국외 암호모듈 검증동향

2025. 7. 15.

국가보안기술연구소

CONTENTS

01

암호모듈검증제도

NSR

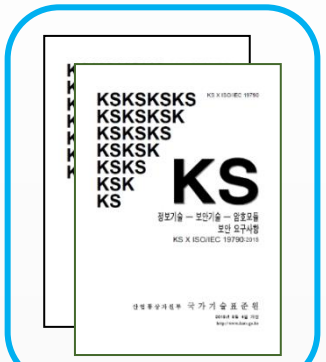
목적 : 비밀이 아닌 중요정보 보호에 검증된 암호모듈 사용
시험 : 안전성 검증(표준) + 구현정확성 검증 + **기타 취약성**

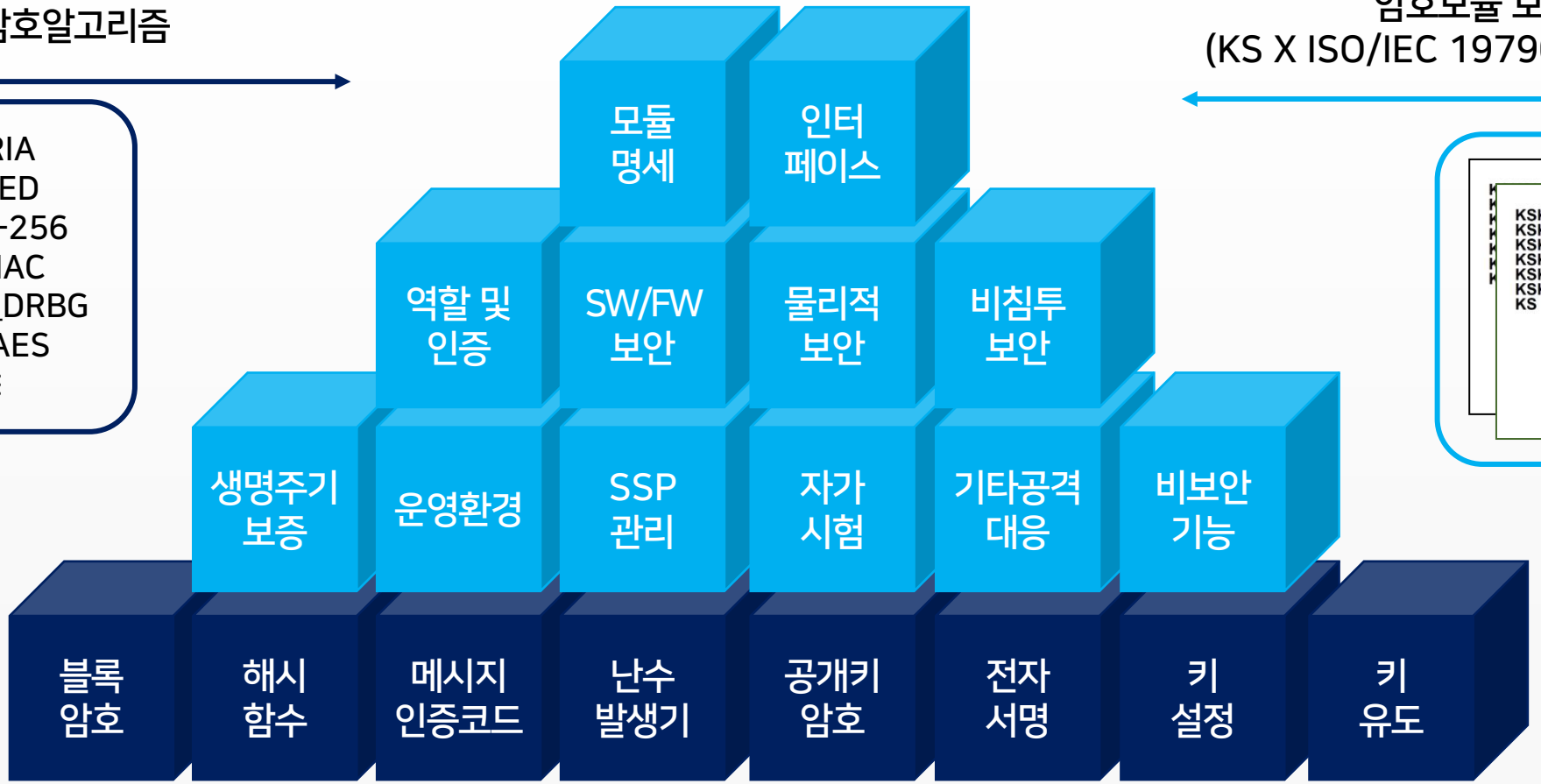
암호모듈 요구사항

검증대상 암호알고리즘

ARIA
SEED
SHA-256
HMAC
Hash_DRBG
RSAES
⋮

암호모듈 보안요구사항
(KS X ISO/IEC 19790/24759)





검증대상 암호알고리즘

분류	검증대상 암호알고리즘
블록암호	ARIA, SEED, LEA, HIGHT, AES(`26)
해시함수	SHA-2, SHA-3, LSH
메시지인증코드	HMAC, GCM, CCM, CMAC
난수발생기	Hash_DRBG, HMAC_DRBG, CTR_DRBG
공개키암호	RSAES
전자서명	RSA-PSS, KCDSA, ECDSA, EC-KCDSA, PQ-DSA(?)
키 설정	DH, ECDH, PQ-KEM(?)
키 유도	KBKDF, PBKDF

검증대상 암호알고리즘 선정 시
국내·외 표준 암호기술의 **안전성, 신뢰성, 상호 운용성** 등 고려

총 391개 시험항목

보안요구사항을 시험하기 위한 시험자/개발자 요구사항(TE/VE) 기술

영역	AS	TE
암호모듈 명세	32	53
암호모듈 인터페이스	22	42
역할, 서비스 및 인증	59	67
소프트웨어/펌웨어 보안	21	16
운영환경	29	51
물리적 보안	86	81

영역	AS	TE
비침투 보안	7	5
중요보안매개변수 관리	37	59
자가시험	55	79
생명주기 보증	39	46
기타 공격에 대한 대응	4	5
총합	391	504

