การยกระดับความปลอดภัยของ Digital ID ด้วย การใช้ Mobile Network Open APIs ร่วมกับการยืนยันตัวตน: แนวทางสำหรับหน่วยงานผู้พิสูจน์และยืนยันตัวตน

1. บทนำ: ปัญหาความมั่นคงปลอดภัยของการยืนยันตัวตนโดยการใช้ SMS OTP

ปัจจุบัน การยืนยันตัวตนผู้ใช้บริการโดยการส่งรหัสลับแบบใช้ครั้งเดียวในรูปแบบของข้อความสั้น (SMS OTP) ที่ส่งผ่านทางโครงข่ายโทรศัพท์สาธารณะ (Public Switched Telephone Network: PSTN) เป็นวิธีที่ได้รับความนิยมสูง [1] เนื่องจากสามารถพัฒนาได้ง่าย ประหยัด และเหมาะกับผู้ใช้บริการหลากหลายกลุ่ม โดยเฉพาะกลุ่มผู้สูงอายุหรือผู้ที่อาศัยในพื้นที่ห่างไกล อย่างไรก็ตามการยืนยันตัวตนด้วยวิธีนี้กลับมีช่องโหว่ในด้านความมั่นคงปลอดภัยหลายประการ เช่น การโจมตีแบบ SIM Swap, การสกัดกั้นข้อมูลผ่านเครือข่ายโทรศัพท์ รวมถึงช่องโหว่ต่างๆ ในระบบโทรคมนาคม

สมาคมผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ระดับโลก หรือ GSMA ได้ตระหนักถึงปัญหาเหล่านี้ และได้ระบุว่า "ระบบ SMS OTP แบบดั้งเดิมไม่สามารถรับรองความปลอดภัยได้อย่างสมบูรณ์แบบในสภาพแวดล้อมทางไซเบอร์ในปัจจุบัน ซึ่งภัยคุกคามมีความซับซ้อนมากขึ้น" ด้วยเหตุนี้ GSMA จึงริเริ่มมาตรฐานระดับโลกที่เรียกว่า GSMA Open Gateway ในโครงการของ CAMARA เพื่อกำหนด APIs ที่จะช่วยเพิ่มประสิทธิภาพ ความน่าเชื่อถือ และความปลอดภัยในการใช้บริการของผู้ให้บริการโทรศัพท์เคลื่อนที่ ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

2. GSMA Open Gateway และโครงการ CAMARA คืออะไร

GSMA Open Gateway เป็นโครงการริเริ่มสำคัญของสมาคมผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ระดับโลก หรือ GSMA (Global System for Mobile Communications Association) ซึ่งมีสมาชิกประกอบด้วยผู้ให้บริการเครือข่ายโทรศัพท์มือถือทั่วโลก [3] โครงการนี้มุ่งหมายที่จะสร้างมาตรฐานกลางใน

