เลขที่สิทธิบัตร 114190

สป/200 - ข

สิทธิบัตรการประดิษฐ์

อาศัยอำนาจตามความในพระราชบัญญัติสิทธิบัตร พ.ศ. 2522
อธิบดีกรมทรัพย์สินทางปัญญาออกสิทธิบัตรฉบับนี้ให้แก่

มหาวิทยาลัยธรรมศาสตร์

สำหรับการประดิษฐ์ตามรายละเอียดการประดิษฐ์ ข้อถือสิทธิ และรูปเขียน (ถ้ามี) ดังที่ปรากฏในสิทธิบัตรนี้

เลขที่คำขอ	0901005707
วันขอรับสิทธิบัตร	18 ธันวาคม 2552
ผู้ประดิษฐ์	ศาสตราจารย์อาณัติ ลีมัคเดช
ชื่อที่แสดงถึงการประดิษฐ์	ระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษ

ให้ผู้ทรงสิทธิบัตรนี้มีสิทธิและหน้าที่ตามกฎหมายว่าด้วยสิทธิบัตรทุกประการ

ออกให้ ณ วันที่ 31 เดือน ตุลาคม พ.ศ. 2568

หมดอายุ ณ วันที่ 17 เดือน ธันวาคม พ.ศ. 2572

(นายอาวุธ วงศ์สวัสดิ์)
รองอธิบดีกรมทรัพย์สินทางปัญญา ปฏิบัติราชการแทน
อธิบดีกรมทรัพย์สินทางปัญญา
ผู้ออกสิทธิบัตร

พนักงานเจ้าหน้าที่

หมายเหตุ
1. ผู้ทรงสิทธิบัตรต้องชำระค่าธรรมเนียมรายปีเริ่มตั้งแต่ปีที่ 5 ของอายุสิทธิบัตร มิฉะนั้น สิทธิบัตรนี้จะสิ้นอายุ
2. ผู้ทรงสิทธิบัตรจะขอชำระค่าธรรมเนียมรายปีล่วงหน้าโดยชำระทั้งหมดในคราวเดียวได้
3. การอนุญาตให้ใช้สิทธิตามสิทธิบัตรและการโอนสิทธิบัตรต้องทำเป็นหนังสือและจดทะเบียนต่อพนักงานเจ้าหน้าที่

Ref.256801088768885

รายละเอียดการประดิษฐ์

ชื่อที่แสดงถึงการประดิษฐ์

ระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษ

สาขาวิทยาการที่เกี่ยวข้องกับการประดิษฐ์

เทคโนโลยีสารสนเทศ

ลักษณะและความมุ่งหมายของการประดิษฐ์

ระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษเป็นระบบที่ออกแบบขึ้น เพื่อสนับสนุนการทำธุรกรรมอิเล็กทรอนิกส์ โดยระบบสามารถแปลงลายมือชื่อดิจิตัลให้อยู่ในรูปตัวอักษร และนำมาประกอบกับไฟล์เอกสารหรือข้อความอิเล็กทรอนิกส์ดั้งเดิม เพื่อให้สามารถพิมพ์เป็นเอกสารกระดาษสำหรับผู้ทำธุรกรรมเก็บเป็นหลักฐานได้ และเมื่อต้องการตรวจสอบเอกสารกระดาษดังกล่าว ระบบสามารถแปลงกระดาษตามกระบวนการที่ได้ออกแบบไว้ให้กลับไปอยู่ในรูปอิเล็กทรอนิกส์ เพื่อยืนยันความถูกต้องของเอกสารหลักฐานและยืนยันตัวบุคคลผู้ลงลายมือชื่อได้

ความมุ่งหมายของการประดิษฐ์ระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษนี้ เพื่อลดปัญหาความไม่คุ้นเคยในการใช้ลายมือชื่อดิจิตัลในกระบวนการธุรกรรมอิเล็กทรอนิกส์ ซึ่งโดยทั่วไปกระบวนการลงลายมือชื่อดิจิตัลจะอยู่ในรูปแบบอิเล็กทรอนิกส์ทั้งหมด ผู้ทำธุรกรรมไม่สามารถมองเห็นหรือมีหลักฐานที่จับต้องได้ ทำให้เกิดการหลีกเลี่ยงการใช้เทคโนโลยีดังกล่าว และมีผลให้การใช้ลายมือชื่อดิจิตัลไม่เป็นที่แพร่หลายมากนัก แต่ระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษสามารถแปลงไฟล์ลายมือชื่อดิจิตัลให้กลายเป็นตัวอักษร โดยใช้วิธีการเข้ารหัสแบบ BASE64 และระบบสามารถสร้างยูอาร์แอล (URL) เพื่อใช้ในการตรวจสอบเนื้อความของเอกสารที่พิมพ์ออกมาหรือที่อยู่ในระบบ เอกสารกระดาษที่ได้จากระบบ จะประกอบด้วยข้อความของเอกสารตั้งต้นเดิม ลายมือชื่อดิจิตัล (ที่อยู่ในรูปชุดอักขระที่ผสมผสานทั้งตัวอักษรภาษาอังกฤษพิมพ์เล็กพิมพ์ใหญ่ สัญลักษณ์ และตัวเลข) และ Link address สำหรับการตรวจสอบ หากผู้ทำธุรกรรมต้องการตรวจสอบความถูกต้องของเอกสาร สามารถตรวจสอบ โดยเข้าไปที่ยูอาร์แอล (URL) ที่ระบุในเอกสาร และนำเอาลายมือชื่อที่ปรากฏในเอกสารมาค้นหาในระบบ ดังนั้น ผู้ทำธุรกรรมสามารถตรวจสอบได้ว่าเอกสารกระดาษที่มีการลงลายมือชื่อดิจิตัลไว้นั้น มีการเปลี่ยนแปลงเนื้อความจากต้นฉบับหรือไม่ และใครเป็นผู้ลงลายมือชื่อดังกล่าว

ภูมิหลังของศิลปะหรือวิทยาการที่เกี่ยวข้อง

กระบวนการทำธุรกรรมต่างๆ มักจะยึดถือการลงลายมือชื่อของผู้ที่เกี่ยวข้องบนกระดาษเพื่อเป็นหลักฐานยืนยันว่าผู้ลงลายมือชื่อนั้นยินดีผูกมัดต่อเงื่อนไขตามที่ระบุนั้น เมื่อเปลี่ยนการทำธุรกรรมมาเป็นแบบอิเล็กทรอนิกส์ การลงลายมือชื่อแบบกระดาษจะเปลี่ยนเป็นการลงลายมือชื่อดิจิตัล (Digital Signature) ซึ่งประเทศไทยกำหนดให้ลายมือชื่อดิจิตัลที่ถูกสร้างตามมาตรา 26 ของพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มีผลเสมือนการลงลายมือชื่อบนกระดาษ

ลายมือชื่อดิจิตัล คือ ไฟล์อิเล็กทรอนิกส์ที่มีการเข้ารหัสคู่กับกุญแจส่วนตัว (Private Key) ที่ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ เช่น บริษัท ทีโอที จำกัด (มหาชน) หรือ บริษัท กสท โทรคมนาคม จำกัด