설계 암호모듈에 적용되는 시험항목 선정 필요(제외 항목 근거 필요)

시험 수행 내용

문서검토 | 소스코드 분석 | 기능 및 운영시험

구분	시험항목	고려사항
	암호모듈 명세	암호모듈의 전체적인 구조 이해 검증대상 운영모드 및 알고리즘, 핵심보안매개변수 확인
	암호모듈 인터페이스	문서와 코드의 일치 여부 확인 불분명한 정보흐름 및 암호 알고리즘 운용 확인
	역할, 서비스 및 인증	동시 사용자 지원 여부
	소프트웨어/펌웨어 보안	검증대상 무결성 방법 확인
	운영환경	지원하는 모든 운영환경에 대한 시험
	물리적 보안	탬퍼 탐지 및 대응 메커니즘
	비침투보안	현재 구체적인 시험방법론 없음
	중요보안매개변수 관리	엔트로피 분석, DRBG의 이용 키 생명주기 관리(생성, 저장, 입/출력, 제로화) 확인
	자가시험	Positive & Negative 자가시험
	생명주기보증	개발환경 확인 암호모듈 실행에 따른 유한상태모델 일치여부
	기타 공격에 대한 대응	소스코드를 통한 대응방법 구현 여부

02

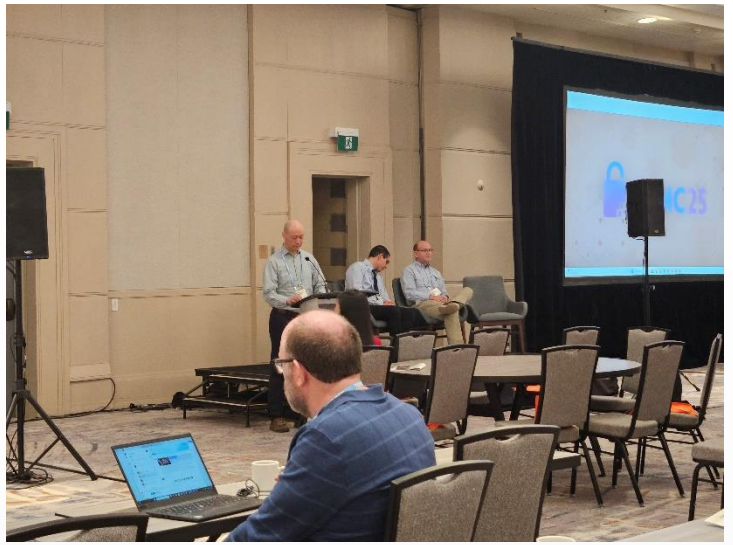
국외 암호모듈 검증 동향

1. ICMC(International Cryptographic Module Conference) 학회
   - 전세계 암호모듈 검증제도(CMVP)의 검증기관, 시험기관, 업체 등이 참여하는 학회
   - CMVP 관련 정책·검증·시험 관련 동향 발표 (keynote + talk + panel + exhibition)

2. ICMC 2025 일정 및 장소
   - 일정: 2025.4.7 ~ 4.10(4일)
     ※ PQ Cyber Day(1일: 2025.4.7)
   - 장소: 캐나다 토론토

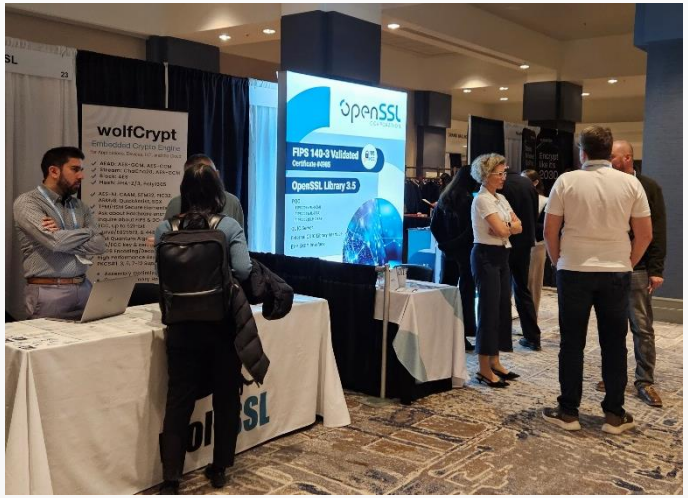
3. ICMC 2026 일정 및 장소
   - 일정: 2026.4.20 ~ 4.23(4일)
   - 장소: 미국 알링턴(Renaissance Arlington Capital View)

