มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับธุรกรรมภาษีทางอิเล็กทรอนิกส์

ว่าด้วยการเชื่อมโยงและแลกเปลี่ยนข้อมูล

RD ICT Standard for Electronic Tax Transactions

: Data Exchange

RD STD. [04-2566]

กรมสรรพากร

Version 01.00.0000

คำนำ

กรมสรรพากร มีการพัฒนาและยกระดับหน่วยงานให้สอดคล้องกับทิศทางการขับเคลื่อนของประเทศ ตามแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นบริการพื้นฐานที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล ทำให้มีการทำงานของแต่ละหน่วยงานอย่างไร้รอยต่อ ปัจจุบัน ประเทศไทยมีแพลตฟอร์มการแลกเปลี่ยนข้อมูลที่ให้บริการหลายรูปแบบ ขึ้นอยู่กับแนวทางและพันธกิจในการดำเนินงาน เป็นผลทำให้การบูรณาการข้อมูลร่วมกันของหน่วยงานจำเป็นต้องขับเคลื่อนด้วยการสร้างมาตรฐานหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล ดังนั้น กรมสรรพากร จึงได้จัดทำมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารสำหรับธุรกรรมภาษีทางอิเล็กทรอนิกส์ ว่าด้วยการเชื่อมโยงและแลกเปลี่ยนข้อมูลของกรมสรรพากร เพื่อใช้ในการแลกเปลี่ยนข้อมูลระหว่างกรมสรรพากรกับผู้มีส่วนได้ส่วนเสียทั้งหน่วยงานของรัฐและหน่วยงานเอกชน เพื่อให้เกิดการบูรณาการข้อมูลร่วมกันได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด

ประกอบกับการรองรับกฎกระทรวงฉบับที่ 384 (พ.ศ. 2565) ตามความในประมวลรัษฎากร ว่าด้วยการดำเนินการเกี่ยวกับเอกสารหลักฐานหรือหนังสือด้วยกระบวนการทางอิเล็กทรอนิกส์ และประกาศอธิบดีกรมสรรพากร (ฉบับที่ 48) เรื่อง กำหนดมาตรฐานเกี่ยวกับรูปแบบ วิธีการส่ง การเก็บรักษาเอกสารหลักฐานหรือหนังสือ และความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับการดำเนินการที่เกี่ยวข้องกับกระบวนการทางอิเล็กทรอนิกส์ โดยกำหนดลักษณะการยื่นหรือส่งเอกสารหลักฐานหรือหนังสือแก่กรมสรรพากร เพื่อเชื่อมต่อระบบอิเล็กทรอนิกส์กับระบบอิเล็กทรอนิกส์ของกรมสรรพากรด้วย

ประวัติการปรับปรุงเอกสาร

Version	รายละเอียด	วันที่
01.00.0000	เวอร์ชันแรก	23 สิงหาคม 2566

สารบัญ

เรื่อง **หน้าที่**

สารบัญตาราง

หน้าที่

สารบัญภาพ

หน้าที่

1. ขอบข่าย

มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับธุรกรรมภาษีทางอิเล็กทรอนิกส์ ฉบับนี้ นำเสนอมาตรฐานที่เกี่ยวข้อง ดังนี้

มาตรฐานการเชื่อมโยง ประกอบด้วย รายการมาตรฐานที่ใช้ในการเชื่อมโยงระบบ รวมถึงแนวทางการเชื่อมโยงข้อมูลในระดับโปรโตคอลมาตรฐานต่าง ๆ เช่น โปรโตคอล HTTP และ sFTP โปรโตคอลการแลกเปลี่ยนข้อความผ่าน Web Service รวมถึงแนวทางในการใช้เทคโนโลยีทางเลือกอื่น ๆ เช่น J2EE, CORBA, JMS เป็นต้น

มาตรฐานการแลกเปลี่ยนข้อมูล ประกอบด้วย รายการมาตรฐานที่ครอบคลุมถึงเทคโนโลยีและมาตรฐานต่าง ๆ สำหรับการจัดโครงสร้างข้อมูล (Structure) และการเข้ารหัสข้อมูล (Encode) เพื่อการแลกเปลี่ยนข้อมูล โดยกรมสรรพากร ใช้มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูล ประกอบด้วยข้อกำหนด 4 ด้าน ดังนี้

(1) การบริหารจัดการ Authentication และ Access Control และบัญชีผู้ใช้งาน Accounting

(2) การบริหารจัดการ Token และ Session

(3) โปรโตคอล (Protocol) สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูล

(4) การกำหนด Namespace ของระบบ

2. นิยาม

นิยามคำศัพท์ที่เกี่ยวข้องกับมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับกรมสรรพากร

ตารางที่ 1 รายการมาตรฐานที่ใช้ในการเชื่อมโยงข้อมูล

(ตามกรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ เวอร์ชัน ๒.๐ (Thailand e-Government Interoperability Framework version 2.0) และรายงานทางเทคนิค กรอบการทำงานร่วมกันของกระเป๋าดิจิทัล สำหรับเอกสารรับรอง (เมษายน 2566))

ลำดับ	วัตถุประสงค์การนำไปใช้	ชื่อย่อ	ชื่อเต็มและรายละเอียด
1	Hypertext transfer protocols	HTTP	Hyper Text Transfer Protocols HTTP v1.1
2	E-mail Transport	SMTP	Simple Mail Transfer Protocol RFC2821
3	Mailbox access	POP3	Post Office Protocol RFC 2449 Version 3
		IMAP	Internet Mail Access Protocol RFC 2060
4	Mail Attachment	MINE	Multipart Internet Mail Extension MIME v1.0
5	Directory	LDAPv2	Light Weight Directory Access Protocol Version 2
		LDAPv3	Light Weight Direction Access Protocol Version 3
6	Domain name service	DNS	Domain Name Service Protocol RFC 1035
7	File Transfer protocols	FTP	File Transfer Protocol RFC 959
8	Newsgroup service	NNTP	Network News Transfer Protocol RFC 3977
9	Real-time messaging Service	IMPP	Instance Messaging and Presence Protocol
		XMPP	Instance Messaging and Presence Protocol XMPP v0.13 draft
		SIP	Session Initiation Protocol RFC 3261
10	LAN/WAN interworking	IPv4	Internet Protocol version 4.0 RFC 791
		IPv6	Internet Protocol version 6.0 RFC 5095
11	Transport	TCP	Transport Control Protocol RFC 793
		UDP	User Datagram Protocol RFC 768
12	GPRS	GPRS	General Packet Radio Service GPRS v2.1.8
13	SMS	SMS	Short Message Service SMS v9.0
14	MMS	MMS	Multimedia Message Service MMS v1.3
15	Video Conference Assembly	H323	Protocol Suite For Video Conference
16	Distributed Process	CORBA	Common Object Request Broker Architecture CORBA v2.3

ลำดับ	วัตถุประสงค์การนำไปใช้	ชื่อย่อ	ชื่อเต็มและรายละเอียด
17	Mobile Content Protocol	WAP	Wireless Application Protocol WAP 2.0
18	Network Time Protocol	NTPv4	Network Time Protocol RFC 2030 Version 4.0
19	Certificate Status Protocol	OCSP	Open Certificate Status Protocol RFC 2560
20	Thai Government Language Protocol	TGL Protocol	Thai Government Language Protocol
21	SSH File Transfer Protocol	SFTP	SSH File Transfer Protocol
22	Representational State Transfer	REST API	Representational State Transfer Application Programming Interface เป็นการเชื่อมโยงเพื่อแลกเปลี่ยนข้อมูลระหว่างกรมสรรพากรและผู้ใช้บริการข้อมูลด้วยวิธีการ RESTful API
23	Open Authentication 2.0	OAuth 2.0	Open Authentication industry-standard protocol for authorization
24	OpenID connect for verifiable credential issuance	OpenID4VCI	OpenID connect for verifiable credential issuance เป็นโพรโทคอลสำหรับการออกเอกสารรับรองผ่านทาง API

ตารางที่ 2 รายการมาตรฐานที่นำมาใช้ในการแลกเปลี่ยนข้อมูล

(ตามกรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ เวอร์ชัน ๒.๐ (Thailand e-Government Interoperability Framework version 2.0) และเอกสารนำเสนอความรู้พื้นฐานและรายงานทางเทคนิคของกระเป๋าดิจิทัลสำหรับเอกสารรับรองกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (Interoperable Framework of Digital Wallets for Verifiable Credentials))

ลำดับ	วัตถุประสงค์การนำไปใช้	ชื่อย่อ	ชื่อเต็มและรายละเอียด
1	Data integration metadata/meta language	XML	Extensible Markup Language XML
2	Data integration metadata definition	XML Schema	XML Schema XML Schema v1.1
3	Data transformation	XSL	Extensible Stylesheet Language XSL v1.1
		XSLT	Extensible Stylesheet Language Transformation
4	Data description language	RDF	Resource Description Framework
5	Data modelling exchange	XMI	XML Metadata Exchange XML ME v1.1