นายสุวัจชัย บุญอารี

(มหาชน) เป็นผู้ออกให้ ปัญหาของลายมือชื่อดิจิตัล คือ กระบวนการทุกอย่างที่เกี่ยวข้องอยู่ในรูปแบบอิเล็กทรอนิกส์ทั้งหมด ตั้งแต่การเข้ารหัส ตลอดจนถึงการถอดรหัสเพื่อตรวจสอบ ซึ่งผู้ทำธุรกรรมไม่สามารถมองเห็นหรือมีหลักฐานที่จับต้องได้ ดังเช่นในระบบกระดาษ ทำให้เป็นอุปสรรคต่อการทำธุรกรรมอิเล็กทรอนิกส์

สิ่งประดิษฐ์นี้ถูกออกแบบให้กระบวนการทำธุรกรรมอิเล็กทรอนิกส์สามารถแปลงมาสู่กระดาษ และสามารถแปลงกระดาษตามกระบวนการที่ออกแบบไว้นี้แปลงกลับไปอยู่ในรูปแบบอิล็กทรอนิกส์ เพื่อทำการตรวจสอบ ยืนยันตัวตนได้ ซึ่งจะทำให้ผู้ทำธุรกรรมมีความไว้วางใจ เพราะมีหลักฐานเป็นกระดาษซึ่งสามารถอ่านออกด้วยตาเปล่า ที่ถูกแปลงจากลายมือชื่อดิจิตัลเก็บไว้ด้วย

สิ่งประดิษฐ์นี้ใช้หลักการแปลงไฟล์ลายมือชื่อดิจิตัลที่เก็บในรูปอักขระฐาน 2 คือ 0 และ 1 ให้อยู่รูปชุดอักขระฐาน 64 ด้วยการเข้ารหัสแบบ BASE64 ผลลัพธ์ที่ได้ คือ ชุดอักขระที่ผสมผสานทั้งตัวอักษรภาษาอังกฤษพิมพ์เล็กพิมพ์ใหญ่ สัญลักษณ์ และตัวเลข เมื่อลายมือชื่อดิจิตัลกลายเป็นตัวอักษร จึงสามารถนำมาประกอบกับไฟล์เอกสารหรือข้อความอิเล็กทรอนิกส์ดั้งเดิมได้ โดยการแทรกต่อท้ายไฟล์เอกสารหรือข้อความนั้นๆ เข้าไป เมื่อผู้ใช้งานต้องการพิมพ์ออกมาเป็นกระดาษจะได้กระดาษที่มีข้อความต้นฉบับ และมีลายมือชื่อดิจิตัลในรูปแบบชุดอักขระฐาน 64 รับรองอยู่ด้านท้าย ซึ่งหมายความว่า สามารถแปลงการรับรองเชิงอิเล็กทรอนิกส์ให้อยู่ในรูปของกระดาษได้ และหากต้องการตรวจสอบความถูกต้อง ตรงกันของข้อความที่ปรากฏอยู่บนกระดาษกับลายมือชื่อดิจิตัลก็สามารถบันทึกชุดอักขระฐาน 64 นี้เข้าสู่ระบบฐานข้อมูลเพื่อตรวจสอบได้ เท่ากับสามารถแปลงจากระบบกระดาษให้อยู่ในรูปอิเล็กทรอนิกส์ได้เช่นกัน

<u>คำอธิบายรูปเขียนโดยย่อ</u>

รูปที่ 1 แสดงกระบวนการบันทึกลายมือชื่อดิจิตัลของระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษ

รูปที่ 2 แสดงกระบวนการจัดเก็บลายมือชื่อดิจิตัลลงฐานข้อมูล

รูปที่ 3 แสดงลักษณะตารางสำหรับจัดเก็บข้อมูลในฐานข้อมูลลายมือชื่อดิจิตัล

รูปที่ 4 แสดงลักษณะตารางสำหรับจัดเก็บข้อมูลในเครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server)

รูปที่ 5 แสดงกระบวนการแสดงลายมือชื่อดิจิตัลบนกระดาษ

รูปที่ 6 แสดงตัวอย่างเอกสารตั้งต้นพร้อมด้วยลายมือชื่อดิจิตัลบนกระดาษ

รูปที่ 7 แสดงกระบวนการตรวจสอบลายมือชื่อดิจิตัล

รูปที่ 8 แสดงกระบวนการตรวจสอบความถูกต้องของเอกสารและยืนยันตัวผู้ส่ง

รูปที่ 9 แสดงลักษณะการทำงานของส่วนป้องกันการเปลี่ยนแปลงข้อมูลโดยผู้ดูแลระบบ

รูปที่ 10 แสดงตัวอย่างหน้าจอผลการตรวจสอบลายมือชื่อดิจิตัลของระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษ

นายสุวัจชัย บุญอารี

<u>การเปิดเผยการประดิษฐ์โดยสมบูรณ์</u>

รายละเอียดของระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษประกอบด้วยขั้นตอน 3 ขั้นตอนหลัก คือ

1. การบันทึกจัดเก็บลายมือชื่อดิจิตัล

กระบวนการบันทึกลายมือชื่อดิจิตัลเป็นไปดัง***รูปที่ 1*** เมื่อมีการลงลายมือชื่อดิจิตัลบนเอกสารอิเล็กทรอนิกส์ ระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษจะนำเอกสารตั้งต้น ***1*** ไปผ่านกระบวนการเข้ารหัสแบบ SHA-1 (Secure Hash Algorithm -1) ***2*** ผลลัพธ์ที่ได้ คือ เมสเซจไดเจสต์ (Message Digest) ***3*** ซึ่งเป็นข้อความที่ใช้เป็นตัวแทนของเนื้อหาเอกสารตั้งต้น ***1*** โดยปกติข้อความสรุปจะมีความยาวน้อยกว่าความยาวของเอกสารตั้งต้น ***1*** มาก กล่าวคือมักมีความยาวอยู่ระหว่าง 128 ถึง 256 บิตโดยไม่ขึ้นกับขนาดความยาวของเอกสารตั้งต้น ***1*** หากมีการเปลี่ยนแปลงข้อมูลตั้งต้นแม้เพียง 1 บิต จะทำให้ เมสเซจไดเจสต์ (Message Digest) ที่ได้ต่างไปโดยสิ้นเชิง หลังจากนั้นระบบจะนำเมสเซจไดเจสต์ (Message Digest) ***3*** มาผ่านกระบวนการเข้ารหัสลายมือชื่อดิจิตัล (Digital Signature Algorithm) ***5*** ด้วยกุญแจส่วนตัว (Private Key) ***4*** (ใช้อัลกอริทึม RSA) ของผู้สร้างข้อมูล จะได้ผลลัพธ์เป็นลายมือชื่อดิจิตัล (Digital Signature) ***6*** ที่อยู่ในรูป BASE64 ขั้นตอนถัดมาระบบจะนำเอาเอกสารตั้งต้น ***1*** เมสเซจไดเจสต์ (Message Digest) ***3*** และลายมือชื่อดิจิตัล ***6*** ไปจัดเก็บลงฐานข้อมูล