Keynote



Talk

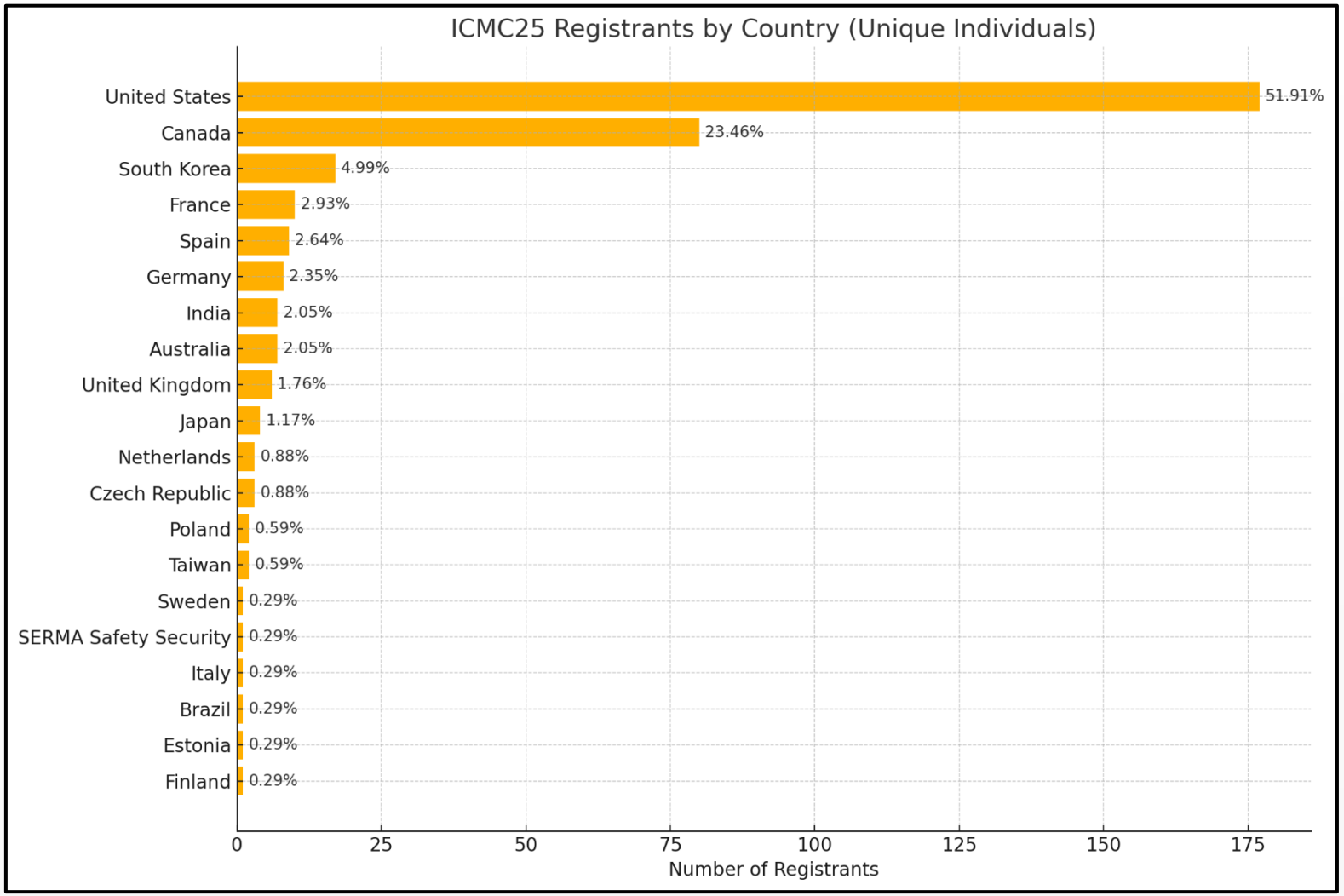
Pannel Discussion



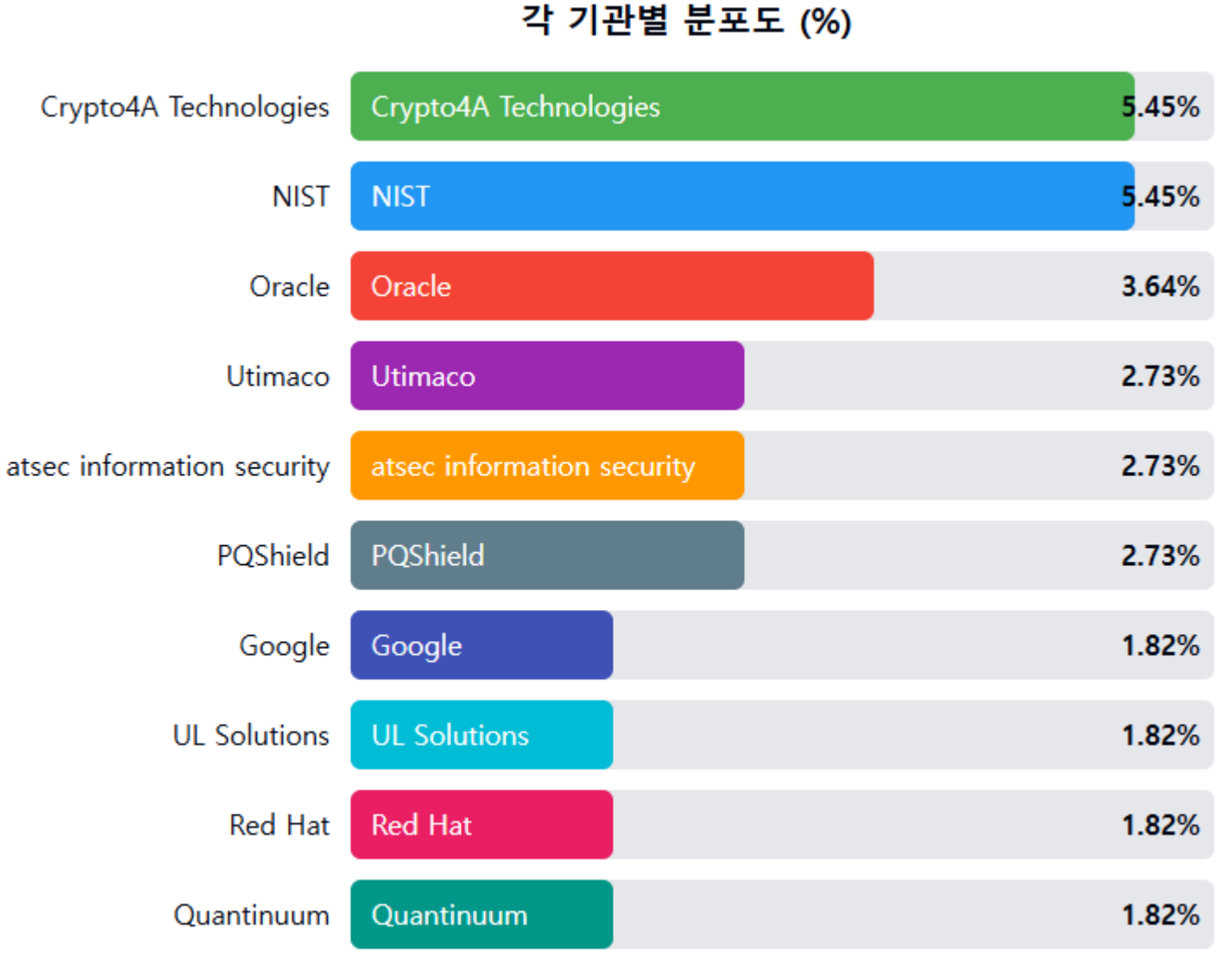
Exhibition

등록자: 341명(19개국)