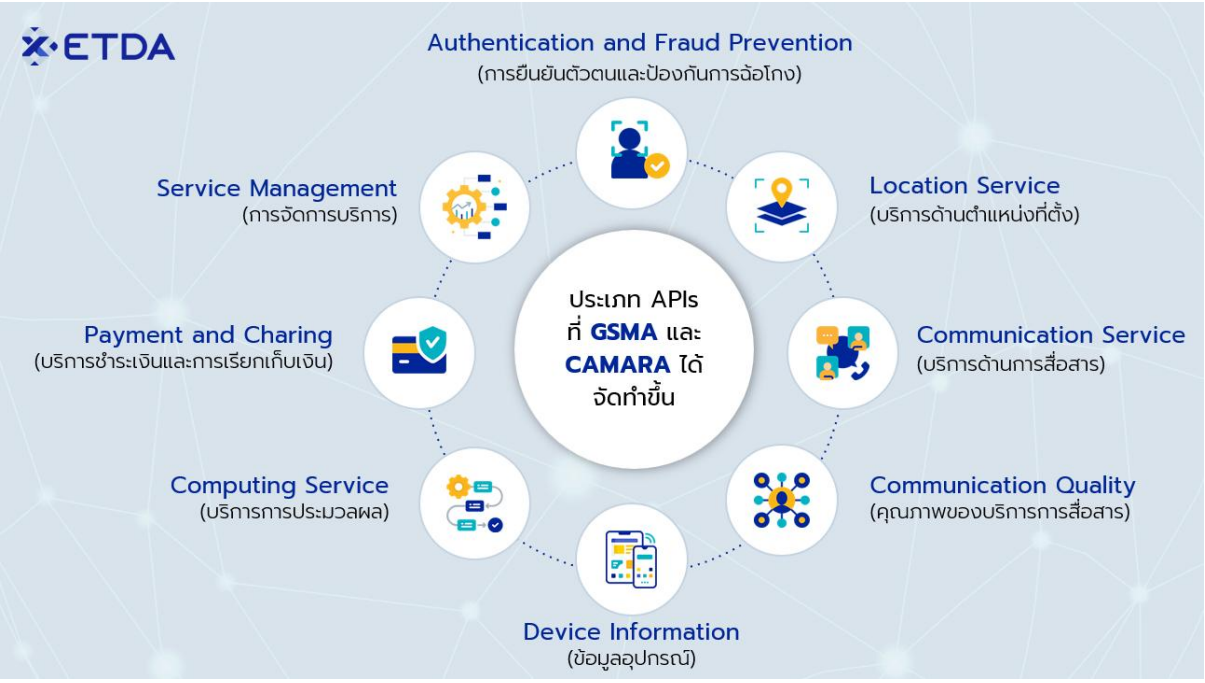
การเชื่อมต่อระหว่างแอปพลิเคชันหรือระบบบริการต่างๆ กับเครือข่ายโทรคมนาคม เพื่อให้นักพัฒนาและผู้ให้บริการด้านดิจิทัลสามารถใช้งานฟังก์ชันที่เกี่ยวข้องกับการสื่อสารและความปลอดภัยได้ง่ายขึ้น เช่น การพิสูจน์และยืนยันตัวตน การตรวจสอบตำแหน่งพิกัดของผู้ใช้บริการ และการป้องกันการฉ้อโกง ตัวอย่าง เช่น การสลับซิมการ์ดเพื่อรับรหัส OTP ที่ส่งทาง SMS เพื่อให้สามารถควบคุมบัญชีต่างๆ ของเหยื่อได้ หรือการปลอมแปลงตำแหน่งเพื่อเข้าถึงเนื้อหาหรือบริการที่มีข้อจำกัดทางภูมิศาสตร์ เป็นต้น

ส่วนโครงการ **CAMARA** เป็นความร่วมมือระหว่าง GSMA กับ Linux Foundation [4] โดย CAMARA เป็นโครงการโอเพนซอร์สที่มีวัตถุประสงค์หลักในการกำหนดรายละเอียด API (Application Programming Interface) เกี่ยวกับด้านโทรคมนาคมที่ชัดเจนและได้มาตรฐานมากยิ่งขึ้น พร้อมทั้งจัดทำเอกสาร คำแนะนำ และเครื่องมือทดสอบที่ช่วยให้ผู้ให้บริการและนักพัฒนาสามารถนำ API ไปใช้ได้อย่างสะดวกรวดเร็ว โดยโครงการนี้เน้นการสร้างความโปร่งใส และความมีส่วนร่วมจากผู้เชี่ยวชาญและนักพัฒนาทั่วโลก เพื่อให้ API ที่ถูกพัฒนาขึ้นมีประสิทธิภาพในการใช้งานจริงและเป็นที่ยอมรับในระดับสากล

GSMA และ CAMARA ทำหน้าที่ร่วมกันเป็นเสมือนเป็นสะพานเชื่อมระหว่างผู้ให้บริการโทรศัพท์เคลื่อนที่กับผู้ให้บริการดิจิทัล เพื่อให้สามารถนำข้อมูลสำคัญที่มีอยู่บนเครือข่ายโทรศัพท์มาใช้ในการเพิ่มประสิทธิภาพและความปลอดภัยให้กับบริการต่างๆ เช่น การยืนยันตัวตนผ่าน SMS OTP การตรวจสอบความถูกต้องของหมายเลขโทรศัพท์ และการป้องกันภัยคุกคามที่เกี่ยวข้องกับโทรศัพท์เคลื่อนที่ในยุคดิจิทัล ยกเช่น หากผู้ให้บริการต้องการยืนยันว่าผู้ใช้บริการยังคงเป็นเจ้าของซิมการ์ดเดิม ก็สามารถเรียกใช้ SIM Swap API เพื่อตรวจสอบข้อมูลการเปลี่ยนซิมการ์ดจากผู้ให้บริการโทรศัพท์เคลื่อนที่ได้ทันที

