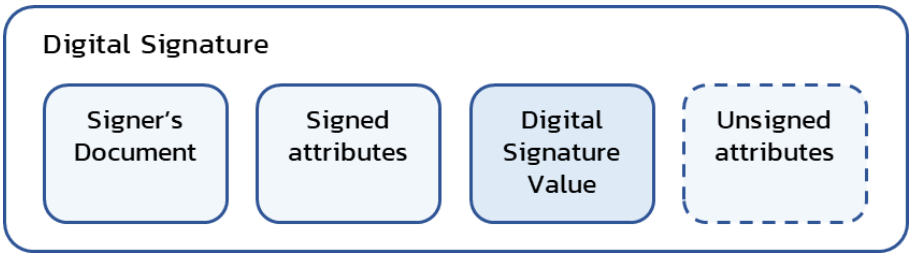
ทำอย่างไรให้ ลายมือชื่อดิจิทัล (digital signature) มีคุณสมบัติรองรับการตรวจสอบความถูกต้องในระยะยาว (long-term digital signature) ?

ลายมือชื่อดิจิทัล (digital signature) เป็นลายมือชื่ออิเล็กทรอนิกส์ (electronic signature) ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์หรือแฮชของข้อมูลอิเล็กทรอนิกส์ ด้วยกุญแจส่วนตัว (private key) ในระบบรหัสแบบอสมมาตร (asymmetric cryptography) ซึ่งมีคุณสมบัติด้านความมั่นคงปลอดภัยที่ช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อ (authentication) และสามารถตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้นับแต่เวลาที่สร้างลายมือชื่ออิเล็กทรอนิกส์ขึ้น (data integrity) รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ (non-repudiation) [1]

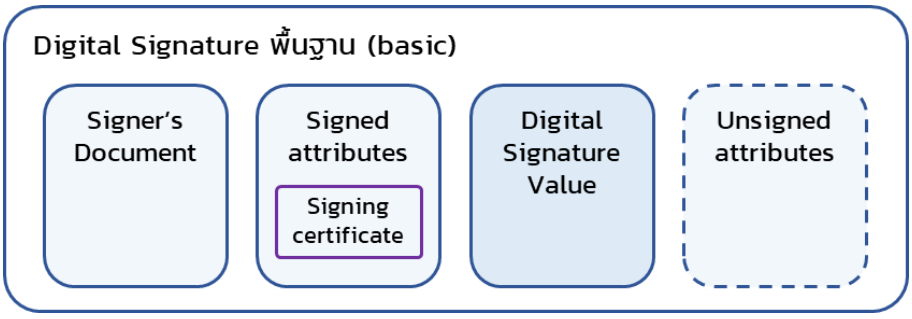
โดยทั่วไป โครงสร้างข้อมูลของลายมือชื่อดิจิทัล (ตามรูปที่ 1) จะประกอบด้วยส่วนประกอบหลัก ดังนี้ [2]

(1) เอกสารที่จะลงลายมือชื่อของเจ้าของลายมือชื่อ (signer's document)
(2) แอตทริบิวต์ที่ถูกลงลายมือชื่อ (signed attributes) ซึ่งเป็นรายการข้อมูลเกี่ยวกับลายมือชื่อที่นำเข้ามาใช้คำนวณค่าลายมือชื่อดิจิทัล
(3) ค่าลายมือชื่อดิจิทัล (digital signature value) ซึ่งเป็นค่าที่คำนวณได้จากกระบวนการเข้ารหัสลับเอกสารที่จะลงลายมือชื่อและแอตทริบิวต์ที่ถูกลงลายมือชื่อ ด้วยกุญแจส่วนตัวของเจ้าของลายมือชื่อ และ
(4) แอตทริบิวต์ที่ไม่ต้องถูกลงลายมือชื่อ (unsigned attributes) ซึ่งเป็นรายการข้อมูลเกี่ยวกับลายมือชื่อที่ไม่ถูกนำเข้ามาใช้คำนวณค่าลายมือชื่อดิจิทัล



