米国の動向と日本・欧州との比較

株式会社コスモス・コーポレイション
濱口　総志

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

FPKI and comparison to Japan/EU

株式会社コスモス・コーポレイション
濱口　総志

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

米国　FPKIの背景

E Governance Act of 2002
連邦政府の電子化に向けた法律

FISMA(Federal Information Security Management→Modernization Act)
連邦情報セキュリティマネジメント法
連邦政府機関のセキュティ強化を義務化。NISTにセキュリティ規格やガイドラインの開発を義務化。

ICAM (Identity, Credential and Access Management)
適切な個人が適切な理由で適切な情報に適切な時にアクセスできるようにする

FICAM (Federal Identity, Credential and Access Management)
米国連邦政府のICAMの実装であり、政府機関統一のICAM基準、ベストプラクティス、実装ガイドを提供

OMB M-04-04
NIST SP 800-63
認証の保証レベル(LoA)を規定（IAL, FAL, AAL）

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

Back ground of US Federal PKI

E Governance Act of 2002
Law for digitalization of federal government

FISMA(Federal Information Security Management→Modernization Act)
Mandating security enforcement to federal agencies. NIST to develop FIPS(Federal Information Processing Standards) to s upport FISMA risk management framework.

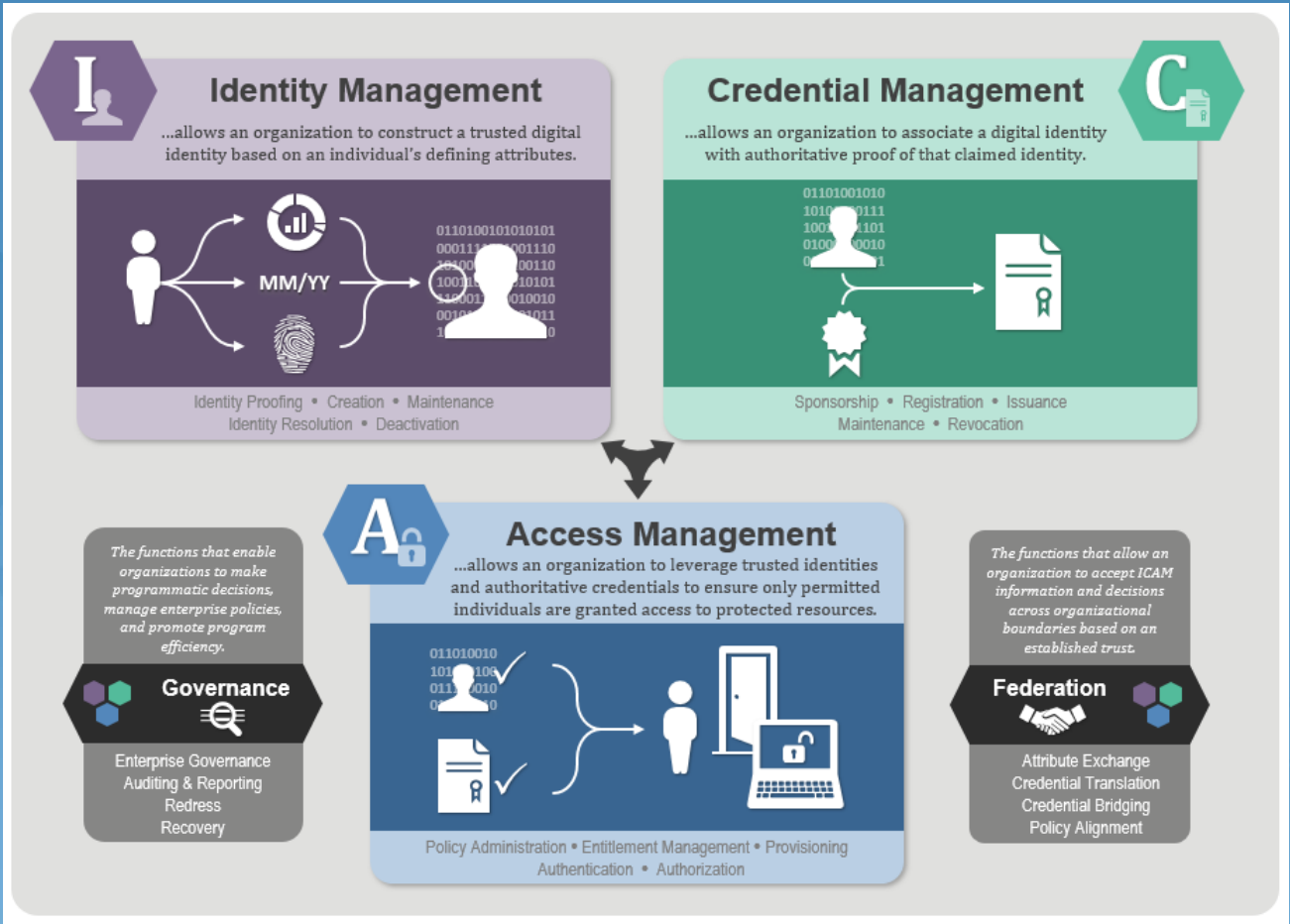
ICAM (Identity, Credential and Access Management)
Right person is accessing the right information at the right time for the right reason.

FICAM (Federal Identity, Credential and Access Management)
ICAM implementation of US federal government and provides ICAM standards, best practices and implementation guida nce.

OMB M-04-04
NIST SP 800-63
Defines Level of Assurance (LoA)for electronic authentication（IAL, FAL, AAL）

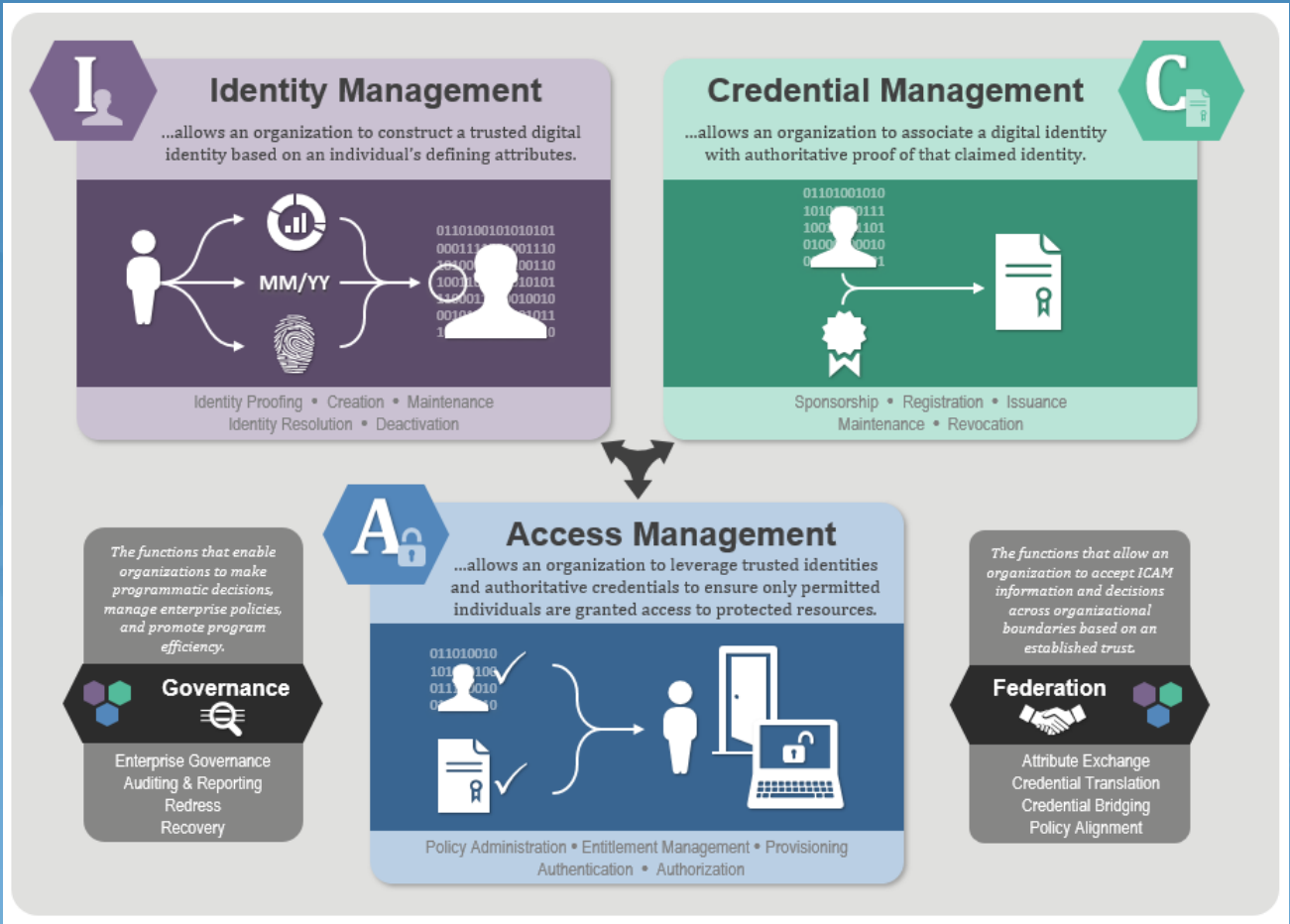
Cosmos
POFESSIONALS OF SAFETY ENGINEERING