3. ประเภทของ APIs ที่ GSMA และ CAMARA ได้จัดทำขึ้น

GSMA และ CAMARA ได้ร่วมกันพัฒนา APIs เพื่อรองรับการใช้งานที่หลากหลาย โดยสามารถแบ่งได้ดังนี้

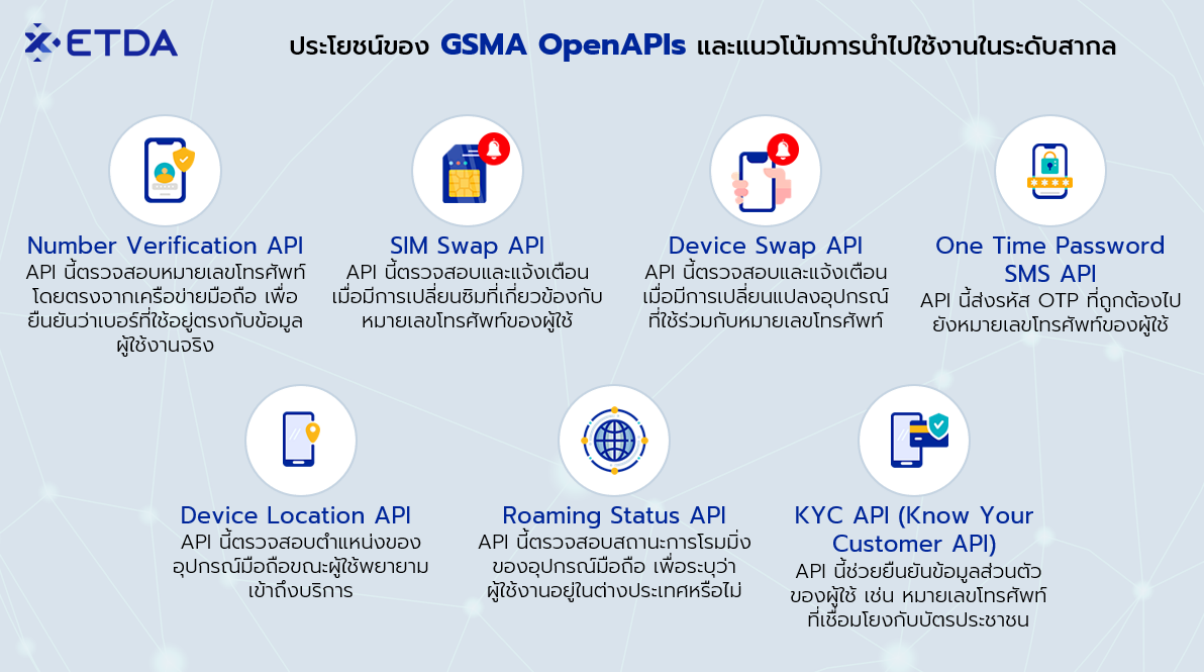


- กลุ่ม Authentication and Fraud Prevention (การยืนยันตัวตนและป้องกันการฉ้อโกง) เพื่อเสริมสร้างความมั่นคงปลอดภัยของกระบวนการยืนยันตัวตนและลดความเสี่ยงจากการฉ้อโกงในรูปแบบต่างๆ
- กลุ่ม Location Services (บริการด้านตำแหน่งพิกัด) เพื่อการตรวจสอบและดึงข้อมูลตำแหน่งทางภูมิศาสตร์ของอุปกรณ์ ซึ่งเป็นประโยชน์อย่างยิ่งในการป้องกันการฉ้อโกงจากการทำธุรกรรมจากพื้นที่หรือพิกัดที่ต่างไปจากการใช้งานตามปกติของผู้ใช้บริการ
- กลุ่ม Communication Services (บริการด้านการสื่อสาร) เพื่อประโยชน์ด้านการสื่อสารและการจัดการการโทรแบบเรียลไทม์ เช่น การโทรผ่านเทคโนโลยี WebRTC (Web Real-Time Communication)
- กลุ่ม Communication Quality (คุณภาพของบริการการสื่อสาร) เพื่อการควบคุมและปรับปรุงคุณภาพการสื่อสารของเครือข่าย เพื่อให้แอปพลิเคชันสามารถทำงานได้อย่างมีประสิทธิภาพสูงสุด
- กลุ่ม Device Information (ข้อมูลอุปกรณ์สื่อสาร) เพื่อให้บริการข้อมูลที่จำเป็นเกี่ยวกับอุปกรณ์ของผู้ใช้และสถานะเครือข่ายปัจจุบัน ซึ่งสามารถนำไปใช้เพื่อเพิ่มความปลอดภัย การเพิ่มประสิทธิภาพเครือข่าย และการป้องกันการฉ้อโกง
- กลุ่ม Computing Services (บริการการประมวลผล) เพื่อใช้ในการค้นหา Edge Computing zones ในเครือข่ายที่อยู่ใกล้กับผู้ใช้บริการมากที่สุด เพื่อลดความหน่วงในการประมวลผลข้อมูลต่าง ๆ ของแอปพลิเคชัน
- กลุ่ม Payments and Charging (บริการชำระเงินและการเรียกเก็บเงิน) เพื่ออำนวยความสะดวกในการชำระเงินโดยตรงผ่านผู้ให้บริการโทรศัพท์เคลื่อนที่ ซึ่งเป็นวิธีการชำระเงินที่สะดวกและปลอดภัย
- กลุ่ม Service Management (จัดการการให้บริการ) เพื่อจัดการส่วนงานและทรัพยากรต่าง ๆ ภายในระบบของผู้ให้บริการ