รูปที่ 1 โครงสร้างข้อมูลของลายมือชื่อดิจิทัล

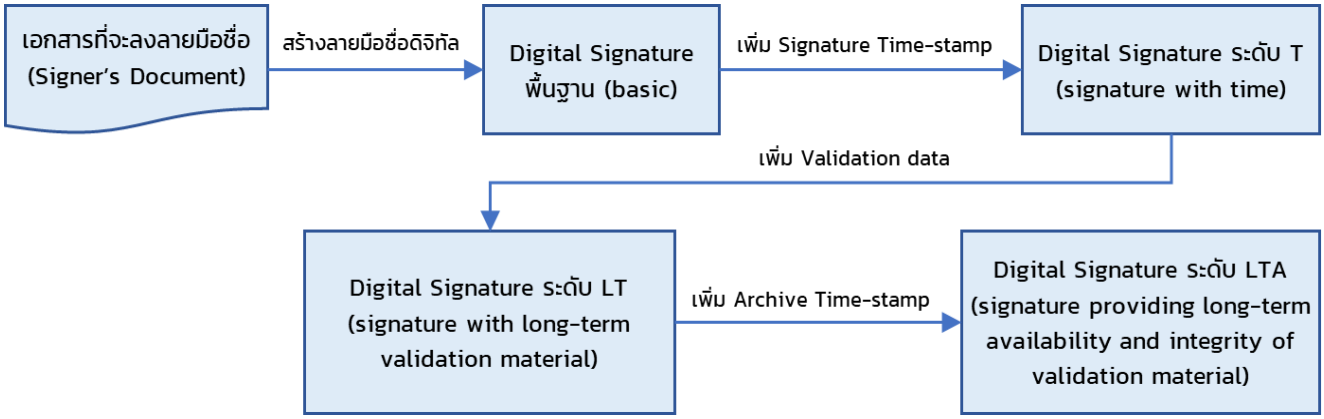
ทั้งนี้ ลายมือชื่อดิจิทัลพื้นฐาน (basic) จะมีข้อมูลอ้างอิงถึงใบรับรองที่ใช้ลงลายมือชื่อ (reference to the signing certificate) เป็นแอตทริบิวต์ที่ถูกลงลายมือชื่อ (signed attribute) (ตามรูปที่ 2) โดยการระบุใบรับรองที่จะใช้ตรวจสอบความถูกต้องของลายมือชื่อนั้นจะทำให้สามารถป้องกันความเสี่ยงจากเหตุการณ์การแทนที่ใบรับรองด้วยใบรับรองอันอื่นหรือใบรับรองอันใหม่ (simple substitution and reissuing attacks) อย่างไรก็ตาม ลายมือชื่อดิจิทัลพื้นฐานจะสามารถตรวจสอบความถูกต้องได้ตราบใดที่ใบรับรองที่เกี่ยวข้องยังไม่ถูกเพิกถอน (revoked) หรือหมดอายุ (expired)



รูปที่ 2 ลายมือชื่อดิจิทัลพื้นฐาน (basic)

เพื่อให้ลายมือชื่อดิจิทัลมีความสามารถในการตรวจสอบความถูกต้องได้ในอนาคต แม้ว่าใบรับรองที่เกี่ยวข้องหรือข้อมูลอื่นที่จำเป็นสำหรับการตรวจสอบความถูกต้องอาจจะถูกเพิกถอน (revoked) หมดอายุ (expired) หรือไม่สามารถเข้าถึงทางออนไลน์ได้ หรืออัลกอริทึมเข้ารหัสลับ (cryptographic algorithm) ที่ใช้สร้างลายมือชื่อดิจิทัลอาจจะไม่มีความแข็งแรงเพียงพอที่จะเชื่อถือได้ ลายมือชื่อดิจิทัลพื้นฐาน (basic) จำเป็นต้องมีการเพิ่มคุณสมบัติลายมือชื่อดิจิทัล (signature augmentation) ให้รองรับการตรวจสอบความถูกต้องได้ในระยะยาว (long-term validation) ภายหลังจากการสร้างลายมือชื่อดิจิทัลแล้ว