미국 177명(51.9%), 캐나다 80명(23.4%), 한국 17명(4.9%) 비중 차지



기관: **NIST**, **atsec, AWS** 등 시험기관 및 업체

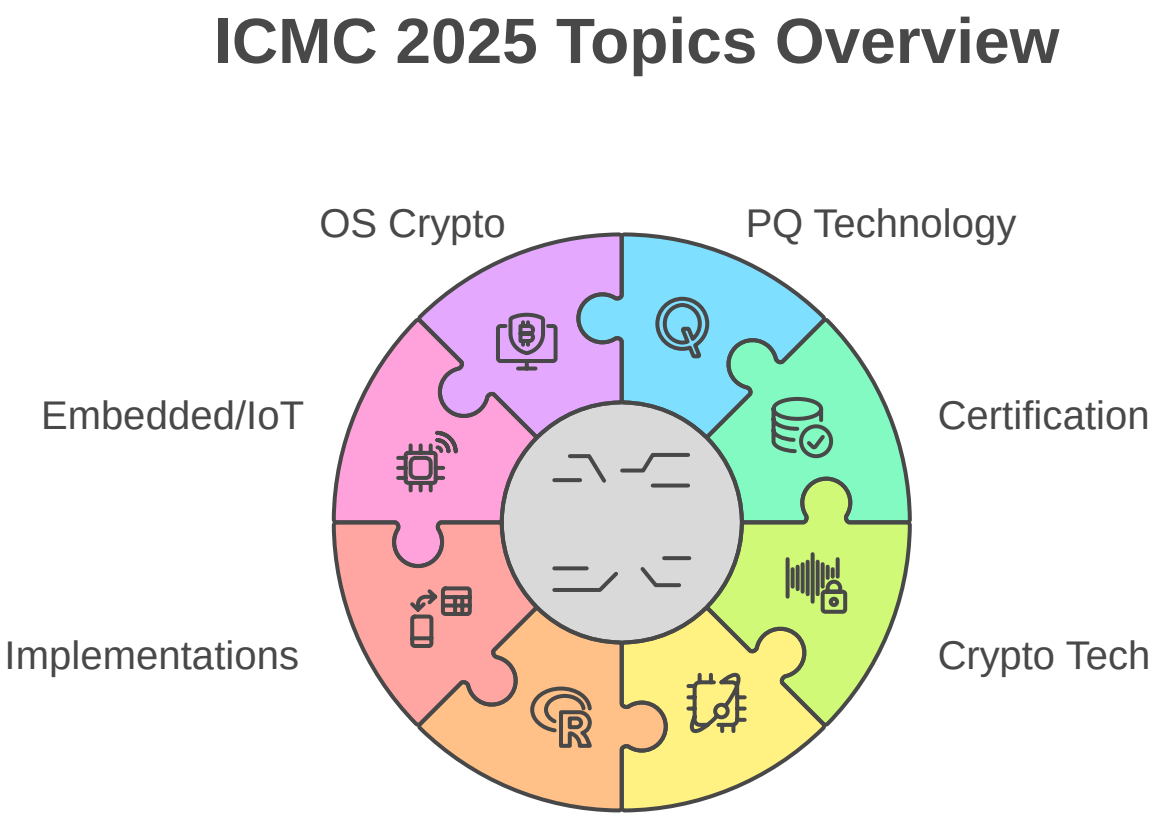


세션: 30개 세션(keynote(2) + talk(80) + panel discussion(7))

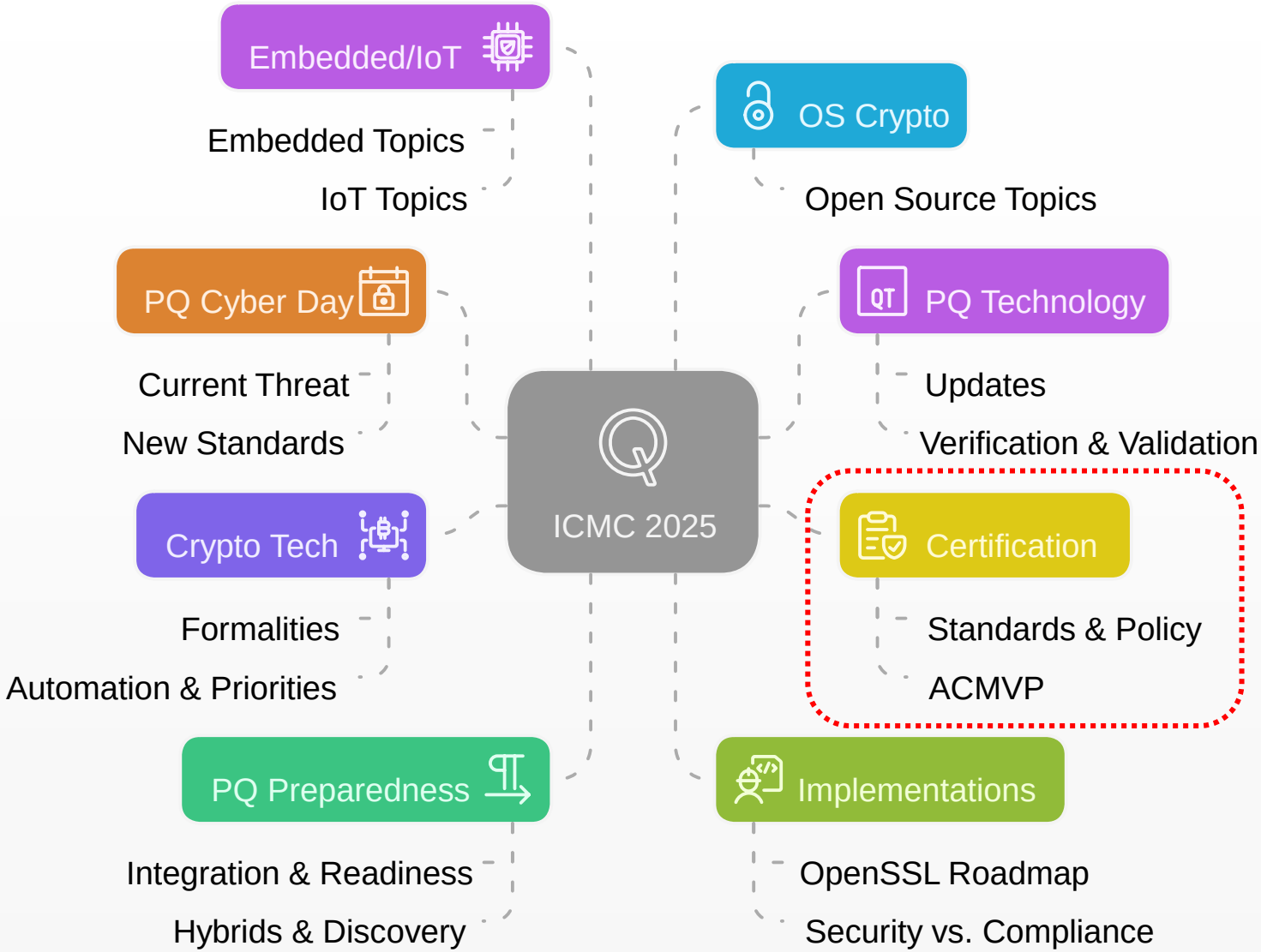
13:00-15:00 TRACK SESSIONS

Salon CD	Salon AB	Crush Space
PQ Technology (Q12)	**Certification** (C12)	**Crypto Tech** (G12)
Updates, Verification & Validation	Standards & Policy	Formalities
Moderator: Roberta Faux, Head of Cryptography and Field CTO, Arqit, United States	**Moderator:** Fiona Stewart, Security Assurance Consultant, Assurgo, United States	**Moderator:** Brian Wood, Program Manager, Google, United States
13:00 **Titbits: Latest Updates on PQC Deployments** (Q12a) Nils Gerhardt, CTO, Utimaco, Germany	13:00 **Mind the Gap: Navigating the Gray Areas of 19790:2025** (C12a) Carolyn French, Manager – Product Assurance and Standards, Canadian Centre for CyberSecurity (CCCS), Canada	13:00 **Formal Methods within Certification Programs: Status Update** (G12a) Nicky Mouha, Researcher, FedWriters, United States
13:30 **PQSecure Formality: Formal Verification and Assurance in Hardware for Post-Quantum Cryptography** (Q12b) Reza Azarderakhsh, Professor and CEO, PQSecure and Florida Atlantic University, United States	13:30 **The Technical Guideline BSI-TR 02102 (Cryptographic Mechanisms: Recommendations and Key Lengths) and Its Impact** (C12b) Werner Schindler, Section Head, Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany	13:30 **Ensuring Correctness and Security in High-Speed Post-Quantum Cryptography: Leveraging Formal Verification Tools** (G12b) Pierre-Yves Strub, Lead Formal Verification Researcher, PQShield, France
14:00 **Overview of Validating Falcon (FIPS 206 FN-DSA)** (Q12c) Pierre Ciadoux, NIST Foreign Guest Researcher, National Institute of Standards and Technology (NIST), United States	14:00 **NIAP Policy 5 Updates** (C12c) Edward Morris, CST Lab Manager, Gossamer Security Solutions, United States	14:00 **Public ledger integration with HSMs** (G12c) Noah Bouma, Technical Product Manager, Crypto4A Technologies, Canada
14:30 **The Big Picture of Lattice Signature Thresholdization** (Q12d) Thomas Espitau, Lead Crpytographic Researcher, PQShield, France	14:30 **Cloud Management and Security Standard for Financial Services** (C12d) Smita Mahapatra, Senior Security Industry Specialist, AWS, United States	14:30 **Secure HSM Auditing at a Distance: Enabling Remote Oversight** (G12d) Jean-Pierre Fiset, Principal System Architect, Crypto4A , Canada

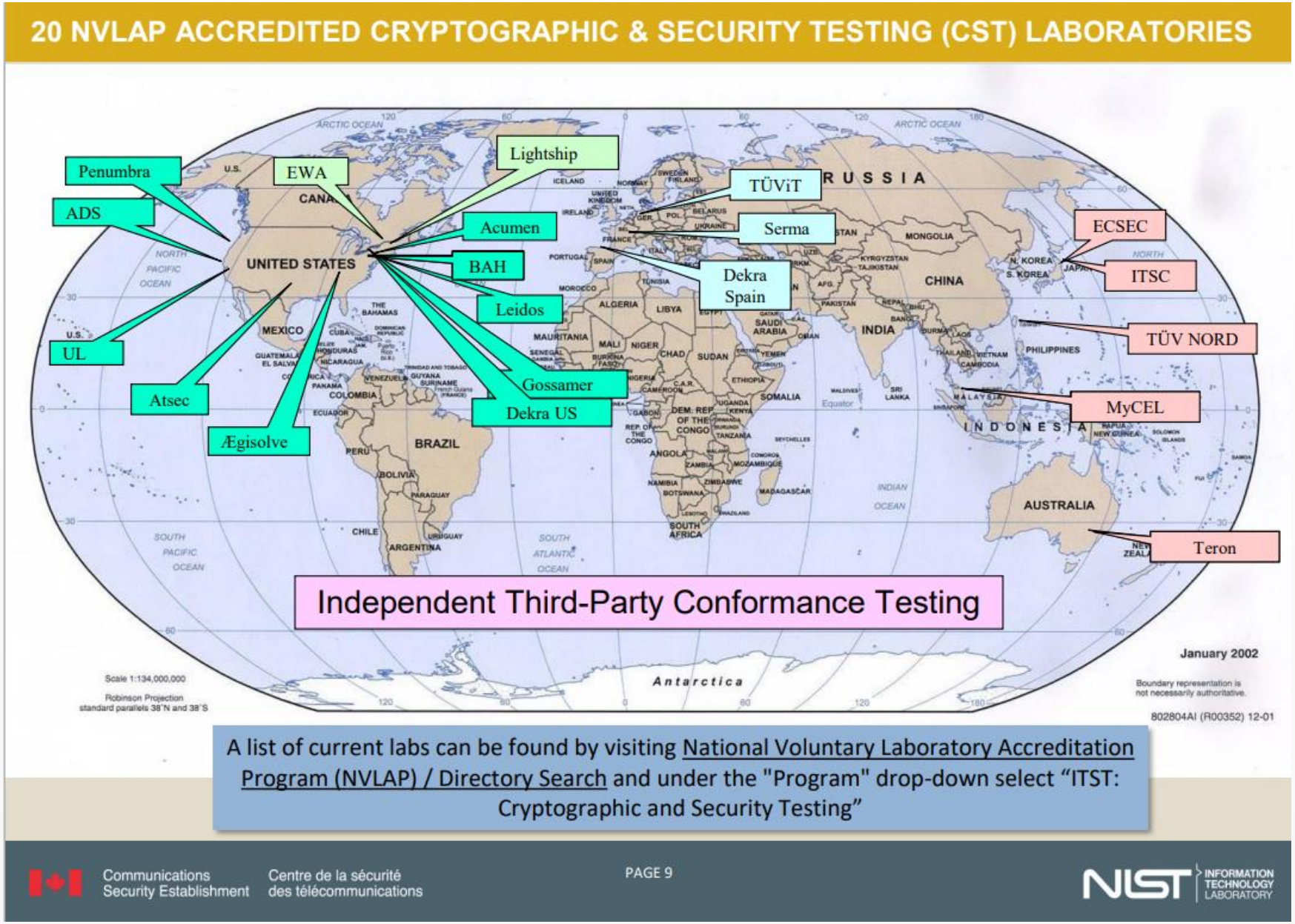
세션 주제: 8개 영역('24년 6개 -> '25년 8개)