ลำดับ	วัตถุประสงค์การนำไปใช้	ชื่อย่อ	ชื่อเต็มและรายละเอียด
6	Minimum interoperable character set	UTF-8	8 bit Unicode Transformation Format ISO/IEC 10646:2003/Amd.5:2008(E)
7	JavaScript Object Notation	JSON	JavaScript Object Notation รูปแบบของโครงสร้างข้อมูลที่ใช้แลกเปลี่ยนผ่าน REST API
8	DIDComm Message	DIDComm	Decentralized Identifier Communications เป็นการส่งข้อความที่มีการเข้ารหัส

3. ข้อกำหนด

3.1 การบริหารจัดการ Authentication และ Access Control และบัญชีผู้ใช้งาน Accounting

ข้อกำหนดสำคัญบนสถาปัตยกรรมการเชื่อมโยงและแลกเปลี่ยนข้อมูล ประกอบด้วย การยืนยันตัวตน (Authentication) การควบคุมสิทธิในการเข้าถึง (Access Control) และการบริหารจัดการบัญชีการใช้งาน (Accounting) เพื่อให้เกิดความปลอดภัยสูงสุดต่อผู้ให้บริการและผู้ใช้บริการเกิดความมั่นใจในการใช้งานระบบ

3.1.1 การยืนยันตัวตน (Authentication)

การยืนยันตัวตน คือ การที่ผู้ขอใช้บริการยืนยันตัวตนเพื่อขอใช้บริการจากกรมสรรพากร มี 2 วิธี คือ

3.1.1.1 การยืนยันตัวตนด้วย API Key

เป็นการยืนยันตัวตนที่ทำงานด้วยการให้ผู้ใช้บริการล็อกอินเข้าระบบด้วยชื่อผู้ใช้ในระดับองค์กร (Username) และรหัสผ่าน (Password) มีระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level : IAL) เป็นระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ ซึ่งการกำหนดระดับ IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนที่ผิดพลาด โดยแบ่งออกเป็น 3 ระดับ ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน (ขมธอ. 18-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566 และข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (ขมธอ. 19-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566 มีรายละเอียด ดังนี้

(1) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับ 1 (IAL1)

มีการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) ทั้งนี้ อาจมีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์หรือการตรวจสอบ ความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์ด้วยวิธีการอื่น ๆ ตามความเสี่ยงของบริการธุรกรรม

(2) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับ 2 (IAL2)

กำหนดให้มีการขอหลักฐานแสดงตน การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า (face-to-face) หรือแบบไม่พบเห็นต่อหน้า (non face-to-face) ซึ่งผู้พิสูจน์และยืนยันตัวตน ที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับผู้ให้บริการภาครัฐ ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

ระดับ IAL2 แบ่งออกเป็น 3 ระดับย่อย คือ IAL2.1, IAL2.2 และ IAL2.3 โดยพิจารณาจากความเข้มงวดของวิธีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์และวิธีการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

(3) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ระดับ 3 (IAL3)

กำหนดให้มีการตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์ด้วยการเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่นและการลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL3 ต้องทำแบบพบเห็นต่อหน้า (face-to-face) เท่านั้น ซึ่งผู้พิสูจน์และยืนยันตัวตน ที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับผู้ให้บริการภาครัฐ ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

นอกจากระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) แล้ว ต้องคำนึงถึงความเข้มงวดของระบบการยืนยันตัวตนจะขึ้นอยู่กับจำนวนของปัจจัยของการยืนยันตัวตน โดยแบ่งสิ่งที่ใช้ยืนยันตัวตนได้เป็น 2 แบบ ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน (ขมธอ. 18-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566 ดังนี้

(1) การยืนยันตัวตนแบบปัจจัยเดียว (Single-factor Authenticator)

เป็นการยืนยันตัวตนที่ใช้สิ่งที่ใช้ยืนยันตัวตนเพียง 1 ปัจจัย เช่น ผู้ใช้บริการแสดงรหัสผ่านในการเข้าระบบ ซึ่งรหัสผ่านเป็นสิ่งที่ผู้ใช้บริการรู้

(2) การยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authenticator) มีการใช้ปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย สามารถทำได้ 2 วิธี ดังนี้ (1) การใช้ปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัยเพื่อยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนโดยตรง เช่น ผู้ใช้บริการต้องกรอกทั้งรหัสผ่าน (สิ่งที่คุณรู้) และข้อมูลลับที่ส่งมายังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการทาง SMS (สิ่งที่คุณมี) เพื่อยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (2) การใช้ปัจจัยของการยืนยันตัวตนบางปัจจัยเพื่อปกป้องข้อมูลลับก่อนที่จะใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน เช่น การใช้ลายนิ้วมือ (สิ่งที่คุณเป็น) เพื่อปกป้องกุญแจส่วนตัว (สิ่งที่คุณมี) ในโทรศัพท์เคลื่อนที่ โดยผู้ใช้บริการต้องสแกนลายนิ้วมือเพื่อทำให้ซอฟต์แวร์เข้ารหัสลับ (cryptographic software) ในโทรศัพท์เคลื่อนที่สามารถเรียกใช้กุญแจส่วนตัวเพื่อยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