กระบวนการจัดเก็บลายมือชื่อดิจิตัลลงฐานข้อมูลเป็นไปตาม***รูปที่ 2*** ขั้นตอนนี้มีทางเลือกให้ผู้ใช้งาน 2 ทางได้แก่ จำกัดสิทธิการเข้าถึงเอกสารตั้งต้น ***1*** หรือไม่จำกัดสิทธิ หากเลือกจำกัดสิทธิระบบจะไม่เก็บเอกสารตั้งต้น ***1*** ลงฐานข้อมูลลายมือชื่อดิจิตัล ***12*** โดยตรง แต่จะนำไปผ่านกระบวนการเข้ารหัส (Encrypt Algorithm) ***9*** ด้วย กุญแจสาธารณะ (Public Key) ***10*** ของกลุ่มผู้ได้รับสิทธิ เพื่อให้ได้ข้อความที่ผ่านกระบวนการเข้ารหัส (Encrypted Message) ***11*** และนำไปบันทึกลงฐานข้อมูลลายมือชื่อดิจิตัล ***12*** สำหรับกรณีที่ไม่จำกัดสิทธิระบบจะนำเอาเอกสารตั้งต้น ***1*** บันทึกลงฐานข้อมูลลายมือชื่อดิจิตัล ***12*** โดยตรง นอกจากการบันทึกเอกสารตั้งต้น ***1*** หรือ ข้อความที่ผ่านกระบวนการเข้ารหัส (Encrypted Message) ***11*** แล้ว เมสเซจไดเจสต์ (Message Digest) ***3*** และลายมือชื่อดิจิตัล ***6*** จะถูกบันทึกลงฐานข้อมูลลายมือชื่อ ดิจิตัล ***12*** ในเวลาเดียวกัน เมื่อเกิดการบันทึกระบบจะสร้างรหัสอ้างอิง ***13*** ซึ่งเป็นตัวเลขที่ไม่ซ้ำกัน (Unique Number) สำหรับแต่ละลายมือชื่อดิจิตัลโดยอัตโนมัติ (ตัวเลขที่ไม่ซ้ำกันจะเริ่มต้นจาก 1 ไปจนถึง 9,999,999,999,999) ข้อมูลทั้งหมดจะถูกบันทึกลงตารางในฐานข้อมูล ***16*** ที่มีลักษณะดัง***รูปที่ 3*** นอกจากนี้ยังมีการส่งข้อมูลส่วนหนึ่งผ่านเครือข่ายอินเตอร์เน็ตด้วยโปรโตคอล TCP/IP ไปเก็บไว้ที่เครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server) ***14***

เครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server) ***14*** ถูกจัดตั้งแยกออกจากระบบหลักที่ใช้งาน มีการรักษาความปลอดภัยเป็นไปตามมาตรฐาน ISO BS17799 ผู้ดูแลระบบหลักไม่สามารถเข้าถึงเครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server) ***14*** นี้ได้ ผู้ที่เข้าถึงได้จะเป็นเพียงผู้ตรวจสอบข้อมูล (Auditor) เท่านั้น ข้อมูลที่ถูกส่งไปจัดเก็บที่เครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server) ***14*** ได้แก่ รหัสอ้างอิง ***13*** ที่ได้จากระบบหลัก ***15*** และเมสเซจไดเจสต์ (Message Digest) ***3*** มีลักษณะตารางสำหรับจัดเก็บข้อมูล ***17*** ดัง***รูปที่ 4***

นายสุวัจชัย บุญอารี

การแสดงลายมือชื่อดิจิตัลบนกระดาษ

การแสดงลายมือชื่อดิจิตัลบนกระดาษในที่นี้ คือ การแสดงเอกสารตั้งต้นพร้อมกับลายมือชื่อดิจิตัลในกระดาษแผ่นเดียวหรือชุดเดียวกัน โดยมีกระบวนการทำงานดัง***รูปที่ 5*** โดยเริ่มจากการสั่งพิมพ์เอกสารตั้งต้นพร้อมแสดงลายมือชื่อดิจิตัล ***18*** ผ่านระบบ ระบบจะดึงข้อมูลจากฐานข้อมูลลายมือชื่อดิจิตัล ***12*** ได้แก่ ลายมือชื่อดิจิตัล ***6*** และเอกสารตั้งต้น ***1*** ในกรณีที่มีการจำกัดสิทธิการเข้าถึงเอกสารตั้งต้น ***1*** จะใช้การนำ ข้อความที่ผ่านกระบวนการเข้ารหัส (Encrypted Message) ***11*** จากฐานข้อมูลมาผ่านกระบวนการถอดรหัส (Decrypt Algorithm) ***19*** ด้วยกุญแจส่วนตัว (Private Key) ***20*** ของผู้สั่งพิมพ์ เพื่อให้ได้เอกสารตั้งต้น ***1*** เช่นเดียวกับเอกสารที่ไม่ถูกจำกัดสิทธิ เมื่อได้ลายมือชื่อดิจิตัล ***6*** และเอกสารตั้งต้น ***1*** แล้ว ระบบจะสร้างยูอาร์แอล (URL) ***22*** สำหรับการเรียกตรวจสอบผ่านเครือข่ายอินเตอร์เน็ตเพื่อใช้ในการตรวจสอบเนื้อความของเอกสารที่พิมพ์ออกมาหรือที่อยู่ในระบบ เมื่อผ่านกระบวนการผนวกเอกสารและลายมือชื่อดิจิตัล ***21*** รวม 3 องค์ประกอบ และพิมพ์ผ่านเครื่องพิมพ์เอกสาร ***23*** จะได้เอกสารใหม่ คือ เอกสารตั้งต้นพร้อมแสดงลายมือชื่อดิจิตัล ***24*** ที่มีข้อความของเอกสารตั้งต้น ***1*** ลายมือชื่อดิจิตัล ***6*** และยูอาร์แอล (URL) ***22*** สำหรับการเรียกตรวจสอบต่อท้าย โดยลายมือชื่อดิจิตัล ***6*** จะปรากฏในรูปอักขระจำนวน 436 อักขระภายในกรอบสี่เหลี่ยม ตัวอย่างของเอกสาร คือ ***รูปที่ 6***

2. การตรวจสอบลายมือชื่อดิจิตัล

กระบวนการตรวจสอบโดยรวมเป็นไปดัง***รูปที่ 7*** แบ่งเป็น

- ☐ ส่วนสำหรับตรวจสอบลายมือชื่อดิจิตัลและความถูกต้องของเอกสาร
- ☐ ส่วนสำหรับป้องกันการเปลี่ยนแปลงข้อมูลโดยผู้ดูแลระบบ

ในส่วนแรก ผู้ที่ต้องการตรวจสอบเอกสารตั้งต้นพร้อมแสดงลายมือชื่อดิจิตัล ***24*** ที่พิมพ์ออกมาบนกระดาษ สามารถทำได้โดยพิมพ์ยูอาร์แอล (URL) ***22*** ที่ระบุในเอกสารเพื่อเข้าสู่ส่วนค้นหาลายมือชื่อดิจิตัล ***25*** จากนั้น ระบบตรวจสอบความถูกต้องของเอกสารและยืนยันตัวผู้ส่ง ***26*** จะทำการตรวจสอบว่าเอกสารนั้นๆ มีการเปลี่ยนแปลงหรือไม่ ใครเป็นผู้ลงลายมือชื่อดังกล่าว ในขั้นตอนนี้ผู้ตรวจสอบสามารถสังเกตเอกสารตั้งต้นที่ปรากฏในยูอาร์แอล (URL) ***22*** ที่เรียกดูด้วยตาเปล่าเพื่อดูว่าตรงกับกระดาษที่กำลังตรวจสอบหรือไม่ กระบวนการตรวจสอบโดยระบบเป็นไปดัง***รูปที่ 8*** เริ่มจากการดึงข้อมูล เมสเซจไดเจสต์ (Message Digest) ***3*** และลายมือชื่อดิจิตัล ***6*** จากฐานข้อมูลลายมือชื่อดิจิตัล ***12*** ที่กำลังตรวจสอบ ถัดมาระบบจะนำลายมือชื่อดิจิตัล ***6*** มาผ่านกระบวนการถอดรหัส ***28*** ด้วยกุญแจสาธารณะ(Public Key) ***29*** ของผู้สร้างเอกสาร จะทำให้ได้เมสเซจไดเจสต์ (Message Digest) ***30*** อีกตัวหนึ่ง จากนั้นทำการเปรียบเทียบเมสเซจไดเจสต์ (Message Digest) ***31*** ทั้ง 2 ด้วยกัน และแสดงผลการตรวจสอบ ***32*** ให้ผู้ตรวจสอบทราบ โดย เมสเซจไดเจสต์ (Message Digest) ***3*** และ เมสเซจไดเจสต์ (Message Digest) ***30*** ทั้ง 2 ตัว จะต้องตรงกัน จึงจะกล่าวได้ว่าเอกสารไม่ได้ถูกเปลี่ยนแปลง หากไม่ตรงกันหมายความว่าเอกสารมีการเปลี่ยนแปลงเกิดขึ้น ***รูปที่ 10*** แสดงตัวอย่างผลลัพธ์ตรวจสอบเอกสาร

