

สัมมนาเผยแพร่ความรู้และผลการศึกษา
ลายมือชื่อดิจิทัล ครั้งที่ 2

ผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับ
ลายมือชื่อดิจิทัล

วันศุกร์ที่ 19 กรกฎาคม 2567 | เวลา 10.00 – 12.00 น.

ผ่านโปรแกรม Microsoft teams

หัวข้อการสัมมนา

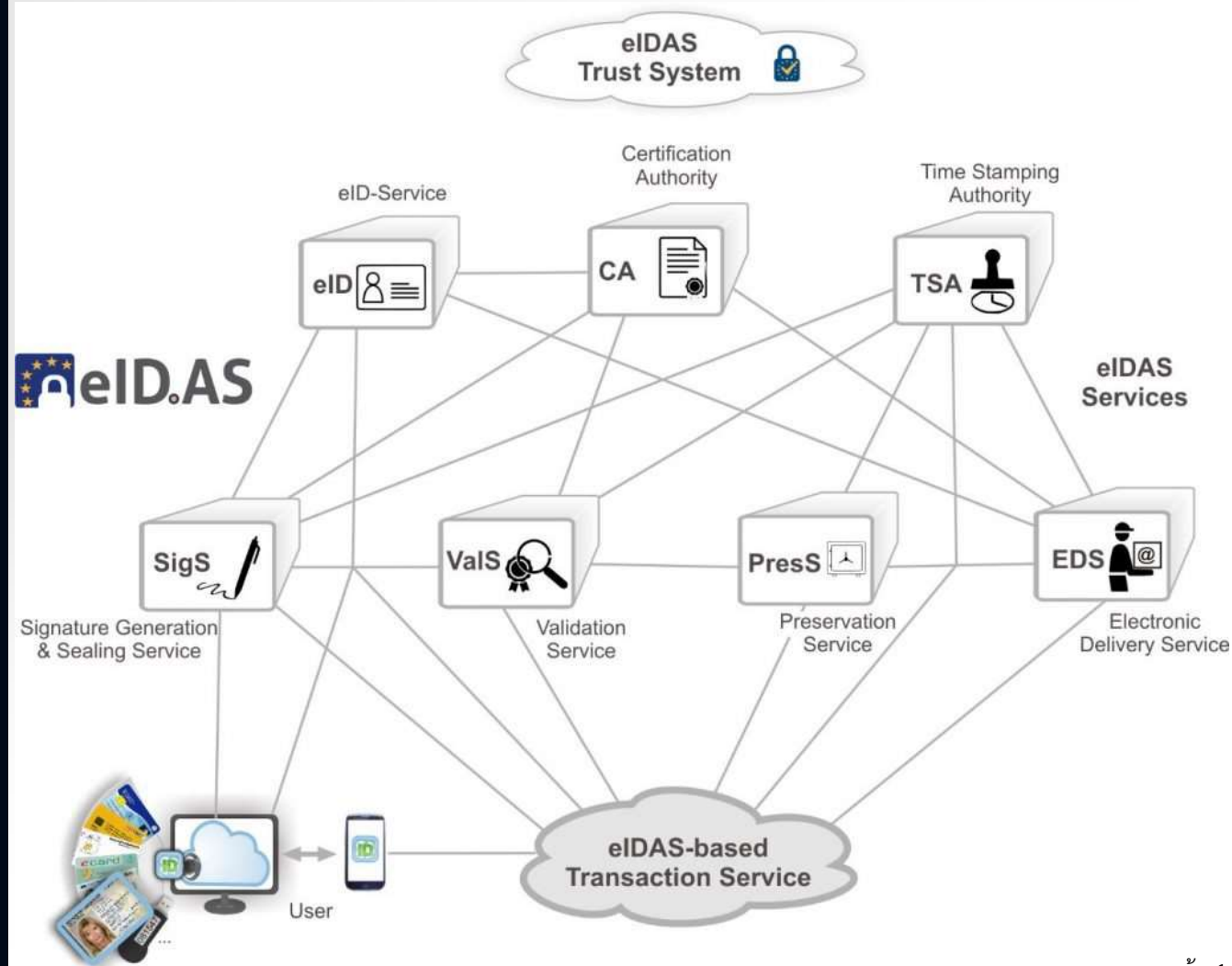
- ภาพรวมของผู้ให้บริการที่เชื่อถือได้
- นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การเปรียบเทียบนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

หัวข้อการสัมมนา

- ภาพรวมของผู้ให้บริการที่เชื่อถือได้
- นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การเปรียบเทียบนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