จำนวนปัจจัยของการยืนยันตัวตน มีผลกับระดับความน่าเชื่อถือของการยืนยันตัวตน (Authenticator Assurance Level : AAL) เป็นระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้สมัครใช้บริการ ซึ่งการกำหนดระดับ AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนที่ผิดพลาด โดยแบ่งออกเป็น 3 ระดับ ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน

(ขมธอ. 18-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566 และข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (ขมธอ. 20-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566 มีรายละเอียด ดังนี้

(1) ระดับความน่าเชื่อถือของการยืนยันตัวตน ระดับที่ 1 (AAL1)

กำหนดให้ใช้การยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) เป็นอย่างน้อย โดยการสื่อสารระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน ต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

(2) ระดับความน่าเชื่อถือของการยืนยันตัวตน ระดับที่ 2 (AAL2)

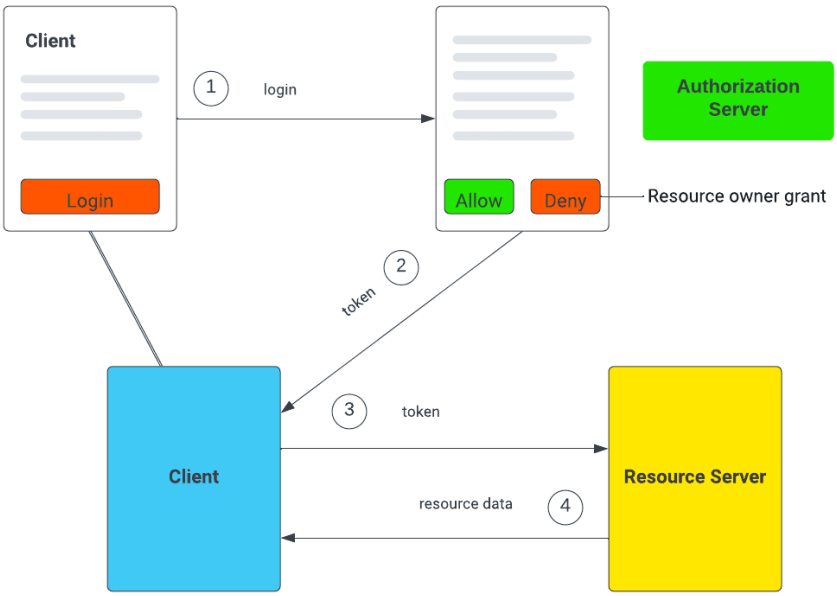
กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตน (authentication factor) ที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย สามารถทำได้ 2 วิธี ดังนี้ (1) การใช้สิ่งที่ใช้ยืนยันตัวตนแบบปัจจัยเดียว (single-factor authenticator) ซึ่งเป็นปัจจัยที่แตกต่างกัน จำนวน 2 อัน เช่น การกรอกรหัสผ่าน (สิ่งที่คุณรู้) และข้อมูลลับที่ส่งมายังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการทาง SMS (สิ่งที่คุณมี) เพื่อยืนยันตัวตน (2) การใช้สิ่งที่ใช้ยืนยันตัวตนแบบหลายปัจจัย (multi-factor authenticator) จำนวน 1 อัน เช่น อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ซึ่งจะสร้างรหัสผ่านใช้ครั้งเดียว (OTP) หลังจากผู้ใช้บริการกรอกเลขรหัสส่วนตัวหรือสแกนลายนิ้วมือสำเร็จ จากนั้น ผู้ใช้บริการจะนำ OTP ที่แสดงผลบนอุปกรณ์ไปกรอกเพื่อยืนยันตัวตน โดยการสื่อสารระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

(3) ระดับความน่าเชื่อถือของการยืนยันตัวตน ระดับที่ 3 (AAL3)

กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย และใช้สิ่งที่ใช้ยืนยันตัวตนที่มีคุณสมบัติเป็นฮาร์ดแวร์ (hardware-based) บรรจุกุญแจเข้ารหัส (cryptographic key) และสามารถป้องกันผู้พิสูจน์และยืนยันตัวตนตัวปลอม (IdP impersonation resistance) ทั้งนี้ ปัจจัยที่แตกต่างกัน 2 ปัจจัยต้องดำเนินการด้วยเกณฑ์วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย รวมถึงการแสดงให้เห็นว่ากุญแจเข้ารหัสต้องดำเนินการด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol)

3.1.1.2 การยืนยันตัวตนด้วยมาตรฐาน OAuth 2.0

OAuth 2.0 คือ มาตรฐานหนึ่งของระบบยืนยันตัวตน และจัดการสิทธิ์การเข้าใช้งาน (Authentication & Authorization) ระบบต่าง ๆ ของ Client เพื่อให้ได้รับ Access Token ซึ่งสามารถใช้ทดแทน Username และ Password ทำให้มีความปลอดภัยมากขึ้น รวมถึงสามารถจำกัดสิทธิ์การใช้งานในบริการได้ โดยต้องใช้คู่กับ HTTPS เพื่อความปลอดภัยสูงสุด โดยแสดงขั้นตอนการทำงานตาม IETF องค์กรวางมาตรฐานอินเทอร์เน็ต IETF (Internet Engineering Task Force) เพื่อส่งเสริมการใช้งานอินเตอร์เน็ตอย่างมีประสิทธิภาพ ดังรูปที่ 1



รูปที่ 1 ขั้นตอนการทำงานของ OAuth 2.0

ขั้นตอนการทำงานของ OAuth 2.0 มีดังนี้

1. ผู้ใช้งานเข้าใช้งานระบบจากแอพพลิเคชัน
2. เมื่อผู้ใช้คลิกปุ่มเข้าสู่ระบบ แอปพลิเคชันจะเปลี่ยนเส้นทางไปยังหน้าอนุญาตของ Authorization Server
3. ผู้ใช้งานอนุญาตการเข้าถึงข้อมูลที่ต้องการ
4. Authorization Server ส่งรหัสเข้าใช้งาน Access Token ไปยังแอพพลิเคชัน ซึ่งแอพพลิเคชันใช้ Access Token เพื่อเข้าถึงข้อมูลต่าง ๆ โดย Access Token มีเวลาจำกัดในการใช้งาน เมื่อ Token หมดอายุ ต้องทำการขอใหม่ และเมื่อเลิกใช้งานสามารถขอยกเลิก Access Token ได้ มีรูปแบบการใช้งาน 4 รูปแบบ ดังนี้

(1) Authorization Code ใช้สำหรับ Web Server ที่ใช้ Code ในการเชื่อมต่อกับ OAuth Server โดยไม่เปิดเผยให้สาธารณะรับรู้

(2) Implicit ลักษณะการทำงานคล้ายกับ Authorization Code แต่เป็นวิธีที่เปิดเผยการเชื่อมต่อให้สาธารณะเห็น

(3) Password Credentials ใช้สำหรับ Application ที่มีการจัดการสิทธิเอง แต่ต้องการยืนยันตัวตนเท่านั้น ซึ่งวิธีนี้จะไม่ Redirect ไปที่ผู้ให้บริการอื่น วิธีนี้เหมาะกับการใช้งานที่เป็นบริการของตัวเอง เพราะ Username กับ Password จะปรากฏในเครื่องที่ส่งขอ Access Token จึงไม่เหมาะกับการนำไปใช้บน Server ที่ไม่ได้เป็นเจ้าของ เนื่องจาก มีความเสี่ยงข้อมูลรั่วไหล

(4) Client Credentials ใช้ในกรณีที่เป็นการคุยระหว่าง Application กับ Service ที่ไม่เกี่ยวข้องกับผู้ใช้ เนื่องจากไม่มีการใช้งาน Username กับ Password แต่จะใช้ ID และ Secret เพื่อขอ Access Token ในการเข้าถึง Service

3.1.2 การควบคุมสิทธิในการเข้าถึง (Access Control)

การควบคุมสิทธิในการเข้าถึง ข้อกำหนดในส่วนนี้มีจุดประสงค์เพื่อให้ผู้ใช้บริการมั่นใจว่าระบบหรือบุคคลที่จะเข้าถึงบริการของกรมสรรพากร ได้นั้นเป็นผู้ที่ได้รับอนุญาตเท่านั้น โดยหลังจากผู้ให้บริการตรวจสอบว่าผู้ใช้บริการยืนยันตัวตนผ่านแล้ว จึงตรวจสอบต่อไปว่าผู้ใช้บริการมีรายชื่อตามที่ลงทะเบียนใช้บริการของกรมสรรพากรไว้ เมื่อยืนยันว่าผู้ใช้บริการมีสิทธิในการเข้าถึงบริการของกรมสรรพากรนั้น ๆ แล้วจึงทำการอนุญาตและส่งข้อมูล กลับไปยังผู้ขอใช้บริการ

3.1.3 การบริหารจัดการบัญชีการใช้งาน (Accounting)