นายสุวัจชัย บุญอารี

ส่วนที่สอง คือ การป้องกันการเปลี่ยนแปลงข้อมูลโดยผู้ดูแลระบบ จะใช้ข้อมูลจาก 2 แหล่งมาทำการเปรียบเทียบ คือ จากฐานข้อมูลลายมือชื่อดิจิตัล ***12*** ของระบบหลัก ***15*** และจากเครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server) ***14*** ขั้นตอนดัง ***รูปที่ 7*** ผู้ที่เป็นผู้ตรวจสอบข้อมูล (Auditor) เท่านั้นจึงจะใช้งานส่วนนี้ได้ เมื่อผู้ตรวจสอบข้อมูล (Auditor) ผ่านการพิสูจน์ตัวตน (Authentication) ***33*** แล้วจะต้องระบุรหัสอ้างอิงที่ต้องการตรวจสอบ ***34*** เข้าในระบบ จากนั้นส่วนป้องกันการเปลี่ยนแปลงข้อมูลโดยผู้ดูแลระบบ ***27*** จะดึงข้อมูลจากเครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server) ***14*** ผ่านโปรโตคอล TCP/IP โดยดึงข้อมูลเฉพาะที่มีรหัสอ้างอิงตรงกับที่ผู้ตรวจสอบข้อมูล (Auditor) ได้ระบุรหัสอ้างอิงที่ต้องการตรวจสอบ ***34*** ระบบจะนำเมสเซจไดเจสต์ (Message Digest) จากระบบหลัก ***15*** และเครื่องแม่ข่ายที่เชื่อถือได้ (Trusted Server) ***14*** ที่มีรหัสอ้างอิงตรงกันมาเปรียบเทียบกัน ดัง***รูปที่ 9*** โดยเมสเซจไดเจสต์ (Message Digest) จากทั้ง 2 แหล่งนี้จะต้องตรงกันจึงจะถือว่าไม่มีการเปลี่ยนแปลงโดยผู้ดูแลระบบของระบบหลัก

<u>วิธีการในการประดิษฐ์ที่ดีที่สุด</u>

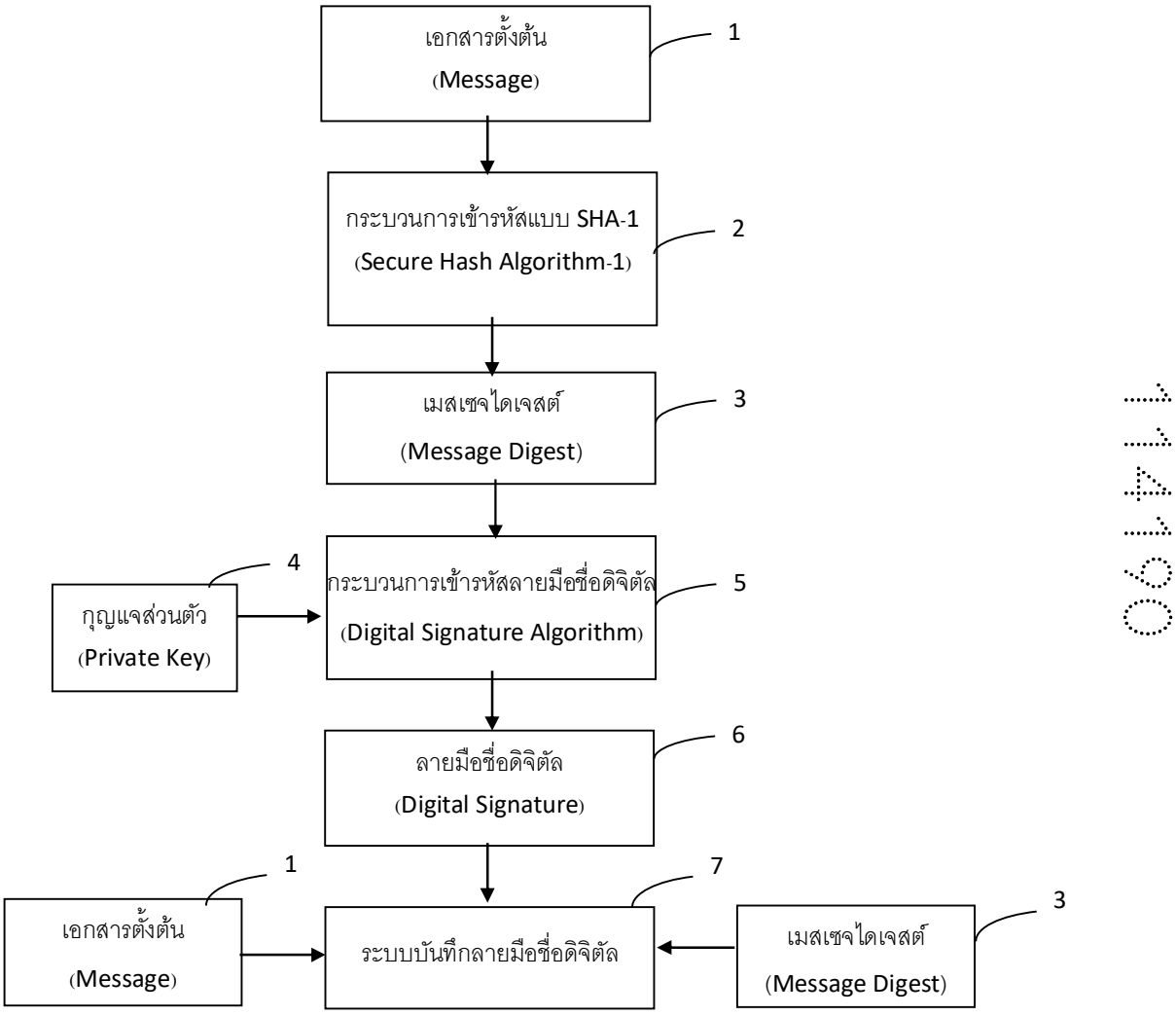
วิธีการประดิษฐ์ที่ดีที่สุดได้บรรยายไว้ในหัวข้อการเปิดเผยการประดิษฐ์โดยสมบูรณ์แล้ว

นายสุวัจชัย บุญอารี

ข้อถือสิทธิ

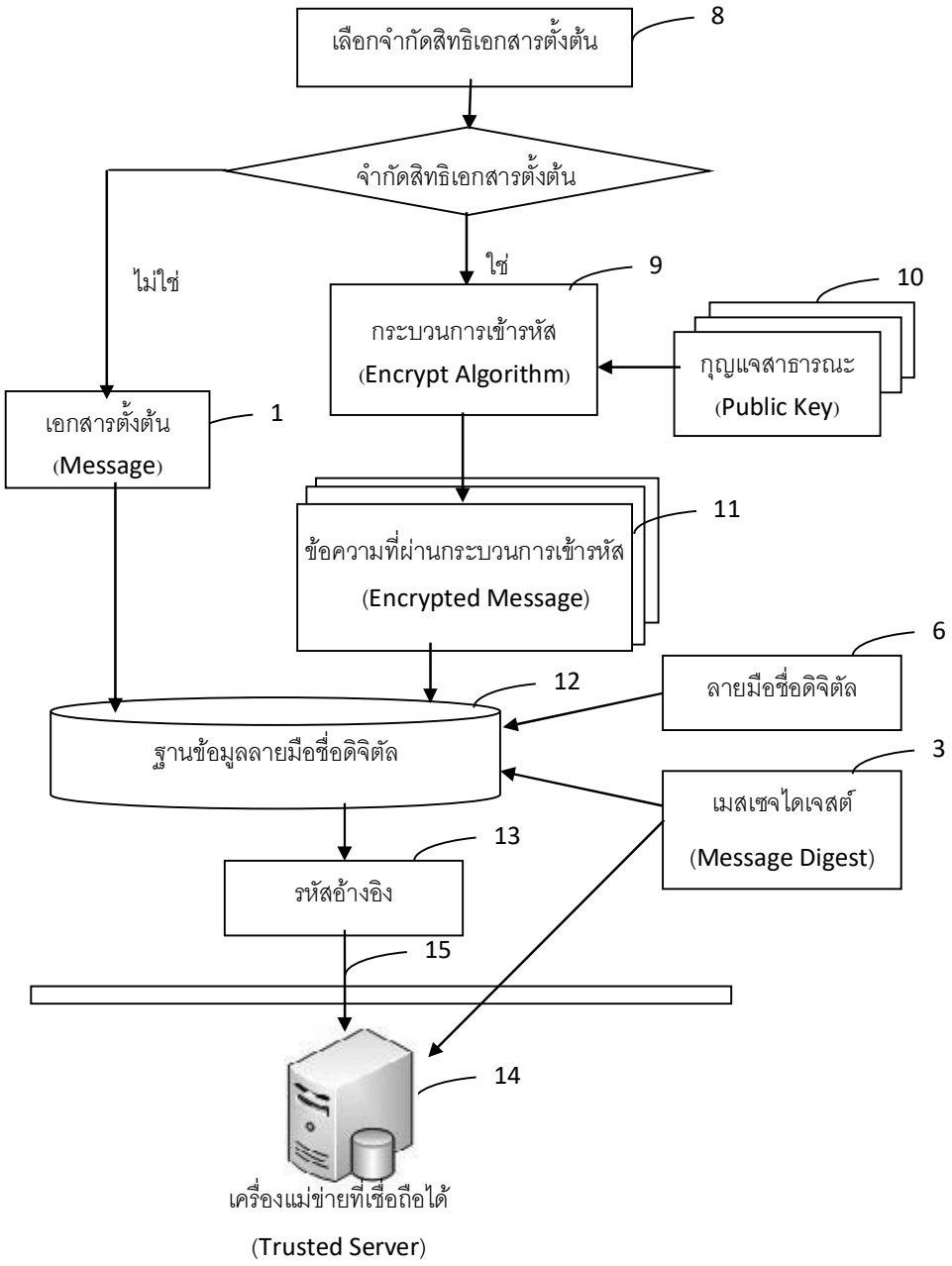
1. กระบวนการตรวจสอบลายมือชื่อดิจิตัลเพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยผู้ดูแลระบบ ใช้กระบวนการบันทึกจัดเก็บลายมือชื่อดิจิตัลลงฐานข้อมูล 2 แห่งแยกออกจากกัน คือ ฐานข้อมูลลายมือชื่อดิจิตัล (12) ของระบบหลัก (15) และฐานข้อมูลจากเครื่องแม่ข่ายที่เชื่อถือได้ (14) โดยที่ระบบหลัก (15) เก็บเอกสารตั้งต้น (1) หรือข้อความที่ผ่านกระบวนการเข้ารหัส (11) เมสเซจไดเจสต์ (3) และลายมือชื่อดิจิตัล (6) พร้อมรหัสอ้างอิง (13) ซึ่งเป็นเลขที่ไม่ซ้ำกันเริ่มต้นจาก 1 ไปจนถึง 9,999,999,999,999 ขณะที่เครื่องแม่ข่ายที่เชื่อถือได้ (14) เก็บเฉพาะเมสเซจไดเจสต์ (3) และรหัสอ้างอิง (13) ที่ได้จากระบบหลัก (15) การส่งข้อมูลไปยังเครื่องแม่ข่ายที่เชื่อถือได้ (14) ใช้การส่งข้อมูลผ่านโปรโตคอล TCP/IP บนเครือข่ายอินเตอร์เน็ต ในการตรวจสอบ ผู้ตรวจสอบข้อมูล (Auditor) ที่มีสิทธิเข้าถึงข้อมูลได้ จะระบุรหัสอ้างอิงที่ต้องการตรวจสอบ (34) เพื่อเปรียบเทียบกับรหัสอ้างอิง (13) จากเครื่องแม่ข่ายที่เชื่อถือได้ (14) ระบบจะนำเมสเซจไดเจสต์ (3) จากเครื่องแม่ข่ายที่เชื่อถือได้ (14) และจากระบบหลัก (15) มาเปรียบเทียบกัน หากเมสเซจไดเจสต์ทั้ง 2 แหล่งนี้ตรงกันจะถือได้ว่าไม่มีการเปลี่ยนแปลงโดยผู้ดูแลระบบของระบบหลัก (15)

นายสุวัจชัย บุญอารี



รูปที่ 1

นายสุวัจชัย บุญอารี



รูปที่ 2

นายสุวัจชัย บุญอารี

16

รหัสอ้างอิง	เมสเซจไดเจสต์ (Message Digest)	ลายมือชื่อดิจิตัล (Digital Signature)	เอกสารตั้งต้น (Message)	ข้อความที่ผ่านกระบวนการเข้ารหัส (Encrypted Message)	,,,

