



ชื่อของออนไลน์ปลอดภัย ด้วยเทคโนโลยี 3D Secure

เผยแพร่วันที่ 27 ตุลาคม 2564

ในอดีตการจับจ่ายซื้อสินค้าและบริการยังไม่ได้อยู่ในรูปแบบออนไลน์มากนัก เมื่อลูกค้าไปซื้อสินค้าหรือบริการที่ร้านค้าและชำระเงินด้วยบัตรเครดิตหรือบัตรเดบิต ลูกค้าจะต้องแสดงบัตรเครดิตหรือบัตรเดบิตเพื่อให้ร้านค้าใช้ทำรายการชำระเงิน นั่นคือหากลูกค้าไม่มีตัวบัตรเครดิตหรือบัตรเดบิตก็จะไม่สามารถทำการชำระเงินด้วยบัตรที่ร้านค้าได้ แต่ปัจจุบันโลกออนไลน์ได้เข้ามามีบทบาทอย่างมากในชีวิตประจำวัน การซื้อของเปลี่ยนไปอยู่ในรูปแบบออนไลน์มากขึ้น ดังนั้นการซื้อสินค้าออนไลน์ และชำระเงินด้วยบัตรเครดิตและบัตรเดบิตแบบออนไลน์จึงได้รับความนิยมเพิ่มมากขึ้น เพื่อให้ตอบโจทย์กับการใช้งานบนโลกออนไลน์และยังคงมีความปลอดภัยที่ทำให้มั่นใจได้ว่าเจ้าของบัตรเป็นผู้ทำรายการซื้อของออนไลน์เอง จึงเป็นที่มาของการนำเทคโนโลยี 3D Secure มาใช้งาน

3D Secure คืออะไร

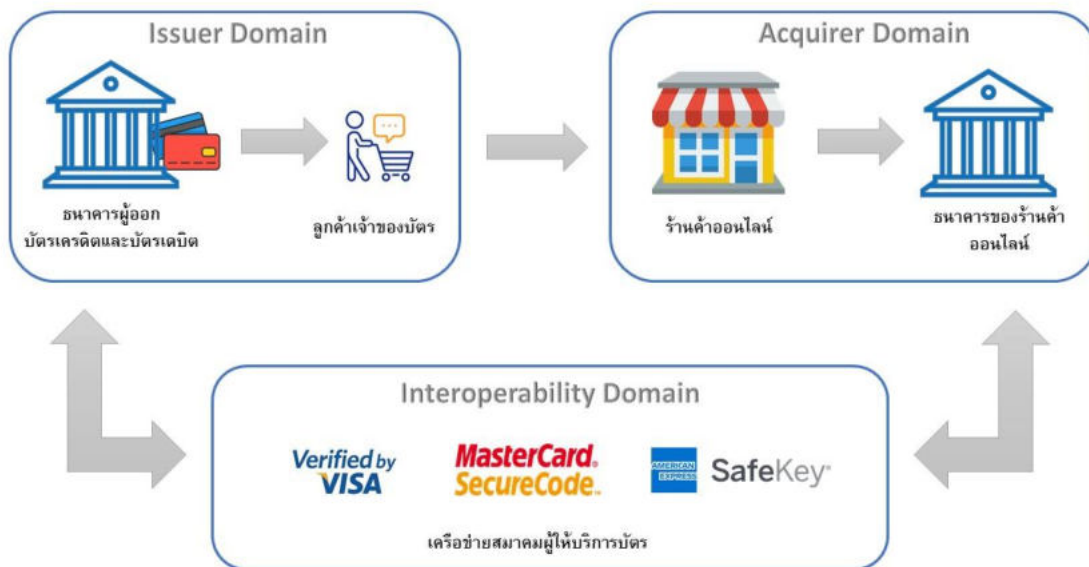
3D Secure เป็นโครงสร้างความปลอดภัยบนระบบการชำระเงินธุรกรรมออนไลน์ที่ช่วยป้องกันการฉ้อโกงในธุรกรรมบัตรเครดิตและบัตรเดบิต โดยพัฒนาการทำงานร่วมกันสำหรับการบริการชำระเงินและผู้ให้บริการชำระเงิน โดยเน้นความสำคัญ คือ การเพิ่มความแข็งแกร่งในกระบวนการยืนยันตัวตนของลูกค้า (Strong Customer Authentication) ระหว่างการทำรายการชำระเงินผ่านธุรกรรมออนไลน์ ในเวอร์ชันแรกถูกพัฒนาขึ้นในปี 1999 โดย Arcot Systems (ปัจจุบันคือ CA Technologies บริษัท Broadcom) และในยุคหลัง บริษัทผู้ให้บริการบัตรชำระเงินรายใหญ่ทุกราย เช่น VISA, MasterCard และ American Express ก็ได้นำ 3D Secure มาใช้ในการชำระเงินผ่านธุรกรรมออนไลน์เช่นกัน โดยเราอาจจะเคยเห็นในหน้าแสดงรายการชำระเงิน หรือรู้จักในชื่อตามแบรนด์ต่าง ๆ ดังรูป