ภายในแต่ละกลุ่มนั้น ประกอบด้วย API ที่ออกแบบสำหรับใช้งานในด้านต่างๆ ซึ่งอาจช่วยเพิ่มความมั่นคงปลอดภัยและเสริมประสิทธิภาพของระบบการให้บริการของหน่วยงานหรือองค์กรที่นำ API เหล่านี้ไปใช้

4. API ที่หน่วยงานอาจพิจารณาแนวทางการนำมาใช้งาน เพื่อช่วยเพิ่มความมั่นคงปลอดภัยในการพิสูจน์และยืนยันตัวตนผู้ใช้บริการ

ในการเพิ่มระดับความมั่นคงปลอดภัยของการยืนยันตัวตนโดยการใช้ SMS OTP นั้น หน่วยงานอาจพิจารณาแนวทางการนำมาใช้งานของ API ดังต่อไปนี้



1) Number Verification API

- **นิยาม :** API สำหรับการยืนยันตัวตนผ่านหมายเลขโทรศัพท์ที่ใช้ในการทำธุรกรรม โดยที่ผู้ใช้บริการไม่จำเป็นต้องกรอกรหัส OTP หรือรหัสผ่านใด ๆ [5]
- **กลไลการทำงาน:** เมื่อผู้ใช้ต้องการเข้าสู่ระบบ แอปพลิเคชันจะส่งคำขอตรวจสอบไปยัง API ผ่านเครือข่ายโทรศัพท์มือถือ จากนั้นระบบของผู้ให้บริการเครือข่ายจะตรวจสอบและยืนยันว่าหมายเลขโทรศัพท์ ซิมการ์ด และอุปกรณ์ที่กำลังใช้งานอยู่นั้นตรงกันจริงหรือไม่ เมื่อการตรวจสอบสำเร็จผู้ใช้บริการจึงจะสามารถเข้าสู่ระบบได้
- **บทบาทและความสำคัญต่อ Digital ID:** API นี้เป็นรากฐานที่สำคัญของ Digital ID เพราะช่วยสร้างความเชื่อมโยงที่น่าเชื่อถือระหว่างตัวตนดิจิทัลกับอุปกรณ์ที่ผู้ใช้บริการครอบครองจริง ทำหน้าที่เป็นกลไกการยืนยันตัวตนที่ปลอดภัย ช่วยป้องกันการหลอกลวงในรูปแบบ Phishing ได้อย่างมีประสิทธิภาพ เนื่องจากไม่มีการกรอกข้อมูลใดๆ ที่ผู้โจมตีจะสามารถดักจับได้

