT/ICS & IoT

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Questions? Feedback?

nccoe.nist.gov

@NISTcyber