การบริหารจัดการบัญชีการใช้งาน เป็นข้อกำหนดแนวทางปฏิบัติให้มีความปลอดภัยทั้งระหว่างการจัดเก็บและการรับส่งข้อมูลสำหรับทั้งผู้ให้บริการ ผู้ใช้บริการ โดยแบ่งออกเป็น 2 กลุ่มตามประเภทของการยืนยันตัวตน คือ บัญชีใช้งานประเภท API Key ใช้สำหรับการยืนยันตัวตนด้วย API Key และบัญชีใช้งานที่รองรับมาตรฐาน OAuth 2.0

ข้อกำหนดในส่วนนี้ ตัวอย่างเช่น บัญชีใช้งานประเภท API Key กำหนดให้ผู้ให้บริการไม่ควรกำหนด API Key ไว้ใน Source Code และให้เก็บในที่ปลอดภัย อาทิ ฐานข้อมูล หรือบัญชีใช้งานที่รองรับมาตรฐาน OAuth 2.0 กำหนดให้ผู้ให้บริการควรให้บริการ REST API ผ่าน HTTPS (SSL) เท่านั้น และการออก Access Token ควรมีระยะเวลาการใช้งานได้จำกัด

3.2 การบริหารจัดการ Token และ Session

Token เป็นสัญลักษณ์ที่ใช้ในการแทนตัวผู้ใช้ โดยส่ง Token ต่าง ๆ ไปยังแอปพลิเคชันในการตรวจสอบสิทธิ์

Session เป็นการบันทึกข้อมูลของผู้ใช้ในแอปพลิเคชันอินเตอร์เน็ต โดยจะมีการบันทึกเวลาเริ่มใช้งานและการใช้งานต่าง ๆ ในแอปพลิเคชัน

การบริหาร Token และ Session จะช่วยให้แอปพลิเคชันสามารถตรวจสอบสิทธิ์ของผู้ใช้และระบุตัวผู้ใช้ในแอปพลิเคชันได้อย่างถูกต้องและปลอดภัย

3.3 โปรโตคอล (Protocol) สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูล แบ่งออกเป็น

3.3.1 โปรโตคอลด้านการสื่อสาร

- โปรโตคอล HTTP (HyperText Transfer Protocol) ใช้ในการรับส่งข้อมูลประเภทโฮมเพจผ่านเครือข่ายคอมพิวเตอร์

- โปรโตคอล SMTP (Simple Mail Transfer Protocol) ใช้ในการรับส่งข้อมูลประเภทจดหมายอิเล็กทรอนิกส์ผ่านเครือข่ายคอมพิวเตอร์

3.3.2 โปรโตคอลด้านความปลอดภัย

- โปรโตคอล SSL (Secure Socket Layer) ใช้ในการปกป้องข้อมูลบนอินเทอร์เน็ตที่ต้องการความปลอดภัยสูง ไม่สามารถอ่านได้โดยบุคคลที่ไม่เกี่ยวข้อง สามารถใช้งานได้ทั้งการเชื่อมต่อระหว่างเซิร์ฟเวอร์ กับไคลเอนท์, เซิร์ฟเวอร์ กับเซิร์ฟเวอร์

- โปรโตคอล HTTPS (HyperText Transfer Protocol over Secure Socket Layer) ใช้ในการรับส่งข้อมูลประเภทโฮมเพจผ่านเครือข่ายคอมพิวเตอร์ และมีการเข้ารหัสเพื่อรักษาความลับหรือรักษาความมั่นคงปลอดภัยของข้อมูลที่รับส่งระหว่างกัน

- โปรโตคอล SFTP (Secure File Transfer Protocol) ใช้ในการปกป้องไฟล์ที่ส่งผ่านระบบเครือข่าย ที่มีรูปแบบ Batch File สำหรับเรียกคำสั่งบน Windows และมีนามสกุล .bat คำสั่งที่อยู่ใน Batch file จะถูกรันอย่างเป็นทางการใน Command Prompt โดยมีประโยชน์ในการทำงานบน Windows ซ้ำ ๆ หรือสำหรับการเรียกใช้งานหลาย ๆ โปรแกรมในครั้งเดียว ซึ่งมีการเรียกใช้ผ่าน SFTP เป็นวิธีถ่ายโอนข้อมูลอย่างปลอดภัย โดยใช้การเข้ารหัส และจะไม่โอนข้อมูลไฟล์ที่เป็น clear-text