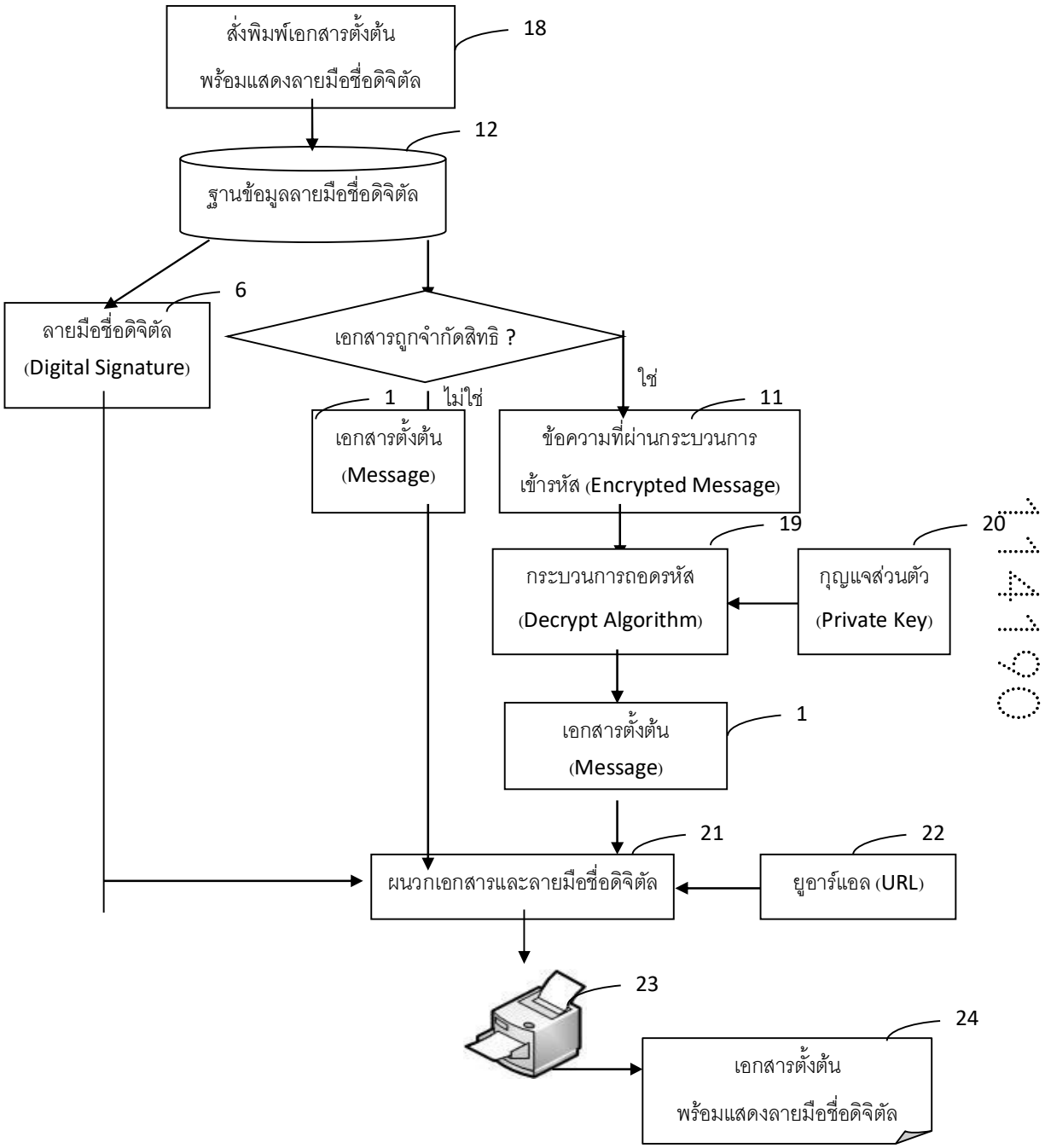
รูปที่ 3

17

รหัสอ้างอิง	เมสเซจไดเจสต์ (Message Digest)	,,,

รูปที่ 4

นายสุวัจชัย บุญอารี



รูปที่ 5

นายสุวัจชัย บุญอารี

รูปเขียน

ที่ ทส 2552/2

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เลขที่ 120 ม.3 ชั้น 6-9 อาคารรวมหน่วยราชการบี
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพฯ 10210

31 กรกฎาคม 2552

เรื่อง ขอสงวนสิทธิการหักเงินค่าจ้างเหมาเอกชนทำงาน

เรียน นายนิยม ชมชอบ

อ้างถึง 1. ข้อตกลงจ้างเหมาเอกชน เลขที่ 001/2552 ลงวันที่ 1 มกราคม 2552
2. รายงานเวลามาปฏิบัติงาน ที่ กคพ.บก.

ตามหนังสือที่อ้างถึง 1 สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ว่าจ้าง นายนิยม ชมชอบ เป็นผู้รับจ้างทำงาน เป็นเงินจำนวน 132,360.00 บาท (หนึ่งแสนสามหมื่นสองพันสามร้อยหกสิบบาทถ้วน) โดยในขอบเขตการทำงาน 4 กำหนดไว้ว่า ในกรณีที่ผู้รับจ้างมาสายเกินกว่าเวลาที่กำหนดหักเงินค่าจ้างเป็นรายชั่วโมง ดังนี้ มาสายตั้งแต่เวลา 08.46-09.30 น. คิดเป็น 1 ชั่วโมง และส่วนเกินของแต่ละชั่งโมงคิดค่าปรับเป็น 1 ชั่วโมง (ชั่วโมงละ 43.00 บาท) นั้น

ปรากฏว่า วันที่ 1, 2, 22 ผู้รับจ้างมาสายเกินกว่าเวลาที่กำหนดหักเงินค่าจ้างเป็นรายชั่งโมง วันที่ 3, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17, 20, 27, 28, 29, 30, 31 ผู้รับจ้างขาดงาน สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้คำนวณค่าปรับที่ผู้รับจ้างจะต้องชำระตามข้อตกลงแล้ว จำนวน 3 ชั่วโมง x 43.00 เป็นเงินจำนวน 129.00 บาท (หนึ่งร้อยยี่สิบเก้าบาทถ้วน) ขาดงาน 17 วัน x 337.00 เป็นเงินจำนวน 5,729.00 บาท (ห้าพันเจ็ดร้อยยี่สิบเก้าบาทถ้วน)

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจึงขอสงวนสิทธิการหักเงินค่าจ้างและเรียกค่าปรับตามจำนวนดังกล่าวข้างต้น โดยจะดำเนินการหักเงินค่าปรับจากเงินค่าจ้างต่อไป

