ประกาศสำนักงานนโยบายและแผนการขนส่งและจราจร

เรื่อง การบริหารจัดการระบบตั๋วร่วมและมาตรฐานทางเทคโนโลยีของระบบตั๋วร่วม

พ.ศ. ๒๕๖๙

อาศัยอำนาจตามความในมาตรา ๑๓ (๓) (ก) (ข) (ค) และ (ง) แห่งพระราชบัญญัติการบริหารจัดการระบบตั๋วร่วม พ.ศ. ๒๕๖๘ ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร โดยความเห็นชอบของคณะกรรมการนโยบายระบบตั๋วร่วม จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานนโยบายและแผนการขนส่งและจราจร เรื่อง การบริหารจัดการระบบตั๋วร่วมและมาตรฐานทางเทคโนโลยีของระบบตั๋วร่วม พ.ศ. ๒๕๖๙”

ข้อ ๒ ในประกาศนี้

“บัตรชำระค่าโดยสาร” หมายความว่า บัตรหรือสิ่งอื่นใดที่ใช้แทนบัตรเพื่อชำระค่าโดยสารระบบขนส่งสาธารณะ

“เครื่องอ่านบัตร” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ติดตั้ง ณ ประตูผ่านเข้าออกสถานี (Gate) หรือจัดให้มีไว้ที่พาหนะที่ใช้ในระบบขนส่งสาธารณะ เพื่อใช้ตรวจสอบสิทธิในการเดินทางจากบัตรชำระค่าโดยสาร และจัดส่งข้อมูลธุรกรรมไปยังระบบประมวลผล

“มาตรฐาน Thai ABT” (Thai Account-Based Ticketing) หมายความว่า มาตรฐานการชำระค่าโดยสารสำหรับระบบขนส่งสาธารณะแบบอ้างอิงบัญชีผู้ใช้ (Account-Based Ticketing) ของประเทศไทย

ข้อ ๓ มาตรฐานสำหรับการดำเนินการของผู้รับใบอนุญาตประกอบกิจการระบบตั๋วร่วม รวมทั้งการพัฒนาและการปรับปรุงระบบและอุปกรณ์ให้เป็นไปตามที่กำหนดในประกาศนี้

หมวด ๑
มาตรฐานทางเทคโนโลยีของระบบตั๋วร่วมและรูปแบบของบัตรโดยสาร

ข้อ ๔ บัตรชำระค่าโดยสารแต่ละประเภทต้องเป็นไปตามมาตรฐานทางเทคโนโลยีของระบบตั๋วร่วมอย่างหนึ่งอย่างใด ดังต่อไปนี้

(๑) บัตรชำระค่าโดยสารประเภทบัตรอิเล็กทรอนิกส์แบบไร้สัมผัสมาตรฐาน EMV (EMV Contactless Card) และอุปกรณ์สื่อสารระยะใกล้ (NFC) ต้องเป็นไปตามข้อกำหนดทางเทคนิค EMV Contactless Specifications ล่าสุดที่กำหนดโดยองค์กร EMVCo และต้องได้รับการรับรอง (Type Approval) จากเครือข่ายชำระเงิน (Payment Scheme) ที่เกี่ยวข้อง

(๒) บัตรชำระค่าโดยสารประเภทรหัสคิวอาร์ (QR Code) ต้องเป็นไปตามแนวนโยบายการใช้มาตรฐาน Thai ABT ในธุรกรรมการชำระเงินที่ธนาคารแห่งประเทศไทยกำหนด และมาตรฐาน QR Code ตามที่กำหนดโดยภาคอุตสาหกรรมการชำระเงินของไทย

ข้อ ๕ เครื่องอ่านบัตรต้องมีคุณลักษณะทางเทคนิคที่สามารถรองรับการอ่านบัตรชำระค่าโดยสารได้ทุกประเภท ได้แก่ บัตรอิเล็กทรอนิกส์แบบไร้สัมผัสมาตรฐาน EMV (EMV Contactless Card) อุปกรณ์สื่อสารระยะใกล้ (NFC) และบัตรชำระค่าโดยสารประเภทรหัสคิวอาร์ (QR Code) ทั้งนี้ ต้องเป็นไปตามมาตรฐานทางเทคโนโลยี ดังต่อไปนี้

