Idpassglobal

MULTI-FACTOR

AUTHENTICATION

PRESENTATION - 2025

www.idpassglobal.co

ความเป็นมา

ทุกวันนี้เราปฏิเสธไม่ได้เลยว่าเทคโนโลยีสารสนเทศนั้นเข้ามามีบทบาทในชีวิตประจำวันของเรามากยิ่งขึ้น เพราะช่วยเพิ่มความสะดวกสบาย และความรวดเร็วให้กับชีวิตประจำวันของผู้คนทั่วโลก แต่สิ่งที่เราหลีกเลี่ยงไม่ได้เลยนั้นก็คือเรื่องของอาชญากรรมทางไซเบอร์ ปัจจุบันอาชญากรรมทางไซเบอร์กลายเป็นความท้าทายครั้งสำคัญของทุกประเทศ สำหรับประเทศไทยสถิติอันน่าตกใจจากสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.) เมื่อเดือนมีนาคม 2565 เผยว่า ชาวไทยกว่า 50% เคยมีประสบการณ์ถูกหลอกลวงทางออนไลน์ระหว่างช่วง 1 ปีที่ผ่านมา

Authentication คืออะไร

คือกระบวนการพิสูจน์ว่าข้อเท็จจริงหรือเอกสารบางอย่างเป็นของจริง ในทางวิทยาการคอมพิวเตอร์ คำนี้มักเกี่ยวข้องกับการพิสูจน์ตัวตนของผู้ใช้ โดยทั่วไป ผู้ใช้จะพิสูจน์ตัวตนโดยการให้ข้อมูลประจำตัว ซึ่งก็คือข้อมูลที่ตกลงร่วมกันระหว่างผู้ใช้และระบบ

ตัวอย่างที่รู้จักกันดีคือการเข้าถึงบัญชีผู้ใช้บนเว็บไซต์หรือผู้ให้บริการ เช่น Facebook หรือ Gmail ก่อนที่คุณจะสามารถเข้าถึงบัญชีของคุณได้ คุณต้องพิสูจน์ว่าคุณเป็นเจ้าของข้อมูลประจำตัวในการเข้าสู่ระบบ โดยทั่วไปแล้วระบบจะแสดงหน้าจอที่ขอชื่อผู้ใช้และรหัสผ่าน จากนั้นจะเปรียบเทียบข้อมูลที่ผู้ใช้ป้อนกับค่าที่เก็บไว้ในที่เก็บข้อมูลภายในก่อนหน้านี้

Authentication Factor

Something you know อะไรที่เรารู้และเราจำมันได้ อาทิเช่น Password หรือ PIN

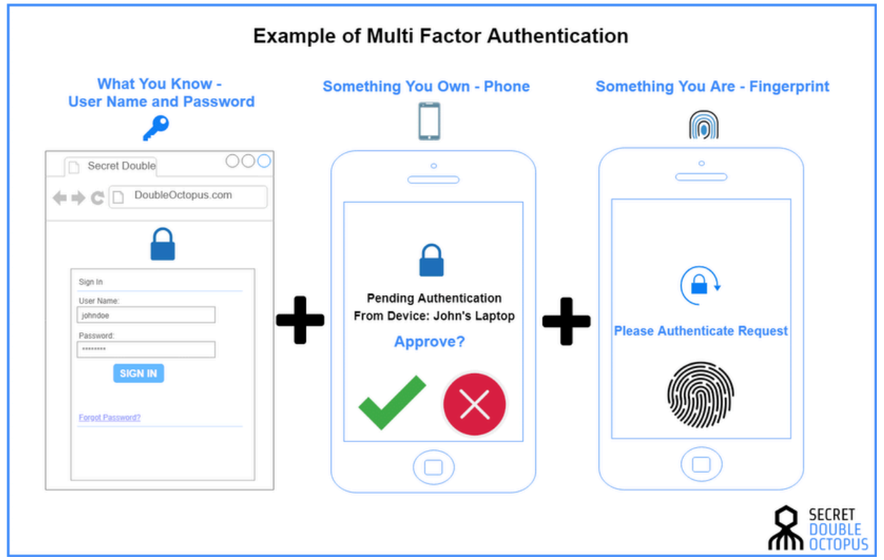
Something you have เป็นสิ่งที่เราสามารถพกมันติดตัวไว้ด้วยตลอด

Something you are การใช้ข้อมูลทางชีวภาพ เช่น ลายนิ้วมือ, ฝ่ามือ, เสียง, ม่านตา, ใบหน้า ดีเอ็นเอ, ลายเซ็นต์

Somewhere you are ตรวจสอบตำแหน่งที่อยู่ของเราโดยใช้ IP Address

Something you do ตรวจจับลักษณะท่าทาง บุคลิกการเดิน ความยาวของก้าวการแกว่งแขน

ประเภทของข้อมูล/อุปกรณ์จำเพาะบุคคลเช่น ชื่อผู้ใช้และรหัสผ่าน มักถูกเรียกว่าปัจจัยการยืนยันตัวตน แม้ว่าการยืนยันตัวตนด้วยรหัสผ่านจะเป็นประเภทการยืนยันตัวตนที่เป็นที่รู้จักมากที่สุด แต่ก็ยังมีปัจจัยการยืนยันตัวตนอื่นๆ อีกมาก



ลักษณะปัจจัยที่นิยมใช้ในการยืนยันตัวตนในปัจจุบัน

- การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Password-based authentication)
- การพิสูจน์ตัวตนโดยใช้ PIN (PIN authentication)
- การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP)
- การพิสูจน์ตัวตนโดยอัตลักษณ์ของบุคคล (Biometric authentication)
- Software & Hardware Token ที่ใช้สร้าง รหัสผ่านซึ่งมันจะมีการเปลี่ยนแปลงอยู่
- การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key cryptography)
- การพิสูจน์ตัวตนโดยใช้การถาม-ตอบ (zero-knowledge proofs)

Password-based

รหัสผ่านเป็นวิธีการพิสูจน์ตัวตนที่ใช้มานานและพบบ่อยที่สุด โดยที่รหัสผ่านจะประกอบไปด้วยตัวอักษร ตัวเลขหรืออักขระพิเศษ แต่อย่างไรก็ตามวิธีนี้ก็ถือว่าไม่ค่อยปลอดภัยมากเท่าที่ควร หากนำมาใช้งานแค่รหัสผ่านอย่างเดียวตามที่กล่าวไปแล้วก่อนหน้า เนื่องจากคนทั่วไปมักมี User หลายๆ User ทำให้มีรหัสผ่านจำนวนมากที่ต้องจำ ส่งผลให้หลายคนตั้งรหัสผ่านที่ใกล้ๆตัวเราแทน เช่นชื่อตัวเอง ชื่อแฟน วันเดือนปีเกิด เป็นต้น เพื่อที่จะได้จำได้ง่าย ๆ และก็จะตั้งรหัสผ่านเดียวแล้วใช้กับหลาย ๆ User ด้วยก็จะมีความเสี่ยงขึ้นไปอีก

One-Time Password: OTP

เป็นรหัสผ่านที่สามารถนำมาใช้ได้เพียง 1 ครั้ง และหลังจากนั้นรหัสผ่านนี้ก็จะไม่สามารถนำมาใช้ได้อีก เช่น OTP แรกที่ได้รับคือ “246810” ในเวลาต่อมาหากมีการทำรายการอีกครั้ง OTP จะเปลี่ยนเป็นเลขอื่นที่ไม่ใช่ “246810” อีกต่อไป ฉะนั้นจึงเป็นการยากต่อผู้อื่นในการที่จะคาดเดาได้ว่า OTP ของเราคือรหัสอะไร และมักจะนำ OTP มาให้ใช้ประกอบกับ Factor อื่นอยู่เสมอเช่นกัน

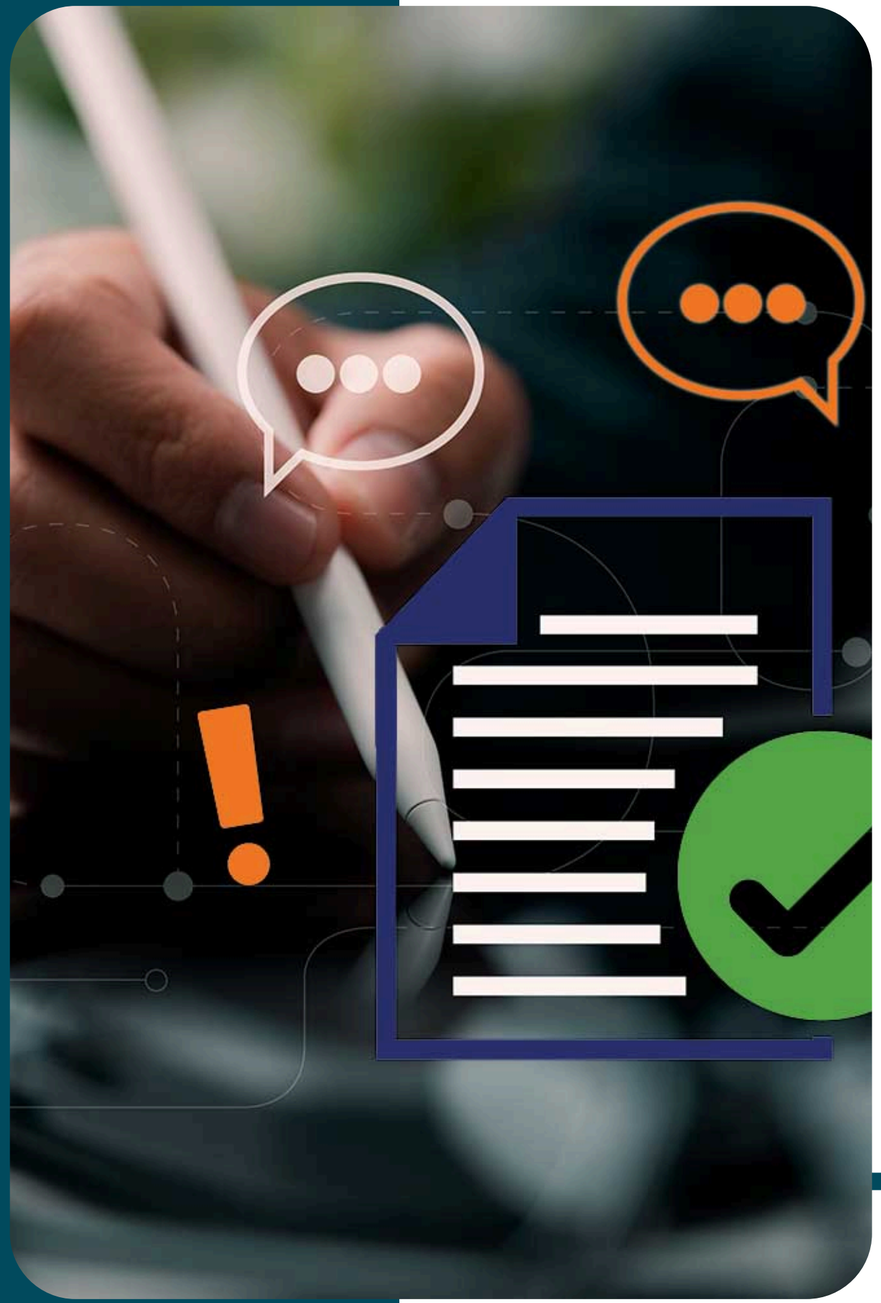
Biometric authentication

เป็นการนำเอาอัตลักษณ์ทางกายภาพของบุคคลซึ่งเป็นลักษณะเฉพาะที่ลอกเลียนแบบกันไม่ได้เช่น ใบหน้า ลายนิ้วมือ ม่านตา ลายเส้นเลือดฝอย มาใช้ในการพิสูจน์ตัวตน โดยวิธีการนี้จำต้องมีอุปกรณ์ฮาร์ดแวร์สนับสนุน เพื่อช่วยในการพิสูจน์ทราบอัตลักษณ์ดังกล่าว

Software & Hardware Token

ใช้ฮาร์ดแวร์ทำการสร้างรหัสผ่านซึ่งมันจะมีการเปลี่ยนแปลงอยู่ตลอดเป็น Dynamics Password โดยแบ่งวิธีการดังนี้

- การพิสูจน์ตัวตนแบบ Event-synchronous Authentication เมื่อเราต้องการที่จะเข้าสู่ระบบ เราก็จะต้องกด Token เพื่อให้ Token มัน Generate รหัสผ่านให้ จากนั้นนำรหัสผ่านที่ได้ไปเข้าใช้งานระบบ
- การพิสูจน์ตัวตนแบบ Time-synchronous authentication เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุกๆ 30 วินาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่รหัสผ่าน เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับ Server ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเซิร์ฟเวอร์จริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ



Public-key cryptography

เป็นการใช้เทคโนโลยี PKI มาช่วยในการพิสูจน์ตัวตน เนื่องจากข้อมูลใดก็ตามที่สร้างโดย Private Key ของคนๆนั้น จะถอดได้โดยใช้ Public Key ของคนๆนั้นเท่านั้น ดังนั้นหากเรายืนยันได้ว่า Public Key ที่นำมาใช้ถอดรหัสเป็นของคนนั้นจริง และสามารถถอดรหัสได้ เราก็สามารถยืนยันได้ว่าข้อความนั้นมาจากคนๆ นั้นจริง

สรุปภาพรวม

Single-factor authentication (SFA)

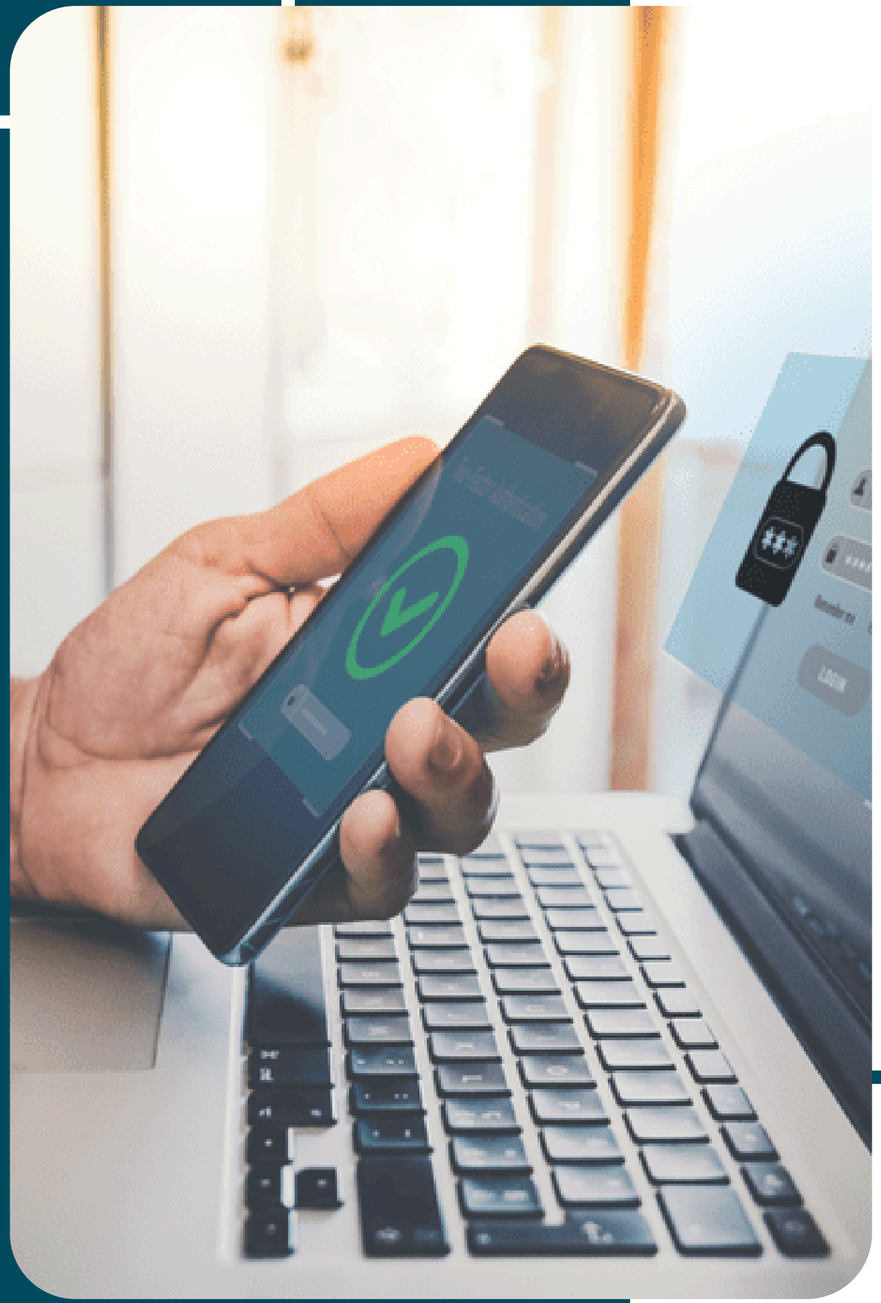
Whether you call it one-factor authentication or SFA, the idea is the same: using one set of credentials to access a secure system. It's the most traditional type of authentication and typically involves entering a username and password to log in to an app, platform or tool.

Two-factor authentication (2FA)

As the name suggests, 2FA adds an extra layer of protection by requiring two authentication factors. Rather than simply entering a username and password, 2FA goes one step further and requests another piece of information from users.

Multi-factor authentication (MFA)

An extension of 2FA is MFA. It provides one of the highest levels of security, like swapping your flimsy patterned phone case for a smashproof one. By now, you know that passwords alone often don't provide enough protection - especially when highly sensitive information is involved.



Multi-factor Authentication

การยืนยันตัวตนโดยใช้หลายปัจจัย (MFA) เป็นกระบวนการเข้าสู่ระบบแบบหลายขั้นตอน โดยกำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน ยกตัวอย่าง ระบบอาจขอให้ผู้ใช้ป้อนรหัสที่ส่งไปยังอีเมล์ ตอบคำถามลับ หรือสแกนลายนิ้วมือร่วมกับการป้อนรหัสผ่าน

ประโยชน์ของ MFA

ลดความเสี่ยงต่อการรักษาความปลอดภัย

การยืนยันตัวตนโดยใช้หลายปัจจัยลดความเสี่ยงที่เกิดจากความผิดพลาดของมนุษย์ การทำรหัสผ่านหาย และอุปกรณ์สูญหาย

ทำให้โครงการดิจิทัลเป็นไปได้

องค์กรสามารถดำเนินโครงการดิจิทัลได้ด้วยความมั่นใจ ธุรกิจใช้การยืนยันตัวตนโดยใช้หลายปัจจัยเพื่อช่วยปกป้องข้อมูลขององค์กรและข้อมูลผู้ใช้ เพื่อให้สามารถดำเนินการโต้ตอบและทำธุรกรรมทางออนไลน์ได้อย่างปลอดภัย

ปรับปรุงการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย

สามารถกำหนดค่าระบบการยืนยันตัวตนโดยใช้หลายปัจจัยเพื่อส่งการแจ้งเตือนในเชิงรุกเมื่อใดก็ตามที่ระบบตรวจพบความพยายามเข้าสู่ระบบที่น่าสงสัย ซึ่งเป็นประโยชน์ทั้งสำหรับบริษัทและบุคคลเพื่อให้ตอบสนองต่อการโจมตีทางไซเบอร์ได้เร็วขึ้น ซึ่งจะลดความเสียหายใด ๆ ที่อาจเกิดขึ้นได้

Our partner

HID CORPORATION

HID Global Corporation เป็นผู้พัฒนาผลิตภัณฑ์ยืนยันตัวตนจากสหรัฐอเมริกา เป็นบริษัทในเครือของ Assa Abloy ซึ่งเป็นกลุ่มบริษัทรักษาความปลอดภัยระดับโลกของสวีเดน ปัจจุบันมีคุณ Björn Lidefelt เป็นซีอีโอโดยเข้าดำรงตำแหน่งเมื่อวันที่ 27 มกราคม 2020

HID Global ก่อตั้งขึ้นในปี ค.ศ. 1991 ในชื่อ Hughes Identification Devices ซึ่งเป็นบริษัทในเครือของ Hughes Aircraft Company ซึ่งมีสำนักงานในรัฐแคลิฟอร์เนียและสกอตแลนด์ เริ่มแรกพัฒนาเทคโนโลยี RFID แบบ 125 กิโลเฮิรตซ์และ 400 กิโลเฮิรตซ์ ซึ่งริเริ่มโดย Destron/IDI (เดิมชื่อ Identification Devices Inc.) ในเมืองโบลเดอร์ รัฐโคโลราโด โดยส่วนใหญ่ใช้สำหรับการระบุสัตว์และระบบควบคุมการเข้าถึงแบบ Proximity และมีบางส่วนใช้ในกระบวนการผลิต การติดตามยางรถยนต์ และทรัพย์สิน Hughes Aircraft Company ซึ่งเป็นผู้จัดจำหน่ายไมโครชิปความถี่ต่ำให้กับ Destron/ID อยู่แล้ว ได้รับสิทธิ์แต่เพียงผู้เดียวในตลาดระบบควบคุมการเข้าถึงและอุตสาหกรรม ซึ่งนำไปสู่การก่อตั้ง Hughes Identification Devices

www.hidglobal.com

Björn Lidefelt
Executive Vice President and Head of HID Global

Idpassglobal

THANK YOU

เชิญซักถามข้อสงสัยในเรื่องเกี่ยวกับเทคโนโลยียืนยันตัวตนแบบหลายปัจจัย ตลอดจนแนวโน้มอาชญากรรมทางไซเบอร์/สงครามไซเบอร์ ความก้าวหน้าเทคโนโลยีปัญญาประดิษฐ์ส่งผลอย่างไรต่อ Cyber Security

PRESENTATION - 2025

www.idpassglobal.co