FICAM



出典：Idmanagement.gov

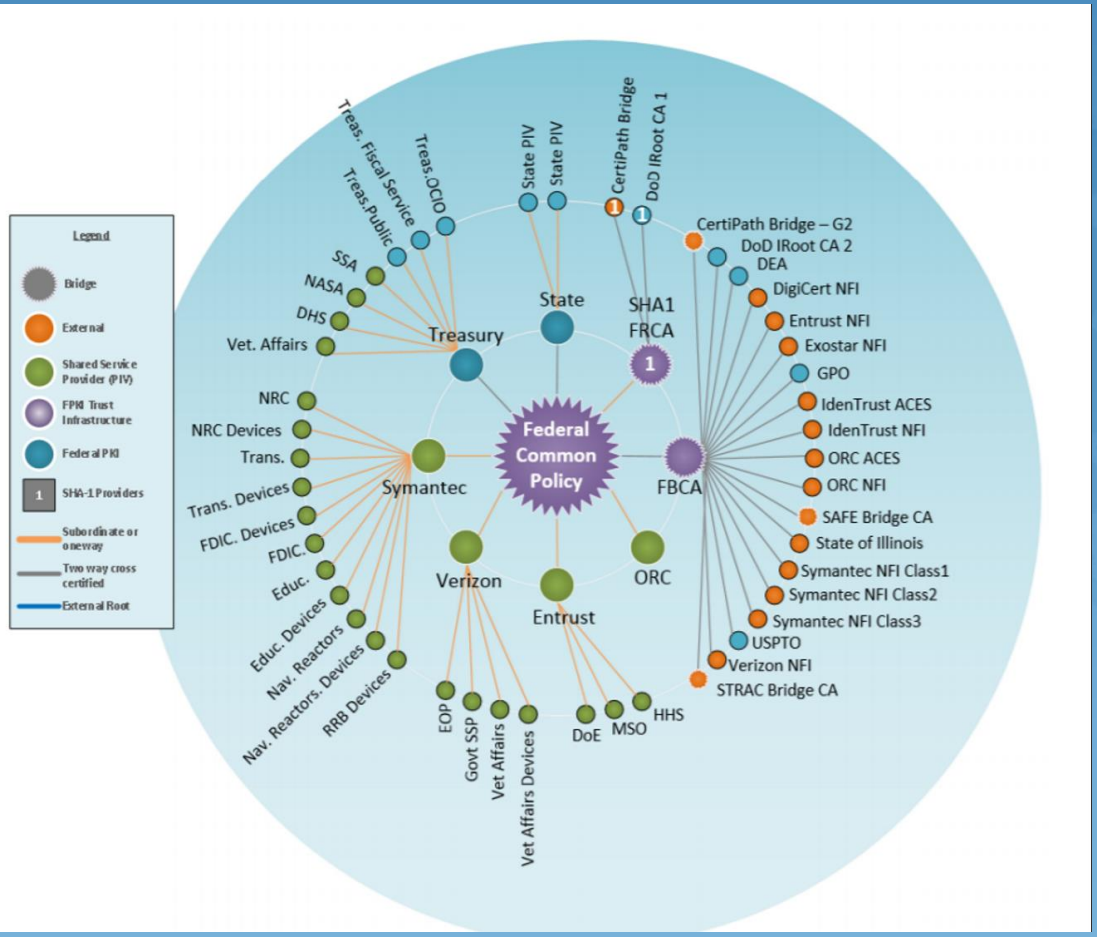
FICAM



Cosmos
POFESSIONALS OF SAFETY ENGINEERING

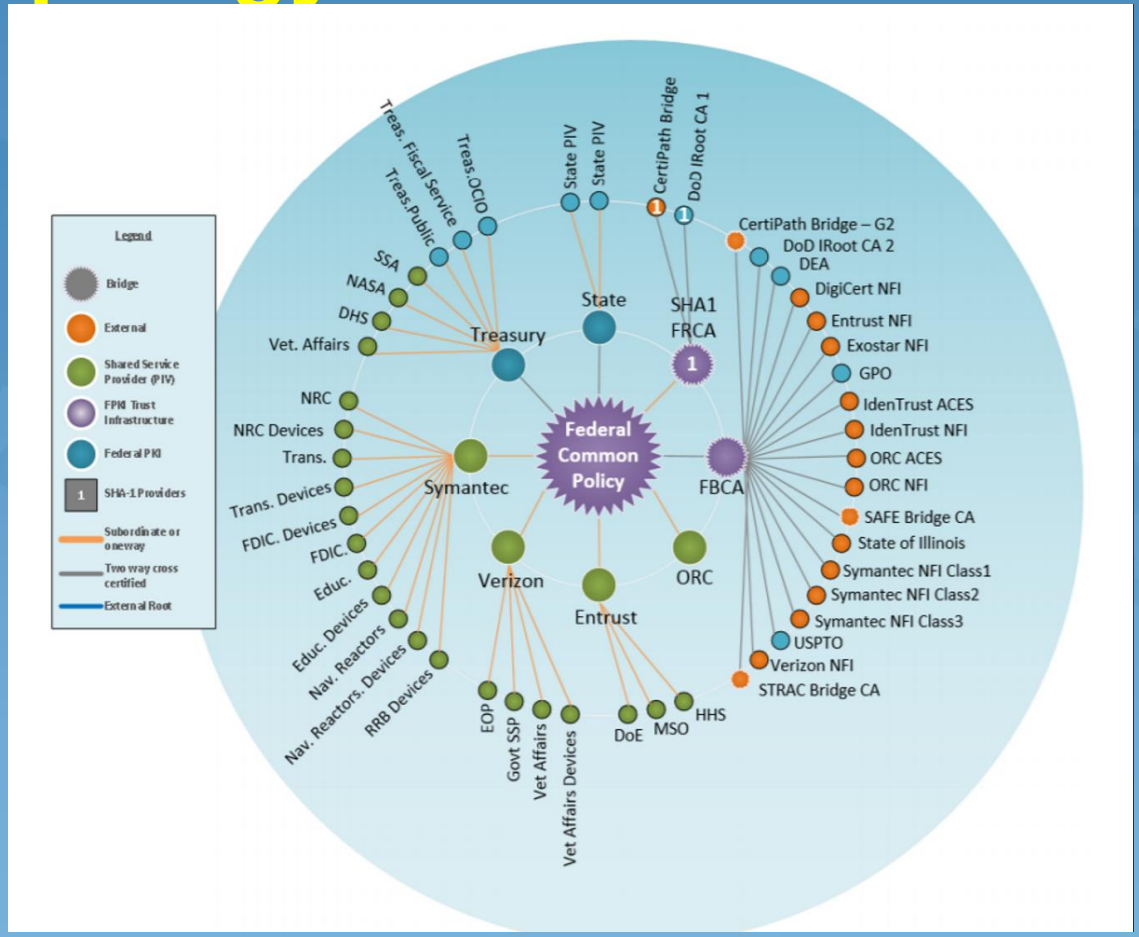
出典：Idmanagement.gov

FPKIのトポロジー



出典：Idmanagement.gov

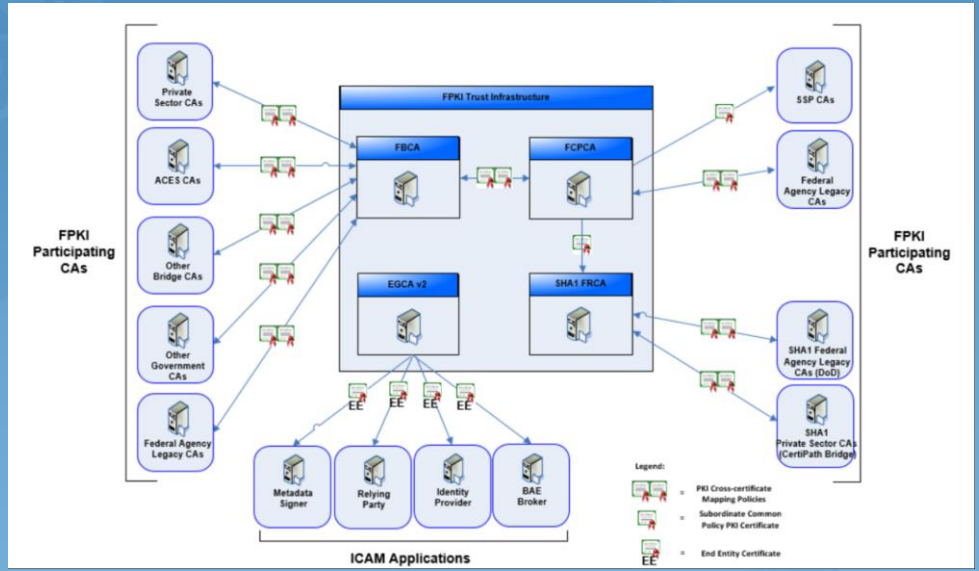
FPKI Topology



出典：Idmanagement.gov

FPKIトポロジーのコア

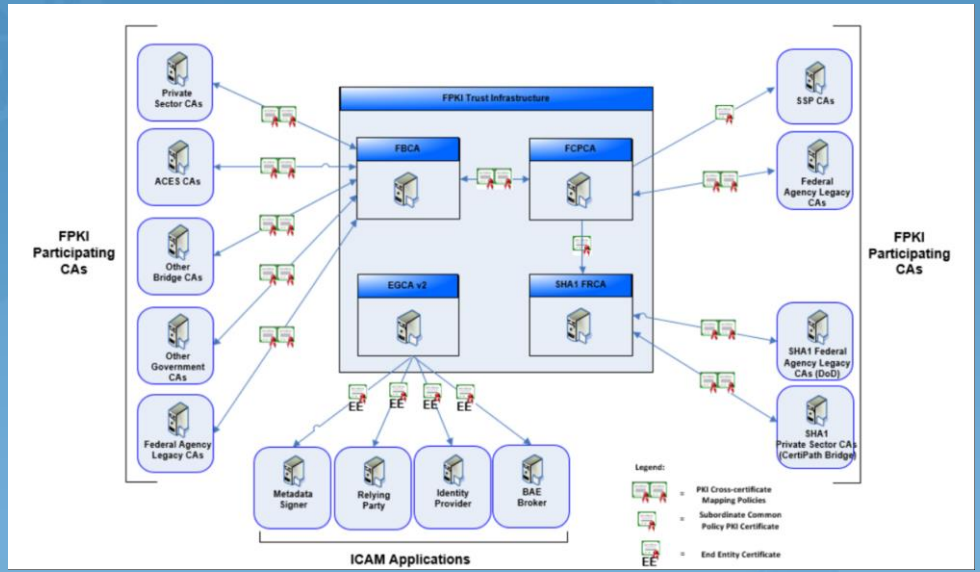
- FCPCA, Federal Common Policy CA
  - FPKIのトラストアンカー
- SHA1 FRCA
  - レガシー
- FBCA, Federal Bridge CA
  - トラストハブ、ブリッジ
- EGCA, e-Gov CA
  - ICAM Application
- SSA, Shared Service Provider
  - 政府専用認証局（民間／政府機関）



出典：Idmanagement.gov

Core Components of FPKI Topology

- FCPCA, Federal Common Policy CA
  - Trust anchor of FPKI
- SHA1 FRCA
  - Legacy system
- FBCA, Federal Bridge CA
  - Trust Hub, Bridge.
- EGCA, e-Gov CA
  - ICAM Applications
- SSA, Shared Service Provider
  - CA dedicated for Federal Agency



出典：Idmanagement.gov

FPKI × LoA (NIST SP 800-63)

Certificate Policy	ID Proofing	Token	Token and Credential Management	Overall LOA Equivalence
Common-Auth PIV-I Auth SHA1 Auth	LOA 4	LOA 4	LOA 4	LOA 4
Common –SW	LOA 4	LOA 3	LOA 4	LOA 3
Common-HW PIV-I HW SHA1-HW	LOA 4	LOA 4	LOA 4	LOA 4
Common-High FBCA-High	LOA 4	LOA 4	LOA 4	LOA 4
FBCA Basic	LOA 3	LOA 3	LOA 3	LOA 3
FBCA Medium FBCA Medium CBP	LOA 3	LOA 3	LOA 4	LOA 3
FBCA MediumHW FBCA MediumHW-CBP	LOA 3	LOA 4	LOA 4	LOA 3
Common-cardAuth PIVI-cardAuth SHA1-cardAuth	LOA 4	LOA 2	LOA 4	LOA 2