(๑) มาตรฐานเพื่อรองรับบัตรอิเล็กทรอนิกส์และอุปกรณ์สื่อสารระยะใกล้ (NFC) ต้องสอดคล้องตามมาตรฐานอุตสาหกรรม ISO/IEC 14443 และรองรับมาตรฐาน NFC Forum ภายใต้มาตรฐาน EMVCo ดังนี้

(ก) EMVCo Level 1 Contactless Interface Approval สำหรับส่วนฮาร์ดแวร์และภาครับส่งสัญญาณวิทยุ

(ข) EMVCo Level 2 Contactless Kernel Approval สำหรับส่วนซอฟต์แวร์ประมวลผลคำสั่งโดยต้องรองรับเคอร์เนล (Kernel) ของผู้ให้บริการบัตรรายหลักได้อย่างน้อย ๓ ราย

(๒) มาตรฐานเพื่อรองรับรหัสคิวอาร์ ต้องมีโมดูลอ่านภาพที่สามารถประมวลผลรหัสคิวอาร์ได้ทั้งรูปแบบภาพนิ่ง (Static QR Code) และรูปแบบพลวัต (Dynamic QR Code) แนวนโยบายการใช้มาตรฐาน Thai ABT ในธุรกรรมการชำระเงินที่ธนาคารแห่งประเทศไทยกำหนด และมาตรฐาน QR Code ตามที่กำหนดโดยภาคอุตสาหกรรมการชำระเงินของไทย

เครื่องอ่านบัตรในแต่ละจุดต้องมีมาตรฐานตาม (๑) และ (๒) ในอุปกรณ์เดียวหรือหลายอุปกรณ์ร่วมกันก็ได้

เครื่องอ่านบัตรที่รองรับเคอร์เนลครบถ้วนตาม (๑) (ข) แต่มาจากผู้ผลิตต่างรายต้องได้รับการยอมรับให้นำมาใช้ทำงานร่วมกัน (Interoperability) กับระบบศูนย์บริหารจัดการรายได้กลาง

ข้อ ๖ ประสิทธิภาพในการประมวลผลรายการ (Transaction Speed) ของเครื่องอ่านบัตรต้องเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

(๑) ระยะเวลาตั้งแต่เริ่มแตะสื่อชำระค่าโดยสารจนถึงการแสดงผลหรือการเปิดประตู (Tap-to-Action) ไม่เกิน ๕๐๐ มิลลิวินาที (๐.๕ วินาที) สำหรับบัตรชำระค่าโดยสารประเภท EMV และไม่เกิน ๗๐๐ มิลลิวินาที (๐.๗ วินาที) สำหรับบัตรชำระค่าโดยสารประเภทรหัสคิวอาร์ (QR Code) เว้นแต่เป็นข้อจำกัดของระบบซึ่งต้องได้รับความเห็นชอบจากสำนักงาน

(๒) สามารถรองรับอัตราการไหลเวียนของผู้โดยสาร (Throughput) ได้ไม่น้อยกว่า ๔๕ คนต่อนาที ต่อหนึ่งช่องทาง เว้นแต่เป็นข้อจำกัดของระบบซึ่งต้องได้รับความเห็นชอบจากสำนักงาน

ข้อ ๗ เครื่องอ่านบัตรต้องมีหน่วยความจำภายในสำหรับจัดเก็บ “บัญชีระงับสิทธิ” (Deny List/ Blacklist) และต้องมีความสามารถในการตรวจสอบสถานะของสื่อชำระค่าโดยสารกับบัญชีระงับสิทธิได้ทันที (Local Validation) โดยไม่ต้องรอการเชื่อมต่อกับระบบศูนย์บริหารจัดการรายได้กลางในขณะทำรายการ

ทั้งนี้ การจัดการบัญชีระงับสิทธิดังกล่าวต้องสอดคล้องกับการดำเนินการของศูนย์บริหารจัดการรายได้กลาง

ข้อ ๘ ในกรณีที่ระบบเครือข่ายสื่อสารขัดข้อง เครื่องอ่านบัตรต้องมีความสามารถในการทำงานแบบออฟไลน์ (Offline Capability) โดยการบันทึกข้อมูลธุรกรรม (Store and Forward) ไว้ในหน่วยความจำภายในได้อย่างน้อย ๗ วัน โดยเครื่องอ่านบัตรต้องมีความจุหน่วยความจำขั้นต่ำที่เพียงพอต่อข้อมูลธุรกรรมที่ค้างส่งและพื้นที่จัดเก็บบัญชีระงับสิทธิ (Deny List) และต้องจัดให้มีการเข้ารหัสข้อมูลขณะจัดเก็บ (Encryption-at-rest) การป้องกันการแก้ไขข้อมูลย้อนหลัง (Integrity/Anti-tamper) การควบคุมสิทธิ์การเข้าถึง และต้องส่งข้อมูลดังกล่าวไปยังศูนย์บริหารจัดการรายได้กลางทันทีเมื่อระบบเครือข่ายกลับมาใช้งานได้ปกติ