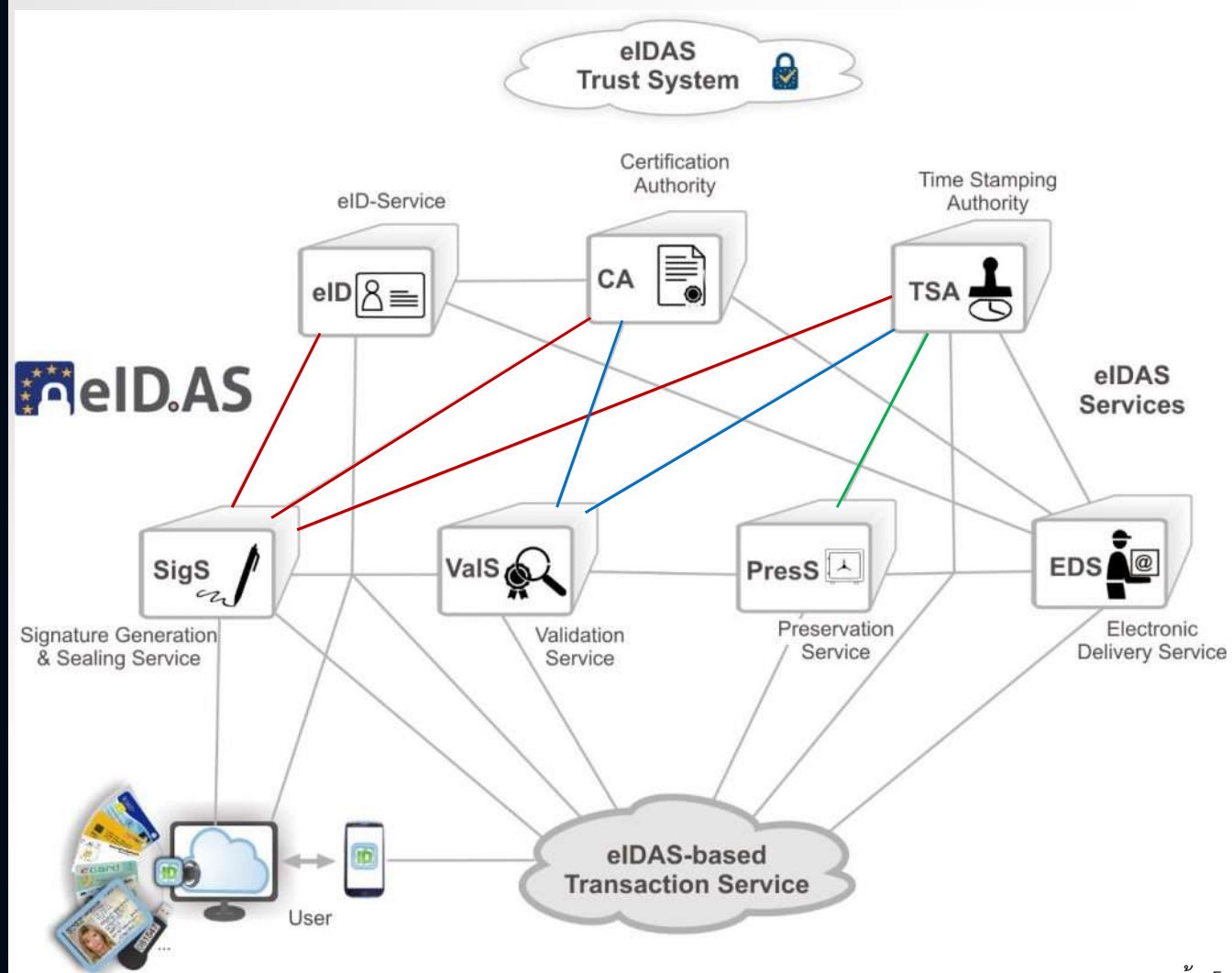
eIDAS Trust System

บริการที่เชื่อถือได้ (trust services)
ภายใต้กฎหมายเอดาของสหภาพยุโรป



eIDAS Trust System

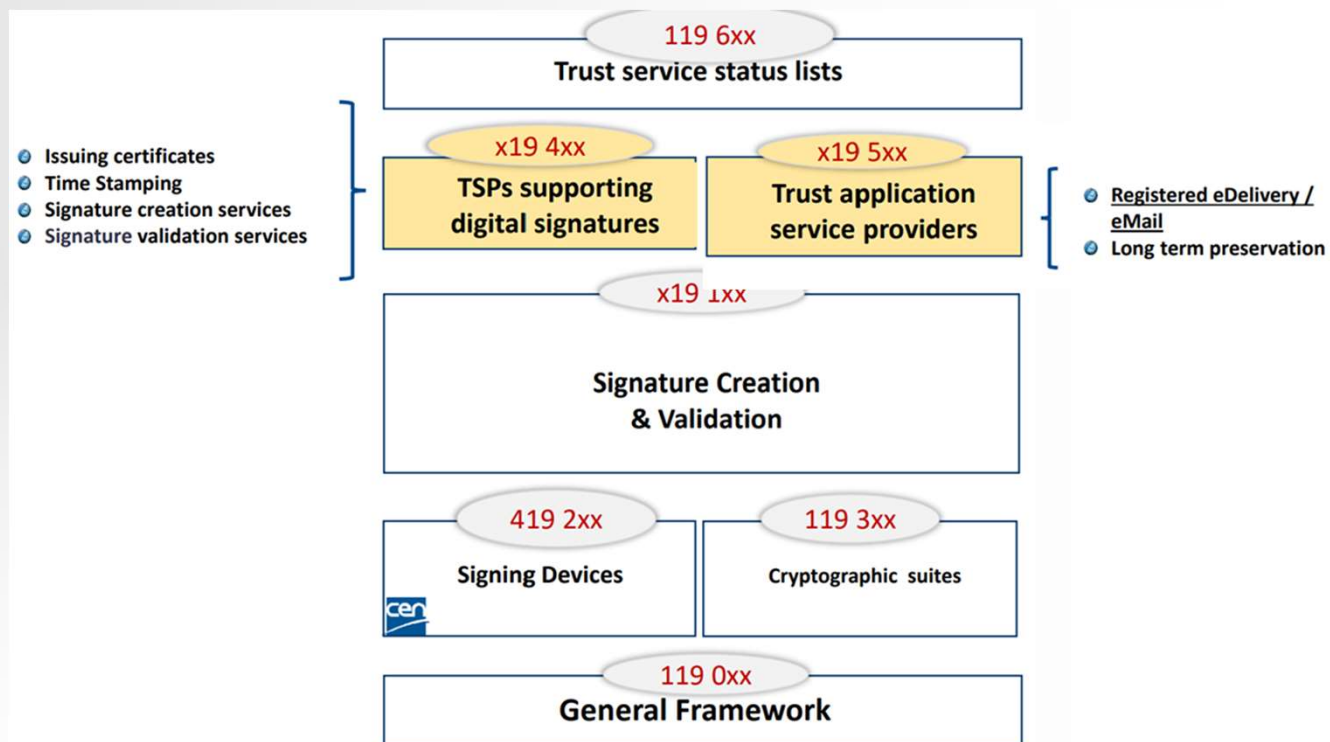
บริการที่เชื่อถือได้ (trust services)
ภายใต้กฎหมายเอดาของสหภาพยุโรป



ETSI TR 119 000

The framework for standardization of digital signatures and trust services

มาตรฐานที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
และบริการที่เชื่อถือได้



eIDAS Dashboard

บริการที่เชื่อถือได้ (trust services)

What type of service are you looking for? step 1/2

Check all

Qualified trust services

- | | | |
|--|--|---|
| <input type="checkbox"/> Qualified certificate for electronic signature | <input type="checkbox"/> Qualified certificate for electronic seal | <input type="checkbox"/> Qualified certificate for website authentication |
| <input type="checkbox"/> Qualified validation service for qualified electronic signature | <input type="checkbox"/> Qualified preservation service for qualified electronic signature | <input type="checkbox"/> Qualified validation service for qualified electronic seal |
| <input type="checkbox"/> Qualified preservation service for qualified electronic seal | <input type="checkbox"/> Qualified time stamp | <input type="checkbox"/> Qualified electronic registered delivery service |

Non-qualified trust services

- | | | |
|--|--|---|
| <input type="checkbox"/> Certificate for electronic signature | <input type="checkbox"/> Certificate for electronic seal | <input type="checkbox"/> Certificate for website authentication |
| <input type="checkbox"/> Validation service for electronic signature | <input type="checkbox"/> Generation service for electronic signature | <input type="checkbox"/> Preservation service for electronic signature |
| <input type="checkbox"/> Validation service for electronic seal | <input type="checkbox"/> Generation service for electronic seal | <input type="checkbox"/> Preservation service for electronic seal |
| <input type="checkbox"/> Time stamp service | <input type="checkbox"/> Electronic registered delivery service | <input type="checkbox"/> Non-regulatory, nationally defined trust service |
| <input type="checkbox"/> Undefined type | | |

eIDAS Dashboard

ผู้ให้บริการที่เชื่อถือได้ (trust service providers)

Business, Economy, Euro

Home / Trust Services / Browse the eIDAS Lists / EU/EEA Trusted Lists / Search by type of service

Trust service providers results(12)

Share New Search

Currently active trust service providers

	A-Trust GmbH	QCert for ESig	QCert for ESeal	QWAC	QTimestamp	Cert for ESig	Cert for ESeal	WAC	
	PrimeSign GmbH	QCert for ESig	QCert for ESeal						
	Rundfunk und Telekom Regulierungs-GmbH		Cert for ESeal						
	SwissSign GmbH	QCert for ESig							
	Swisscom IT Services Finance S.E.	QCert for ESig	QCert for ESeal	QTimestamp	Cert for ESig	Cert for ESeal			
	e-commerce monitoring GmbH	QCert for ESig	QCert for ESeal	QWAC	QTimestamp	Cert for ESig	Cert for ESeal	WAC	Timestamp
	Adobe Systems Software Ireland Ltd.			QTimestamp					
	Entaksi Solutions SpA Irish Branch	QCert for ESig	QCert for ESeal	QPres for QESig	QPres for QESeal	QTimestamp			
	TrustPro QTSP Ltd	QCert for ESig	QCert for ESeal	QTimestamp					

ETSI TR 119 400

Guidance on the use of standards for trust service providers supporting digital signatures and related services

มาตรฐานสำหรับผู้ให้บริการที่เชื่อถือได้ (TSP)
ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

ผู้ให้บริการที่เชื่อถือได้ (trust service provider) ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. TSP issuing certificates
2. TSP issuing time-stamps
3. TSP providing signature generation services
4. TSP providing signature validation services

โดยมาตรฐานนี้จะได้กล่าวถึง ผู้ให้บริการแอปพลิเคชันที่เชื่อถือได้ (trust application service provider) ซึ่งจะอยู่ในเล่มมาตรฐาน ETSI TR 119 500 Business Driven Guidance for Trust Application Service Provider ได้แก่

- Electronic Registered Delivery Service (ERDS)
- Registered Electronic Mail (REM)
- Data Preservation Service (DPS)

หัวข้อการสัมมนา

- ภาพรวมของผู้ให้บริการที่เชื่อถือได้
- นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การเปรียบเทียบนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers โดยแบ่งข้อกำหนดได้ 4 กลุ่ม ดังนี้
 - 1.1 การประเมินความเสี่ยง (risk assessment)
 - 1.2 การจัดทำนโยบายและข้อปฏิบัติ (policy and practice)
 - 1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation)
 - 1.4 มาตรการปฏิบัติตามข้อกำหนดทางกฎหมาย (compliance)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers โดยแบ่งข้อกำหนดได้ 4 กลุ่ม ดังนี้
 - 1.1 การประเมินความเสี่ยง (risk assessment)
 - 1.2 การจัดทำนโยบายและข้อปฏิบัติ (policy and practice)
 - 1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation)
 - 1.4 มาตรการปฏิบัติตามข้อกำหนดทางกฎหมาย (compliance)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers

1.1 การประเมินความเสี่ยง (risk assessment)

REQ-5 การประเมินความเสี่ยง (risk assessment) ของสินทรัพย์สำคัญของบริการสรุปข้อกำหนดสำคัญ REQ-5-01 – REQ.5-05 ประกอบด้วย ผู้ให้บริการที่เชื่อถือได้ต้องดำเนินการประเมินความเสี่ยงเพื่อระบุ วิเคราะห์ และประเมินความเสี่ยงต่อบริการด้วยกระบวนการประเมินความเสี่ยงที่สามารถจัดระดับความรุนแรงของความเสียหายได้ มีการกำหนดมาตรการด้านความมั่นคงปลอดภัยเพื่อแก้ไขความเสี่ยงตามที่ระบุไว้ในเอกสารนโยบายความมั่นคงปลอดภัยขององค์กร มีการทบทวนการประเมินความเสี่ยงเป็นประจำ และการประเมินความเสี่ยงและการยอมรับความเสี่ยงต้องผ่านการอนุมัติของฝ่ายบริหารของผู้ให้บริการที่เชื่อถือได้

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers โดยแบ่งข้อกำหนดได้ 4 กลุ่ม ดังนี้
 - 1.1 การประเมินความเสี่ยง (risk assessment)
 - 1.2 การจัดทำนโยบายและข้อปฏิบัติ (policy and practice)
 - 1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation)
 - 1.4 มาตรการปฏิบัติตามข้อกำหนดทางกฎหมาย (compliance)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers

1.2 การจัดทำนโยบายและข้อปฏิบัติ (policy and practice)

- REQ-6.01-01 ถึง REQ-6.01-11
รายละเอียด เงื่อนไข ความรับผิดชอบของผู้ให้บริการที่เชื่อถือได้
- REQ-6.2-01 ถึง REQ-6.2-06
ข้อจำกัดในการใช้บริการ ข้อมูลติดต่อกับผู้ให้บริการที่เชื่อถือได้
- REQ-6.3-03 ถึง REQ-6.3-10
นโยบายความมั่นคงปลอดภัยทางสารสนเทศ (information security policy)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers โดยแบ่งข้อกำหนดได้ 4 กลุ่ม ดังนี้
 - 1.1 การประเมินความเสี่ยง (risk assessment)
 - 1.2 การจัดทำนโยบายและข้อปฏิบัติ (policy and practice)
 - 1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation)
 - 1.4 มาตรการปฏิบัติตามข้อกำหนดทางกฎหมาย (compliance)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers

1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation)

- REQ-7.1.1-01 ถึง REQ-7.1.1-10 การบริหารจัดการภายในองค์กร (internal organization)
- REQ-7.1.2-01 การแบ่งแยกหน้าที่ (segregation of duties)
- REQ-7.2-01 ถึง REQ-7.2-17 การบริหารจัดการทรัพยากรบุคคล (human resources)
- REQ-7.3.1-01 ถึง REQ-7.3.1-02 การจัดการสินทรัพย์ (asset management)
- REQ-7.3.2-01 ถึง REQ-7.3.2-03 การจัดการสื่อบันทึกข้อมูล (media handling)
- REQ-7.4-01 ถึง REQ-7.4-10 การควบคุมการเข้าถึง (access control)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers

1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation) (ต่อ...)

- REQ-7.5-01 การใช้งานการเข้ารหัสลับ (cryptographic controls)
- REQ-7.6-01 ถึง REQ-7.6.-05 การรักษาความมั่นคงปลอดภัยทางกายภาพ (physical and environmental security)
- REQ-7.7-01 ถึง REQ-7.7-09 การปฏิบัติงานด้านความมั่นคงปลอดภัย (operation security)
- REQ-7.8-01 ถึง REQ-7.8-0 การรักษาความมั่นคงปลอดภัยของระบบเครือข่าย (network security)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers

1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation) (ต่อ...)

- REQ-7.9-01 ถึง REQ-7.9-12 การบริการจัดการสถานการณ์ความไม่มั่นคงปลอดภัย (incident management)
- REQ-7.10-01 ถึง REQ-7.10-08 การเก็บรวบรวมพยานหลักฐาน (collection of evidence)
- REQ-7.11-01 ถึง REQ-7.11-02 การบริหารจัดการความต่อเนื่องของบริการ (business continuity management)
- REQ-7.12-01 ถึง REQ-7.12-11 การเลิกกิจการและแผนการยกเลิกบริการ (TSP termination and termination plans)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers โดยแบ่งข้อกำหนดได้ 4 กลุ่ม ดังนี้
 - 1.1 การประเมินความเสี่ยง (risk assessment)
 - 1.2 การจัดทำนโยบายและข้อปฏิบัติ (policy and practice)
 - 1.3 การบริหารจัดการและดำเนินการของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation)
 - 1.4 มาตรการปฏิบัติตามข้อกำหนดทางกฎหมาย (compliance)

ETSI EN 319 401

General Policy Requirements for Trust Service Providers

ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
(policy & security requirements)

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

1. ข้อกำหนดทั่วไป ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย (policy & security requirements) ตามมาตรฐาน ETSI EN 319 401 General Policy Requirements for Trust Service Providers

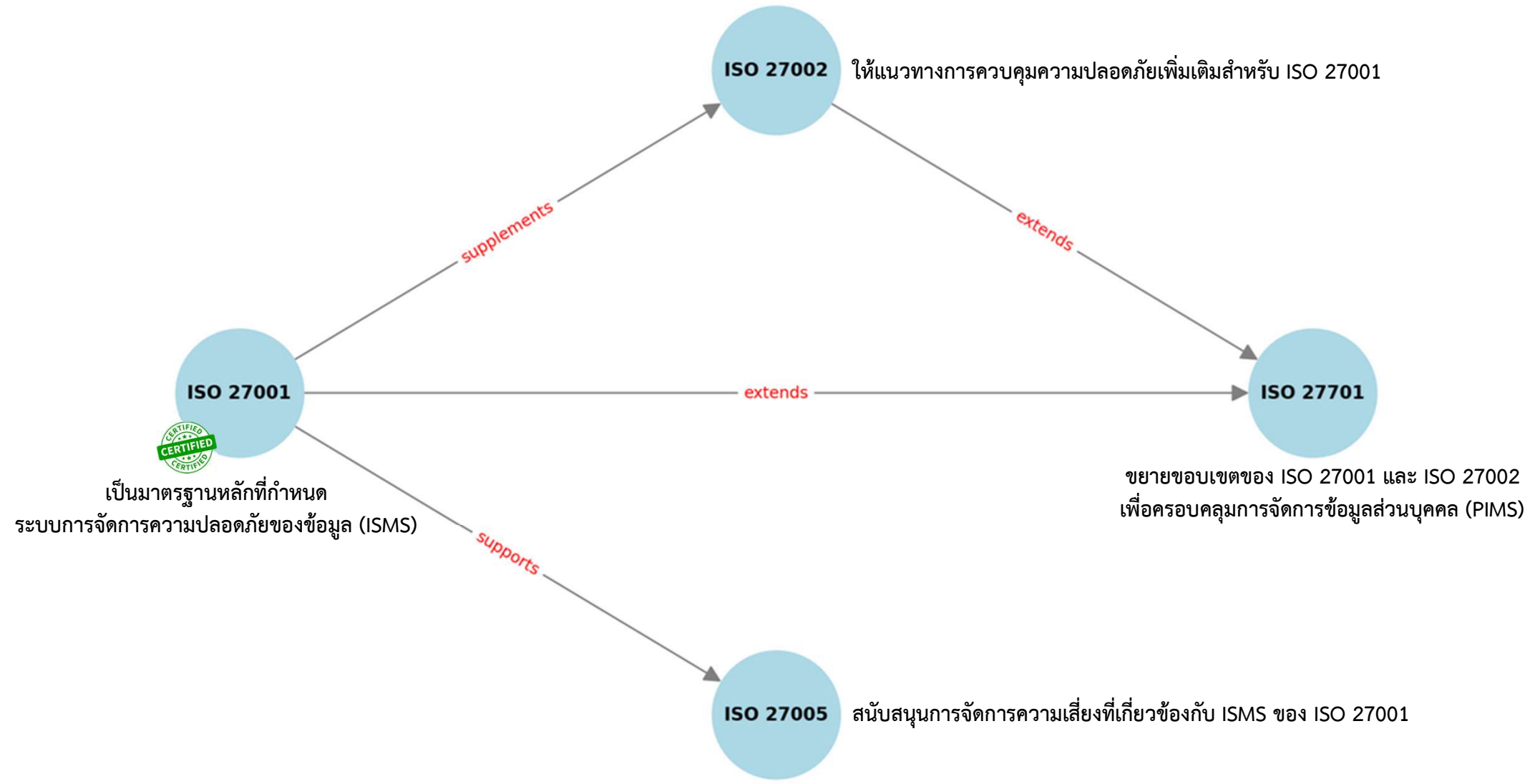
1.4 มาตรการปฏิบัติตามข้อกำหนดทางกฎหมาย (compliance)

REQ-7.13-01 ถึง REQ-7.13-05 (compliance) ผู้ให้บริการที่เชื่อถือได้ ต้องแน่ใจว่าการปฏิบัติงานเป็นไปตามกรอบของกฎหมายและมีความน่าเชื่อถือ ต้องสามารถนำเสนอพยานหลักฐานที่สนับสนุนถึงการปฏิบัติงานได้ตามกรอบของกฎหมายที่เกี่ยวข้อง และต้องปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายเป็นต้น

เปรียบเทียบ ข้อกำหนดทั่วไป ของ **ETSI EN 319 401** กับ **ISO/IEC 27002:2013**
 สำหรับผู้ให้บริการที่เชื่อถือได้ (TSP) ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล



ETSI EN 319401 V 2.3.1 (2021-05)	ISO 27002 :2013 (<i>Code of practice for information security controls</i>)
REQ-5 การประเมินความเสี่ยง (Risk Assessment)	Risk management (ISO 27005)
REQ-6 นโยบายและข้อปฏิบัติ (Policies and practices): REQ-6.1 Trust Service Practice Statement, REQ-6.2 Terms and conditions, REQ-6.3 Information security policy	Clause 5 Information security policies
REQ-7 การบริหารจัดการและการดำเนินงานของผู้ให้บริการที่เชื่อถือได้ (TSP management and operation): REQ-7.1 Internal organization	Clause 6 Organization of information security
REQ-7.2 Human resources	Clause 7 Human resource security
REQ-7.3 Asset management	Clause 8 Asset management
REQ-7.4 Access control	Clause 9 Access control
REQ-7.5 Cryptographic controls	Clause 10 Cryptography
REQ-7.6 Physical and environmental security	Clause 11 Physical and environmental security
REQ 7.7 Operation security	Clause 12 Operations security
REQ 7.8 Network security	Clause 13 Communication security
REQ 7.9 Incident management, Req 7.10 Collection of Evidence	Clause 16 Information security incident management
REQ 7.11 Business continuity management	Clause 17 Information security aspect of business continuity mgt.
REQ 7.12 TSP termination and termination plans	
REQ 7.13 Compliance	Clause 18 Compliance



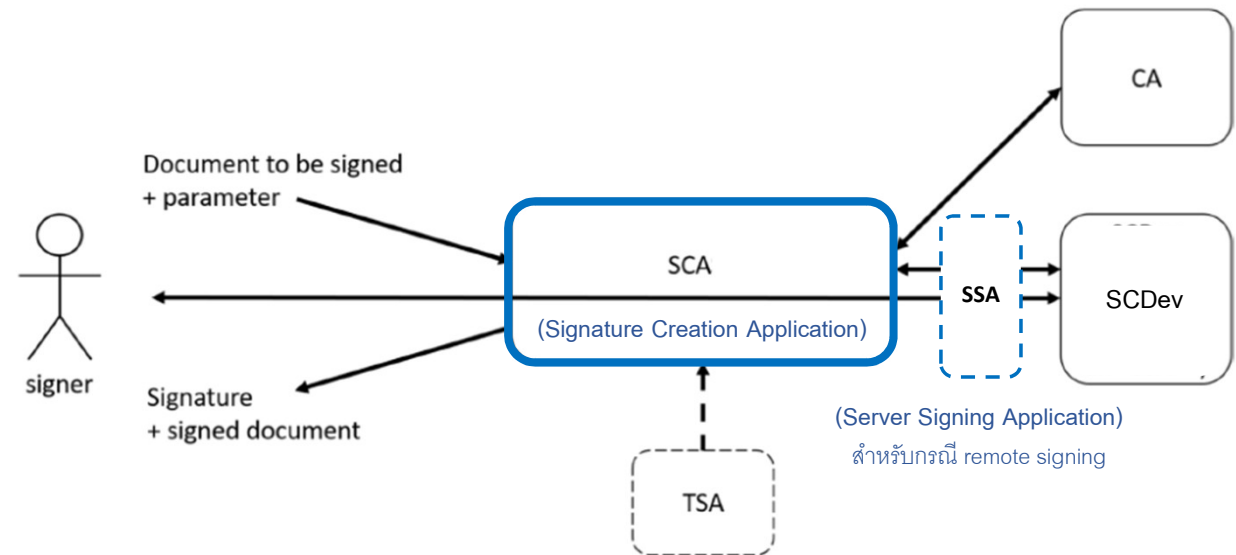
ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

- ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ



ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. **ข้อกำหนดเฉพาะ** ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ

- 2.1 มาตรฐาน ETSI TS 119 431-1 Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev ([SSA: Server Signing Application](#))
- 2.2 มาตรฐาน ETSI TS 119 431-2 Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation ([SCA: Signature Creation Application](#))

ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ

- 2.1 มาตรฐาน ETSI TS 119 431-1 Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev ([SSA: Server Signing Application](#))
- 2.2 มาตรฐาน ETSI TS 119 431-2 Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (SCA: Signature Creation Application)

ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ

2.1 มาตรฐาน ETSI TS 119 431-1 Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev (SSA)

ข้อกำหนดเฉพาะภายใต้มาตรฐานนี้ ประกอบด้วย

- การสร้างกุญแจสำหรับสร้างลายมือชื่อ (signing key generation) มีรหัสด้วยอักษรย่อหน้าหน้าเป็น GEN-6.2 และการสำรองและกู้คืนกุญแจสำหรับสร้างลายมือชื่อ มีรหัสด้วยอักษรย่อหน้าหน้าเป็น GEN-6.3.3

ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่
เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย สำหรับผู้ให้บริการสร้างลายมือชื่อ

2.1 มาตรฐาน ETSI TS 119 431-1 Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev (SSA)

ข้อกำหนดเฉพาะภายใต้มาตรฐานนี้ ประกอบด้วย (ต่อ...)

- การเชื่อมโยงใบรับรองและอีไอดี (Certificate/eID means linking) มีรหัสด้วย
อักษรย่อหน้าหน้าเป็น LNK-6.2
- การสั่งสร้างลายมือชื่อ (signature activation) มีรหัสด้วยอักษรย่อหน้าหน้า
เป็น SIG-6.3.1

ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ

2.1 มาตรฐาน ETSI TS 119 431-1 Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev (SSA)

ข้อกำหนดเฉพาะภายใต้มาตรฐานนี้ ประกอบด้วย (ต่อ...)

- การลบกุญแจสำหรับสร้างลายมือชื่อ (signing key deletion) มีรหัสด้วยอักษรย่อหน้าหน้าเป็น DEL-6.3.2
- บริการอีไอดี (eID means provision) มีรหัสด้วยอักษรย่อหน้าหน้าเป็น EID-6.2.4 ที่เกี่ยวข้องกับการยืนยันตัวตนของเจ้าของลายมือชื่อที่เชื่อถือได้

ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ

- 2.1 มาตรฐาน ETSI TS 119 431-1 Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev (SSA: Server Signing Application)
- 2.2 มาตรฐาน ETSI TS 119 431-2 Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation ([SCA: Signature Creation Application](#))

ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. **ข้อกำหนดเฉพาะ** ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ

2.2 มาตรฐาน ETSI TS 119 431-2 Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (SCA)

ข้อกำหนดเฉพาะภายใต้มาตรฐานนี้ ประกอบด้วย

- ASI-8.1 กำหนดให้ผู้ให้บริการที่เชื่อถือได้ต้องปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับส่วนติดต่อ (interface)

ผู้ให้บริการสร้างลายมือชื่อ

TSP providing signature generation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการสร้างลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

2. ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการสร้างลายมือชื่อ

2.2 มาตรฐาน ETSI TS 119 431-2 Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (SCA)

ข้อกำหนดเฉพาะภายใต้มาตรฐานนี้ ประกอบด้วย (ต่อ...)

- ASI-8.2 กำหนดให้ผู้ให้บริการที่เชื่อถือได้ต้องปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับการสร้างลายมือชื่อดิจิทัลในการเลือกใช้กระบวนการเข้ารหัสลับ การแจ้งหรือเปิดให้เข้าถึงข้อมูลสำคัญต่าง ๆ

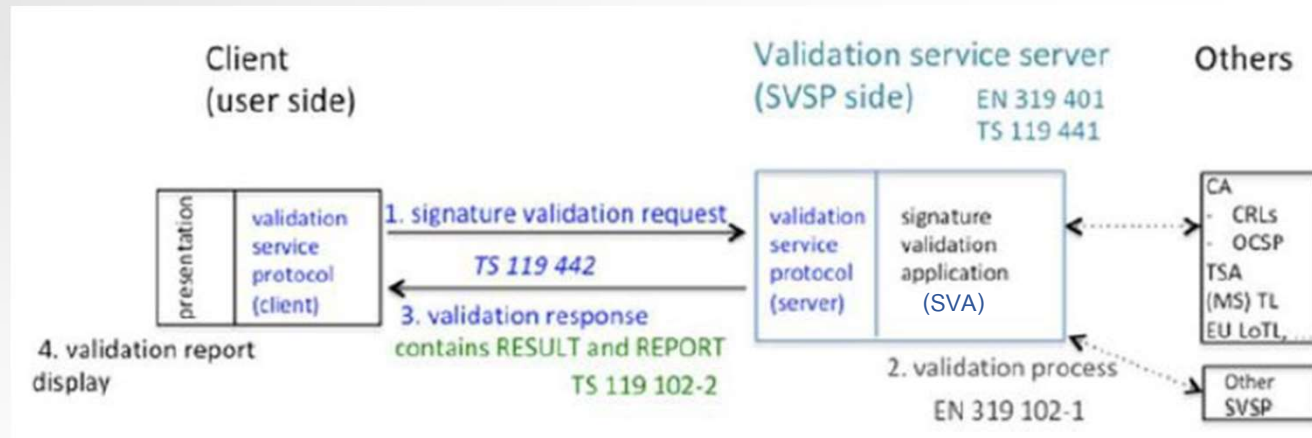
ผู้ให้บริการตรวจสอบ ความถูกต้องลายมือชื่อ

TSP providing signature validation services

ข้อกำหนดเฉพาะ ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการตรวจสอบความถูกต้องลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่
เกี่ยวข้องกับลายมือชื่อดิจิทัล

- ข้อกำหนดเฉพาะ ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการตรวจสอบความถูกต้องลายมือชื่อ ETSI TS 119 441 Policy and
security requirements for TSP providing validation services (SVA: Signature
Validation Application)



ผู้ให้บริการตรวจสอบ ความถูกต้องลายมือชื่อ

TSP providing signature validation services

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการตรวจสอบความถูกต้องลายมือชื่อ

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

3. **ข้อกำหนดเฉพาะ** ของประเภทนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการตรวจสอบความถูกต้องลายมือชื่อ ETSI TS 119 441 Policy and security requirements for TSP providing validation services (SVA)
 - SVP-8.2 กำหนดโพรโทคอลการตรวจสอบความถูกต้องของลายมือชื่อ (signature validation protocol)
 - SVP-8.3 เป็นข้อกำหนดด้านความมั่นคงปลอดภัยของช่องทางสื่อสารระหว่างผู้ใช้งานกับผู้ให้บริการตรวจสอบความถูกต้องของลายมือชื่อ
 - VPR-8.1 กำหนดกระบวนการตรวจสอบความถูกต้องของลายมือชื่อ (signature validation process)
 - SVR-8.2 กำหนดข้อกำหนดสำหรับรายงานผลการตรวจสอบความถูกต้องของลายมือชื่อ (signature validation report)

ผู้ให้บริการออกใบรับรอง

TSP issuing certificates

ข้อกำหนดเฉพาะ ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการออกใบรับรอง

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

4. **ข้อกำหนดเฉพาะ** ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการออกใบรับรอง ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1 (CSP: Certification Service Provider)

- ข้อกำหนดเฉพาะบริการลงทะเบียน (registration service) มีรหัสด้วยอักษรย่อหน้า เป็น REG-6.2 ข้อกำหนดเกี่ยวกับการพิสูจน์และยืนยันตัวตน รวมถึงการตรวจสอบข้อมูลที่ระบุถึงเจ้าของใบรับรอง เพื่อใช้เป็นข้อมูลในบริการสร้างใบรับรอง บริการนี้จะรวมถึงการตรวจสอบการครอบครอง หรือควบคุมกุญแจส่วนตัวของเจ้าของลายมือชื่อที่ไม่ได้ถูกสร้างจากผู้ออกใบรับรอง

ผู้ให้บริการออกใบรับรอง

TSP issuing certificates

ข้อกำหนดเฉพาะ ของประเภตมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการออกใบรับรอง

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

4. **ข้อกำหนดเฉพาะ** ของประเภตมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการออกใบรับรอง ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1 (CSP: Certification Service Provider) (ต่อ...)

- ข้อกำหนดเฉพาะบริการสร้างใบรับรอง (certification generation service) มีรหัสด้วยอักษรย่อหน้าเป็น GEN-6.3.2 กระบวนการขอใบรับรอง (certificate application process) และ GEN-6.3.3 การออกใบรับรอง (certificate issuance) และมีเนื้อหาครอบคลุมถึงการสร้างและลงลายมือชื่อในใบรับรองด้วยไอดีนิติและข้อมูลที่ระบุถึงเจ้าของใบรับรองที่ผ่านการตรวจสอบจากบริการลงทะเบียน (registration service) บริการนี้สามารถรวมกระบวนการสร้างคู่กุญแจด้วยก็ได้

ผู้ให้บริการออกใบรับรอง

TSP issuing certificates

ข้อกำหนดเฉพาะ ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการออกใบรับรอง

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

4. **ข้อกำหนดเฉพาะ** ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการออกใบรับรอง ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1 (CSP: Certification Service Provider) (ต่อ...)

- ข้อกำหนดเฉพาะบริการส่งหรือเผยแพร่ข้อมูลใบรับรอง (dissemination service) มีรหัสด้วยอักษรย่อหน้าเป็น DIS-6.1 การเผยแพร่ข้อมูลใบรับรอง (publication and repository responsibilities) DIS-6.5 การเผยแพร่ข้อมูลและสถานะของใบรับรองหรือกุญแจสาธารณะของผู้ออกใบรับรอง

ผู้ให้บริการออกใบรับรอง

TSP issuing certificates

ข้อกำหนดเฉพาะ ของประเภมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการออกใบรับรอง

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

4. ข้อกำหนดเฉพาะ ของประเภมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการออกใบรับรอง ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1 (CSP: Certification Service Provider) (ต่อ...)

- ข้อกำหนดเฉพาะบริการรับคำขอและดำเนินการเพิกถอนใบรับรอง (revocation management service) มีรหัสด้วยอักษรย่อหน้าเป็น REV-6.2.4 กระบวนการยืนยันตัวตนในการร้องขอเพิกถอนใบรับรอง REV-6.3.9 การเพิกถอนหรือระงับการใช้งานใบรับรอง (certificate revocation and suspension) และ REV-6.4.5 การบันทึกข้อมูลคำขอเพิกถอนและการดำเนินการต่าง ๆ ที่เกี่ยวข้อง

ผู้ให้บริการออกใบรับรอง

TSP issuing certificates

ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบาย
และข้อกำหนดด้านความมั่นคงปลอดภัย
สำหรับผู้ให้บริการออกใบรับรอง

นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

4. ข้อกำหนดเฉพาะ ของประเภทมาตรฐานนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการออกใบรับรอง ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1 (CSP: Certification Service Provider) (ต่อ...)

- ข้อกำหนดเฉพาะบริการแสดงสถานะการเพิกถอนใบรับรอง (revocation status service) มีรหัสด้วยอักษรย่อหน้าเป็น CSS-6.3.10 การให้บริการข้อมูลสถานะการเพิกถอนของใบรับรองกับคู่กรณีต่าง ๆ (certificate status service)
- ข้อกำหนดเฉพาะบริการจัดเตรียมอุปกรณ์สำหรับเจ้าของลายมือชื่อ (subject device provision service) มีรหัสด้วยอักษรย่อหน้าเป็น SDP-6.3.3 และ SDP-6.3.12 การกู้คืนกุญแจ SDP-6.4.5 การจัดเก็บข้อมูลบันทึกที่เกี่ยวข้องกับการจัดเตรียมอุปกรณ์สำหรับเจ้าของลายมือชื่อ SDP-6.5.1 และ SDP-6.5.4 การสร้างคู่กุญแจและให้บริการอุปกรณ์เข้ารหัสลับที่มีความมั่นคงปลอดภัยหรืออุปกรณ์อื่นกับเจ้าของใบรับรอง

หัวข้อการสัมมนา

- ภาพรวมของผู้ให้บริการที่เชื่อถือได้
- นโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล
- การเปรียบเทียบนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการที่เชื่อถือได้ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

ตารางเปรียบเทียบ ข้อกำหนดทั่วไป
สำหรับผู้ให้บริการที่เชื่อถือได้ (TSP) ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

General TSP 319401	CSP/CA 319411	SCASP 119431-2	SSASP 119431-1	SVSP 119441
REQ-5 Risk Assessment	OVR-6.4.1-01	OVR-5-01	OVR-6.4.1-01	OVR-5-01
REQ-6 Policies and practices: REQ-6.1 TS Practice Statement, REQ-6.2 Terms and conditions, REQ-6.3 Information security policy	OVR-5.2-01 OVR-6.8.13-01 OVR-6.4.1-01	OVR-6.1-01 OVR-6.2-01 OVR-6.3-01	OVR-5.1-01 OVR-6.8.4-01 OVR-6.7.6-01	OVR-6.1-01 OVR-6.2-01 OVR-6.3-01
REQ-7 TSP management and operation REQ-7.1 Internal org.	OVR-6.8.2-01, OVR-6.9.1-01	OVR-7.1-01	OVR-6.8.1-01	OVR-7.1-01
REQ-7.2 Human resources	OVR-6.4.4-01	OVR-7.2-01	OVR-6.4.4-01	OVR-7.2-01
REQ-7.3 Asset management	OVR-6.4.1-01	OVR-7.3-01	OVR-6.4.1-01	OVR-7.3-01
REQ-7.4 Access control	OVR-6.3.1-01, OVR-6.5.5-01	OVR-7.4-01	OVR-6.5.3-01	OVR-7.4-01
REQ-7.5 Cryptographic controls	OVR-6.5.1-01	OVR-7.5-01	-	OVR-7.5-01
REQ-7.6 Physical and environmental security	OVR-6.4.2-01	OVR-7.6-01	OVR-6.4.2-01	OVR-7.6-01
REQ 7.7 Operation security	OVR-6.5.6-01	OVR-7.7-01	OVR-6.5.4-01	OVR-7.7-01
REQ 7.8 Network security	OVR-6.5.7-01	OVR-7.8-01	OVR-6.5.5-01	OVR-7.8-01
REQ 7.9 Incident management	OVR-6.4.8-01	OVR-7.9-01	OVR-6.4.8-01	OVR-7.9-01
Req 7.10 Collection of Evidence	OVR-6.4.5-01	OVR-7.10-01	OVR-6.4.5-01	OVR-7.10-01
REQ 7.11 Business continuity management	OVR-6.4.8-01	OVR-7.11-01	OVR-6.4.8-01	OVR-7.11-01
REQ 7.12 TSP (CSP,SSASP,SVSP) termination and termination plans	OVR-6.4.9-01	OVR-7.12-01	OVR-6.4.9-01	OVR-7.12-01
REQ 7.13 Compliance	OVR-6.8.4.-01, OVR-6.8.15- 01, OVR-6.9.3-01	OVR-7.13-01	OVR-6.7.4-01, OVR- 6.7.15-01, OVR-6.8.3-01	OVR-7.13-01

ตารางเปรียบเทียบ ข้อกำหนดเฉพาะ
สำหรับผู้ให้บริการที่เชื่อถือได้ (TSP) ที่เกี่ยวข้องกับลายมือชื่อดิจิทัล

ส่วนประกอบบริการ	CSP/CA 319411	SCASP 119431-2	SSASP 119431-1	SVSP 119441
Registration Service	REG			
Certification generation Services	GEN			
Dissemination Service	OVR, DIS			
Revocation management service	REV			
Revocation status service	CSS			
Subject device provisioning services	SDP			
AdES signing interface services		ASI		
Signing key generation service			GEN	
Certificate/eID means linking service			LNK	
Signature activation service			SIG	
Signing key deletion service			DEL	
eID mean provision			EID	
Signature Validation Protocol				SVP
Signature Validation Process				VPR
Signature Validation Report				SVR

- OVR ข้อกำหนดทั่วไป / GEN บริการสร้างใบรับรอง / REG บริการลงทะเบียน / DIS บริการเผยแพร่ / SDP ข้อกำหนดเกี่ยวกับอุปกรณ์ของเจ้าของใบรับรอง (subject) / CSS บริการสถานภาพใบรับรอง
- ASI ข้อกำหนดส่วนติดต่อของการลงลายมือชื่อดิจิทัล (AdES signing interface)
- GEN ข้อกำหนดบริการสร้างกุญแจสำหรับลงลายมือชื่อ / LNK ข้อกำหนดเกี่ยวกับบริการเชื่อมโยงใบรับรองและอีไอดี / SIG ข้อกำหนดบริการสั่งให้สร้างลายมือชื่อ / DEL ข้อกำหนดการลบกุญแจสำหรับลงลายมือชื่อ / EID ข้อกำหนดเกี่ยวกับอีไอดี
- SVP ข้อกำหนดโพรโทคอลการตรวจสอบความถูกต้องของลายมือชื่อ / VPR ข้อกำหนดเกี่ยวกับกระบวนการตรวจสอบความถูกต้องของลายมือชื่อ / SVR ข้อกำหนดบริการรายงานการตรวจสอบความถูกต้องของลายมือชื่อ

Q&A