ICMC 발표세션(3/3)


Embedded/IoT
Embedded Topics
IoT Topics
OS Crypto
Open Source Topics
PQ Cyber Day
Current Threat
New Standards
PQ Technology
Updates
Verification & Validation
ICMC 2025
Crypto Tech
Formalities
Automation & Priorities
Certification
Standards & Policy
ACMVP
PQ Preparedness
Integration & Readiness
Hybrids & Discovery
Implementations
OpenSSL Roadmap
Security vs. Compliance

|주요내용(1): CMVP 시험기관 현황



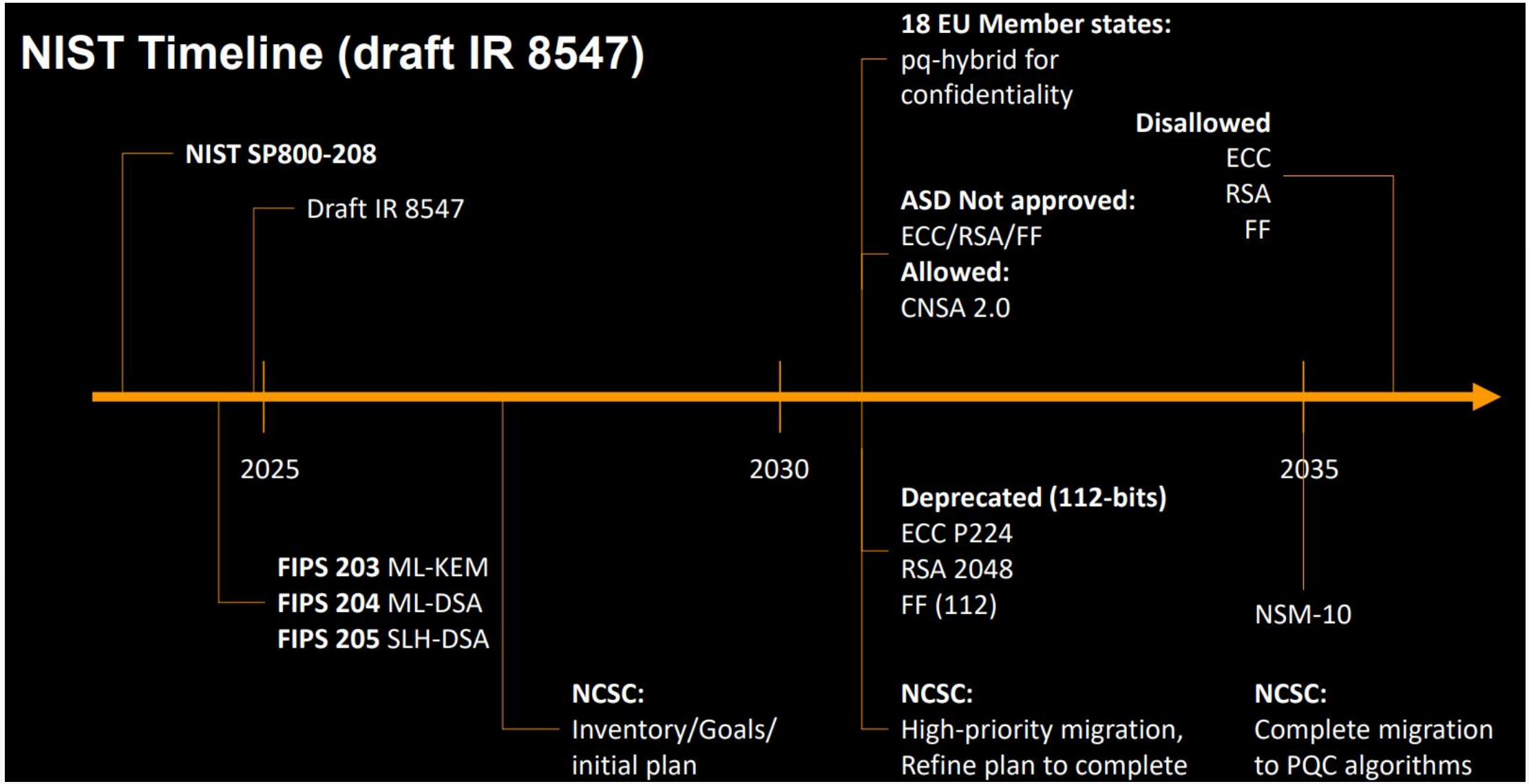
Reminder (Aug 13, 2024):

- FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) were published.
  - Same day support for both the CMVP and CAVP!