出典：Idmanagement.gov

FPKI × LoA (NIST SP 800-63)

Certificate Policy	ID Proofing	Token	Token and Credential Management	Overall LOA Equivalence
Common-Auth PIV-I Auth SHA1 Auth	LOA 4	LOA 4	LOA 4	LOA 4
Common –SW	LOA 4	LOA 3	LOA 4	LOA 3
Common-HW PIV-I HW SHA1-HW	LOA 4	LOA 4	LOA 4	LOA 4
Common-High FBCA-High	LOA 4	LOA 4	LOA 4	LOA 4
FBCA Basic	LOA 3	LOA 3	LOA 3	LOA 3
FBCA Medium FBCA Medium CBP	LOA 3	LOA 3	LOA 4	LOA 3
FBCA MediumHW FBCA MediumHW-CBP	LOA 3	LOA 4	LOA 4	LOA 3
Common-cardAuth PIVI-cardAuth SHA1-cardAuth	LOA 4	LOA 2	LOA 4	LOA 2

出典：Idmanagement.gov

ポリシーマッピング

- 相互認証（Cross-certificate)の前提条件としてのポリシーマッピング
- 相互認証する認証局が互いの証明書ポリシーを確認し、
比較可能であり、同等であることを認める

FCPCA Policy	FCPCA OID	FBCA OID	FBCA Policy
common-policy	2.16.840.1.101.3.2.1.3.6	2.16.840.1.101.3.2.1.3.3	FBCA-medium
common-High	2.16.840.1.101.3.2.1.3.16	2.16.840.1.101.3.2.1.3.4	FBCA-High
common-HW	2.16.840.1.101.3.2.1.3.7	2.16.840.1.101.3.2.1.3.12	FBCA-mediumHW
common-devices	2.16.840.1.101.3.2.1.3.8	2.16.840.1.101.3.2.1.3.37	FBCA-mediumDevice
common-devicesHW	2.16.840.1.101.3.2.1.3.36	2.16.840.1.101.3.2.1.3.38	FBCA-mediumDevice-HW

出典：Idmanagement.gov

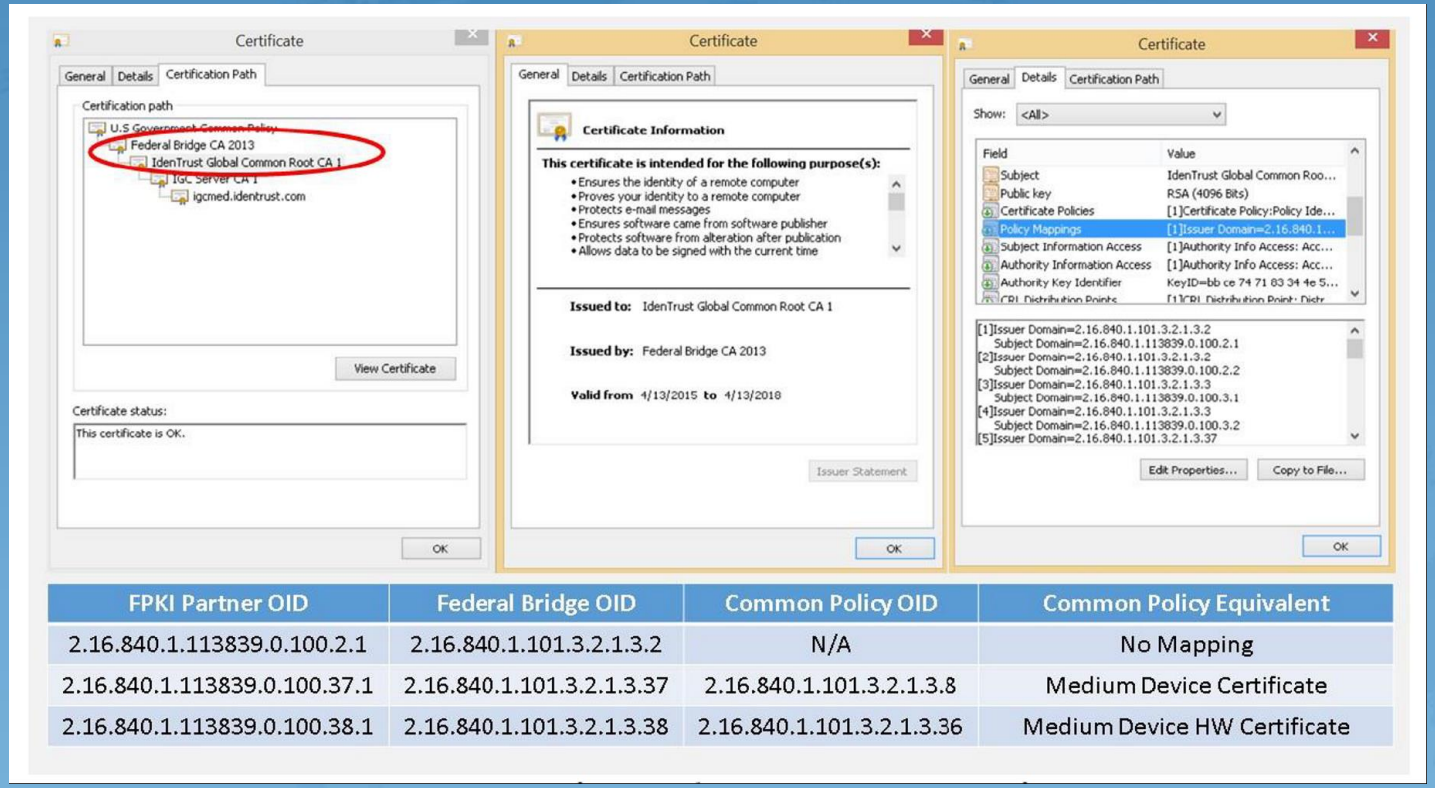
Policy Mapping

- Policy mapping as precondition of Cross-certificate with Bridge CA
- CAs need to check the each other's certificate policy and recognize them as comparable and equivalent.