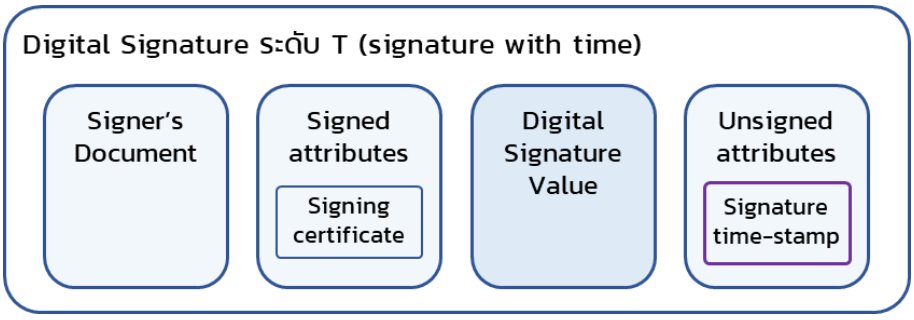
ลายมือชื่อดิจิทัลที่มีคุณสมบัติรองรับการตรวจสอบความถูกต้องในระยะยาว (long-term digital signature) จะมีการเพิ่มเติมแอตทริบิวต์ที่ไม่ต้องถูกลงลายมือชื่อ (unsigned attributes) ด้วยข้อมูลเกี่ยวกับโทเคนประทับเวลา (time-stamp token) และข้อมูลสำหรับตรวจสอบความถูกต้องลายมือชื่อดิจิทัล (validation data) (ตามรูปที่ 3) เพื่อให้เวลาที่ลงลายมือชื่อ (signing time) สามารถระบุได้ การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ข้อมูลเกี่ยวกับลายมือชื่อและข้อมูลสำหรับตรวจสอบความถูกต้องลายมือชื่อดิจิทัลสามารถจะตรวจพบได้ และเกิดการทำงานร่วมกันได้ (interoperability) ระหว่างแอปพลิเคชันที่เกี่ยวข้องกับลายมือชื่อดิจิทัล



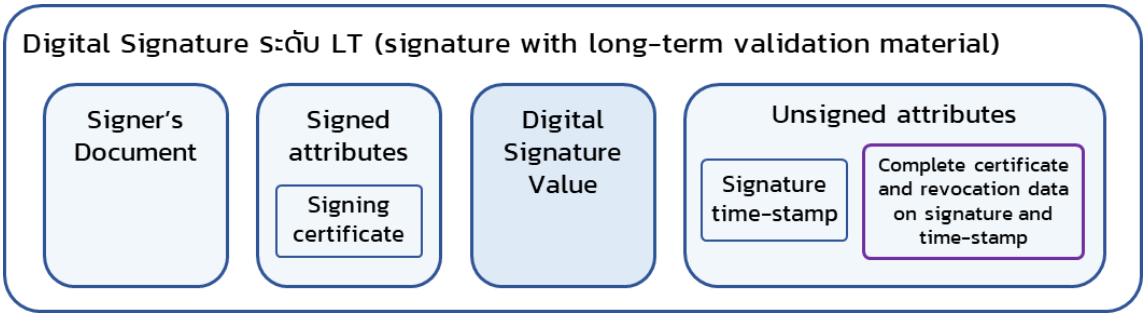
รูปที่ 3 การเพิ่มคุณสมบัติลายมือชื่อดิจิทัลให้รองรับการตรวจสอบความถูกต้องได้ในระยะยาว

ลายมือชื่อดิจิทัลที่มีคุณสมบัติรองรับการตรวจสอบความถูกต้องในระยะยาว (long-term digital signature) สามารถแบ่งออกเป็น 3 ระดับ (signature class) ดังนี้ [2]