โดยตัวอักษร “D” ที่ระบุใน 3D Secure หมายถึง Domain นั่นคือ โครงสร้าง 3 โดเมนที่เกี่ยวข้องกัน สำหรับการเสริมสร้างความปลอดภัยในการชำระเงินผ่านธุรกรรมออนไลน์ ประกอบด้วย

- (1) Issuer Domain หรือ โดเมนผู้ออกบัตร หมายถึง ธนาคารผู้ออกบัตรเครดิตหรือบัตรเดบิต และลูกค้าเจ้าของบัตร
- (2) Acquirer Domain หรือ โดเมนผู้รับบัตร หมายถึง ร้านค้าออนไลน์ และธนาคารของร้านค้าออนไลน์
- (3) Interoperability Domain หรือ โดเมนเครือข่ายระบบการชำระเงิน หมายถึง องค์กรประกอบเครือข่ายที่รองรับการรับส่งข้อมูลเพื่อให้สามารถทำธุรกรรมระหว่างสองโดเมนข้างต้นได้ และเพื่อบริหารจัดการเครือข่ายกับบริการของสมาคมบัตร โดยมีผู้ให้บริการบัตรที่สำคัญ ได้แก่ VISA, MasterCard และ American Express เป็นต้น



รูปที่ 1 แสดงองค์ประกอบโครงสร้าง 3D Secure

สำหรับการทำงานของเทคโนโลยี 3D Secure (Verified by VISA/ MasterCard SecureCode) มีขั้นตอนดังนี้

1. ลูกค้าเลือกซื้อของบนร้านค้าออนไลน์ และเมื่อต้องการชำระค่าสินค้า ร้านค้าออนไลน์จะแสดงหน้าจอให้ลูกค้ากรอกข้อมูลบัตรเครดิตหรือบัตรเดบิต สำหรับร้านค้าที่รองรับเทคโนโลยี 3D Secure บนหน้าจอที่



ให้กรอกข้อมูลบัตรเครดิตหรือบัตรเดบิต จะแสดงสัญลักษณ์ Verified by VISA หรือ MasterCard SecureCode

2. ด้วยความปลอดภัยแบบ 3D Secure ธนาคารผู้ออกบัตรจะส่งรหัสผ่าน OTP ไปยังมือถือของลูกค้า เจ้าของบัตร กรณีลูกค้าทำการชำระสินค้าแล้วไม่ได้รับรหัสผ่าน OTP ลูกค้าสามารถติดต่อสอบถามข้อมูลได้จากธนาคารผู้ออกบัตรนั้น
3. ลูกค้ากรอกรหัสผ่าน OTP ที่ได้รับบนหน้าจอทำการชำระค่าสินค้า เพื่อยืนยันตัวตนในการทำรายการชำระเงิน
4. ระบบ 3D Secure ทำการตรวจสอบข้อมูล หากตรวจสอบแล้วข้อมูลถูกต้อง ธนาคารก็จะอนุมัติการทำรายการ สำหรับกรณีที่มีข้อมูลผิดพลาด ธนาคารก็จะปฏิเสธการทำรายการ และส่งผลลัพธ์ให้กับร้านค้าออนไลน์เพื่อดำเนินการต่อไป