FCPCA Policy	FCPCA OID	FBCA OID	FBCA Policy
common-policy	2.16.840.1.101.3.2.1.3.6	2.16.840.1.101.3.2.1.3.3	FBCA-medium
common-High	2.16.840.1.101.3.2.1.3.16	2.16.840.1.101.3.2.1.3.4	FBCA-High
common-HW	2.16.840.1.101.3.2.1.3.7	2.16.840.1.101.3.2.1.3.12	FBCA-mediumHW
common-devices	2.16.840.1.101.3.2.1.3.8	2.16.840.1.101.3.2.1.3.37	FBCA-mediumDevice
common-devicesHW	2.16.840.1.101.3.2.1.3.36	2.16.840.1.101.3.2.1.3.38	FBCA-mediumDevice-HW

出典：Idmanagement.gov

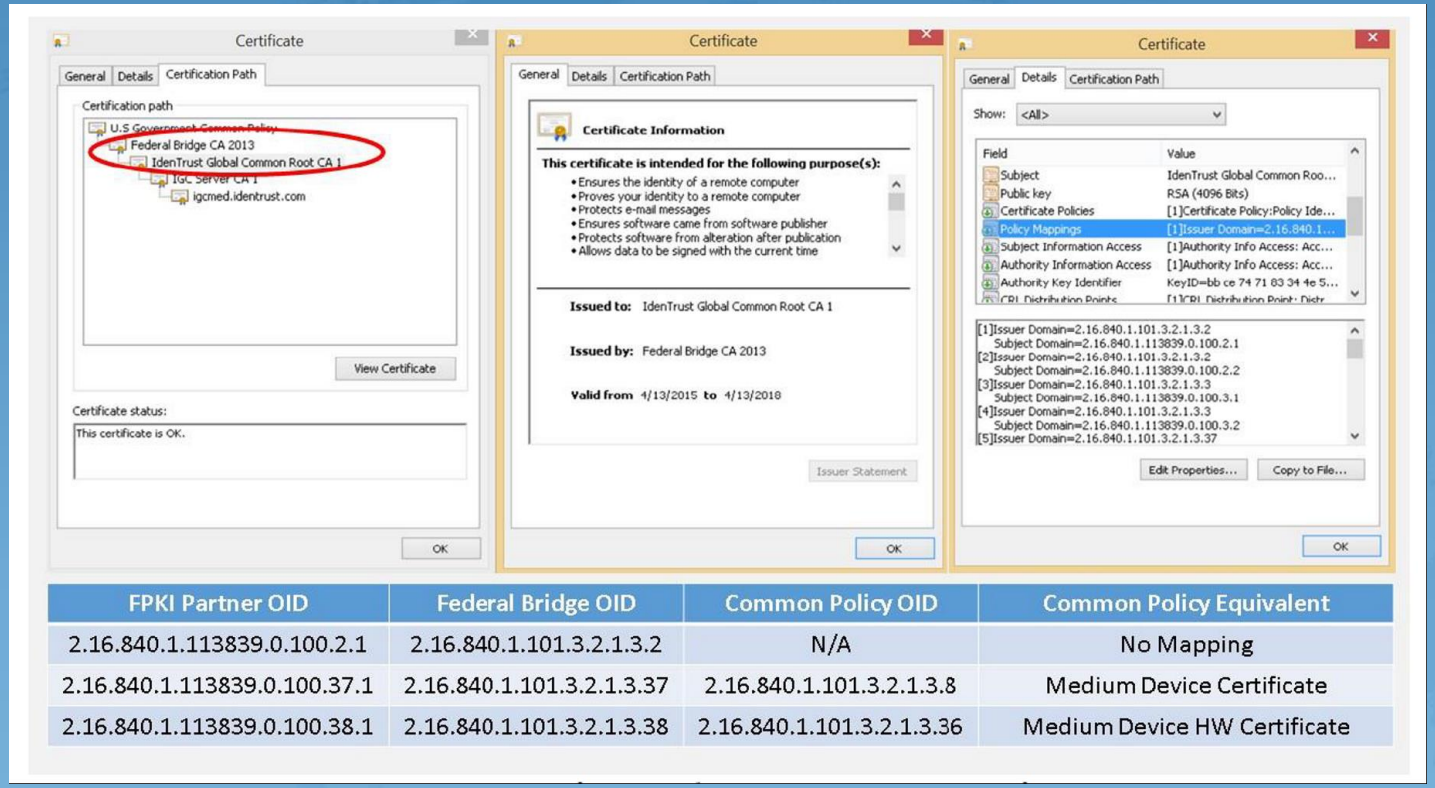
ポリシーマッピング(証明書の拡張領域)



FPKI Partner OID	Federal Bridge OID	Common Policy OID	Common Policy Equivalent
2.16.840.1.113839.0.100.2.1	2.16.840.1.101.3.2.1.3.2	N/A	No Mapping
2.16.840.1.113839.0.100.37.1	2.16.840.1.101.3.2.1.3.37	2.16.840.1.101.3.2.1.3.8	Medium Device Certificate
2.16.840.1.113839.0.100.38.1	2.16.840.1.101.3.2.1.3.38	2.16.840.1.101.3.2.1.3.36	Medium Device HW Certificate

出典：Idmanagement.gov

Policy Mapping (in Certificate extension)



FPKI Partner OID	Federal Bridge OID	Common Policy OID	Common Policy Equivalent
2.16.840.1.113839.0.100.2.1	2.16.840.1.101.3.2.1.3.2	N/A	No Mapping
2.16.840.1.113839.0.100.37.1	2.16.840.1.101.3.2.1.3.37	2.16.840.1.101.3.2.1.3.8	Medium Device Certificate
2.16.840.1.113839.0.100.38.1	2.16.840.1.101.3.2.1.3.38	2.16.840.1.101.3.2.1.3.36	Medium Device HW Certificate

出典：Idmanagement.gov

PIV (Personal Identity Verification)

連邦政府職員（及び契約者）向けIDカード

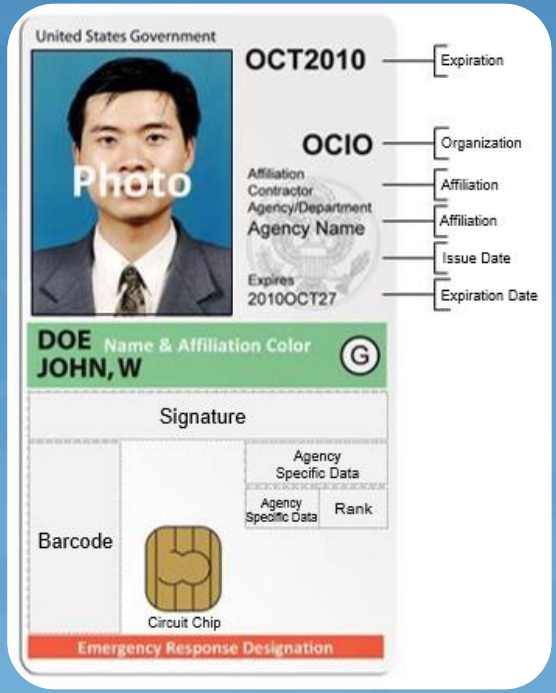
- HSPD12 (Homeland Security Presidential Directive)
- NIST FIPS 201

証明書

- PIV Authentication
- Card Authentication
- Digital Signature
- Encryption

用途：

- PACS、LACS
- 署名
- 暗号化



Cosmos
POFESSIONALS OF SAFETY ENGINEERING

出典：Wikipedia

PIV (Personal Identity Verification)

ID card for employees of Federal Agency (and Contractor)

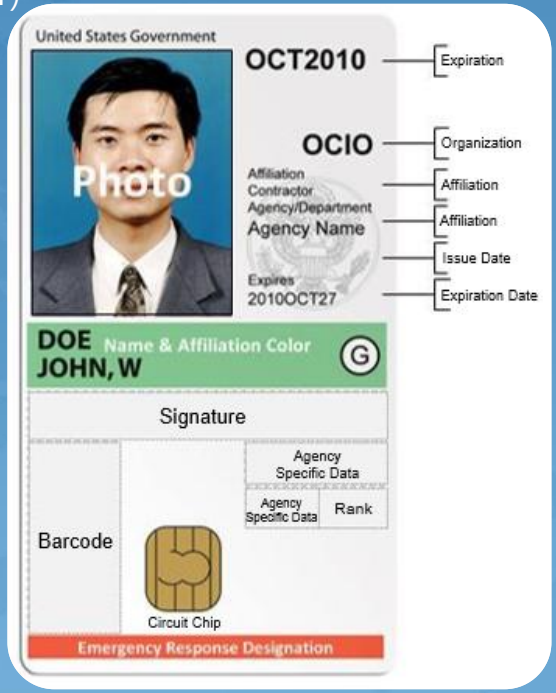
- HSPD12 (Homeland Security Presidential Directive)
- NIST FIPS 201