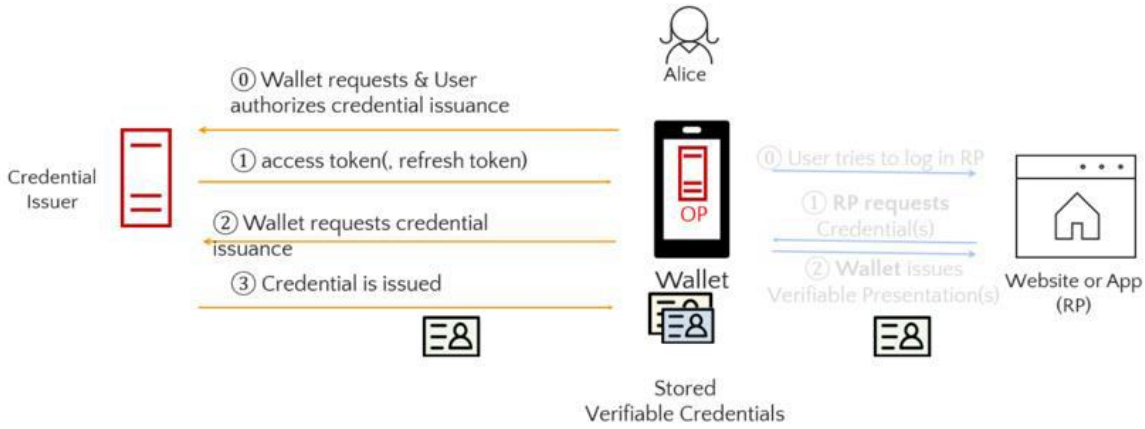
3.3.3 โปรโตคอลการแลกเปลี่ยนข้อมูล

- โปรโตคอล SOAP (Simple Object Access Protocol) ใช้ในการรับส่งข้อมูลระหว่างผู้ให้บริการและผู้ใช้บริการ ที่มีรูปแบบการจัดเก็บตามมาตรฐานเอ็กซ์เอ็มแอล (XML) ผ่านเครือข่ายอินเตอร์เน็ต โดย SOAP จะใช้ HTTP Protocol ช่วยในการส่งข้อมูลเปรียบเสมือน SOAP เป็นจดหมาย และ HTTP Protocol เป็นผู้ส่งจดหมาย สามารถทำได้ 2 วิธี คือ แบบ Remote Procedure Call (RPC) และแบบ Documents

นอกจากนี้ การแลกเปลี่ยนข้อมูลแบบ Restful API สามารถใช้งานผ่าน HTTP (Hypertext Transfer Protocol) หรือ HTTPS (Hypertext Transfer Protocol Secure) ได้ โดยรองรับรูปแบบข้อมูลหลายประเภท เช่น XML, JSON, MIME, Text เป็นต้น

3.3.4 โปรโตคอลการออกเอกสารรับรอง (Issuance Protocol) [6] ใช้กับเอกสารรับรองในรูปแบบ JSON web token (JWT) และ SD-JWT หรือ JSON for linked data (JSON-LD)

- โปรโตคอล OpenID connect for verifiable credential issuance (OpenID4VCI) เป็นโปรโตคอลสำหรับการออกเอกสารรับรองผ่านทาง API โดยรองรับมาตรฐานเอกสารรับรองหลากหลายรูปแบบ รวมถึง W3C Verifiable Credentials และ ISO/IEC 18013-5 mDL โดยมีลำดับการทำงานตามเอกสารนำเสนอความรู้พื้นฐานและรายงานทางเทคนิคของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสาหรับเอกสารรับรอง (Interoperable Framework of Digital Wallets for Verifiable Credentials) ดังรูปที่ 2

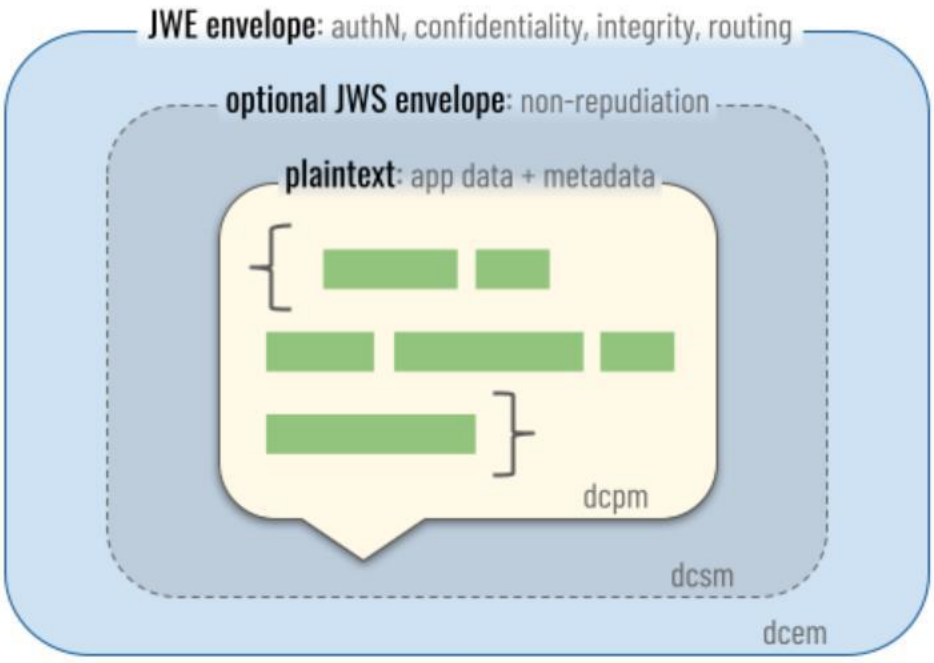


รูปที่ 2 ขั้นตอนการทำงานของการออกเอกสารรับรอง

ขั้นตอนการทำงานของการออกเอกสารรับรอง มีดังนี้

0. end-user เริ่มต้นปฏิสัมพันธ์กับผู้ออกเอกสารเพื่อร้องขอเอกสารรับรอง
1. ผู้ออกเอกสารส่ง access token กลับมาให้อุปกรณ์ของ end-user
2. อุปกรณ์ของ end-user ดาเนินการร้องขอเอกสารรับรอง
3. ผู้ออกเอกสารออกและส่งเอกสารรับรองให้ end-user

- โปรโตคอล DIDComm เป็นการแลกเปลี่ยนข้อมูล ซึ่งมีโครงสร้างข้อมูลตามเอกสารนำเสนอความรู้พื้นฐานและรายงานทางเทคนิคของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสาหรับเอกสารรับรอง (Interoperable Framework of Digital Wallets for Verifiable Credentials) ดังรูปที่ 3



รูปที่ 3 องค์ประกอบของข้อความ DIDComm

ประกอบไปด้วยข้อมูล 3 ชั้น ดังนี้

1. DIDComm plaintext message เป็นข้อความในรูปแบบ plaintext ที่อยู่ชั้นในสุด

2. DIDComm signed message เป็นชั้นถัดมาซึ่งอาจมีหรือไม่ก็ได้ (optional) ทำหน้าที่ลงลายมือชื่อดิจิทัล ในรูปแบบ JSON Web Signature (JWS) เพื่อตรวจสอบที่มาของข้อความ

3. DIDComm encrypted message เป็นชั้นนอกสุดเป็นชั้นที่ทำการเข้ารหัส (encryption) ในรูปแบบ JSON Web Encryption (JWE) โดยทำหน้าที่รับรองความสมบูรณ์ (integrity) ของข้อความ

3.4 การกำหนด Namespace ของระบบ

Namespace หมายถึง การจัดแยกชื่ออินพุตของระบบ เพื่อป้องกันการซ้ำซ้อนของชื่ออินพุตในระบบคอมพิวเตอร์หรือระบบประยุกต์ การกำหนด Namespace จะช่วยให้การจัดการชื่ออินพุตของระบบมีความสามารถในการจัดการและป้องกันปัญหาในการอ้างอิงชื่ออินพุตในระบบได้อย่างมีประสิทธิภาพ ทำให้เข้าใจบริบทของทรัพยากร ช่วยจัดกลุ่มของทรัพยากร เพื่อให้ผู้ดูแลทรัพยากรสามารถกำหนดขอบเขตหรือสิทธิ์การเข้าถึงทรัพยากรได้

บรรณานุกรม

[1] สำนักส่งเสริมและพัฒนารัฐบาลอิเล็กทรอนิกส์, กรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ เวอร์ชัน ๒.๐ (Thailand e-Government Interoperability Framework version 2.0).

[2] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2566). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน (ขมธอ. 18-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566

[3] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2566). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (ขมธอ. 19-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566

[4] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2566). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (ขมธอ. 20-2566) ลงวันที่ 23 กุมภาพันธ์ พ.ศ. 2566

[5] IETF องค์กรวางมาตรฐานอินเทอร์เน็ต IETF (Internet Engineering Task Force) เพื่อส่งเสริมการใช้งานอินเตอร์เน็ตอย่างมีประสิทธิภาพ.

[6] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2566). รายงานทางเทคนิค กรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (เมษายน 2566)

[7] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2566). เอกสารนำเสนอความรู้พื้นฐานและรายงานทางเทคนิคของกระเป๋าดิจิทัลสำหรับเอกสารรับรองกรอบการทำงานร่วมกันของกระเป๋าดิจิทัลสำหรับเอกสารรับรอง (Interoperable Framework of Digital Wallets for Verifiable Credentials)