จึงเรียนมาเพื่อโปรดทราบ

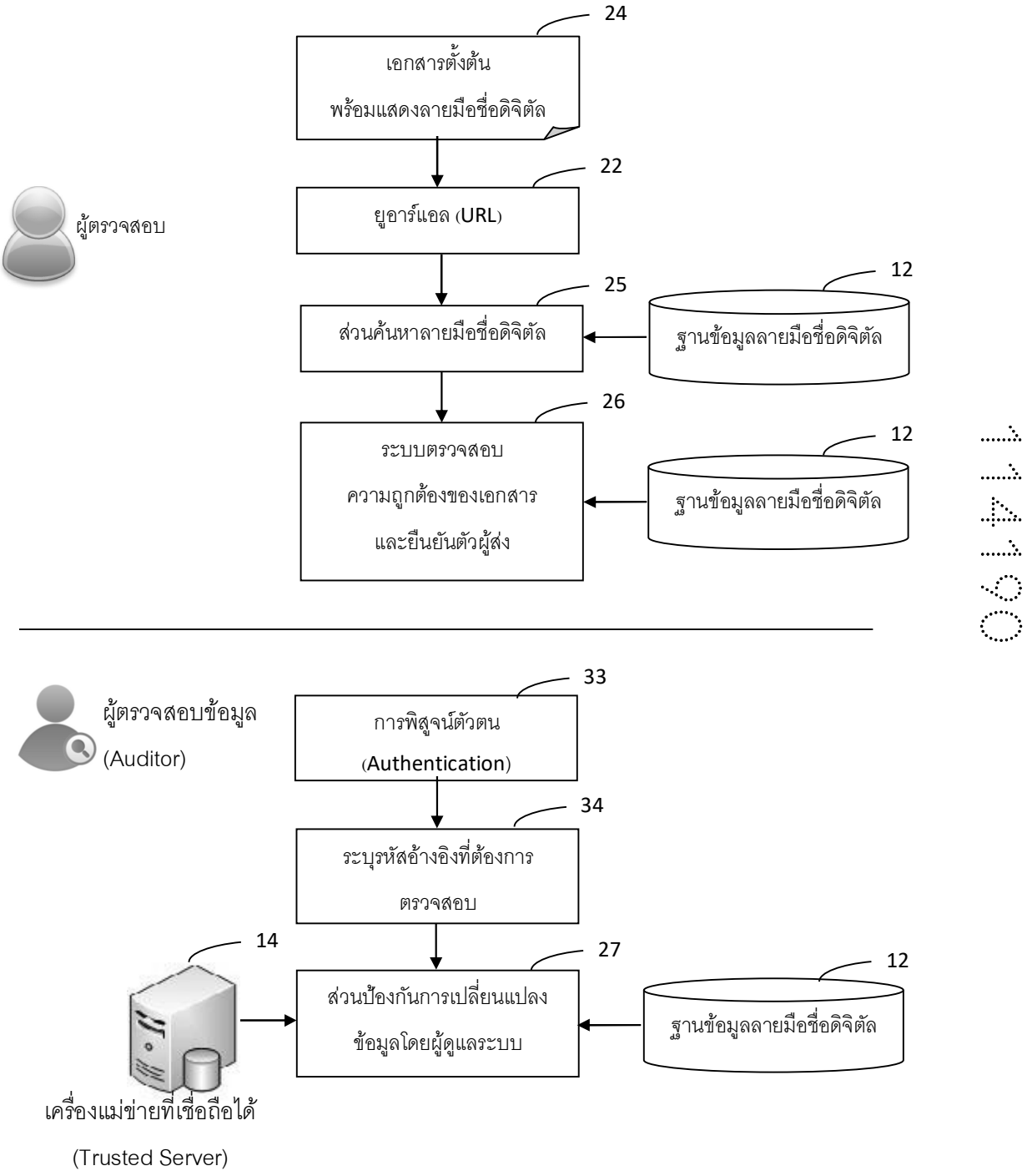
ความเห็น ผอ.บก. เห็นชอบ
เหตุผล :

(นายนิยม ชมชอบ)
ผอ.กคพ.ปฏิบัติราชการแทน
ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

MIIE0gYJKoZIhvcNAQcCoIIEwzCCBL8CAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
DQEHAaCCA3AwggNsMIICVKADAgECAgMDSMowDQYJKoZIhvcNAQEFBQAwfDELMAkG
A1UEBhMCVEgxEDAOBgNVBAcTB0Jhbmdrb2sxLzAtBgNVBAoTJlRPVCBDb3Jwb3Jh
dGlvbiBQdWJsaWMgQ29tcGFueSBMaW1pdGVkMRkwFwYDVQQLExBlQnVzaW5lc3Mg
AQUABIGADGpU+A/nAkDVi0Rpxq4XRHetHi4n6aOWHPOIgsEzeDiZVS+VWhSn65Ia
J7zn9L7ndZFi+PMPLXtlQC5pKMdKM8XwFwcCmbYFtijXkBhwff/xqv/6yJXwCJtj
GXl0r231ArdboDsccyfvmPDCXnHq+HWIGoOYb5AvKuYBmLDZYTE=

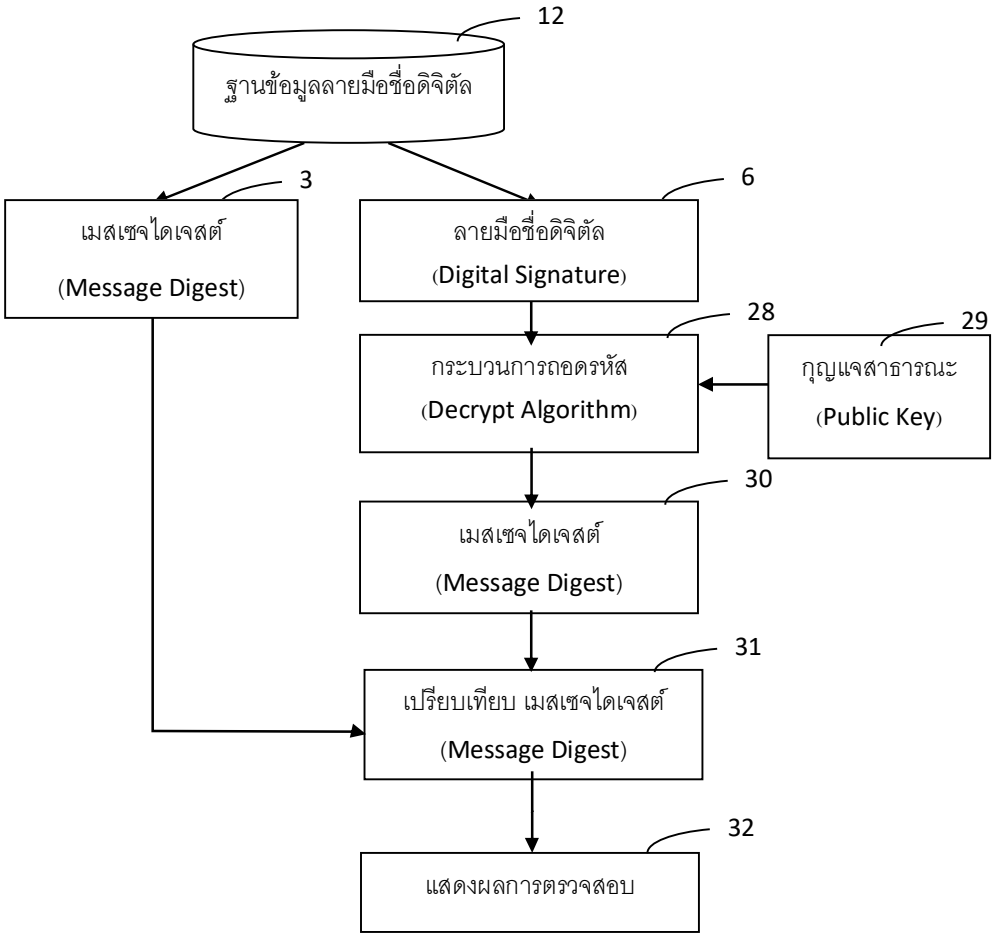
รูปที่ 6

นายสุวัจชัย บุญอารี



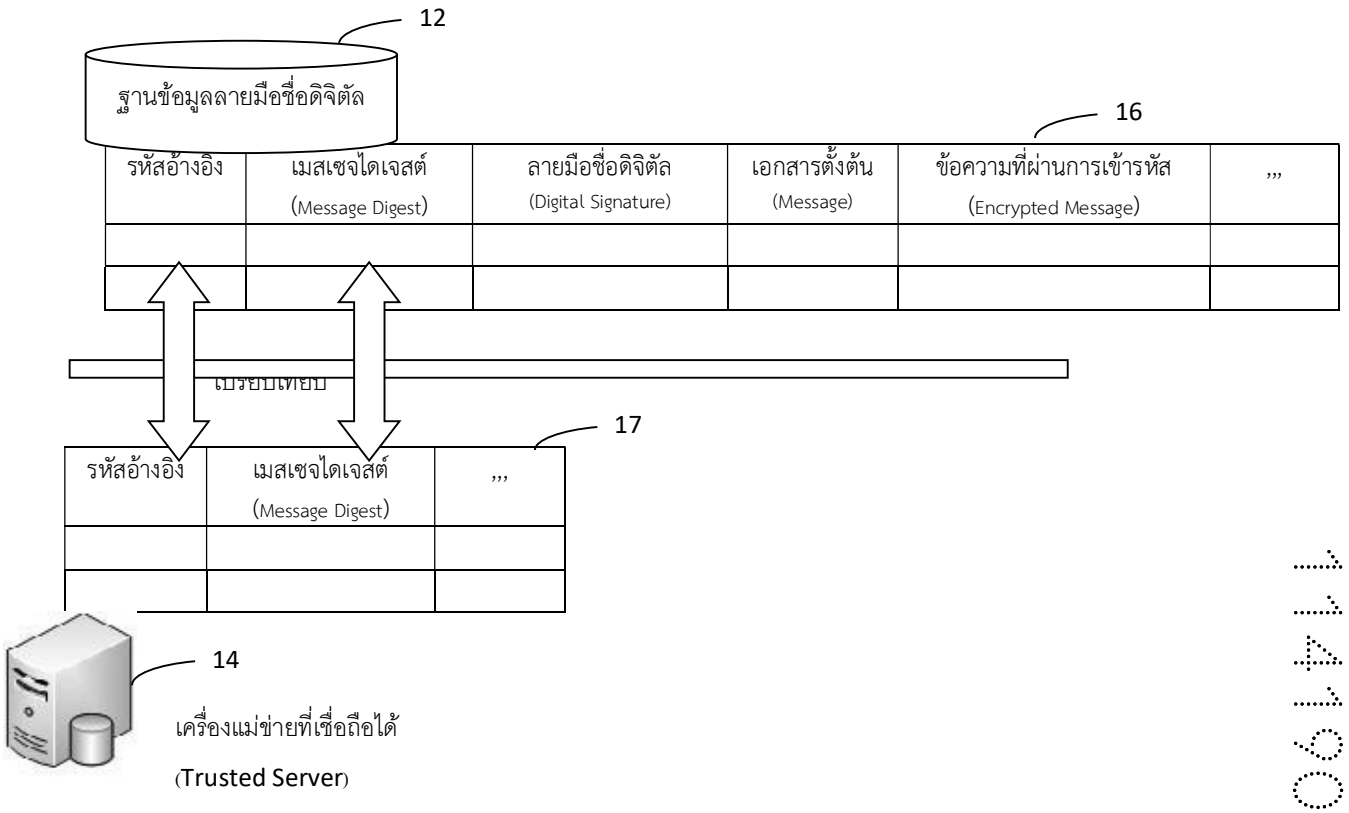
รูปที่ 7

นายสุวัจชัย บุญอารี

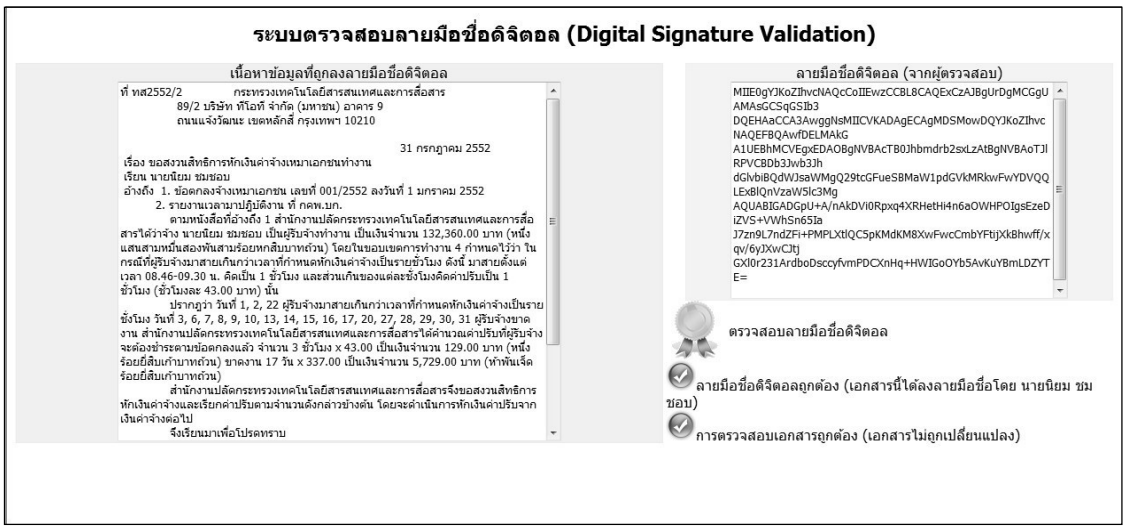


รูปที่ 8

นายสุวัจชัย บุญอารี



รูปที่ 9



รูปที่ 10

นายสุวัจชัย บุญอารี

บทสรุปการประดิษฐ์

ระบบแสดงและตรวจสอบลายมือชื่อดิจิตัลบนกระดาษนี้ เป็นระบบที่ออกแบบขึ้นเพื่อสนับสนุนการใช้ลายมือชื่อดิจิตัลในการทำธุรกรรมอิเล็กทรอนิกส์ โดยระบบสามารถแปลงไฟล์ลายมือชื่อดิจิตัลให้อยู่ในรูปชุดอักขระที่ผสมผสานทั้งตัวอักษรภาษาอังกฤษพิมพ์เล็ก พิมพ์ใหญ่ สัญลักษณ์ และตัวเลข โดยวิธีการเข้ารหัสแบบ BASE64 และนำลายมือชื่อดิจิตัลที่กลายเป็นตัวอักษรนี้มาประกอบกับไฟล์เอกสารหรือข้อความอิเล็กทรอนิกส์ดั้งเดิมได้ โดยการแทรกต่อท้ายไฟล์เอกสารหรือข้อความนั้นๆ เข้าไป พร้อมทั้งสร้าง Link Address (URL) เพื่อการตรวจสอบความถูกต้องของเนื้อความในเอกสาร เมื่อผู้ใช้งานต้องการพิมพ์ออกมาเป็นกระดาษจะได้กระดาษที่มีข้อความต้นฉบับ และมีลายมือชื่อดิจิตัลในรูปแบบชุดอักขระฐาน 64 รับรองอยู่ด้านท้าย กระบวนการดังกล่าว ทำให้สามารถแปลงการรับรองเชิงอิเล็กทรอนิกส์ให้อยู่ในรูปของกระดาษได้

หากผู้ใช้งานต้องการตรวจสอบข้อมูลอิเล็กทรอนิกส์พร้อมลายมือชื่อดิจิตัลที่พิมพ์ออกมาบนกระดาษ สามารถใช้ Link address (URL) ที่ระบุในเอกสารเพื่อเข้าสู่กระบวนการตรวจสอบ ระบบจะตรวจสอบความถูกต้องของเอกสารและยืนยันตัวบุคคล โดยทำการตรวจสอบว่าเอกสารนั้นๆ มีการเปลี่ยนแปลงจากต้นฉบับหรือไม่ และผู้ลงลายมือชื่อเป็นใคร กระบวนการดังกล่าวจึงเท่ากับสามารถแปลงจากระบบกระดาษให้กลับมาอยู่ในรูปอิเล็กทรอนิกส์ได้เช่นกัน

นายสุวัจชัย บุญอารี