Certificates

- PIV Authentication
- Card Authentication
- Digital Signature
- Encryption

Usage：

- PACS、LACS
- Signature
- Encryption



Cosmos

POFESSIONALS OF SAFETY ENGINEERING

出典：Wikipedia

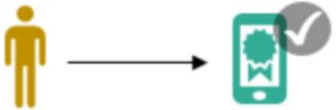
Derived PIV

PIVカードの所持者が、PIVクレデンシャルをスマホに格納する仕組み
LoA3orLoA4

1. Request Issued

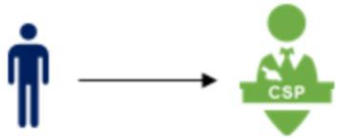
- An individual requests a derived PIV from an approval authority

2. Request Approved



- The approval authority reviews the request. If valid, it is approved.

3. Authentication



- The individual contacts a CSP that provides derived PIVs and is authenticated using their PIV card.
  Authentication may occur virtually (LOA3) or in person (LOA3 & LOA4).

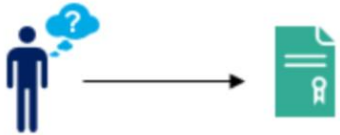
4. Token Generated

- The CSP generates the credential token and securely issues it to the individual.
  The issuer could be a person or a system.

5. Token Issued

- The credential is securely issued to the individual's mobile device.

6. Token Activated



- The individual is prompted to activate the token by establishing a shared secret.

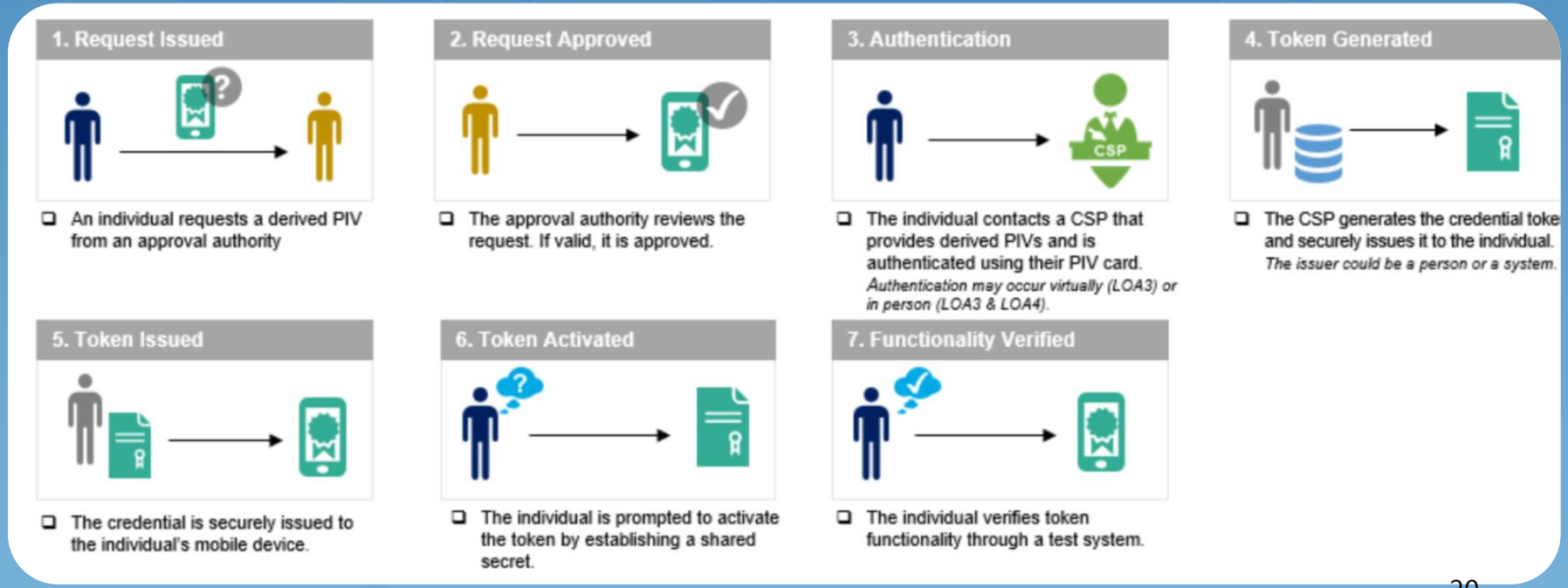
7. Functionality Verified

- The individual verifies token functionality through a test system.