2) SIM Swap API

- **นิยาม:** API ที่ถูกออกแบบมาเพื่อตรวจสอบว่าซิมการ์ดที่ผูกกับหมายเลขโทรศัพท์นั้น มีการแจ้งขอเปลี่ยนซิมการ์ดใหม่โดยยังคงเป็นหมายเลขโทรศัพท์เดิม ภายในช่วงระยะเวลาไม่นานก่อนการทำธุรกรรมหรือไม่ [6]
- **กลไลการทำงาน:** ก่อนการทำธุรกรรม แอปพลิเคชันจะส่งคำขอไปยัง API เพื่อตรวจสอบประวัติการเปลี่ยนซิมการ์ด โดย API นี้ จะส่งข้อมูลกลับมาว่ามีการสลับซิมการ์ดเกิดขึ้นล่าสุดเมื่อใด หากตรวจพบว่ามีการสลับซิมเกิดขึ้นไม่นาน ระบบจะมองว่าเป็นเหตุการณ์ที่มีความเสี่ยงและอาจระงับการทำธุรกรรมเพื่อทำการตรวจสอบเพิ่มเติม

- **บทบาทและความสำคัญต่อ Digital ID:** API นี้ทำหน้าที่เป็นกลไกตรวจจับการฉ้อโกงสำหรับ Digital ID แบบเรียลไทม์ โดยพุ่งเป้าไปที่การป้องกันการโจมตีแบบ SIM Swap โดยตรง ซึ่งเป็นวิธีที่ผู้ไม่หวังดีใช้เพื่อเข้าควบคุมเบอร์โทรศัพท์และดักรับรหัส OTP การผสานการตรวจสอบนี้เข้ากับระบบ Digital ID จะช่วยป้องกันการเข้ายึดบัญชี ลดโอกาสที่ตัวตนดิจิทัลของผู้ใช้บริการจะถูกขโมยไปใช้ทำธุรกรรมที่มีความเสี่ยงสูง

3) Device Swap API

- **นิยาม:** API ที่ใช้ในการตรวจสอบว่ามีการสลับซิมการ์ดจากอุปกรณ์เดิมที่ใช้กับหมายเลขโทรศัพท์หนึ่งๆ ไปยังอุปกรณ์ใหม่ภายในช่วงระยะเวลาไม่นานก่อนการทำธุรกรรมหรือไม่ [7]
- **กลไลการทำงาน:** แอปพลิเคชันส่งคำขอตรวจสอบผ่านทาง API ไปยังผู้ให้บริการโทรศัพท์เคลื่อนที่เพื่อเปรียบเทียบรหัสจำเพาะของอุปกรณ์ (IMEI) ปัจจุบันกับข้อมูลในฐานข้อมูล หากพบว่ามีการเปลี่ยนแปลงอุปกรณ์เกิดขึ้นในระยะเวลาไม่นาน API จะส่งข้อมูลกลับมา เพื่อให้ผู้ให้บริการดิจิทัลประเมินความเสี่ยงในการให้บริการ
- **บทบาทและความสำคัญต่อ Digital ID:** API นี้ช่วยเพิ่มความปลอดภัยให้กับ Digital ID ในการตรวจสอบตัวตนดิจิทัลที่มักจะผูกอยู่กับอุปกรณ์ที่ผู้ใช้บริการไว้วางใจ การเปลี่ยนแปลงอุปกรณ์ในระยะเวลาไม่นานจึงเป็นสัญญาณที่ควรจับตามอง ว่าเป็นการพยายามเข้าควบคุมบัญชีของผู้อื่นหรือไม่ สำหรับระบบ Digital ID ข้อมูลนี้ช่วยให้สามารถทำการยืนยันตัวตนตามระดับความเสี่ยง (Risk-Based Authentication) ได้ เช่น การร้องขอการยืนยันตัวตนที่เข้มงวดขึ้นเมื่อมีการใช้งานจากอุปกรณ์เครื่องใหม่ที่ไม่เคยรู้จักมาก่อน

4) One Time Password API

- **นิยาม:** API สำหรับช่วยเหลือผู้ให้บริการดิจิทัลในการยืนยันตัวตนผู้ใช้บริการ โดยใช้การส่ง SMS OTP ที่มีกลไกการรักษาความปลอดภัยเพิ่มเติม เพื่อให้มั่นใจว่าผู้ที่กำลังทำธุรกรรมนั้น เป็นเจ้าของหมายเลขโทรศัพท์ตัวจริง [8]
- **กลไกการทำงาน:** การทำงานของ API นี้จะแตกต่างจาก SMS Gateway ทั่วไป ซึ่ง API นี้ใช้ช่องทางการส่ง SMS OTP ที่ปลอดภัยกว่า ซึ่งให้บริการโดยผู้ให้บริการโทรศัพท์เคลื่อนที่โดยตรง และสามารถตรวจสอบสถานะการส่ง SMS OTP ถึงปลายทางได้อย่างแม่นยำ เพื่อให้แน่ใจว่า SMS OTP ไม่ถูกเปลี่ยนเส้นทางหรือถูกสกัดกั้นโดยผู้ไม่หวังดี
- **บทบาทและความสำคัญต่อ Digital ID:** แม้ OTP จะเป็นส่วนสำคัญของ Digital ID แต่จุดอ่อนหลักคือความปลอดภัยของช่องทางการส่ง ซึ่ง API นี้อาจสามารถเสริมความแข็งแกร่งในจุดดังกล่าว ทำให้กระบวนการยืนยันตัวตนด้วย SMS OTP มีความน่าเชื่อถือและสามารถป้องกันการดักจับข้อความได้อย่างมีประสิทธิภาพมากขึ้น

5) Device Location API

- **นิยาม:** API ที่ช่วยให้ผู้ให้บริการดิจิทัลสามารถร้องขอข้อมูลตำแหน่งทางภูมิศาสตร์ของอุปกรณ์เคลื่อนที่ของผู้ที่กำลังทำธุรกรรม โดยใช้ข้อมูลที่น่าเชื่อถือและตรวจสอบได้จากผู้ให้บริการโทรศัพท์เคลื่อนที่ [9]
- **กลไลการทำงาน:** แอปพลิเคชันส่งคำขอตำแหน่งของอุปกรณ์ไปยัง API ซึ่งจะใช้ข้อมูลจากโครงข่ายโทรศัพท์เคลื่อนที่ เช่น ตำแหน่งเสาสัญญาณ เพื่อระบุตำแหน่งโดยประมาณของอุปกรณ์ โดยข้อมูลตำแหน่งที่ได้จากเครือข่ายนี้มักจะปลอมแปลงได้ยากกว่าข้อมูล GPS จากอุปกรณ์โดยตรง จากนั้น API จะส่งข้อมูลตำแหน่งกลับมายังแอปพลิเคชัน เพื่อให้ผู้ให้บริการใช้ข้อมูลตำแหน่งในการประเมินความเสี่ยงในการให้บริการต่อไป
- **บทบาทและความสำคัญต่อ Digital ID:** API นี้ใช้ในการร้องขอข้อมูลที่สำคัญต่อความปลอดภัยของ Digital ID หากมีการพยายามใช้ Digital ID เพื่อทำธุรกรรมจากสถานที่ที่ผิดปกติไปจากเดิม เหตุการณ์นี้ถือเป็นสัญญาณเตือนการฉ้อโกงที่ชัดเจน การตรวจจับ "ความไม่สอดคล้องกันของตำแหน่ง" นี้ ช่วยให้ผู้ให้บริการดิจิทัลสามารถยับยั้งการทำธุรกรรมที่น่าสงสัยและปกป้องตัวตนดิจิทัลของผู้ใช้บริการจากการถูกนำ Digital ID ไปใช้ในทางที่ผิด

6) Roaming Status API

- **นิยาม:** API นี้ใช้ในการตรวจสอบสถานะการใช้งานเครือข่ายของอุปกรณ์ว่ากำลังเชื่อมต่อกับเครือข่ายในประเทศ (Home Network) หรือกำลังใช้บริการข้ามแดนอัตโนมัติ (Roaming) [10]
- **กลไลการทำงาน:** แอปพลิเคชันส่งคำขอไปยัง API เพื่อตรวจสอบสถานะ Roaming ของผู้ที่กำลังทำธุรกรรม จากนั้นระบบของผู้ให้บริการโทรศัพท์เคลื่อนที่จะตอบกลับว่าสถานะ Roaming เป็นจริงหรือเท็จ
- **บทบาทและความสำคัญต่อ Digital ID:** API นี้ให้ข้อมูลสำหรับการประเมินความเสี่ยงของ Digital ID ตัวอย่างเช่น หากมีการเข้าสู่ระบบด้วย IP Address ในประเทศ แต่ API ยืนยันว่าอุปกรณ์กำลังโรมมิ่งอยู่ต่างประเทศ เหตุการณ์นี้อาจบ่งชี้ถึงการใช้ VPN หรือการพยายามเข้าควบคุมบัญชี ความขัดแย้งของข้อมูลนี้ช่วยให้ผู้ให้บริการดิจิทัล สามารถขอให้ผู้ใช้บริการทำการการยืนยันตัวตนเพิ่มเติม (Challenge) และอาจร้องขอหลักฐานเพิ่มเติมเพื่อพิสูจน์ความเป็นผู้ใช้บริการตัวจริงได้

7) KYC API (Know Your Customer API)

- **นิยาม:** API ที่ช่วยให้ผู้ให้บริการดิจิทัลสามารถเปรียบเทียบและตรวจสอบข้อมูลที่ผู้ใช้บริการเคยใช้ในการพิสูจน์ตัวตน และถูกจัดเก็บในฐานข้อมูล ว่าตรงกับข้อมูลที่จัดเก็บโดยผู้ให้บริการโทรศัพท์เคลื่อนที่หรือไม่ [11]
- **กลไกการทำงาน:** ผู้ให้บริการดิจิทัลส่งข้อมูลที่ต้องการตรวจสอบ (เช่น ชื่อ, หมายเลขบัตรประชาชน) ไปยัง API จากนั้น API จะทำการเปรียบเทียบกับฐานข้อมูล KYC ของผู้ให้บริการโทรศัพท์เคลื่อนที่ จากนั้นจึงตอบกลับเป็นผลลัพธ์ว่าข้อมูลนั้น "ตรงกัน" หรือ "ไม่ตรงกัน" เพื่อเป็นการยืนยันความถูกต้องของข้อมูลของผู้ใช้บริการ

- **บทบาทและความสำคัญต่อ Digital ID:** API นี้มีความสำคัญในการสร้าง "รากฐานความน่าเชื่อถือ" (Root of Trust) ให้กับ Digital ID โดยการช่วยป้องกันการสร้างบัญชีปลอมโดยใช้ข้อมูลเท็จหรือข้อมูลสังเคราะห์ ทำให้มั่นใจได้ว่า Digital ID ที่ถูกสร้างขึ้นนั้นผูกกับอัตลักษณ์ของบุคคลที่มีตัวตนจริง

5. สรุป

การใช้ SMS OTP ที่ส่งผ่านโครงข่ายโทรศัพท์สาธารณะ (PSTN) โดยไม่มีการตรวจสอบสถานะของหมายเลขโทรศัพท์และอุปกรณ์ที่ใช้ร่วมกันนั้น อาจก่อให้เกิดช่องโหว่ที่ผู้ไม่หวังดีสามารถใช้เทคนิคต่าง ๆ เช่น SIM Swap Attack, Number Porting หรือการสกัดกั้นข้อความผ่านช่องโหว่ของระบบ SS7 [2] ในการสร้างความเสียหายต่อผู้ใช้บริการ การใช้ Mobile Network Open APIs เช่น SIM Swap API, Device Swap API และ Number Verification API เพื่อเพิ่มความสามารถในการตรวจสอบสถานะการใช้งานได้ของหมายเลขโทรศัพท์ และยืนยันความเป็นเจ้าของของหมายเลขโทรศัพท์และอุปกรณ์ของผู้ใช้บริการจะช่วยยกระดับความมั่นคงปลอดภัยของการให้บริการได้มากยิ่งขึ้น

เอกสารอ้างอิง

[1] “Public Switch Telephone Network (PSTN)”, GOV.UK. Accessed: Jul. 03, 2025. [Online]. Available: https://www.gov.uk/government/collections/public-switch-telephone-network-pstn

[2] C. Quintin and B. Ngene, “EFF to FCC: SS7 is Vulnerable, and Telecoms Must Acknowledge That”, Electronic Frontier Foundation. Accessed: Jul. 03, 2025. [Online]. Available: https://www.eff.org/deeplinks/2024/07/eff-fcc-ss7-vulnerable-and-telecoms-must-acknowledge

[3] “GSMA Open Gateway - Open Gateway - GSMA”, Open Gateway. Accessed: Jul. 03, 2025. [Online]. Available: https://www.gsma.com/solutions-and-impact/gsma-open-gateway/

[4] “Camara Project – Linux Foundation Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/

[5] “Number Verification – Camara Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/number-verification/

[6] “Sim Swap – Camara Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/sim-swap/

[7] “Device Swap – Camara Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/device-swap/

[8] “One Time Password SMS – Camara Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/one-time-password-sms/

[9] “Device Visit Location – Camara Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/device-visit-location/

[10] “Device Roaming Status – Camara Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/device-roaming-status/

[11] “Know Your Customer Match – Camara Project”, Accessed: Jul. 03, 2025. [Online]. Available: https://camaraproject.org/know-your-customer-match/