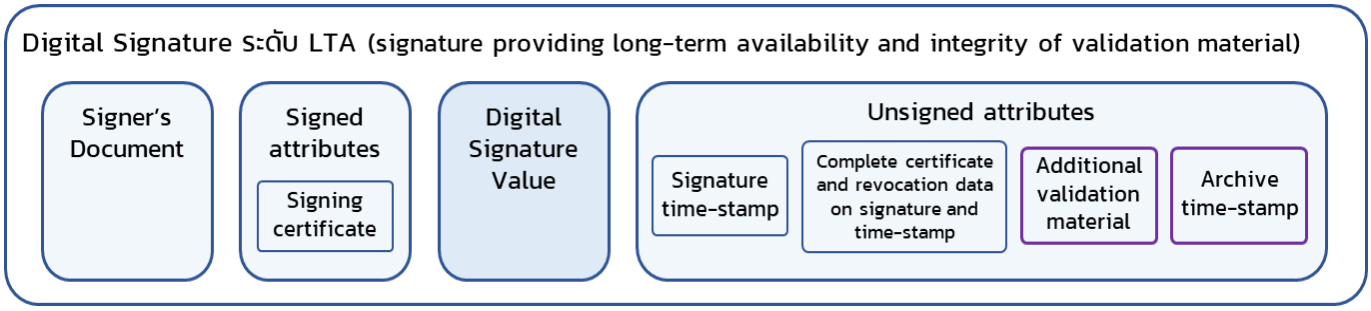
(1) ลายมือชื่อดิจิทัลระดับ T (signature with time)
(2) ลายมือชื่อดิจิทัลระดับ LT (signature with long-term validation material)
(3) ลายมือชื่อดิจิทัลระดับ LTA (signature providing long-term availability and integrity of validation material)



รูปที่ 4 ลายมือชื่อดิจิทัลระดับ T (signature with time)



รูปที่ 5 ลายมือชื่อดิจิทัลระดับ LT (signature with long-term validation material)



รูปที่ 6 ลายมือชื่อดิจิทัลระดับ LTA (signature providing long-term availability and integrity of validation material)

ทั้งนี้ คุณสมบัติและแอตทริบิวต์ (attributes) ที่เพิ่มเข้าไปของลายมือชื่อดิจิทัลที่มีคุณสมบัติรองรับการตรวจสอบความถูกต้องในระยะยาว (long-term digital signature) แต่ละระดับ มีรายละเอียดตามตารางที่ 1

ตารางที่ 1 ระดับของลายมือชื่อดิจิทัลที่มีคุณสมบัติรองรับการตรวจสอบความถูกต้องในระยะยาว (long-term digital signature)