หมวด ๒
มาตรฐานการเชื่อมต่อระบบตั๋วร่วมระหว่างผู้รับใบอนุญาต

ข้อ ๙ ระบบฐานข้อมูลของผู้รับใบอนุญาตการให้บริการออกบัตรชำระค่าโดยสารในระบบตั๋วร่วมและผู้รับใบอนุญาตการให้บริการระบบตั๋วร่วมในระบบขนส่งสาธารณะจะต้องเชื่อมต่อข้อมูลไปยังระบบของศูนย์บริหารจัดการรายได้กลาง โดยระบบฐานข้อมูลดังกล่าวจะต้องเป็นไปตามโครงสร้างฐานข้อมูลและพจนานุกรมข้อมูล (Data Dictionary) ที่ศูนย์บริหารจัดการรายได้กลางกำหนด ซึ่งประกอบด้วย ๕ กลุ่มข้อมูล และตารางข้อมูล (Data Table) ดังต่อไปนี้

(๑) กลุ่มข้อมูลโครงสร้างพื้นฐาน (Infrastructure Data) ได้แก่ ตารางข้อมูลผู้ประกอบการ (Operator) ตารางเส้นทางเดินรถ (Line Route) ตารางสถานีและจุดจอด (Station) ตารางช่องทางผ่าน (Gate Lane) และตารางอุปกรณ์เครื่องอ่าน (Device Reader)

(๒) กลุ่มข้อมูลผู้ใช้งานและสื่อ (User & Media Data) ได้แก่ ตารางผู้ออกบัตร (Issuer) ตารางบัญชีผู้ใช้งาน (ABT Account) ตารางสื่อเดินทาง (Card Media) และตารางข้อมูลผู้ใช้บริการ (User Profile) โดยข้อมูลส่วนบุคคลต้องได้รับการเข้ารหัสหรือทำให้นิรนาม (Anonymization) ตามกฎหมาย

(๓) กลุ่มข้อมูลธุรกรรม (Transaction Data) ได้แก่ ตารางเหตุการณ์แตะบัตรดิบ (Raw Tap Event) ตารางธุรกรรมการเดินทางสมบูรณ์ (O-D Transaction) และตารางการเดินทางที่ไม่สมบูรณ์ (Unclosed Journey)

(๔) กลุ่มข้อมูลค่าโดยสารและการเงิน (Fare & Financial Data) ได้แก่ ตารางกฎตรรกะค่าโดยสาร (Fare Table Rule) ตารางส่วนลดและโปรโมชัน (Fare Rebate) และตารางการชำระดุลและจัดสรรรายได้ (Financial Settlement)

(๕) กลุ่มข้อมูลความมั่นคงปลอดภัย (Security & Audit Data) ได้แก่ ตารางบัญชีระงับสิทธิ (Deny List) และตารางบันทึกการตรวจสอบระบบ (Audit Log)

ทั้งนี้ ให้ศูนย์บริหารจัดการรายได้กลางจัดทำพจนานุกรมข้อมูล (Data Dictionary) ฉบับสมบูรณ์ในระดับฟิลด์ข้อมูลร่วมกับผู้รับใบอนุญาตการให้บริการออกบัตรชำระค่าโดยสารในระบบตั๋วร่วม และผู้รับใบอนุญาตการให้บริการระบบตั๋วร่วมในระบบขนส่งสาธารณะ ในขั้นตอนปฏิบัติการให้เหมาะสมกับผู้รับใบอนุญาตแต่ละประเภทในรายละเอียดต่อไป โดยระบุตารางข้อมูล (Data Table) นิยามข้อมูล ผู้สร้าง ผู้ส่ง และผู้รับข้อมูล ขนาดและรูปแบบข้อมูล รหัสมาตรฐาน ความถี่ในการรับส่ง กฎเชิงธุรกิจในการประมวลผลรายการ (Business Rules) ฟิลด์สำรองสำหรับการใช้งานในอนาคต (Reserved Fields) ข้อตกลงระดับการให้บริการของข้อมูล กรรมสิทธิ์ข้อมูล (Data Ownership) ตรรกะการกระทบยอด (Reconciliation Logic) การจัดเวอร์ชันของพจนานุกรมข้อมูล (Data Dictionary Versioning) มาตรการความปลอดภัย และกระบวนการแก้ไขข้อมูลผิดพลาด