What's new:

- PQC FAQ, posted on the FIPS 203/204/205 webpages .
  - FIPS 203/204: Using seeds as a default key format.
  - FIPS 204: Computing *mu* external to the module.
- IG
  - Revising IG 10.3.A to address self-tests consistent with above PQC FAQ.
- FIPS 206 (FN-DSA) Draft coming soon – CAVP tests underway.
  - Related ICMC talk today (**Q12c – 13:00):** "*Overview of Validating Falcon* (FIPS 206 FN-DSA)"

|주요내용(3): PQC 전환 타임라인 동향



AUTOMATED CRYPTOGRAPHIC MODULE VALIDATION PROJECT (ACMVP)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ACMVP Team Panelists

Chris Celi
ACMVP Project Lead, National Institute of Standards and Technology (NIST)

Yi Mao
ACMVP TE WS Co-lead, CEO of atsec US

Stephan Mueller
ACMVP Developer & Principal Consultant, atsec information security

Barry Fussell
ACMVP Developer & Principal Engineer, CISCO Systems

Raoul Gabiam
Infrastructure Team, Principal Cloud and Cybersecurity Engineer, MITRE

Moderator

Courtney Maatta
ACMVP Program Management, AWS

WHAT IS THE NCCOE ACMVP?

The Automated Cryptographic Module Validation Project (ACMVP) was undertaken by the NCCOE to support improvement in the **efficiency and timeliness of CMVP operations and processes.**

BENEFITS OF CMVP AUTOMATION

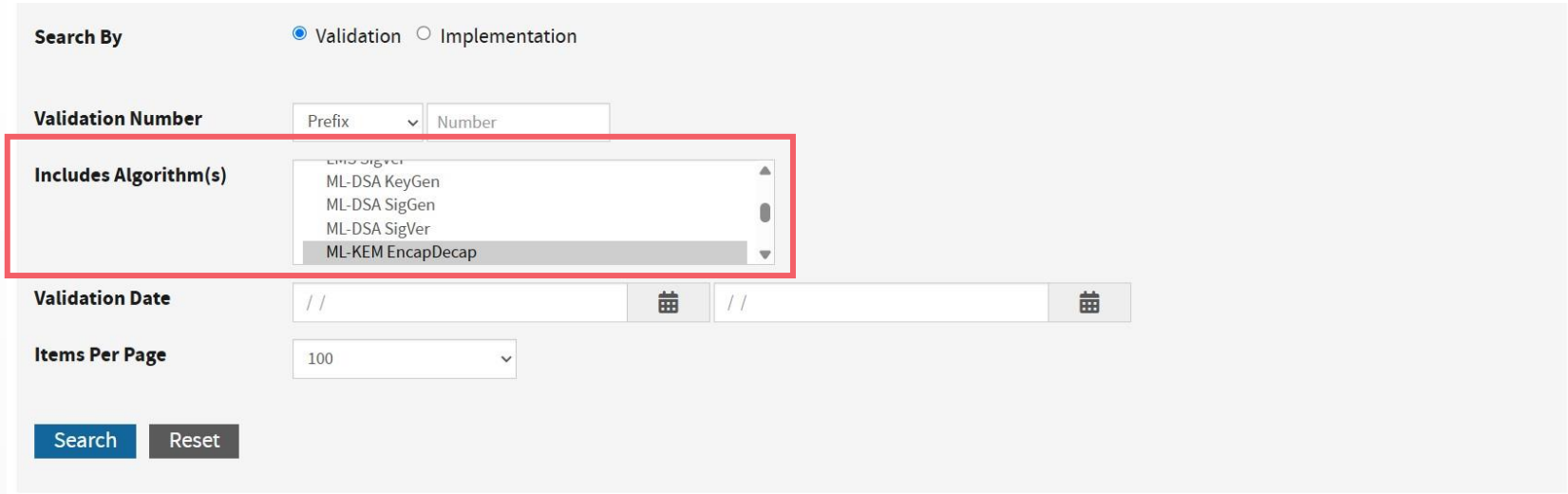
- **Faster certification process** – Reducing the time needed for approval.
- **Increased reliability** – Minimizing human errors in validation.
- **Scalable and efficient** – Making cryptographic validation more accessible to vendors.
- **Standardized compliance framework** – Ensuring industry-wide adoption and security.

03

나아갈 방향

미국 CAVP 검증 현황

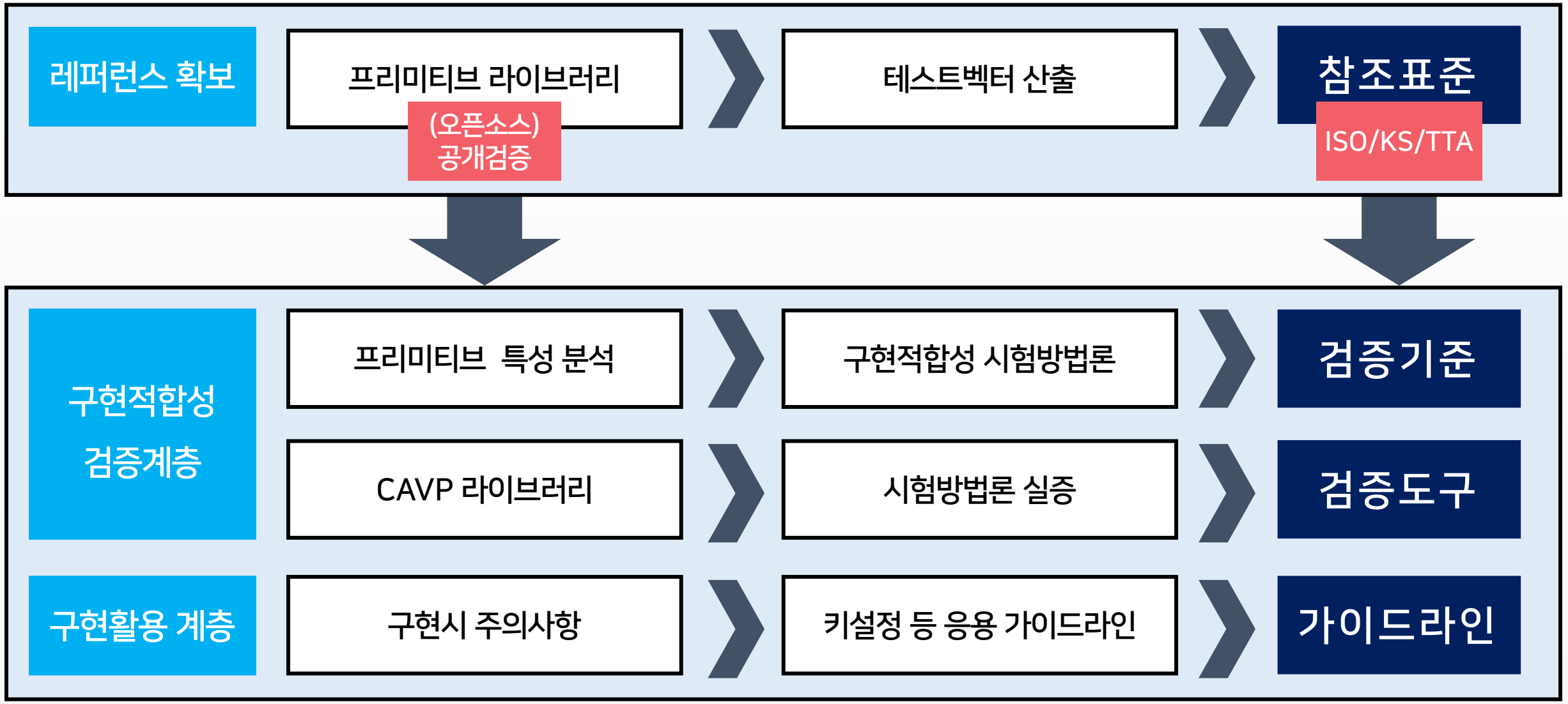
Cryptographic Algorithm Validation Program CAVP



Showing **80** matching records.

Vendor	Implementation	Validation Number	Validation Date
atsec corp.	leancrypto (C)	A5615	8/13/2024
atsec corp.	leancrypto (AVX2)	A5616	8/13/2024
atsec corp.	leancrypto (ARM_ASM)	A5619	8/13/2024
atsec corp.	leancrypto (Kernel_C)	A5621	8/13/2024
atsec corp.	leancrypto (Kernel_AVX2)	A5625	8/13/2024
atsec corp.	leancrypto (C)	A5627	8/13/2024
atsec corp.	leancrypto (ARM_ASM)	A5628	8/13/2024
Crypto4A Technologies, Inc.	QASM Cryptographic Module	A5631	8/14/2024

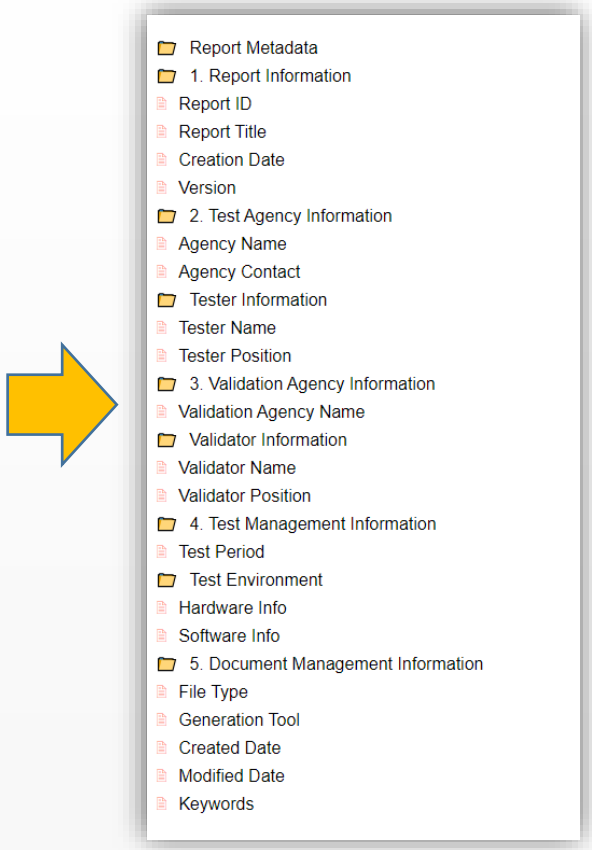
Note. FIPS 203 최종본, 2024년 8월 24일 제정


레퍼런스 확보
프리미티브 라이브러리
(오픈소스)
공개검증
테스트벡터 산출
참조표준
ISO/KS/TTA
구현적합성
검증계층
프리미티브 특성 분석
구현적합성 시험방법론
검증기준
CAVP 라이브러리
시험방법론 실증
검증도구
구현활용 계층
구현시 주의사항
키설정 등 응용 가이드라인
가이드라인

자동화 검증

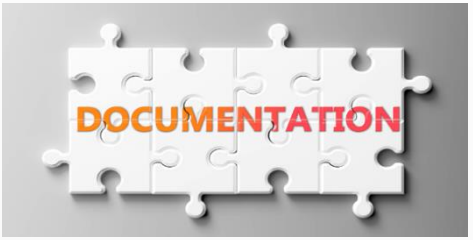
시험결과보고서 템플릿

- ISO/IEC 24759 요구사항 목록화(예, 보안수준 1)
- 보고서 구성 정보 설계
- 메타데이터 모델 설계
- 시험결과보고서 양식



정보 구조화

메타 데이터(예, JSON)



문서 파일
(Word, PDF)


2025
CVC 워크숍
Crypto Validation Crew Workshop
주최
국가정보원
NATIONAL INTELLIGENCE SERVICE
과학기술정보통신부
Ministry of Science and ICT
주관
NSR
국가보안기술연구소
KISA
한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY
KCF
한국암호포럼
Korea Cryptography Forum
CVC

KCMVP 추진방향: 국가 암호 안전성 제고

암호알고리즘
다각화

암호검증 인프라
강화

협력 · 소통

국가보안기술연구소

고맙습니다