รูปที่ 2 แสดงขั้นตอนการทำงานของเทคโนโลยี 3D Secure

ประโยชน์ของระบบ 3D Secure

- เพื่อให้ร้านค้าออนไลน์สามารถรองรับการทำธุรกรรมออนไลน์ได้อย่างปลอดภัย ด้วยมาตรการการยืนยันตัวตนเจ้าของบัตรผ่านช่องทางออนไลน์ที่มีความปลอดภัย
- เพื่อให้การส่งข้อมูลสำหรับการชำระเงินและข้อมูลลูกค้ามีความถูกต้องและปลอดภัยผ่านระบบเครือข่ายการชำระเงินที่เป็นมาตรฐานสากลเดียวกัน ป้องกันการถูกเปิดเผยแก่บุคคลอื่นที่ไม่เกี่ยวข้อง
- เพื่อให้ร้านค้าออนไลน์สามารถตรวจสอบว่าลูกค้าที่ทำรายการสั่งซื้อสินค้าทางออนไลน์คือเจ้าของผู้ถือบัตรที่ถูกต้องตามกฎหมาย ไม่ใช่ผู้ที่อาจขโมยหรือลอกแบบบัตรมาแอบอ้างใช้งาน



- มีการรับประกันมูลค่าความเสียหายโดยบริษัทผู้ให้บริการบัตร เช่น VISA, MasterCard หากเกิดการฉ้อโกงหรือการปฏิเสธการชำระเงินกับธุรกรรมที่ผ่านกระบวนการตรวจสอบแบบ 3D Secure

อย่างไรก็ตามในปัจจุบันยังคงมีร้านค้าออนไลน์ที่ไม่ได้รองรับระบบ 3D Secure อยู่มาก อาจด้วยเหตุผลเป็นร้านค้าขนาดเล็ก และราคาสินค้าค่อนข้างต่ำ ไม่คุ้มกับการลงทุนสร้างระบบเพื่อรองรับเทคโนโลยี 3D Secure ซึ่งร้านค้ากลุ่มนี้จะไม่ขึ้นตอนการยืนยันตัวตนจากลูกค้าเจ้าของบัตรอีกครั้ง หรือไม่มีการใช้รหัสผ่าน OTP ในการทำรายการชำระเงิน ดังนั้นหากเกิดการฉ้อโกงบนร้านค้าเหล่านี้ จะไม่มีการรับประกันมูลค่าความเสียหายที่เกิดขึ้น และร้านค้าจะต้องผู้ดูแลรับผิดชอบเอง ดังนั้นเพื่อความปลอดภัยของผู้ใช้บริการชื่อของออนไลน์ มีคำแนะนำแนวทางปฏิบัติดังต่อไปนี้

1. ปรับลดวงเงินบัตรเดบิตสำหรับการชำระสินค้าให้เหมาะสมกับการใช้จ่ายบนช่องทางออนไลน์ หรือปรับลดวงเงินชำระสินค้าเป็นศูนย์ หากยังไม่มีความต้องการจะใช้บัตรเดบิตซื้อสินค้า
2. หลีกเลี่ยงการผูกข้อมูลบัตรเครดิตหรือบัตรเดบิตบนเว็บไซต์, แอปพลิเคชัน หรือแพลตฟอร์มที่ไม่น่าไว้วางใจ ไม่น่าเชื่อถือ
3. สังเกตการแจ้งเตือนบัญชีเงินเข้า-เงินออกจากธนาคาร และหมั่นตรวจสอบยอดการใช้จ่ายผ่านบัตรเครดิต และบัตรเดบิตทุกรอบบัญชี
4. หากพบรายการบัญชีผิดปกติ ควรติดต่อธนาคารเจ้าของบัตรโดยตรง หรือหากมีข้อสงสัย สามารถติดต่อสอบถามผ่านช่องทางบริการต่าง ๆ ของธนาคาร หรือที่ ธพท.



หมายเลข Call Center ของสถาบันการเงิน

 1333	 0 2111 1111	 1572	 0 2888 8888	 0 2165 5555
 0 2626 7777	 1428	 0 2633 6000	 0 2777 7777	 0 2285 1555
 1327	 0 2724 4000	 0 2629 5588	 0 2697 5454	 0 2679 5566
 1588	 1357	 0 2555 0555	 0 2271 3700	 1115
 0 2645 9000	 1302	 0 2890 9999		

www.1213.or.th [hotline1213](https://www.facebook.com/hotline1213)

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน
Ins.1213 ธนาคารแห่งประเทศไทย

หมายเลข Call Center สถาบันการเงินและ Non-Bank

