NIST Workshop on Crypto Agility

April 17-18, 2025

Agenda

Virtual - Zoom for Government All times are Eastern Daylight Time (New York)

Thursday April 17, 2025	
10:00-10:05	Welcome and open remarks: Matthew Scholl
Session 1- Hardware Session Chair and Moderator: Curt Barker	
10:05 – 11:05	Hardware panel (60 minutes) • Qualcomm – Dan O'Loughlin • HP Inc. – Josh Schiffman • Crypto 4A – Jim Goodman • Thales TCT – Bill Becker • Utimaco – Volker Krummel
Session 2 – Software, API, Applications Session Chair and Moderator: Angela Robinson	
11:05 – 12:05	Software, API, Applications panel (60 minutes) • InfoSec Global – Victoria de Quehen • Google - Sophie Schmieg • Keyfactor – David Hook • Entrust – John Gray
12:05 – 1:00	Meal Break (55 minutes)
Session 3 – Maturity and evaluation Session Chair: Hamilton Silberg	
1:00– 1:50	Maturity and evaluation presentations (50 minutes) • Comcast – Bahman Rashidi - *Crypto Agility Risk Assessment Framework* • ATIS – Ian Deakin - *Defining and Measuring Crypto Agility through KPIs* • Atsec – Stephan Mueller - *Crypto Agility - Ideas from the Field and a FIPS Lab*
Session 4 – Financial Services Session Chair and Moderator: Bill Newhouse	
1:50 – 2:50	Financial services panel (60 minute) • Santander – Jaime Gomez • HSBC – Leon Molchanovsky • Swift – Isabelle Noblesse • Wells Fargo – Jeff Stapleton
3:00	Q & A, Adjourn

Friday April 18, 2025	
Session 5 – Standards Session Chair and Moderator: Lily Chen	
10:00 – 11:00	Standards Panel (60 minutes) • Vigil Security LLC – Russ Housley – *IETF* • AIST – Hirotaka Yoshida – *ISO SC27/WG2* • ASC X9, Inc. – Ralph Poore – *X9* • Kudelski – Brecht Wyseur – *CSA Matter and DLMS/COSEM* • Google – Chris Fenner – *TCG*
Session 6 Resource Constrained Environment Session Chair Noah Waller	
11:00 – 12:05	Presentations (65 minutes) • IDEMIA – Christophe Giraud - *Crypto-agility for smart cards* • NXP – Gareth Davies - *Crypto Agility for Embedded Systems* • Infineon – Steve Hanna - *Considering Resource Constraints More Broadly* • SealSQ - Steve Clark - *Crypto Agility in a Resource Constrained Environment*
12:05 – 12:50	Meal break (45 minutes)
Session 7 – Enterprise Session Chair and Moderator: Donna Dodson	
12:50 – 2:10	Enterprise panel (80 minutes) • IBM – Michael Osborne • Fortanix – Vikram Chandrasekaran • AvinyaSQ - Gireesh Kumar N • JPMChase – Hubert Le Van Gong • InfoSec Global - Vladimir Soukharev • Ericsson – John Mattsson
Session 8 – Techniques for Agility Session Chair Lily Chen	
2:10 – 2:55	Presentations • Samsung SDS – Jihoon Cho - *Software-Defined Cryptography: Enabling Cryptographic Agility in Enterprise IT* • Intel – Brandon Eames - *Cryptographic Autonomy and Agility through the Configurable Cryptographic Controller Die(C3D)* • Virginia Tech – Kigen Fukuda - *Crypto-agility for blockchain protocols*
2:55 – 3:00	Summary and adjourn