ข้อ ๑๐ การแลกเปลี่ยนข้อมูลระหว่างระบบคอมพิวเตอร์ของผู้รับใบอนุญาต การให้บริการออกบัตรชำระค่าโดยสารในระบบตั๋วร่วม และผู้รับใบอนุญาตการให้บริการระบบตั๋วร่วมในระบบขนส่งสาธารณะกับศูนย์บริหารจัดการรายได้กลาง ให้ดำเนินการผ่านส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface : API) ตามมาตรฐาน RESTful API หรือมาตรฐานอื่นที่เทียบเท่าหรือสูงกว่า โดยต้องใช้รูปแบบการแลกเปลี่ยนข้อมูล (Data Interchange Format) เป็น JSON (JavaScript Object Notation) หรือ Protocol Buffers หรือรูปแบบอื่นที่สอดคล้องกับมาตรฐานที่กำหนดโดยธนาคารแห่งประเทศไทย

ข้อ ๑๑ ช่องทางการสื่อสารสำหรับการเชื่อมต่อระบบตั๋วร่วมต้องมีการเข้ารหัสความปลอดภัย (Encryption) ตลอดเส้นทาง (End-to-End Security) โดยใช้โปรโตคอล Transport Layer Security (TLS) เวอร์ชัน ๑.๓ หรือเวอร์ชันใหม่กว่าที่มีความมั่นคงปลอดภัยสูงกว่า เพื่อป้องกันการดักจับ แก้ไข หรือปลอมแปลงข้อมูลระหว่างการรับส่ง

ข้อ ๑๒ เพื่อประสิทธิภาพในการบริหารจัดการความเสี่ยงและการคำนวณค่าโดยสาร ผู้รับใบอนุญาตการให้บริการออกบัตรชำระค่าโดยสารในระบบตั๋วร่วมและผู้รับใบอนุญาตการให้บริการระบบตั๋วร่วมในระบบขนส่งสาธารณะต้องดำเนินการส่งข้อมูลเหตุการณ์การแตะบัตร (Tap Events) จากอุปกรณ์ปลายทางมายังศูนย์บริหารจัดการรายได้กลาง ภายในระยะเวลาไม่เกิน ๕ นาที นับตั้งแต่เกิดเหตุการณ์ขึ้น (Near Real-time Upload) เว้นแต่มีเหตุสุดวิสัยด้านระบบเครือข่าย

ข้อ ๑๓ ศูนย์บริหารจัดการรายได้กลางจะดำเนินการประมวลผลและส่งข้อมูลบัญชีระงับสิทธิ (Deny List) หรือข้อมูลสถานะบัญชีที่มีการเปลี่ยนแปลง กลับไปยังระบบของผู้รับใบอนุญาตการให้บริการระบบตั๋วร่วมในระบบขนส่งสาธารณะเพื่อกระจายไปยังอุปกรณ์เครื่องอ่าน ภายในระยะเวลาไม่เกิน ๓๐ นาที นับตั้งแต่ได้รับข้อมูลการเปลี่ยนแปลงหรือตรวจพบความผิดปกติ (Propagation SLA) เว้นแต่มีเหตุสุดวิสัยด้านระบบเครือข่าย

หมวด ๓
มาตรฐานการบริหารจัดการรหัสความปลอดภัยของระบบตั๋วร่วม

ข้อ ๑๔ ผู้รับใบอนุญาตประกอบกิจการระบบตั๋วร่วมต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนด

ข้อ ๑๕ ผู้รับใบอนุญาตประกอบกิจการระบบตั๋วร่วมต้องจัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) และดำเนินการทดสอบเจาะระบบ (Penetration Testing) อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่มีนัยสำคัญ และต้องรายงานผลการประเมินพร้อมแผนการแก้ไขความเสี่ยงต่อสำนักงาน