出典：Idmanagement.gov

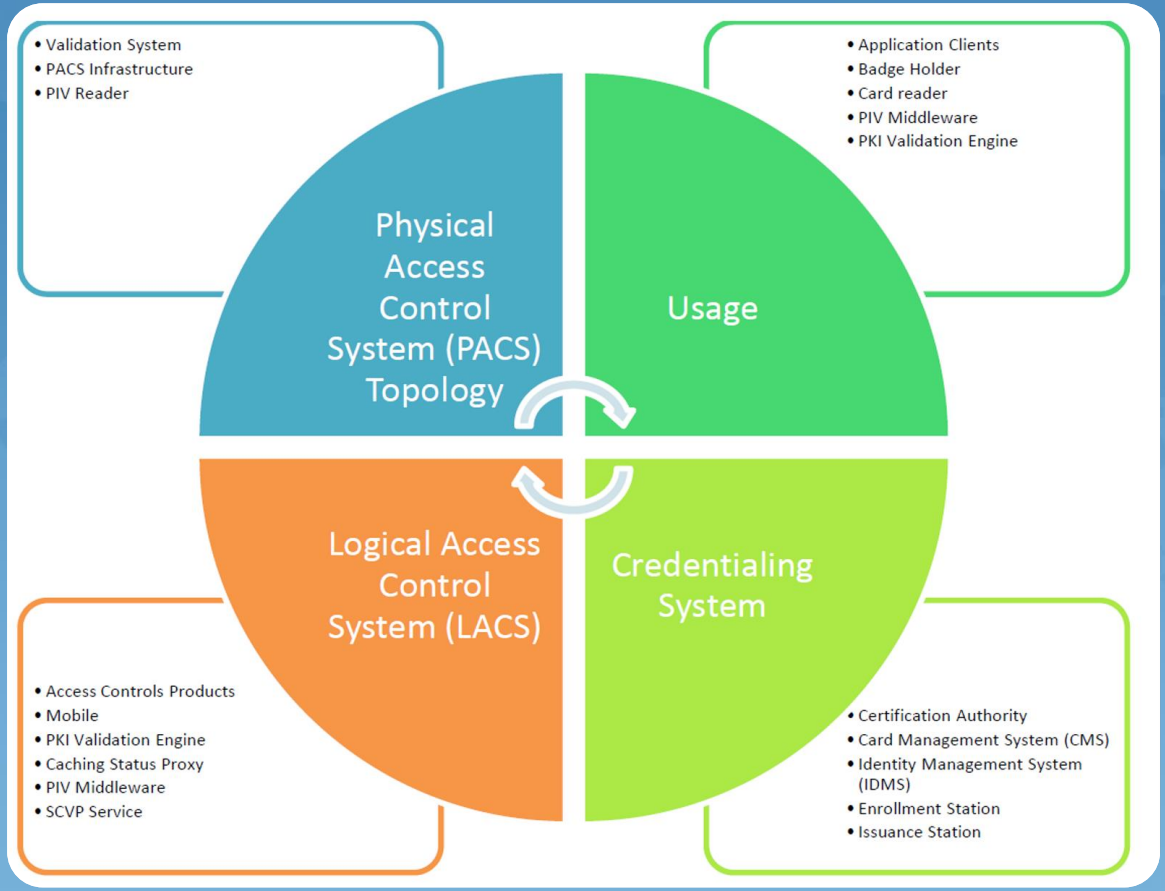
Derived PIV

PIV credential (Certificate) for mobile device(e.g. smartphone)
LoA3orLoA4



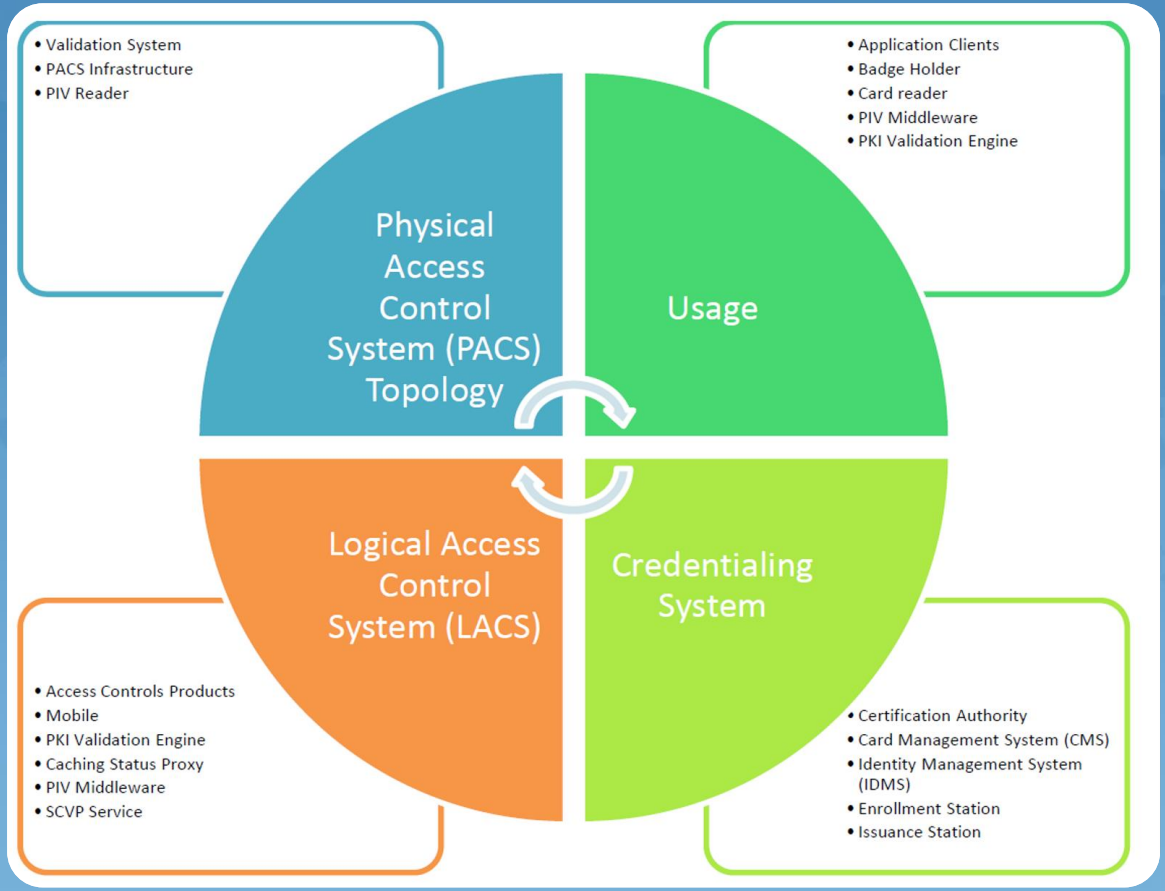
出典：Idmanagement.gov

FICAM Test Program



出典：Idmanagement.gov

FICAM Test Program



出典：Idmanagement.gov

And PIV-I (Interoperable)…

PIVのスキームを民間に拡大

PIVの技術標準に適合した民間向けIDカード＋PIV-I証明書

PIV向け環境（つまり政府システム、政府施設等）で検証可能（相互運用性）

And PIV-I (Interoperable)…

Extension of PIV scheme to private sector

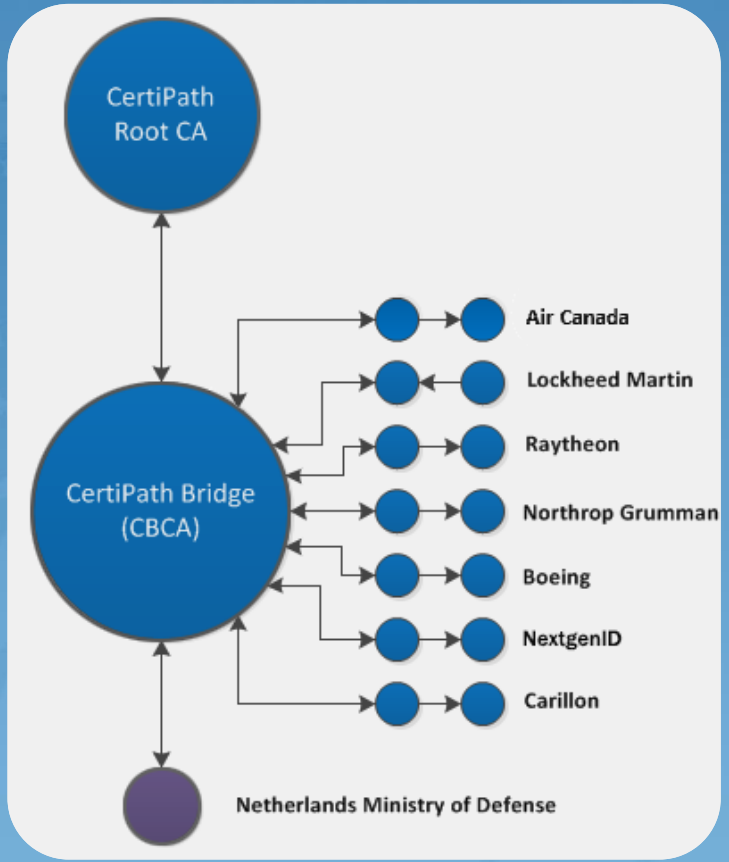
PIV technical conformant ID card and certificate (PIV-I certificate) for public sector

Interoperable with PIV environment (Federal system and facilities)

航空業界向けPKI

- 航空宇宙／防衛産業向けブリッジCA
- CertiPath Bridge CA

- 業界の出資で設立
- CBCAとの相互認証には、PMAの承認が必要



出典：www.certipath.com

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

FPKI for Private sector (A&D)

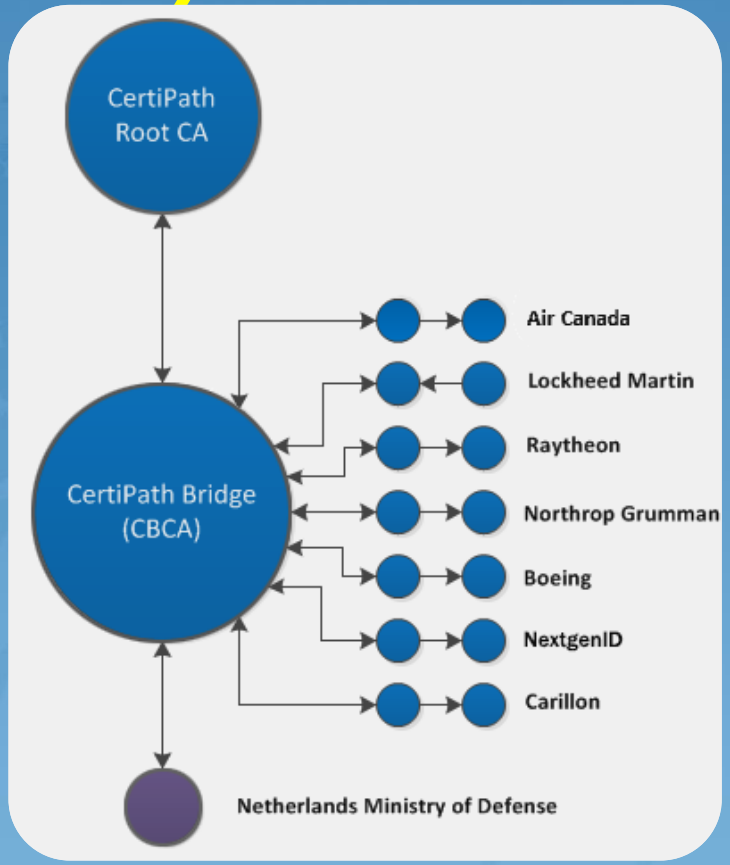
- CertiPath Bridge CA

  Bridge CA for Aerospace and Defense Industry

- Founded by stakeholders;

  Lockheed Martin, Raytheon, Northrop Grumman Boeing and etc.

- Cross certificate with CBCA requires Policy Mapping and PMA approval.



出典：www.certipath.com

FPKI for Private sector (A&D)

DO178CとARINC827

DO178C

FAA（アメリカ連邦航空局）、EASA（欧州航空安全機関）及びTransport Canada（カナダ運輸省）が採用したソフトウェアおよび制御される装置を含むシステムの評価規格

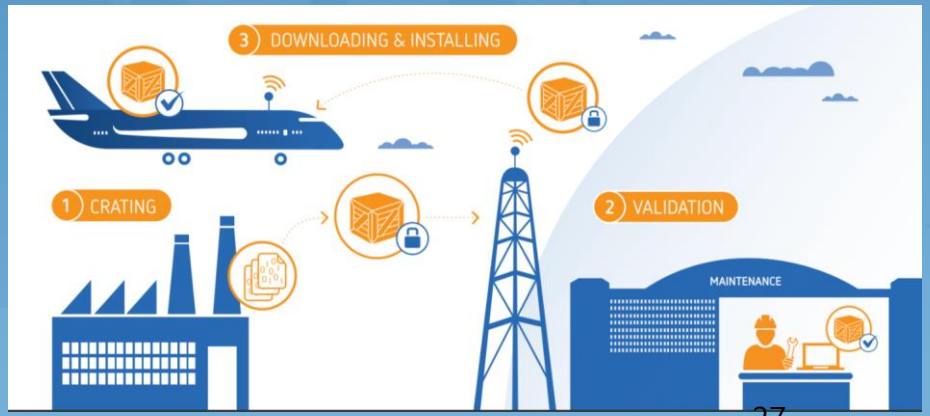
航空機のソフトウェア部品はこの規格による評価／認証が必須

・ソフトウェアライフサイクルをカバー（設計➡開発➡試験（検証））

ARINC827

Airline Electronic Engineering Committeeが作成したソフトウェア部品の電子的な配布に関する規格

ソフトウェア部品をCBCAと相互認証した認証局の証明書で署名



出典：https://www.carillon.ca/

FPKI for Private sector (A&D)

DO178C and ARINC827

DO178C

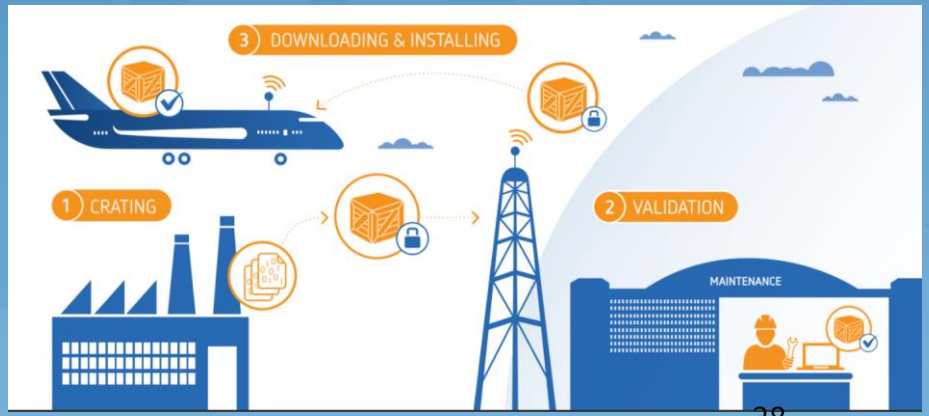
primary document by which the certification authorities such as FAA, EASA and Transport Canada approve all commercial software-based aerospace

・whole software lifecycle from planning, development to test/review is covered.

ARINC827

Standard created by Airline Electronic Engineering Committee for electronic distribution of software parts

Software parts are signed with Certificate issued by CAs cross certified with CBCA.



出典：https://www.carillon.ca/

WebTrust for CA

AICPA(米国公認会計士協会)及びCICA(カナダ勅許会計士協会)によって運営されている認証局の監査プログラム

WebTrust Principles and Criteria for Certification Authority
WebTrust Principles and Criteria for Certification Authority – Extended Validation
WebTrust Principles and Criteria for Certification Authority – Extended Validation Code Signing
WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

何故重要か？

➡

WebTrust for CAの監査(或いはETSIの監査)が主要なブラウザのトラストリストへの登録要の一つになっている

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

WebTrust for CA

Audit Program for organized by AICPA CICA for CAs

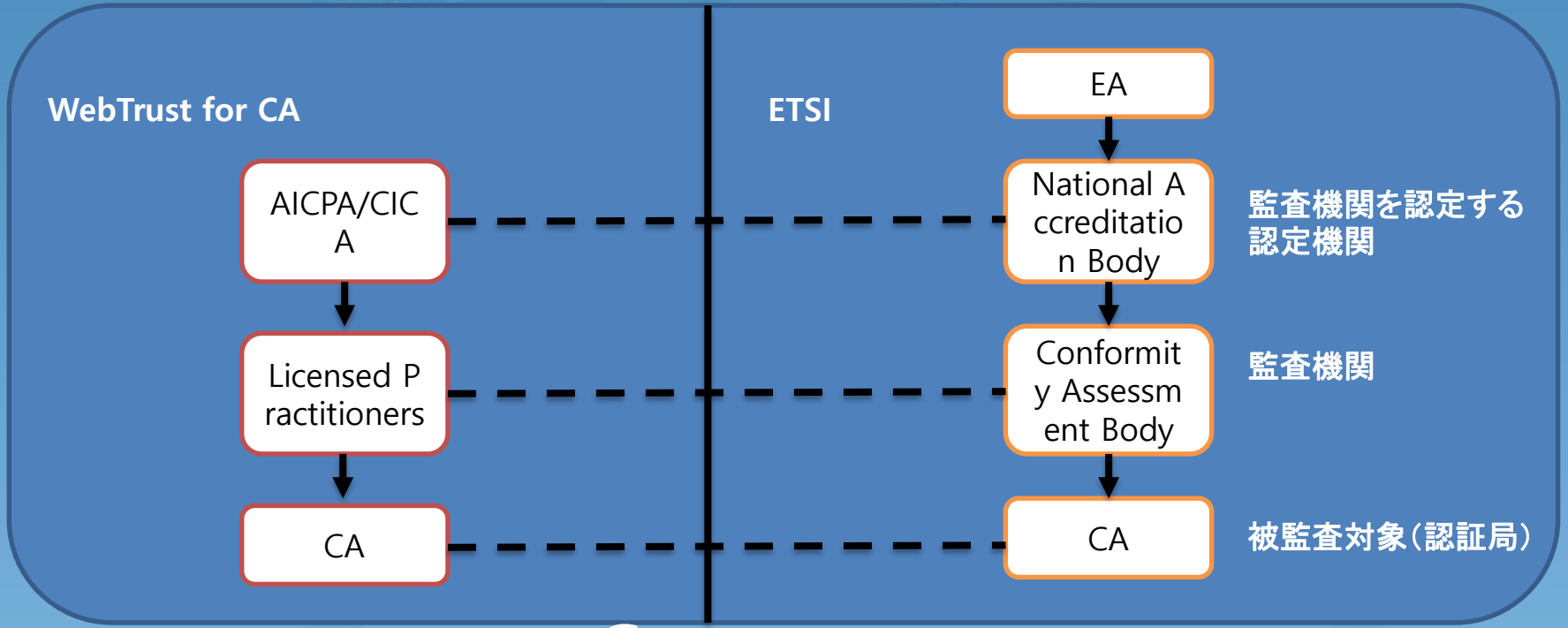
WebTrust Principles and Criteria for Certification Authority
WebTrust Principles and Criteria for Certification Authority – Extended Validation
WebTrust Principles and Criteria for Certification Authority – Extended Validation Code Signing
WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

Why WebTrust for CA so important?

➡

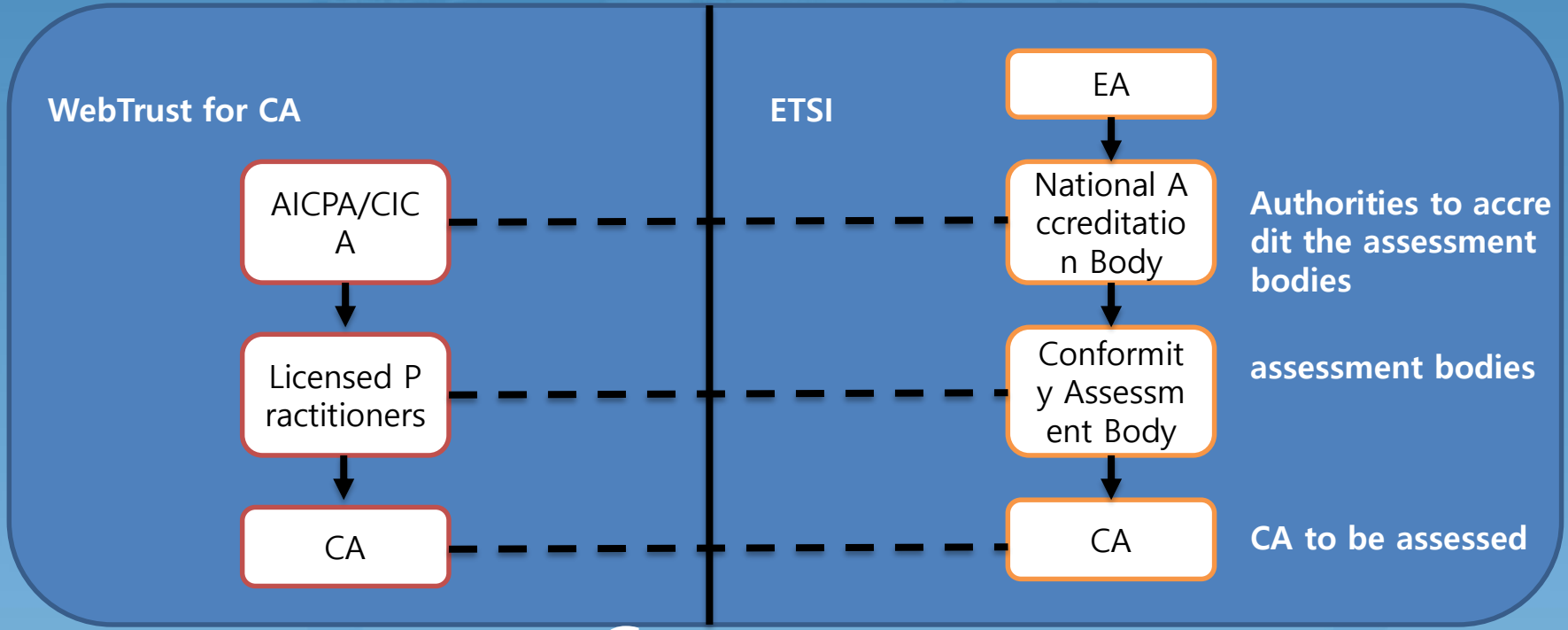
Because WebTrust for CA Audit is a part of trusted root CA program of major browser benders.

PTC監査制度比較



Cosmos
POFESSIONALS OF SAFETY ENGINEERING

PTC audit scheme



Cosmos
POFESSIONALS OF SAFETY ENGINEERING

IMRT-WG（International Mutual Recognition Technical WG）

慶應大学の呼びかけによりPKIをベースとしたトラストの相互承認を技術的観点から検討する為のWGを2018年10月に設立

議長：手塚 悟 特任教授（慶應大学）
メンバー：
US：
Judith Spencer(CertiPath), David Simonetti (SafeBioPharma), Matt King (SafeBioPharma), Patrick Patterson (A4A, Carillon),

EU：
Nick Pope (Thales), Arno Fiedler (Nimbus), Olivier Delos (Sealed), Daniel Kinlock (Entrust Datacard), Viky Manaila (Trans Sped srl),

JP：
Soshi Hamaguchi (Keio University), Kazuo Noguchi (Keio University), Atsushi Inaba (GMO Global Sign),

Others:
Kirk Hall (CA/B Forum, Entrust Datacard)

F2Fミーティング　2回（2018年10月＠ベルリン、2019年5月＠ワシントンD.C）
オンラインミーティング 5回

IMRT-WG（International Mutual Recognition Technical WG）

IMRT-WG will explore the technical foundations of international mutual recognition of trust services giving full support to the implementation of legal recognition agreements.

Chair：Prof. Tezuka Satoru（Keio Univ.）
Member：
US：
Judith Spencer(CertiPath), David Simonetti (SafeBioPharma), Matt King (SafeBioPharma), Patrick Patterson (A4A, Carillon),

EU：
Nick Pope (Thales), Arno Fiedler (Nimbus), Olivier Delos (Sealed), Daniel Kinlock (Entrust Datacard), Viky Manaila (Trans Sped srl),

JP：
Soshi Hamaguchi (Keio University), Kazuo Noguchi (Keio University), Atsushi Inaba (GMO Global Sign),

Others:
Kirk Hall (CA/B Forum, Entrust Datacard)

2 times F2F meetings（2018年10月@berlin、2019年5月@Washington D.C）
5 times online meetings

IMRT-WGの成果紹介

ETSIが定義する4項目		ETSI for PTC	WebTrust for PTC	ETSI for eIDAS	FPKI	Japanese electronic Signature Act
法的背景	法律	CA/Application agreement	CA/Application agreement	eIDAS Regulation	E-Government Act of 2002	電子署名及び認証業務に関する法律
	目的	Acceptance by application root store	Acceptance by application root store	Legal recognition of trust services,	Identity management and trust across organizational, operational, physical and network boundaries.	電子署名の円滑な利用を確保による電子商取引をはじめとするネットワークを利用した社会経済活動の推進
	アプリケーション	Web Servers	Web Servers	Signature, ERDS, Timestamp, e-Seal, Website (server) authentication	Authentication (Personal ID and Device ID) Signature Encryption (Content signing, FIPS201 e.g. PIV) (Card Authentication, FIPS201 e.g. PIV used for PACS) Web Servers (aligned with CAB Forum Requirements, separated root CA)	署名
	コミュニティ	Global Public	Global Public	EU public, business and government	US Public, Business and Government	JP Public, business and government
監督と監査	Governor	Application provider	Application provider	National supervisory body	CIO Council	経済産業省 総務省 法務省
	調和機関	CA/Browser forum	CA/Browser forum	EU Commission	N/A	N/A
	認定機関	National Accreditation Bodies (coordinated via EA)	AICPA/CIPA	National Accreditation Bodies (coordinated via EA)	None (Cross-Cert with FBCA requires Third Party Audit) Audit letter has to be sent FPKI PA.	経済産業省 総務省 法務省
	認証機関	Conformity Assessment Body (Accredited by NAB)	Licensed Practitioners	N/A	FPKI Policy Authority	Same as above
	適合性調査機関	Conformity Assessment Body (Accredited by NAB)	Same as above	Conformity Assessment Body	FPKI Certification Policy Working Grou	指定調査機関
技術要件	共通規格	RFC5280 X.509 RFC3647 FIPS140-2 CC EAL4	RFC5280 X.509 RFC3647	RFC5280 X.509 RFC3647 FIPS 140-2 CC EAL4	RFC5280 X.509 RFC3647 FIPS 140-2	
	技術規格	ETSI Standards	WebTrust Criteria	ETSI Standards	NIST SPs, FIPS 201, FPKIPA Documents	認定基準
	保証レベル	Technical Compliance	Technical Compliance	Legal admissibility + Technical Compliance	Technical Compliance, Interoperability with Federal PKI system	Legal admissibility + Technical Compliance
トラストの公開方法	トラストの公開方法	Browsers/OSs	Browsers/OSs	Trusted List	Federal Bridge CA	官報及びウェブサイト

Output of IMRT-WG

ETSI "Pillar"		ETSI for PTC	WebTrust for PTC	ETSI for eIDAS	FPKI	Japanese electronic Signature Act
Legal context	Law	CA/Application agreement	CA/Application agreement	eIDAS Regulation	E-Government Act of 2002	Act on Electronic Signatures and Certification Business
	Objective	Acceptance by application root store	Acceptance by application root store	Legal recognition of trust services,	Identity management and trust across organizational, operational, physical and network boundaries.	To promote the distribution of e-document through ensuring the smooth use of e-Signatures.
	Application	Web Servers	Web Servers	Signature, ERDS, Timestamp, e-Seal, Website (server) authentication	Authentication (Personal ID and Device ID) Signature Encryption (Content signing, FIPS201 e.g. PIV) (Card Authentication, FIPS201 e.g. PIV used for PACS) Web Servers (aligned with CAB Forum Requirements, separated root CA)	Signature
	Community	Global Public	Global Public	EU public, business and government	US Public, Business and Government	JP Public, business and government
supervision & auditing	Governor	Application provider	Application Provider	National supervisory body	CIO Council	Ministry of Economy, Trade and Industry. Ministry of Internal Affairs and Communications. Ministry of Justice.
	Harmonization Body	CA/Browser forum	CA/Browser forum	EU Commission	N/A	N/A
	Accreditaiton Body	National Accreditation Bodies (coordinated via EA)	AICPA/CIPA	National Accreditation Bodies (coordinated via EA)	None (Cross-Cert with FBCA requires Third Party Audit) Audit letter has to be sent FPKI PA.	Ministry of Economy, Trade and Industry. Ministry of Internal Affairs and Communications. Ministry of Justice.
	Certification Body	Conformity Assessment Body (Accredited by NAB)	Licensed Practitioners	N/A	FPKI Policy Authority	Same as above
	Conformity Assessment Body	Conformity Assessment Body (Accredited by NAB)	Same as above	Conformity Assessment Body	FPKI Certification Policy Working Grou	Designated Investigation Organization
Technical requirements	Harmonized standards	RFC5280 X.509 RFC3647 FIPS140-2 CC EAL4	RFC5280 X.509 RFC3647	RFC5280 X.509 RFC3647 FIPS 140-2 CC EAL4	RFC5280 X.509 RFC3647 FIPS 140-2	
	Supporting Technical Documents	ETSI Standards	WebTrust Criteria	ETSI Standards	NIST SPs, FIPS 201, FPKIPA Documents	Accreditation Criteria
	Assurance to be achieved	Technical Compliance	Technical Compliance	Legal admissibility + Technical Compliance	Technical Compliance, Interoperability with Federal PKI system	Legal admissibility + Technical Compliance
Trust representation	Trust representation	Browsers/OSs	Browsers/OSs	Trusted List	Federal Bridge CA	Official Journal and Websites

ご清聴ありがとうございました

株式会社コスモス・コーポレイション

ITセキュリティ部

濱口　総志
Tel:　0598-30-5911
E-Mail:　s.hamaguchi@cosmos-corp.com
URL:　www.safetyweb.co.jp/

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

Thank you for your attention

Cosmos Corporation co., ltd.

ITセキュリティ部

濱口　総志
Tel:　0598-30-5911
E-Mail:　s.hamaguchi@cosmos-corp.com
URL:　www.safetyweb.co.jp/

Cosmos
POFESSIONALS OF SAFETY ENGINEERING