ลายมือชื่อดิจิทัลที่มีคุณสมบัติรองรับการตรวจสอบความถูกต้องในระยะยาว (long-term digital signature)		
ระดับ	**คุณสมบัติด้านการตรวจสอบความถูกต้องได้ในระยะยาว**	**แอตทริบิวต์ (attributes) ที่เพิ่มเข้าไป**
ลายมือชื่อดิจิทัลระดับ T (signature with time)	ลายมือชื่อดิจิทัลระดับ T เป็นลายมือชื่อดิจิทัลที่ยืนยันการมีอยู่ของลายมือชื่อดิจิทัล ณ จุดเวลาที่ระบุในโทเคนประทับเวลา (time-stamp token) ซึ่งได้รับการรับรองโดยผู้ให้บริการประทับเวลา (time-stamping authority: TSA) โทเคนประทับเวลาบนค่าลายมือชื่อดิจิทัล (signature time-stamp token) ควรระบุเวลาที่ใกล้เคียงกับเวลาที่สร้างลายมือชื่อดิจิทัลให้มากที่สุด เพื่อลดความเสี่ยงจากการปฏิเสธความรับผิดของเจ้าของลายมือชื่อว่าไม่ได้สร้างลายมือชื่อดิจิทัล ณ เวลานั้น ลายมือชื่อดิจิทัลระดับ T มีความสามารถในการตรวจสอบความถูกต้องของลายมือชื่อดิจิทัลได้ แม้ว่าใบรับรองจะถูกเพิกถอน (revoked) ภายหลังจากการสร้างลายมือชื่อดิจิทัลแล้ว อย่างไรก็ตาม จำเป็นต้องสร้างโทเคนประทับเวลาบนค่าลายมือชื่อดิจิทัล ก่อนที่ใบรับรองจะถูกเพิกถอนหรือหมดอายุ หากไม่สามารถทำได้ การตรวจสอบความถูกต้องของลายมือชื่อดิจิทัลอาจไม่สำเร็จ	เพิ่มเติมแอตทริบิวต์จากลายมือชื่อดิจิทัลพื้นฐาน (basic) ดังนี้ – โทเคนประทับเวลาบนค่าลายมือชื่อดิจิทัล (signature time-stamp token) จากผู้ให้บริการประทับเวลา (time-stamping authority: TSA)
ลายมือชื่อดิจิทัลระดับ LT (signature with long-term validation material)	ลายมือชื่อดิจิทัลระดับ LT เป็นลายมือชื่อดิจิทัลที่ให้ความพร้อมใช้งานระยะยาว (long-term availability) ของข้อมูลสำหรับตรวจสอบความถูกต้องลายมือชื่อดิจิทัล (validation data) โดยการรวมข้อมูลทั้งหมดหรือค่าอ้างอิงถึงข้อมูลที่จำเป็นสำหรับการตรวจสอบความถูกต้องลายมือชื่อดิจิทัลเข้าไว้ในลายมือชื่อดิจิทัลด้วย แม้ว่าลายมือชื่อดิจิทัลระดับ T จะสามารถตรวจสอบความถูกต้องได้ตราบใดที่ข้อมูลสำหรับตรวจสอบความถูกต้องลายมือชื่อดิจิทัล (validation data) ยังสามารถเข้าถึงทางออนไลน์ได้โดยผู้ตรวจสอบ อย่างไรก็ตาม ในกรณีที่ไม่แน่ใจว่าข้อมูลสำหรับตรวจสอบความถูกต้องลายมือชื่อดิจิทัลจะยังคงออนไลน์และพร้อมใช้งานโดยผู้ตรวจสอบหรือไม่ หรือผู้ตรวจสอบบางรายจะไม่สามารถเข้าถึงข้อมูลนั้นได้ ก็จำเป็นต้องมีการบันทึกข้อมูลดังกล่าวไว้ในลายมือชื่อดิจิทัลระดับ LT	เพิ่มเติมแอตทริบิวต์จากลายมือชื่อดิจิทัลระดับ T ดังนี้ – ข้อมูลสำหรับตรวจสอบความถูกต้องลายมือชื่อดิจิทัล (validation data) เช่น เส้นทางใบรับรอง (certificate path) และข้อมูลการเพิกถอนใบรับรอง (revocation data) ทั้งหมดที่เกี่ยวข้องกับลายมือชื่อดิจิทัลและโทเคนประทับเวลา