ข้อ ๑๖ อุปกรณ์รับชำระค่าโดยสารและอุปกรณ์เชื่อมต่อเครือข่าย (IoT Devices) ในระบบตั๋วร่วมต้องมีมาตรฐานด้านความปลอดภัยในการใช้งาน ความสามารถในการทำงาน และความมั่นคงปลอดภัยทางไซเบอร์ ตามมาตรฐานสำหรับผลิตภัณฑ์ดิจิทัล dSURE ระดับ ๓ ดาว (dSURE 3 Stars) ที่สำนักงานส่งเสริมเศรษฐกิจดิจิทัลประกาศกำหนด หรือมาตรฐานสากลอื่นที่เทียบเท่าหรือสูงกว่า

ข้อ ๑๗ เครื่องอ่านบัตรต้องรองรับและเปิดใช้งานเทคโนโลยีการเข้ารหัสแบบจุดต่อจุด (Point-to-Point Encryption : P2PE) ตามมาตรฐาน PCI-P2PE หรือมาตรฐานสากลอื่นที่เทียบเท่าตามระดับความสำคัญของข้อมูล เพื่อให้มั่นใจว่าข้อมูลที่สำคัญจะถูกเข้ารหัสทันทีที่จุดรับชำระ (Point of Interaction) และไม่ถูกถอดรหัสในระบบเครือข่ายของผู้รับใบอนุญาตประกอบกิจการระบบตั๋วร่วมหรือระบบอื่นระหว่างทางก่อนถึงอุปกรณ์รักษาความปลอดภัยฮาร์ดแวร์ (HSM) ที่ได้รับอนุญาต

ข้อ ๑๘ ผู้รับใบอนุญาตประกอบกิจการระบบตั๋วร่วมต้องจัดให้มีระบบบริหารจัดการกุญแจเข้ารหัส (Key Management System) ที่มีความมั่นคงปลอดภัยสูง โดยต้องมีกระบวนการสร้าง แจกจ่าย จัดเก็บ เปลี่ยนแปลง และทำลายกุญแจเข้ารหัส (Key Lifecycle Management) ดังต่อไปนี้

(๑) ต้องมีการเปลี่ยนกุญแจเข้ารหัส (Key Rotation) ทันทีที่มีเหตุอันควรสงสัยว่ากุญแจอาจรั่วไหล

(๒) การจัดเก็บกุญแจหลัก (Master Key) ต้องกระทำในอุปกรณ์รักษาความปลอดภัยฮาร์ดแวร์ (Hardware Security Module : HSM) ที่ได้รับมาตรฐาน FIPS 140-2 Level 3 หรือเทียบเท่า

(๓) ต้องจัดให้มีการบริหารจัดการกุญแจหลัก (Master Key Management) สำหรับบัตรชำระค่าโดยสารประเภทรหัสคิวอาร์ (QR Code) ตามมาตรฐานธนาคารแห่งประเทศไทยกำหนดและมาตรฐาน QR Code ตามที่กำหนดโดยภาคอุตสาหกรรมการชำระเงินของไทย

(๔) สำหรับการบริหารจัดการกุญแจเข้ารหัส (Key Management) ของสื่อชำระค่าโดยสารประเภทบัตรอิเล็กทรอนิกส์ตามมาตรฐาน EMV ให้พึ่งพาระบบและกลไกการบริหารจัดการกุญแจเข้ารหัสของเครือข่ายชำระเงินตามมาตรฐาน EMV เป็นหลัก

ข้อ ๑๙ การจัดเก็บข้อมูลส่วนบุคคลและข้อมูลธุรกรรมทางการเงินในฐานข้อมูล ต้องใช้วิธีการเข้ารหัส (Encryption) ด้วยอัลกอริทึมที่มีความยาวกุญแจไม่ต่ำกว่า ๒๕๖ บิต (AES-256) และต้องใช้เทคนิคการแปลงข้อมูลเป็นโทเคน (Tokenization) แทนการจัดเก็บหมายเลขบัตรจริง (Primary Account Number : PAN) เพื่อลดความเสี่ยงในการรั่วไหลของข้อมูล ตามมาตรฐาน PCI DSS หรือมาตรฐานสากลอื่นที่เทียบเท่าหรือสูงกว่า

ประกาศ ณ วันที่ ๒๖ สิงหาคม พ.ศ. ๒๕๖๙
จิรโรจน์ ศุกลรัตน์
ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร