MK group
Smart Digital Security

THẾ GIỚI THẺ

Bản tin nội bộ của MK Group
Số 175 | Tháng 7.2025

02 MK DIGITAL SECURITY SOLUTIONS PLC ĐẠT CHỨNG NHẬN HỆ THỐNG QUẢN LÝ CHẤT LƯỢNG ISO 9001:2015

03 TỪ NGÀY 1/7/2025, THẺ ATM TỪ SẼ BỊ KHÓA VĨNH VIỄN

05 THẾ HỆ GEN Z ƯA THÍCH MUA SẮM TỰ THANH TOÁN

06 BÀN GIAO 10 TỶ CHIP INTEGRITY GUARD - CỘT MỐC KHẲNG ĐỊNH VỊ THẾ DẪN ĐẦU CỦA INFINEON

08 SUMSUB: GIAN LẬN GIẤY TỜ ĐỊNH DANH GIA TĂNG 300%

09 SCOTLAND: EDINBURGH TRAMS RA MẮT HỆ THỐNG THANH TOÁN KHÔNG TIẾP XÚC

09 THỤY SĨ CHUẨN BỊ GIỚI THIỆU THẺ ID SINH TRẮC HỌC

10 NĂM 2025 - BƯỚC NGOẶT TRONG HÀNH TRÌNH "ĐỊNH DANH 3.0"

https://mkgroup.com.vn contact@mkgroup.com.vn

Toàn bộ thông tin hình ảnh trong Bản tin này được sưu tầm từ các nguồn khác nhau và chỉ sử dụng cho mục đích chia sẻ - tham khảo thông tin.

MK DIGITAL SECURITY SOLUTIONS PLC ĐẠT CHỨNG NHẬN HỆ THỐNG QUẢN LÝ CHẤT LƯỢNG ISO 9001:2015

MK Digital Security Solutions PLC (MK DSS) - liên doanh chiến lược giữa MK Group (Việt Nam) và Neuronet (Ethiopia) đã chính thức được cấp Chứng Nhận Hệ Thống Quản Lý Chất Lượng ISO 9001:2015 bởi Ethiopian Conformity Assessment Enterprise (ECAE). Chứng nhận này không chỉ nhấn mạnh cam kết mạnh mẽ của MK DSS trong việc duy trì các tiêu chuẩn quản lý chất lượng cao nhất mà còn làm nổi bật vai trò tiên phong của liên doanh trong việc cung cấp các giải pháp bảo mật kỹ thuật số tại khu vực Đông Phi.

ISO 9001:2015 là một tiêu chuẩn được công nhận toàn cầu, tập trung vào việc đáp ứng các yêu cầu của khách hàng và quy định, nâng cao sự hài lòng của khách hàng và liên tục cải thiện hiệu quả hoạt động. Với chứng nhận này, MK DSS thể hiện khả năng cung cấp nhất quán các sản phẩm và dịch vụ đáp ứng mong đợi của khách hàng cũng như các yêu cầu pháp lý và quy định hiện hành, đặc biệt trong bối cảnh các nhu cầu cụ thể của thị trường Đông Phi đang phát triển.

Phạm vi của chứng nhận bao gồm "Sản xuất, bán hàng và dịch vụ cá nhân hóa thẻ thông minh" (mã IAF 9, 14 & 33). Điều này phản ánh chuyên môn của nhà máy sản xuất thẻ MK DSS trong một lĩnh vực quan trọng, đảm bảo rằng tất cả các quy trình từ sản xuất đến phân phối và cá nhân hóa đều tuân thủ các giao thức quản lý chất lượng nghiêm ngặt nhất, sẵn sàng đáp ứng các tiêu chuẩn và nhu cầu cụ thể của khu vực Đông Phi, từ thẻ căn cước quốc gia, thẻ tài chính đến các loại thẻ chuyên dụng khác.

Việc đạt được Chứng nhận ISO 9001:2015 là một cột mốc quan trọng đối với MK DSS. Đây là minh chứng cho sự cống hiến không ngừng nghỉ của đội ngũ công ty trong việc xây dựng một hệ thống quản lý chất lượng mạnh mẽ, tập trung vào việc mang lại giá trị vượt trội cho khách hàng và đối tác. Là một liên doanh của MK Group, MK DSS cam kết củng cố hơn nữa vị thế của mình như một nhà cung cấp giải pháp thẻ đáng tin cậy, đáp ứng các nhu cầu đang phát triển của khu vực Đông Phi cũng như duy trì các tiêu chuẩn cao này trong tương lai.

Chứng nhận được cấp vào ngày 30 tháng 6 năm 2025 và có hiệu lực đến ngày 29 tháng 6 năm 2028.

Về MK Digital Security Solutions PLC:
MK Digital Security Solutions PLC (MK DSS) là một liên doanh giữa MK Group (Việt Nam) và Neuronet (Ethiopia) - một nhà cung cấp giải pháp thẻ thông minh và xác thực an toàn tại Ethiopia và các quốc gia lân cận. Với việc sở hữu một nhà máy thẻ hiện đại đang được xây dựng tại Addis Ababa, Ethiopia, MK DSS nỗ lực trở thành đối tác đáng tin cậy cho các sản phẩm thẻ thông minh, giải pháp cá nhân hóa, giải pháp định danh điện tử và giải pháp xác thực đa yếu tố cho thị trường nội địa Ethiopia và các quốc gia khác ở Châu Phi.

ECAE Ethiopian Conformity Assessment Enterprise Certification

CERTIFICATE

QUALITY MANAGEMENT SYSTEM

Registration number: No. ECAE/QS/0163

The company

MK DIGITAL SECURITY SOLUTIONS PLC

Address: Addis Ababa, Bole Sub city, Woreda 11, Ethiopian IT Park, Tel: +251114703044

Email: contact@mkdss.et Website: https://mkdss.com.et

has implemented a Quality Management System and complies with the requirements of

ISO 9001:2015 Quality Management System—Requirements

for the following activities:

"Smart Cards manufacturing, sales and personalization service"

(IAF code 9, 14 & 33)

Issued on: 30 June, 2025

Effective date: 30 June, 2025

Date of first issue: 30 June, 2025

Valid Until: 29 June, 2028

The validity of certificate can be checked on www.eca-e.com

Authorized by

https://ecae.org.et

ECAE CD
11145
Addis Ababa, Ethiopia
+251 118 78 75 17
Fax: +251 116 45 97 20
info-cd@eca-e.com

IAF CAS Certification Body QMS0001

የኢትዮጵያ የተስማሚነት ምዘና ድርጅት
Ethiopian Conformity Assessment Enterprise

info-ccmd@ecae.org.et

TIN VẮN NGÂN HÀNG

- **Từ ngày 26/06/2025 đến hết 31/07/2025, Ngân hàng Thương mại cổ phần Ngoại thương Việt Nam (Vietcombank)** thực hiện chương trình ưu đãi giảm tối đa 100.000 VNĐ cho các khách hàng khi giao dịch thanh toán Apple Pay bằng thẻ Vietcombank Connect24 trên thiết bị Payoo POS ở các gian hàng tại AEON MALL trên toàn quốc;

- **Từ ngày 09/06 cho đến hết ngày 09/09/2025, Ngân hàng Thương mại cổ phần Sài Gòn Thương Tín (Sacombank)** triển khai chương trình ưu đãi hoàn tiền lên tới 600.000 VNĐ dành cho các khách hàng mở mới và sử dụng thẻ tín dụng quốc tế Sacombank JCB và JCB Ultimate;

- **Từ 01/06 đến hết 31/08/2025, Ngân hàng thương mại cổ phần Phát triển Thành phố Hồ Chí Minh (HDbank)** triển khai khuyến mãi tặng voucher 50.000 VNĐ khi thêm thẻ tín dụng quốc tế HDBank Mastercard vào ví Apple Pay và tặng thêm voucher lên tới 200.000 VNĐ khi chi tiêu bằng thẻ qua Apple Pay./.

Quý độc giả vui lòng truy cập vào website chính thức hoặc gọi điện trực tiếp cho các ngân hàng và tổ chức thẻ để biết thêm chi tiết.

Từ ngày 1/7/2025, thẻ ATM từ sẽ bị khóa vĩnh viễn

Kể từ ngày 1/7/2025, toàn bộ thẻ ATM sử dụng công nghệ từ sẽ bị ngừng chấp nhận giao dịch trên toàn hệ thống ngân hàng. Quy định này áp dụng với tất cả các loại thẻ có dải từ, bao gồm cả thẻ chỉ có dải từ và thẻ kết hợp chip với từ.

Đây là nội dung quan trọng trong lộ trình hiện đại hóa thanh toán không dùng tiền mặt và đảm bảo an toàn hệ thống tài chính – ngân hàng, được quy định cụ thể tại Thông tư 18/2024/TT-NHNN về hoạt động thẻ ngân hàng và Công văn 1099/NHNN-TT ngày 19/02/2025 của Ngân hàng Nhà nước. Các ngân hàng thương mại như Vietcombank, BIDV, Agribank... đã thông báo rộng rãi đến khách hàng về việc ngừng giao dịch thẻ từ từ mốc thời gian trên.

Ông Phạm Anh Tuấn, Vụ trưởng Vụ Thanh toán (Ngân hàng Nhà nước), cho biết: "Sau khi đánh giá, chúng tôi nhận thấy nhiều tổ chức tội phạm vẫn đang lợi dụng việc sử dụng thẻ từ để thực hiện hành vi đánh cắp dữ liệu qua hình thức skimming tại các máy ATM. Trên cơ sở đó, Ngân hàng Nhà nước quyết định chấm dứt hoàn toàn việc chấp nhận thẻ từ trong giao dịch từ ngày 1/7/2025".

Ông Phạm Anh Tuấn tin tưởng rằng: "Với công nghệ của thẻ chip, kẻ gian sẽ không thể lấy cắp được thông tin khách hàng giao dịch qua các máy tự động, POS. Điều này góp phần tạo sự yên tâm, an ninh và an toàn cho khách hàng khi thanh toán".

Các ngân hàng đang khuyến cáo khách hàng chủ động kiểm tra lại loại thẻ ATM mình đang sử dụng. Nếu mặt sau của thẻ có dải băng từ màu đen mà không có chip tích hợp ở mặt trước, người dùng cần sớm liên hệ ngân hàng để thực hiện chuyển đổi sang thẻ chip nội địa.

Việc chuyển đổi thẻ hiện có thể thực hiện dễ dàng tại chi nhánh, phòng giao dịch hoặc qua các kênh ngân hàng điện tử (mobile banking) tùy theo từng ngân hàng. Với các thẻ đã tích hợp chip, người dùng có thể tiếp tục sử dụng bình thường mà không cần đổi mới.

Sau thời điểm 1/7/2025, những thẻ chưa chuyển đổi sẽ không thể thực hiện các giao dịch như: rút tiền, gửi tiền tại máy ATM và CDM, thanh toán tại các điểm chấp nhận thẻ POS, giao dịch liên ngân hàng... Trong một số trường hợp, thẻ có thể bị khóa hoàn toàn, gây ảnh hưởng lớn đến việc sử dụng tài khoản của khách hàng.

VNgân hàng Nhà nước và các ngân hàng thương mại cũng cảnh báo người dân cần nâng cao cảnh giác trước các hành vi lừa đảo liên quan đến việc chuyển đổi thẻ. Khách hàng không nên cung cấp thông tin cá nhân, mã PIN, mật khẩu hay mã OTP cho bất kỳ cuộc gọi hay tin nhắn nào tự xưng là nhân viên ngân hàng. Trong trường hợp gặp khó khăn khi chuyển đổi qua ứng dụng, khách hàng nên trực tiếp đến quầy giao dịch để được hỗ trợ chính thức, tránh bị lợi dụng trong các tình huống giả mạo.

Không chỉ ngừng giao dịch bằng thẻ từ, từ ngày 1/7/2025, các ngân hàng cũng sẽ tạm ngưng giao dịch đối với các tài khoản tổ chức, doanh nghiệp chưa cập nhật thông tin sinh trắc học của người đại diện pháp luật. Việc này nhằm đảm bảo tuân thủ các yêu cầu định danh khách hàng theo quy định của Ngân hàng Nhà nước, giúp phòng ngừa rủi ro mạo danh, sử dụng tài khoản thuê hoặc mượn để thực hiện hành vi lừa đảo.

(VTV)

Thế hệ Gen Z ưa thích mua sắm tự thanh toán

Báo cáo từ PYMNTS Intelligence, mang tên "Chuyển đổi thương mại: Công nghệ AI và IoT đang định hình lại ngành bán lẻ tự động", hợp tác với Cantaloupe, cho thấy nhu cầu của người tiêu dùng đối với trải nghiệm mua sắm tự động, không ma sát tiếp tục tăng cao. Xu hướng này đang thúc đẩy việc áp dụng mô hình thương mại tự phục vụ vượt ra khỏi ứng dụng ban đầu trong bán lẻ và cả những yêu cầu nảy sinh từ đại dịch.

Hiện nay, ngành bán lẻ đã ra mắt thị trường thế hệ giải pháp tự phục vụ tiên tiến, được thiết kế đặc biệt để xử lý các rủi ro thất thoát và làm cho trải nghiệm mua sắm tiện dụng, trơn tru hơn đối với người tiêu dùng.

Sự ra đời của AI và các mạng lưới IoT – những thiết bị kết nối cho phép trao đổi dữ liệu theo thời gian thực – đã tạo nên các giải pháp đột phá có khả năng giải quyết đồng thời cả các thách thức về nhân lực lẫn vận hành. Từ cửa hàng tiện lợi trong khu phố đến các điểm trung chuyển đông đúc, các công nghệ tự phục vụ thông minh, tiên tiến đang mang đến trải nghiệm an toàn, không ma sát mà khách hàng mong đợi, đồng thời cung cấp cho doanh nghiệp dữ liệu hoạt động cần thiết để vận hành hiệu quả.

Cũng trong bản báo cáo từ PYMNTS Intelligence, dự báo đến năm 2030, hệ thống tự thanh toán (Self-Checkout) sẽ tăng gấp đôi.

50% người tiêu dùng Gen Z tại Mỹ và Anh khi được hỏi đã cho biết rằng họ sẵn sàng chuyển sang mua sắm tại nhà bán lẻ khác nếu có giải pháp tự thanh toán hiện đại và nhanh chóng hơn.

69% giao dịch tại máy bán hàng tự động trong năm 2023 là thanh toán không tiền mặt, trong đó **65% sử dụng phương thức thanh toán không tiếp xúc**. Với trung bình giá trị thanh toán không tiền mặt tại máy bán hàng là 2,26 USD, cao hơn 55% so với thanh toán sử dụng tiền mặt./.

(PYMNTS)

MK group
Smart Digital Security

HỆ SINH THÁI MK BANKID

Các giải pháp xác thực bảo mật trên không gian số

MK eID

Giải pháp định danh, xác thực khách hàng sử dụng thẻ CCCD gắn chip

Xác thực sinh trắc học

Giải pháp thực hiện đối sánh, xác thực sinh trắc học khuôn mặt, vân tay của khách hàng dựa trên các đặc điểm sinh trắc học duy nhất

MK KeyPass OTP

Giải pháp xác thực mạnh KeyPass™ OTP với các phương thức xác thực từ OTP cơ bản, OTP nâng cao có chức năng ký giao dịch

MK FIDO2

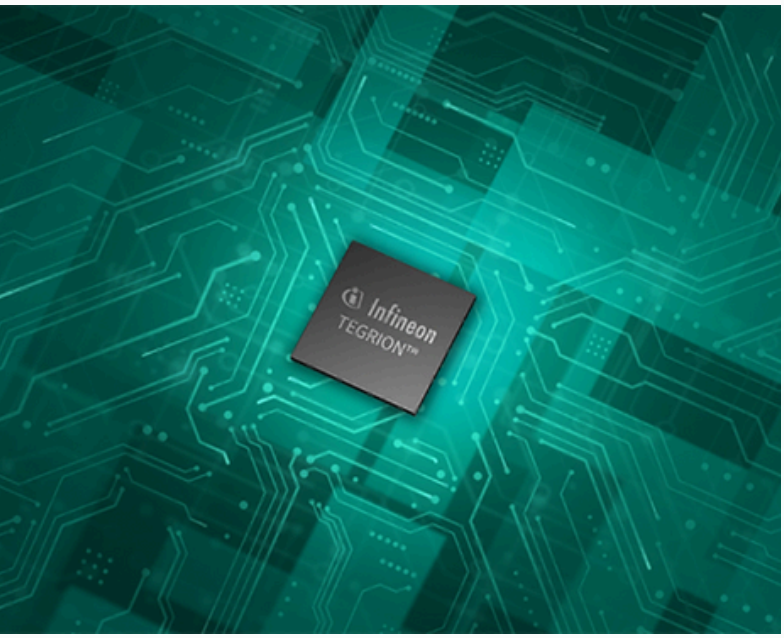
Giải pháp xác thực mạnh tuân thủ chuẩn FIDO2, phương pháp chống phishing hiệu quả

MK SmartCA - Remote signing

Dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa ứng dụng công nghệ đám mây (cloud-based)

Hà Nội: (024) 7100 6781
Tp. Hồ Chí Minh: (028) 3930 1055

Bàn giao 10 tỷ chip Integrity Guard - Cột mốc khẳng định vị thế dẫn đầu của Infineon



Vi xử lý bảo mật là một phần thiết yếu trong đời sống số hiện đại. Chúng được tích hợp trong hộ chiếu điện tử, thẻ căn cước, thẻ thanh toán và điện thoại thông minh, nhằm bảo vệ dữ liệu cá nhân và danh tính điện tử của hàng tỷ người trên toàn cầu. Kể từ khi được giới thiệu, đã có hơn 10 tỷ chip vi xử lý bảo mật dựa trên kiến trúc bảo mật Integrity Guard của Infineon Technologies AG được cung cấp - đánh dấu cột mốc quan trọng trong quá trình công nghệ này được chấp nhận rộng rãi trên toàn cầu.

Để khắc chế những mối đe dọa ngày càng phức tạp, chính các bộ vi xử lý cũng phải đáp ứng các tiêu chuẩn bảo mật cao nhất. Các nguyên lý nền tảng của kiến trúc Integrity Guard- được giới thiệu hơn 15 năm trước cùng với dòng vi xử lý bảo mật 16-bit đầu tiên, SLE78 - kể từ đó đã trở thành thành phần cốt lõi trong danh mục vi xử lý bảo mật của Infineon.

Được thiết kế để mang lại mức độ bảo vệ cao, Integrity Guard được tích hợp trong nhiều dòng sản phẩm vi xử lý bảo mật của Infineon và nổi bật với cấu trúc dual-CPU cùng khả năng phát hiện lỗi dựa trên phần cứng. Đáp ứng nhu cầu ngày càng lớn về bảo mật và chứng nhận, Infineon đang bổ sung một sản phẩm mới vào danh mục vi xử lý bảo mật của Tập đoàn: TEGRION™ SLC27G với kiến trúc bảo mật Integrity Guard 32.

Ông Maurizio Skerlj - Phó Chủ tịch cấp cao kiêm Giám đốc sản phẩm Giải pháp Xác thực và Danh tính tại Infineon Connected Secure Systems - chia sẻ: "Với hơn 10 tỷ vi xử lý bảo mật tích hợp Integrity Guard được xuất xưởng, về mặt thống kê, chúng tôi đã tiếp cận toàn bộ dân số thế giới bằng kiến trúc bảo mật của mình...

Và giá trị của các vi xử lý bảo mật mạnh mẽ nay đã trở nên rõ ràng hơn bao giờ hết. Chúng ta đang phải đối mặt với làn sóng tấn công mạng toàn cầu gia tăng mạnh mẽ, đi kèm với quá trình số hóa ngày càng sâu rộng - vốn mở ra nhiều cánh cửa cho tội phạm mạng, trong khi các quy định pháp lý ngày càng siết chặt như Đạo luật về khả năng phục hồi trên không gian mạng (CRA) của Liên minh châu Âu (EU). Tất cả những vấn đề này cho thấy nhu cầu cấp thiết về các giải pháp bảo mật tiên tiến. Và chính ở đây, sản phẩm mới thuộc dòng Integrity Guard 32 - TEGRION SLC27G - đã xuất hiện".

Vi xử lý giao diện kép và không tiếp xúc TEGRION SLC27G được thiết kế cho các ứng dụng định danh, thanh toán và xác thực bảo mật trong tương lai. Dựa trên bộ lệnh mạnh mẽ 32-bit Arm® v8-M, được Infineon tối ưu hóa với chuyên môn bảo mật của hãng, sản phẩm kết hợp giữa yếu tố an toàn, hiệu suất, tính hiệu quả và khả năng triển khai dễ dàng. Với kiến trúc bảo mật Integrity Guard 32 vượt trội, TEGRION SLC27G được trang bị đầy đủ để phục vụ yêu cầu bảo mật dài hạn và là lựa chọn lý tưởng cho các sản phẩm cần tuân thủ CRA.

Vi xử lý bảo mật TEGRION SLC27G hiện đang được Cơ quan An ninh Thông tin Liên bang Đức (BSI) đánh giá để cấp chứng nhận, với mục tiêu đạt được mức CC EAL6+. Bước đi này một lần nữa nêu bật cam kết không ngừng của Infineon đối với sự phát triển của lĩnh vực bảo mật trên toàn cầu./.

(Infineon)

Alipay tích hợp thanh toán vào kính AR

Alipay đã bắt đầu tích hợp thanh toán bằng mã QR vào kính thực tế tăng cường (AR) do công ty Trung Quốc Rokid sản xuất, nhằm cho phép người dùng khả năng mua sắm tại cửa hàng chỉ bằng cách nhìn vào nhãn.

Hơn 250.000 đơn vị Kính Rokid đã được đặt hàng, tích hợp với công nghệ thanh toán kỹ thuật số của Alipay dành cho kính AR.

Sau khi liên kết tài khoản Alipay của người dùng với ứng dụng Rockid, họ chỉ cần kích hoạt tính năng xác minh bằng giọng nói để bắt đầu và xác nhận giao dịch mua sau khi quét mã QR Alipay tại các cửa hàng.

Alipay cho biết công nghệ thanh toán mới này sẽ hoàn tất trong vài giây so với 20-30 giây đối với hình thức thanh toán QR qua điện thoại./.

(Finextra)

MK group Smart Digital Security
PRIMX MAKE ENCRYPTION HAPPEN

GIẢI PHÁP MÃ HÓA DỮ LIỆU CẤP CAO

BẢO MẬT - TIN CẬY - AN TOÀN

Giải pháp Prim'X áp dụng mã hóa theo một phương thức mới trong tổ chức doanh nghiệp nhằm bảo vệ tốt hơn nguồn tài nguyên dữ liệu, chống thất thoát, bị đánh cắp, rò rỉ và gián điệp kinh tế.

Các giải pháp của Prim'X mang tính tổng thể và trong suốt, có khả năng triển khai quy mô lớn, đáp ứng yêu cầu quản lý bảo mật thông tin qua việc quản lý quyền được biết nhằm chống lại những xâm nhập từ bên ngoài và bên trong tổ chức.

CÁC CHỨNG CHỈ CỦA GIẢI PHÁP PRIM'X

COMMON CRITERIA CERTIFIED EAL3+ · Bundesamt für Sicherheit in der Informationstechnik · EU RESTRICTED · NATO

Hà Nội: (024) 7100 6781
Tp. Hồ Chí Minh: (028) 3930 1055

Sumsub: Gian lận giấy tờ định danh gia tăng 300%

Sumsub vừa công bố báo cáo xu hướng gian lận định danh trong Quý 1 năm 2025, dựa trên dữ liệu nội bộ từ các nền tảng của họ, tiết lộ sự gia tăng đột biến của các hành vi gian lận có sử dụng công nghệ AI đang diễn ra tại Mỹ.

Theo dữ liệu từ Sumsub, gian lận deepfake đã tăng vọt tới 1.100%, trong khi gian lận giấy tờ định danh giả mạo (synthetic identity documents) tăng hơn 300%.

Các đối tượng phạm tội tận dụng công nghệ AI tạo sinh (Generative AI) để tạo ra các giấy tờ tùy thân, hộ chiếu và dữ liệu sinh trắc học giả mạo.

Sumsub đã phân tích hàng triệu lượt kiểm tra xác minh được thực hiện trên nền tảng của mình từ tháng 1 đến tháng 3 năm 2025, trải dài qua các ngành như fintech, thương mại điện tử, y tế công nghệ (healthtech) và công nghệ giáo dục (edtech) để nhận diện những xu hướng gian lận đang nổi lên.

Sự gia tăng của các loại giấy tờ định danh tổng hợp (synthetic ID) là một trong những mối quan ngại cấp thiết nhất, theo Sumsub, khi tội phạm mạng đang khai thác các công cụ AI để tạo ra giấy tờ giả như bằng lái xe hay hộ chiếu.

Những tài liệu giả mạo này thường đủ chân thực để vượt qua các quy trình kiểm tra KYC cơ bản, gây ra thách thức lớn cho các doanh nghiệp trong việc xác minh danh tính.

Sumsub báo cáo rằng gian lận giấy tờ tùy thân tổng hợp đã tăng vọt 311% ở khu vực Bắc Mỹ so với quý 1 năm 2024, khiến nó trở thành xu hướng tăng trưởng đáng báo động nhất của khu vực.

Bên cạnh đó, gian lận deepfake tăng vọt 1.100%, báo hiệu rằng công cụ Generative AI đang được sử dụng rất nhiều nhằm vượt qua các quy trình nhận dạng khuôn mặt và kiểm tra sinh trắc học.

Tại Mỹ, lĩnh vực fintech đặc biệt chứng kiến sự gia tăng mạnh mẽ các nỗ lực gian lận, điều này càng nhấn mạnh nhu cầu cấp thiết về các giải pháp phòng chống gian lận theo thời gian thực và đa lớp.

Trên toàn cầu, gian lận giấy tờ tùy thân tổng hợp đang gia tăng ở tất cả các khu vực, do sự tiếp cận rộng rãi với các công cụ GenAI có thể tạo ra ID giả có độ chân thực cao. Các thị trường hàng đầu về gian lận chứng từ nhận dạng tổng hợp bao gồm: Ethiopia (2,17%), Pakistan (2,08%), Nigeria (1,52%).

Sumsub cũng cảnh báo rằng các cuộc tấn công liên quan đến deepfake đang bùng nổ trên toàn cầu, đặc biệt nhằm đánh lừa, vượt qua hệ thống nhận dạng sinh trắc học – hiện đang là một trong những hình thức gian lận có tốc độ thích ứng và phát triển nhanh nhất.

(BiometricUpdate)

Scotland: Edinburgh Trams ra mắt hệ thống thanh toán không tiếp xúc

Hành khách di chuyển trên tuyến tàu điện Edinburgh Trams ở thành phố Edinburgh hiện có thể "chạm vào" và "chạm ra" khi sử dụng hệ thống giao thông công cộng này.

Từ ngày 19/5, hành khách có thể chạm thẻ hoặc thiết bị không tiếp xúc khi sử dụng mạng lưới xe điện của thành phố thủ phủ Scotland. Họ cần chạm thiết bị vào những chiếc Máy xác nhận tại sân ga khi bắt đầu hành trình, sau đó chạm để ra cổng sau khi rời khỏi tàu điện.

Edinburgh Trams cho biết hệ thống mới sẽ tính toán mức vé rẻ nhất dựa trên số lượng hành trình thực hiện, sau đó trừ tiền trong tài khoản thẻ vào đầu giờ sáng hôm sau. Hệ thống mới hoạt động song song với hệ thống TapTapCap hiện có của Lothian Buses để giới hạn chi phí đi lại bằng xe buýt và xe điện trong thành phố ở mức vé ngày./.

(Railtech)

Thụy Sĩ chuẩn bị giới thiệu thẻ ID sinh trắc học

Quốc gia này đang chuẩn bị ra mắt ID mới để phù hợp với Quy định của Liên minh Châu Âu EU - yêu cầu các quốc gia thành viên phải phát hành thẻ căn cước ID sinh trắc học từ năm 2021.

Mặc dù Thụy Sĩ không phải là thành viên EU, nhưng quốc gia này vẫn đang xây dựng các chiến lược để đáp ứng và tuân thủ các quy định khu vực chung.

Hộ chiếu sinh trắc học hiện tại của quốc gia này đã có chip chứa dữ liệu dấu vân tay và dữ liệu khuôn mặt của công dân chủ sở hữu.

Chính quyền Thụy Sĩ đã thông báo rằng công cuộc chuyển đổi trên thẻ ID sinh trắc học mới đã bắt đầu được tiến hành. Chip trên thẻ ID mới này chứa dữ liệu sinh trắc học sẽ giúp bảo vệ thẻ ID khỏi các hành vi làm giả, trong khi các dữ liệu bên trong thẻ chỉ có thể đọc trực tiếp với thẻ thực. Chỉ những quốc gia có chế độ bảo vệ dữ liệu tương đương với Thụy Sĩ mới có thể truy cập dữ liệu dấu vân tay được lưu trữ bên trong chip.

Cư dân Thụy Sĩ vẫn có thể sử dụng thẻ căn cước cũ, không có sinh trắc học của mình để đi lại khắp EU cho đến khi hết hạn hoặc tối đa trong 10 năm tiếp theo.

(BiometricUpdate)

Năm 2025 - bước ngoặt trong hành trình "định danh 3.0"

Định danh đã trải qua hành trình 20 năm qua. Quay ngược thời gian và định danh đã bắt đầu như một thứ mà chúng ta thực hiện trực tiếp - lòng tin được thiết lập trên cơ sở giữa người với người. Ví dụ, một tài khoản ngân hàng liên quan đến cuộc gặp trực tiếp nhân viên ngân hàng. Bạn tin tưởng nhân viên ngân hàng vì bạn có thể gặp họ ngoài đời, và họ tin tưởng bạn với tư cách là khách hàng khi gặp bạn tại chi nhánh. Đây là "Định danh 1.0".

Tiếp đó, trong 10 năm qua, thế giới đã tăng tốc mạnh mẽ hướng tới kỹ thuật số, chiều hướng chuyển dịch sang mạng trực tuyến và sự ra đời của điện thoại thông minh. Các mối tương tác được thực hiện từ xa, tăng phạm vi tiếp cận của các dịch vụ tài chính xuyên biên giới và xa hơn nữa. Chúng ta đã xây dựng cơ sở hạ tầng ngân hàng và thanh toán có khả năng giao dịch trong vài giây. Xác minh danh tính từ xa - trong đó, một người sử dụng điện thoại cá nhân để chụp ảnh giấy tờ tùy thân và khuôn mặt - là yếu tố quan trọng của không gian thanh toán. Ngày nay, định danh dựa trên tài liệu và sinh trắc học - "Định danh 2.0" - là một phần cốt lõi trong cuộc sống thường nhật của chúng ta.

Nhìn về tương lai, năm 2025 đánh dấu bước ngoặt trọng đại. Chúng ta đang bước vào kỷ nguyên mới: thế giới ưu tiên số hóa, nơi thông tin xác thực danh tính được hình thành trực tuyến, và trực tuyến luôn là lựa chọn số 1. Trong khi đó, bối cảnh hiện nay khác biệt rõ rệt so với 10 năm trước. "Định danh 2.0" đi kèm với những thách thức mới - từ gian lận đến Trí tuệ nhân tạo (AI), rồi đến tuân thủ. Định danh cần thích ứng với môi trường hiện nay để bắt kịp bước tiến của thời đại.

CÁCH TIẾP CẬN MỚI VỚI ĐỊNH DANH

Định danh không còn bị giới hạn trong ranh giới vật lý. Giờ đây, chúng bao gồm mọi thứ liên quan đến cá nhân, tổ chức hoặc thực thể trực tuyến - từ tên người dùng và mật khẩu đến thông tin sinh trắc học, chứng chỉ số và hành vi trực tuyến. Khi phạm vi định danh mở rộng, thì những thách thức đối với nhiệm vụ bảo mật danh tính cũng tăng theo.

GIAN LẬN NGÀY CÀNG DỄ TIẾP CẬN VÀ TINH VI HƠN BAO GIỜ HẾT

Mức độ ngày càng tinh vi của gian lận đòi hỏi những cách tiếp cận tinh vi hơn đối với định danh để ứng phó. Từ deepfake và gian lận dưới dạng dịch vụ, đến các thủ đoạn chia sẻ trực tuyến và phần mềm tinh vi có sẵn trên thị trường hoặc thông qua các nhóm như Telegram, thời đại của gian lận deepfake thời gian thực đã hiện hữu. Đối với các doanh nghiệp, gian lận có thể làm gia tăng tổng thiệt hại - các tổ chức toàn cầu tổn thất bình quân 5% doanh thu mỗi năm vì gian lận. Là ví dụ điển hình về những gì mà người tiêu dùng (NTD) đang bị đe dọa, NTD Mỹ đã mất 12,5 tỷ USD vào năm 2024, trong đó, 2 tỷ USD bị thất thoát thông qua các giao dịch chuyển khoản ngân hàng hoặc thanh toán.

TRẢI NGHIỆM KHÁCH HÀNG ĐẶC BIỆT LÀ ĐIỀU KIỆN TIÊN QUYẾT

Mức độ ngày càng tinh vi của gian lận đòi hỏi những cách tiếp cận tinh vi hơn đối với định danh để ứng phó. Từ deepfake và gian lận dưới dạng dịch vụ, đến các thủ đoạn chia sẻ trực tuyến và phần mềm tinh vi có sẵn trên thị trường

hoặc thông qua các nhóm như Telegram, thời đại của gian lận deepfake thời gian thực đã hiện hữu. Đối với các doanh nghiệp, gian lận có thể làm gia tăng tổng thiệt hại - các tổ chức toàn cầu tổn thất bình quân 5% doanh thu mỗi năm vì gian lận. Là ví dụ điển hình về những gì mà người tiêu dùng (NTD) đang bị đe dọa, NTD Mỹ đã mất 12,5 tỷ USD vào năm 2024, trong đó, 2 tỷ USD bị thất thoát thông qua các giao dịch chuyển khoản ngân hàng hoặc thanh toán.

MỨC ĐỘ PHỨC TẠP VÀ PHẠM VI YÊU CẦU TUÂN THỦ TIẾP TỤC GIA TĂNG

Từ các tiêu chuẩn định danh đang trên đà phát triển - bao gồm ETSI và NIST, đến eIDAS thay đổi luật chơi ở châu Âu với sự ra đời của ví điện tử và eID, yêu cầu tuân thủ đang gia tăng về phạm vi. Nhân loại đang hướng tới một tương lai mà chúng ta sẽ có nhiều phương thức khi đề cập đến danh tính - bao gồm ID vật lý, ID số, cơ sở dữ liệu, tín hiệu trên thiết bị... Viễn cảnh đó đồng nghĩa với việc có nhiều tùy chọn hơn, nhưng cũng đòi hỏi các giải pháp có khả năng mở rộng và linh hoạt hơn khi quản lý danh tính. Chính vì vậy, các nhóm tuân thủ cũng phải hiểu rõ những quy định như Đạo luật Tiếp cận và Đạo luật AI khi áp dụng và triển khai công nghệ.

Không có bất kỳ thách thức nêu trên nào tồn tại một cách riêng lẻ. Ưu tiên chính đối với các doanh nghiệp là quản lý sự cân bằng giữa rủi ro gian lận, bảo mật và trải nghiệm người dùng. Đây là nơi định danh trở thành yếu tố tạo điều kiện, thay vì cản trở. Định danh không phải là việc đặt ra các rào cản hoặc đối đầu với người dùng bằng một bức tường cứng nhắc. Vấn đề là đạt được sự cân bằng phù hợp - mang lại cho khách hàng chân chính quyền tiếp cận dễ dàng và tạo điều

kiện thuận lợi cho trải nghiệm của họ, đồng thời ngăn chặn kẻ gian ngay trong mọi giai đoạn của hành trình khách hàng.

Định danh không chỉ còn dành cho ngày đầu tiên. Thay vào đó, nó kết nối những khoảnh khắc quan trọng trong toàn bộ vòng đời khách hàng. Đảm bảo an toàn cho khách hàng trên mạng trực tuyến không chỉ có nghĩa là chứng minh danh tính trong ngày đầu tiên, mà còn đảm bảo rằng không ai kiểm soát tài khoản của họ vào ngày thứ 2, ngày thứ 20, ngày thứ 100 và xa hơn nữa.

HƯỚNG TỚI ĐỊNH DANH: Ý NGHĨA TRONG THỰC TẾ

Do gian lận ngày càng tinh vi và có khả năng mở rộng cao, khách hàng ngày càng khắt khe hơn bao giờ hết; đồng thời, hệ thống quy định đang đặt ra nhiều hạn chế hơn đối với cách thức hoạt động của doanh nghiệp. Bức tranh toàn cảnh của năm 2025 cho thấy nhiều giải pháp mà doanh nghiệp đang sử dụng hiện không còn phù hợp. Các giải pháp vá víu luôn mở đường cho các tác nhân xấu, cũng như khiến người dùng thực sự khó thực hiện những gì họ cần làm hàng ngày.

Vì vậy, mục tiêu đạt được sự cân bằng phù hợp giữa trải nghiệm người dùng, rủi ro và bảo mật sẽ tiếp tục là thách thức đối với người dùng và các tổ chức trong nhiều năm tới. 66% các tổ chức vẫn tin rằng trải nghiệm khách hàng và phòng ngừa gian lận là những ưu tiên trong cuộc cạnh tranh.

BẢO MẬT DANH TÍNH: ĐẢM BẢO QUYỀN TRUY CẬP TRONG TOÀN BỘ HÀNH TRÌNH KHÁCH HÀNG

Để phát huy toàn bộ sức mạnh của vòng đời khách hàng, cũng như ngăn ngừa gian lận và rủi ro bảo mật, các doanh nghiệp ngày nay cần bảo vệ những khoảnh khắc quan trọng trong hành trình của khách hàng bằng danh tính thực, được xây dựng trên cơ sở sinh trắc học đáng tin cậy, có độ đảm bảo cao ngay từ ấn tượng đầu tiên.

Khi những mối đe dọa ngày càng trở nên phức tạp hơn, các tổ chức phải đi đầu với những biện pháp chủ động góp phần giảm thiểu rủi ro ở mọi giai đoạn của quy trình.

- **Thu hút khách hàng mới:** Tuyến phòng thủ đầu tiên rất quan trọng vì đây là bước rất dễ bị kẻ gian sử dụng thông tin bị đánh cắp hoặc tổng hợp. Nếu không được thực hiện một cách an toàn, nó sẽ mở ra cánh cửa cho hành vi đánh cắp danh tính, nhồi thông tin xác thực và làm tổn hại lòng tin vào những thời điểm sau của vòng đời danh tính.

- **Truy cập hàng ngày:** Khi cá nhân sử dụng tài khoản và thực hiện giao dịch, rủi ro truy cập trái phép tăng lên gấp bội. Đối tượng tấn công có thể chặn thông tin xác thực thông qua lừa đảo, chiếm đoạt phiên hoặc khai thác các phương pháp xác thực yếu. Đây là lý do tại sao xác thực mạnh có vai trò hết sức quan trọng, đặc biệt là trong những thời điểm rủi ro cao như chuyển số tiền lớn hoặc ký các tài liệu mật.

- **Mở rộng dịch vụ:** Mở rộng mối quan hệ với khách hàng - chẳng hạn như cung cấp thẻ tín dụng, khoản vay hoặc dịch vụ mới - đồng nghĩa với nguy cơ tạo ra cơ hội mới cho gian lận. Nếu không xác minh danh tính một cách nhất quán, những điểm tiếp xúc có giá trị cao này có thể trở thành cơ hội kiếm lời cho kẻ xấu.

- **Bảo mật không ngừng:** Thách thức đối với nhiệm vụ duy trì bảo mật không kết thúc sau thiết lập ban đầu hoặc mỗi phiên. Giám sát liên tục là việc làm cần thiết, nhưng tính phức tạp của nhiệm vụ quản lý những mối đe dọa đang phát triển, tuân thủ các quy định và đảm bảo khả năng phản hồi theo thời gian thực có thể khiến nhiều tổ chức choáng ngợp. Các giao thức bảo mật thích ứng chính là chìa khóa để giải quyết cơn đau đầu này, bởi nếu không có chúng, nguy cơ bị xâm phạm dữ liệu, xử phạt theo quy định và thiệt hại do gian lận sẽ tăng cao..

CÁC THÀNH PHẦN CHÍNH CỦA BẢO MẬT DANH TÍNH

Một chiến lược bảo mật danh tính mạnh mẽ phải phản ánh được sự phức tạp nêu trên, kết hợp các công nghệ nhiều lớp xác minh, xác thực và giám sát danh tính ở quy mô lớn để ngăn chặn kẻ xấu tại mọi điểm truy cập trong suốt vòng đời danh tính.

Cách tiếp cận lý tưởng được xây dựng trên nền tảng tích hợp các khả năng thích ứng với những rủi ro và nhu cầu kinh doanh đang thay đổi:

- **Xác minh danh tính:** Xác nhận một người chính là cá nhân mà họ khai báo khi đăng ký sử dụng dịch vụ, thông qua thư viện các tín hiệu xác minh danh tính toàn cầu - bao gồm công nghệ sinh trắc học và tài liệu hỗ trợ AI - để xây dựng lòng tin với mức độ đảm bảo cao và ít gây cản trở, phát hiện gian lận và giải quyết nhu cầu tuân thủ ở quy mô lớn.

- **Quản lý danh tính và quyền truy cập:** Quản lý vai trò và quyền của người dùng để đảm bảo chỉ những cá nhân phù hợp mới được tiếp cận đúng tài nguyên để bạn có thể chống lại hành vi chiếm đoạt tài khoản - từ xác thực dựa trên rủi ro đến sinh trắc học, mã khóa và xác thực dựa trên chứng chỉ hoặc xác thực nâng cao.

- **Điều phối danh tính:** Điều phối mọi bước xác minh và xác thực trên các nền tảng, tự động hóa các quyết định dựa trên những chính sách được thiết lập trước.

- **Tín hiệu phát hiện gian lận:** Theo dõi hành vi và tín hiệu thiết bị theo thời gian thực để đánh dấu những biểu hiện bất thường và ngăn chặn các nỗ lực truy cập đáng ngờ.

- **Ký số:** Ký ở mọi nơi trên thế giới với mức độ bảo mật và tin cậy mà bạn cần. Hoạt động nhanh hơn, hiệu quả hơn và theo phương thức số hóa với sự hỗ trợ cho chữ ký điện tử tiên tiến, chữ ký điện tử đủ điều kiện và niêm phong tài liệu./.

(Entrust)

MK group
Smart Digital Security

KỶ NIỆM 26 NĂM NGÀY THÀNH LẬP MK GROUP
26th ANNIVERSARY 1999 - 2025
TỰ CƯỜNG SẢN XUẤT - TỰ CHỦ CÔNG NGHỆ - ĐỔI MỚI SÁNG TẠO

TRÂN TRỌNG CẢM ƠN QUÝ KHÁCH HÀNG, ĐỐI TÁC VÀ TOÀN THỂ MKERS ĐÃ LUÔN ĐỒNG HÀNH CÙNG MK GROUP SUỐT 26 NĂM PHÁT TRIỂN.

Chúng tôi hy vọng sẽ tiếp tục được sát cánh cùng Quý vị trên hành trình viết tiếp bản lĩnh công nghệ Việt – vươn xa hơn, vững chắc hơn và lan tỏa nhiều giá trị bền vững trong chặng đường phía trước.

https://mkgroup.com.vn
contact@mkgroup.com.vn

Trong trường hợp Quý độc giả không muốn nhận bản tin, hãy phản hồi cho chúng tôi theo địa chỉl:

- **Email: contact@mkgroup.com.vn**
- **Tiêu đề thư: Không nhận bản tin Thế Giới Thẻ MK**

Xin vui lòng truy cập vào website MK Group để hiểu rõ hơn về **Chính sách bảo mật và xử lý dữ liệu cá nhân** của chúng tôi.