ลายมือชื่อดิจิทัลที่มีคุณสมบัติรองรับการตรวจสอบความถูกต้องในระยะยาว (long-term digital signature)		
ระดับ	**คุณสมบัติด้านการตรวจสอบความถูกต้องได้ในระยะยาว**	**แอตทริบิวต์ (attributes) ที่เพิ่มเข้าไป**
ลายมือชื่อดิจิทัลระดับ LTA (signature providing long-term availability and integrity of validation material)	ลายมือชื่อดิจิทัลระดับ LTA เป็นลายมือชื่อดิจิทัลที่ให้ความพร้อมใช้งานและความสามารถตรวจพบการเปลี่ยนแปลงได้ในระยะยาว (long-term availability and integrity) ของข้อมูลสำหรับตรวจสอบความถูกต้องลายมือชื่อดิจิทัล (validation data) และยังสามารถตรวจสอบความถูกต้องของลายมือชื่อดิจิทัลได้ แม้ในกรณีที่มีเหตุการณ์ต่าง ๆ ที่จำกัดความถูกต้องของลายมือชื่อดิจิทัล เช่น เมื่อใบรับรองถูกเพิกถอน (revoked) หรือหมดอายุ (expired) และเมื่อความมั่นคงปลอดภัยของอัลกอริทึมเข้ารหัสลับ (cryptographic algorithm) หรือขนาดของกุญแจเข้ารหัสลับ (key size) ที่ใช้สร้างลายมือชื่อดิจิทัล เป็นที่น่าสงสัยหรือไม่มีความแข็งแรงเพียงพออีกต่อไป ก่อนที่อัลกอริทึม กุญแจ และข้อมูลเข้ารหัสลับอื่น ๆ ที่ใช้ในขณะที่สร้างลายมือชื่อดิจิทัลจะไม่มีความมั่นคงปลอดภัย และฟังก์ชันการเข้ารหัสลับจะมีชางโหว่ หรือก่อนที่ใบรับรองที่สนับสนุนโทเคนประทับเวลาอันก่อนหน้าจะถูกเพิกถอนหรือหมดอายุ ควรมีการป้องกันเอกสารที่จะลงลายมือชื่อ ค่าลายมือชื่อดิจิทัล รวมถึงแอตทริบิวต์ใด ๆ ที่มีอยู่ในลายมือชื่อดิจิทัลระดับ LT ด้วยการยืนยันเวลา (time-assertion) การยืนยันเวลาหรือการสร้างโทเคนประทับเวลาบนข้อมูลทั้งหมดในลายมือชื่อดิจิทัล (archive time-stamp token) เป็นการเชื่อมโยงข้อมูลทั้งหมดกับจุดเวลาเพื่อสร้างหลักฐานว่าข้อมูลดังกล่าวมีอยู่จริง ณ เวลานั้นที่ระบุในโทเคนประทับเวลา ซึ่งได้รับการรับรองโดยผู้ให้บริการประทับเวลา (time-stamping authority: TSA) ทั้งนี้ การยืนยันเวลาหรือการสร้างโทเคนประทับเวลาควรทำซ้ำในเวลาที่เหมาะสมก่อนที่การป้องกันที่ทำไว้โดยโทเคนประทับเวลาอันก่อนหน้าจะไม่มีความมั่นคงปลอดภัย และควรใช้อัลกอริทึมเข้ารหัสลับที่แข็งแกร่งขึ้นหรือขนาดของกุญแจเข้ารหัสลับที่ยาวขึ้นกว่าที่ใช้ในลายมือชื่อดิจิทัลเดิมหรือโทเคนประทับเวลาอันก่อนหน้า	เพิ่มเติมแอตทริบิวต์จากลายมือชื่อดิจิทัลระดับ LT ดังนี้ – โทเคนประทับเวลาบนข้อมูลทั้งหมดในลายมือชื่อดิจิทัล (archive time-stamp token) จากผู้ให้บริการประทับเวลา (time-stamping authority: TSA)

<u>เอกสารอ้างอิง</u>

(1) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ เลขที่ ขมธอ. 23-2563 เวอร์ชัน 1.0.

(2) ETSI EN 319 102-1 ver 1.3.1 (2021-11) Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

(3) ISO 14533-1:2022 Processes, data elements and documents in commerce, industry and administration; Long term signature; Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES).

(4) ISO 14533-2:2021 Processes, data elements and documents in commerce, industry and administration; Long term signature; Part 2: Profiles for XML Advanced Electronic Signatures (XAdES).

(5) ISO 14533-3:2017 Processes, data elements and documents in commerce, industry and administration; Long term signature; Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES).