THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 119 | Tháng 3 - 2021

MK group
Smart Digital Security

Tổng biên tập: *Bà Phan Thị Quỳnh Hoa - Giám đốc Tập đoàn MK* | **Ý kiến đóng góp vui lòng gửi về:** *marketing@mkgroup.com.vn*

Lưu ý: *Toàn bộ thông tin/hình ảnh trong Bản tin điện tử nội bộ Thế Giới Thẻ MK Group được sưu tầm từ các nguồn tin khác nhau và chỉ sử dụng cho mục đích chia sẻ kiến thức.*

CÁC TIN BÀI CHÍNH

MK GROUP : Thông báo chuyển địa điểm văn phòng Hà Nội

Kính gửi Quý khách hàng & Đối tác,

Chúng tôi xin trân trọng thông báo rằng hiện nay Công ty Cổ phần Tập đoàn MK cùng các công ty thành viên:

- Công ty Cổ phần Thông minh MK (MK Smart)
- Công ty Cổ phần MK Vision
- Công ty Cổ phần MK Hi-tek

sẽ chuyển Trụ sở từ địa chỉ cũ là:

Tầng 11-12, tòa nhà TTC, 19 Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội

sang địa chỉ mới tại:

Tòa nhà The Vista, số 4 ngõ 15 Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội
(Đây là tòa nhà do MK Group xây dựng và sở hữu)

Mọi giao dịch liên hệ xin Quý khách hàng & Đối tác vui lòng liên hệ theo địa chỉ mới của MK Group cùng các công ty thành viên hoặc liên hệ theo số điện thoại **+84-24 6266 2703** để được trợ giúp.

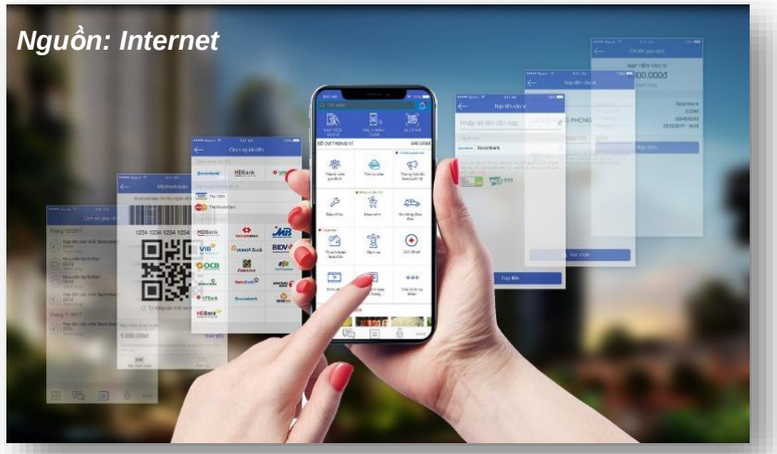
Xin cảm ơn sự lưu tâm của Quý khách hàng & Đối tác.

Trân trọng,

Tòa nhà The Vista, số 4 ngõ 15 Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

Thanh toán online lên ngôi khi các ngân hàng hợp tác cùng ví điện tử



Sự bùng nổ của thanh toán kỹ thuật số trong thời gian qua đã hối thúc các ngân hàng hợp tác với ví điện tử, mang đến hàng loạt ưu đãi cho người tiêu dùng.

Theo ghi nhận của Shopee, tổng số đơn đặt hàng được thanh toán qua ví điện tử AirPay trên toàn khu vực đã tăng trưởng gấp 4 lần. Trong đó, nhóm khách hàng tăng trưởng mạnh nhất ở hầu hết thị trường là những người dùng trên 50 tuổi, chứng tỏ ví điện tử này hoàn toàn dễ tiếp cận, kể cả với độ tuổi thường được xem là khó thích ứng với thanh toán kỹ thuật số nhất.

Ngân hàng không nằm ngoài cuộc chơi thanh toán số

Thực tế, thanh toán kỹ thuật số đang trở thành phương thức giao dịch phát triển mạnh mẽ không chỉ trên các sàn thương mại điện tử, mà còn trong chi tiêu hàng ngày của không ít người tiêu dùng. Số lượng cửa hàng sử dụng hình thức thanh toán qua ví AirPay tại Việt Nam cũng đã tăng gấp 2 lần trong năm 2020, bao gồm những đối tác như 7-Eleven, MyKingdom và Guardian.

Trong bối cảnh Chính phủ đang hướng tới một xã hội không tiền mặt, đại dịch Covid-19 càng thúc đẩy nhanh hơn xu thế này. Theo các khảo sát của Visa trong năm 2020, hơn 85% người Việt Nam sở hữu ít nhất một ví điện tử hoặc ứng dụng thanh toán. Đồng thời, có đến 51% người tiêu dùng tăng cường thanh toán bằng các ví điện tử. Đây là cơ hội cho các ví điện tử nói riêng và cộng đồng đối tác nói chung.

Bởi lẽ đó, các ngân hàng đã nhanh chóng nắm bắt thời cơ, hợp tác với các ví điện tử nhằm mang đến trải nghiệm liền mạch hơn cho khách hàng. Qua đó, ngân hàng cũng gia tăng độ nhận diện và lượng giao dịch thông qua số người dùng ngày càng tăng cao của các ví điện tử./.

(ICTNews)

TIN VẮN THẺ NGÂN HÀNG

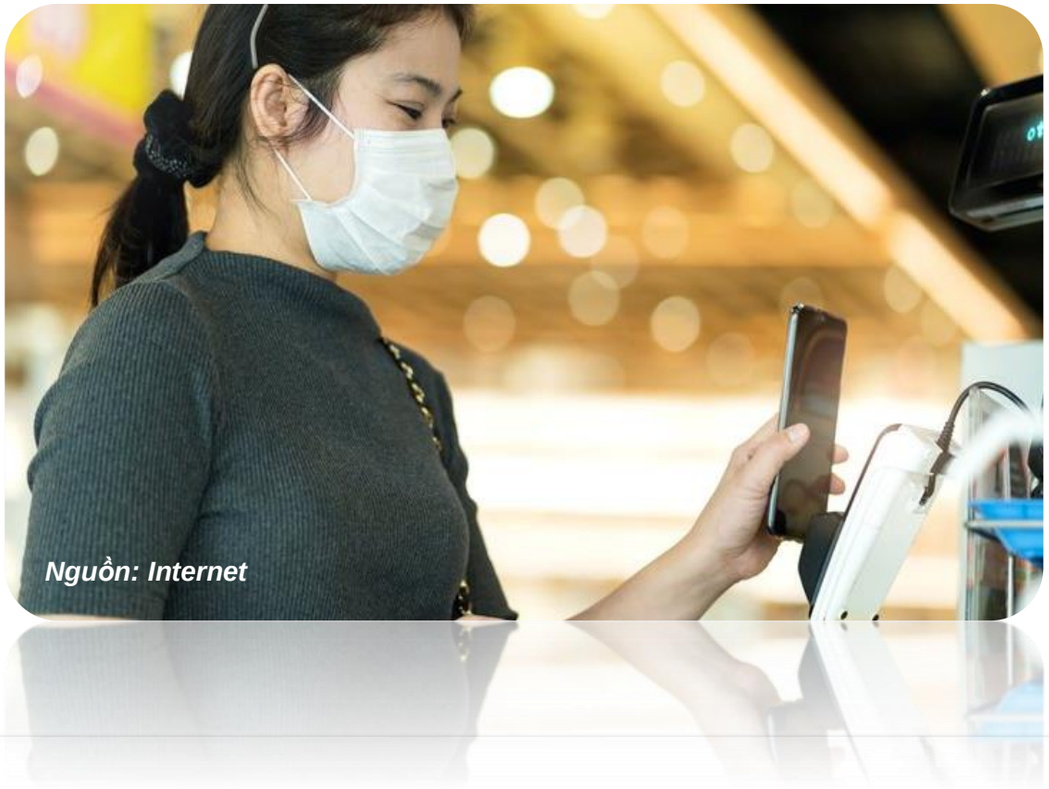
- **Từ ngày 8/3/2021 cho đến hết ngày 31/05/2021, Ngân hàng TMCP Quốc tế Việt Nam (VIB)** triển khai chương trình ưu đãi "Mở thẻ chi tiêu, hoàn tiền nhân ba" đối với bất kỳ khách hàng đăng ký mở thẻ tín dụng của VIB. Cụ thể, mỗi chủ thẻ sẽ được hoàn phí thường niên nếu thỏa mãn điều kiện chi tiêu tối thiểu.

- **Từ ngày 11/3/2021 cho đến hết tháng 3/2021, Ngân hàng Á Châu (ACB)** liên kết với ví điện tử AirPay đưa ra những ưu đãi khuyến khích khách hàng mua sắm trực tuyến trên Shopee. Các chương trình ưu đãi sẽ bao gồm giảm giá, tặng voucher, miễn phí vận chuyển,…

- **Từ 01/03/2021 đến hết 31/05/2021, Ngân Hàng Thương Mại Cổ Phần Ngoại Thương Việt Nam (Vietcombank)** triển khai chương trình ưu đãi dành riêng cho chủ thẻ đồng thương hiệu Saigon Centre – Takashimaya - Vietcombank. Theo đó, khi Khách hàng phát hành mới thẻ tín dụng Đồng thương hiệu này và thực hiện chi tiêu tối thiểu 1.000.000 VNĐ sẽ nhận ngay Thẻ quà tặng 1.000.000 VNĐ với số lượng hạn chế./.

(Tổng hợp từ Internet)

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999



Ấn Độ: Cho phép rút tiền ATM không cần thẻ

Các chủ thẻ tại Ấn Độ hiện đã có thể bắt đầu rút tiền mặt tại các ATM mà không hề phải dùng đến thẻ hay ấn vào màn hình của máy ATM.

AGS Transact Technologies Limited đã tiến hành hợp tác với Mastercard để cho ra mắt hệ thống rút tiền mặt không tiếp xúc đầu cuối bằng ứng dụng di động tại Ấn Độ, theo một báo cáo trên The Quint.

Chủ thẻ ATM giờ đây chỉ cần quét mã QR trên màn hình của máy bằng thiết bị di động của họ và sau đó các giao dịch rút tiền sẽ được thực hiện trên ATM như bình thường mà không cần phải chạm vào bề mặt ATM./.

(ATMmarketplace)

Samsung hợp tác cùng Mastercard ra mắt thẻ thanh toán sinh trắc học

Nguồn: Internet

Chiếc thẻ mới này sẽ sử dụng nhận dạng vân tay để xác minh danh tính của chủ thẻ và sẽ được chấp nhận tại các thiết bị đầu cuối thanh toán Mastercard.

Trên chiếc thẻ sẽ được tích hợp màn hình cảm biến có thể nhận dạng vân tay khi hoạt động và chúng sẽ không cần tới mã PIN.

Mastercard đưa ra giải pháp thẻ thanh toán sinh trắc học này nhằm tăng cường thêm bảo mật cho chủ thẻ dựa trên những sáng kiến chuyên môn tiên tiến về an ninh mạng và mạng lưới thanh toán toàn cầu của họ.

Thẻ này ban đầu sẽ được phát hành tại Hàn Quốc và cung cấp cho các khách hàng doanh nghiệp có giao dịch quốc tế thường xuyên. Samsung sẽ bắt đầu phát hành thẻ doanh nghiệp cho khách hàng Hàn Quốc vào cuối năm 2021./.

(Finextra)

Giao dịch ví di động có xu hướng vượt thanh toán tiền mặt

Nguồn: Internet

FIS mới đây đã phát hành Báo cáo Thanh toán Toàn cầu năm 2021 và nghiên cứu này cho thấy thanh toán bằng ví kỹ thuật số tại các điểm bán hàng POS đang phát triển nhanh hơn so với thanh toán bằng thẻ.

Cũng trong bản báo cáo này cho biết các khoản thanh toán không tiếp xúc tại các cửa hàng được thực hiện bằng phương thức ví di động trên toàn thế giới lần đầu tiên vượt qua thanh toán bằng tiền mặt tại cửa hàng trong năm 2020.

Theo bản báo cáo, việc tiêu dùng tiền mặt đã giảm 10%, ước tính tương đương với 20% trên tổng số thanh toán trực tiếp được thực hiện trên toàn cầu, trong khi số lượng thanh toán bằng ví kỹ thuật số không tiếp xúc tại các điểm bán hàng POS cũng đang tăng nhanh hơn so với các khoản thanh toán bằng thẻ vật lý.

Thống kê cho thấy các khoản thanh toán bằng tiền mặt tại các cửa hàng của các quốc gia như Anh, Canada, Pháp, Na Uy, Thụy Điển và Úc đã giảm từ 50% trở lên trong năm 2020.

Báo cáo dự đoán cho đến năm 2024, tiền mặt sẽ chiếm dưới 10% các khoản thanh toán tại cửa hàng tại Mỹ và chiếm 13% thanh toán trên toàn thế giới, trong khi thanh toán bằng ví kỹ thuật số sẽ tiếp tục tăng trưởng để chiếm 1/3 thanh toán tại cửa hàng trên toàn cầu (~33%).

Các giao dịch thương mại điện tử dựa trên ví kỹ thuật số đã tăng 7% trong năm 2020 và báo cáo dự đoán rằng vào năm 2024, thanh toán ví kỹ thuật số sẽ chiếm hơn một nửa tổng số thanh toán thương mại điện tử trên toàn thế giới" và "việc sử dụng các phương thức thanh toán truyền thống như thẻ và giao hàng tận nơi đang nhanh chóng bị thoái trào và dự kiến sẽ chỉ chiếm dưới 40% phương thức thanh toán giao dịch thương mại điện tử vào năm 2024"./.

(Finextra)

UNCTAD: COVID-19 ảnh hưởng sâu sắc đến lĩnh vực thanh toán số

Theo báo cáo của Hội nghị Liên hợp quốc về Thương mại và Phát triển (UNCTAD), các doanh nghiệp thương mại điện tử tại 23 quốc gia nghèo trên thế giới đã nhận thấy "tốc độ tăng trưởng đáng kể" của hoạt động thanh toán số do tác động của đại dịch COVID-19.

64% số doanh nghiệp thương mại điện tử được khảo sát đã xác nhận về những thay đổi trong các phương thức thanh toán kể từ khi đại dịch bắt đầu bùng phát, cũng như tốc độ tăng trưởng mạnh mẽ của thanh toán di động, Sngân hàng trực tuyến và di động, thanh toán thẻ tín dụng và các nền tảng thanh toán số khác.

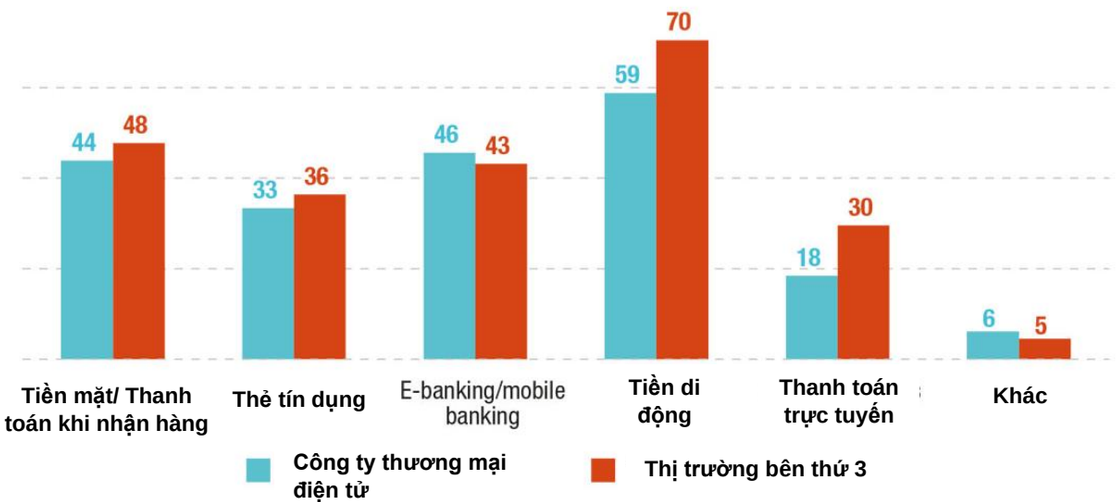
Tuy nhiên, hình thức trả tiền mặt khi giao hàng vẫn là xu hướng chủ đạo, đặc biệt là ở những quốc gia có trình độ phát triển thấp nhất (LDC) được liệt kê trong báo cáo.

Nghiên cứu "COVID-19 và thương mại điện tử: Tác động đến doanh nghiệp và phản hồi chính sách" của UNCTAD cũng cho thấy, "trong khi 58% doanh nghiệp cung cấp các sản phẩm hoặc dịch vụ theo đường trực tuyến bị sụt giảm doanh thu hàng tháng, thì khoảng 64% trong số các thị trường bên thứ 3 đã chứng kiến sự gia tăng đột biến trong doanh số bán hàng".

Báo cáo nhấn mạnh, một số quốc gia châu Á và châu Phi đang khuyến khích sử dụng thanh toán số và hỗ trợ, củng cố môi trường kinh doanh thương mại điện tử./.

(NFCW)

Biểu đồ tăng trưởng các hình thức thanh toán kể từ sau đai dịch COVID-19 bùng phát



Nguồn: Internet

CaixaBank triển khai thay thế thẻ nhựa bằng vật liệu tái chế

Ngân hàng CaixaBank của Tây Ban Nha là ngân hàng cho vay mới nhất bắt đầu triển khai phát hành thẻ làm từ nhựa tái chế và các thành phần có khả năng phân hủy tự nhiên.

Ngân hàng có hơn 18,8 triệu thẻ đã được phát hành cho biết trong năm nay họ sẽ bắt đầu ngừng sử dụng nhựa nguyên sinh để sản xuất thẻ vật lý.

CaixaBank dự kiến 85% số thẻ mới được họ phát hành trong năm 2021 sẽ được làm từ vật liệu bền vững, với khoảng 5 triệu thẻ được làm từ vật liệu mới sẽ được lưu hành vào cuối năm nay.

Hầu hết các thẻ sẽ sử dụng nhựa PVC tái chế, có nguồn gốc từ những thứ như chất thải của ngành xây dựng. Một số sẽ sử dụng PLA, một vật liệu có khả năng phân hủy sinh học với nguồn gốc sinh học, giúp loại bỏ việc sử dụng tài nguyên khó phân hủy.

Bên cạnh đó, kỹ thuật in thông tin chi tiết trên thẻ của khách hàng cũng sẽ thay đổi, được chuyển từ việc in mực sang sử dụng công nghệ in laser nhằm giảm thiểu chất thải được tạo ra và còn giúp tăng tuổi thọ cho thẻ./.

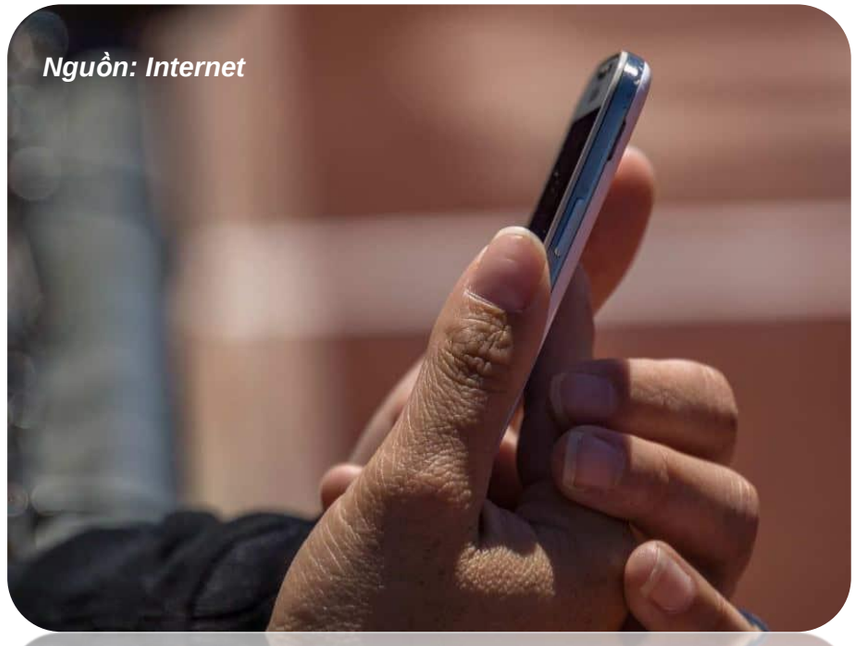
(Finextra)

Ứng dụng của Chính phủ Ấn Độ sắp có giao diện sinh trắc học khuôn mặt và giọng nói

Ứng dụng di động thống nhất dành cho công tác quản trị trong thời đại mới của Ấn Độ (UMANG) sẽ sớm ứng dụng công nghệ nhận dạng khuôn mặt để xác minh bằng các tính năng được tích hợp sẵn trong smartphone. Những thay đổi này được đưa ra sau khi có hơn 200.000 người gửi giấy chứng nhận còn sống thông qua ứng dụng UMANG chỉ trong tháng 11/2020, tăng 200% so với cả năm 2019.

Những người đã nghỉ hưu muốn tạo chứng nhận còn sống sẽ sớm được yêu cầu xác minh danh tính bằng công nghệ sinh trắc học, song ứng dụng của Chính phủ Ấn Độ yêu cầu người dùng phải có 1 trong 10 mẫu smartphone cao cấp tương thích. Ngoài yêu cầu sinh trắc học khuôn mặt, UMANG cũng sẽ giới thiệu giao diện giọng nói dựa trên trí thông minh nhân tạo (AI) để cung cấp khả năng tiếp cận và mở rộng cơ sở người dùng.

Việc hướng tới công nghệ tích hợp trong smartphone sẽ khiến các thiết bị xác minh sinh trắc học của bên thứ 3 trở nên lỗi thời vì điện thoại của người dùng trở thành giải pháp một cửa cho các dịch vụ tiện ích của chính phủ. Trước đây, các thiết bị sinh trắc học chuyên dụng cần được kết nối với smartphone qua cổng USB để đọc vân tay nhằm xác minh danh tính. Tuy nhiên, yếu tố chi phí và hạn chế trong khả năng sử dụng của chúng đã khiến Chính phủ Ấn Độ loại bỏ các thiết bị chuyên dụng và thực hiện xác minh bằng smartphone tích hợp sẵn công nghệ tiên tiến.



Nguồn: Internet

UMANG, do MeitY và NeGD phát triển vào năm 2017, cho phép truy cập vào 2.000 dịch vụ chính phủ điện tử do chính quyền trung ương và chính quyền các bang của Ấn Độ cung cấp. Ứng dụng được kết nối với hệ thống Aadhaar của quốc gia Nam Á này. Để đối phó với tốc độ gia tăng mạnh mẽ trong hoạt động số hóa các dịch vụ công, New Delhi cũng đang nỗ lực thể hiện ứng dụng bằng tất cả 22 ngôn ngữ chính thức của Ấn Độ. Đến nay, UMANG đã hỗ trợ 13 ngôn ngữ trong số đó.

Thành phố Hyderabad, thủ phủ của bang Telangana đã triển khai dịch vụ xác thực sinh trắc học vân tay tại nhà dành cho những người hưu trí để cung cấp giấy chứng nhận lương hưu Jeevan Praman./.

(Biometric Update)

Tự động mã hóa - giải mã giúp doanh nghiệp quản lý an toàn thông tin mạng

GIỚI THIỆU CHUNG:

Phòng vệ

Các tổ chức nhạy cảm và bộ phận công nghệ thông tin (CNTT) cần tổ chức phòng vệ trước những cuộc tấn công mạng. Tổ chức phòng vệ, xây dựng những quy trình chống đánh cắp hoặc do lỗi vô tình làm lộ thông tin sẽ giúp chống lại các nguy cơ thiệt hại tài chính, hủy hoại uy tín và đánh mất tài nguyên của doanh nghiệp. Một trong những giải pháp hiệu quả là thiết lập hệ thống mã hóa và giải mã dữ liệu.

Mã hóa là gì?

Mã hóa là phương pháp dùng thuật toán để coding một file hoặc một nội dung để những người khác không thể sử dụng được và không thể đọc hiểu được cho đến khi nó được giải mã. Một khi đã mã hóa, chỉ người dùng có thẩm quyền và khóa giải mã mới có thể đọc hiểu và truy cập thông tin. Mã hóa sử dụng một thuật toán phức tạp hoặc bộ quy tắc nội bộ để biến dữ liệu gửi đi thành một bí mật. Khi nhận được, dữ liệu này sẽ được giải mã nhờ khóa do người gửi cung cấp.

Hiệu quả bảo vệ của bất cứ công nghệ mã hóa nào được quyết định bởi độ dài của thuật toán, độ phức tạp của mật mã và giải pháp mã hóa được lựa chọn một cách phù hợp.

Quá trình mã hóa sẽ biến đổi các thông tin đang được lưu trữ đâu đó hay đang di chuyển trên hệ thống ở dạng văn bản thuần túy (plain text) thành các file không thể đọc được và chỉ người có thẩm quyền mới truy cập được. Người không được cấp phép chỉ nhìn thấy một chuỗi ký tự lộn xộn chứ không thể hiểu được ý nghĩa của thông tin đó. Hơn nữa, công nghệ mã hóa còn cho phép đảm bảo tính toàn vẹn của thông tin nhờ một số thuật toán chống sửa đổi và giả mạo. Tính năng của công nghệ là bảo mật thông qua việc quản lý khóa mã hóa một cách chặt chẽ của các bên sử dụng nó.

Nguyên lý mã hóa hoạt động như thế nào?

Nguyên lý cơ bản mà các tổ chức cần triển khai là chỉ cấp quyền đọc hiểu thông tin cho người có liên quan. Nhưng mã hóa hoạt động thế nào? Liệu rằng mỗi tình huống khác nhau, người ta lại dùng một loại mã hóa khác nhau? Có thể tích hợp mã hóa vào hạ tầng công nghệ hiện tại không?

Có 2 loại khóa mật mã là Khóa đối xứng và Khóa bất đối xứng:

Khóa đối xứng (hay còn được gọi là "khóa bí mật"): Với hệ thống này, các bên đều sở hữu chung một khóa dùng để mã hóa và giải mã thông tin, và họ buộc phải giữ bí mật về khóa đó.

Để chuyển khóa cho các bên, người dùng phải có cơ chế phân phối khóa một cách an toàn. Tiếp đó, họ cần có các quy tắc bảo mật cần thiết để hạn chế nguy cơ phát tán và thương mại hóa dễ dàng trên một mạng lưới mở như Internet.

Khóa bất đối xứng (hay còn được gọi là "cặp khóa công khai và khóa bí mật": Hệ thống này giải quyết được rủi ro khi phân phát khóa dùng chung trong hệ thống Khóa đối xứng. Có 2 khóa đều được sử dụng trong hệ thống, một khóa phải giữ bí mật và một khóa công khai được gửi cho bất cứ ai. Cặp khóa này liên hệ toán học với nhau, theo đó khóa công khai dùng để mã hóa còn khóa bí mật tương ứng dùng để giải mã.

MỘT SỐ THUẬT NGỮ LIÊN QUAN ĐẾN MÃ HÓA CẦN BIẾT

- **AES (Advanced Encryption Standard)**: Tiêu chuẩn mã hóa tiên tiến là hình thức mã hóa phổ biến được Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ (NIST) công nhận.
- **Thuật toán (hay còn được gọi là "mật mã")**: là những nguyên tắc hoặc câu lệnh đặc thù sử dụng trong quá trình mã hóa. DES, RSA và AES là những thí dụ về Thuật toán hay Mật mã.
- **Văn bản mã hóa (Cipher text)**: Đây là kết quả sau khi một văn bản ở dạng plain text được biến đổi thành mã hóa nhờ sử dụng thuật toán.
- **Giải mã**: là quy trình biến dữ liệu không đọc được thành thông tin có thể hiểu được.
- **Mã hóa Email**: giúp gửi email một cách an toàn qua mạng thông qua một số phương thức như TLS, Mật khẩu, push/pull, S/MIME, PGP hay ZedMail của Prim'X.
- **Mã hóa**: là phương pháp khoa học bảo vệ thông tin bằng cách biến đổi thành định dạng an toàn
- **Khóa**: Một khóa ngẫu nhiên được sinh ra bao gồm nhiều ký tự dùng để Mã hóa/Giải mã. Mỗi khóa là duy nhất và khóa càng dài thì càng khó bẻ. Nhìn chung, khóa bí mật có độ dài từ 128 đến 256 bit, còn khóa công khai có độ dài 2.048 bit.
- **PGP (Pretty Good Privacy)**: là chương trình mã hóa sử dụng khóa mật mã và phương pháp xác thực trong truyền tải dữ liệu.

VÌ SAO MÃ HÓA LẠI QUAN TRỌNG?

Mã hóa đóng vai trò hết sức quan trọng trong bối cảnh các vụ tấn công mạng diễn ra liên tục và tăng dần về số lượng. Hơn nữa, những vụ vô tình rò rỉ thông tin từ nội bộ chiếm hơn 50% tổng số sự cố lộ lọt thông tin. Tương tự, nhiều ngành nghề như ngân hàng, chăm sóc sức khỏe và nhiều lĩnh vực nhạy cảm khác yêu cầu bắt buộc phải mã hóa nhằm đáp ứng các tiêu chuẩn an toàn thông tin.

Khóa thông tin (Locking data) là phương pháp tốt nhất bảo vệ chúng ta khỏi những vụ tấn công có chủ ý hoặc vô tình phát tán, từ đó tránh khỏi nguy cơ thiệt hại về tài chính, uy tín và đánh mất niềm tin của đối tác, bạn hàng.
Dữ liệu cần phải được mã hóa an toàn cả khi truyền tải (Data in transit) và lưu trữ (Data at rest) như trường hợp lưu trữ trên server. Đây là phương thức quan trọng nhất bảo vệ chúng ta trước những cuộc tấn công mạng, và là phòng tuyến cuối cùng trong những hàng rào phòng vệ cần thiết.

Nếu doanh nghiệp của bạn chưa xây dựng hệ thống mã hóa thì đã đến lúc phải đưa ra một chiến lược CNTT chống tấn công mạng. Một số bộ phận quản lý CNTT lựa chọn OpenPGP miễn phí để mã hóa file dữ liệu, một số sử dụng giải pháp quản lý tập trung các file transfer như GoAnywhere MTF để bảo vệ dữ liệu với nhiều tính năng và ưu điểm. Tuy nhiên, sử dụng sản phẩm Prim'X như ZoneCentral (đã bao gồm công nghệ Zed và ZedMail) là giải pháp doanh nghiệp

mang tính tổng thể, toàn bộ, ưu việt nhất, không gây phiền toái cho người dùng và dễ triển khai cho bộ phận CNTT. Mô hình kinh doanh đặc thù của bạn sẽ quyết định bạn nên sử dụng phương án tối ưu nhất.

LỰA CHỌN PHƯƠNG PHÁP MÃ HÓA NÀO PHÙ HỢP NHẤT CHO TỔ CHỨC CỦA BẠN?

Cần cần nhắc một số yếu tố trước khi lựa chọn quy chuẩn mã hóa nào phù hợp với doanh nghiệp của bạn. Hãy thử trả lời một số câu hỏi dưới đây:

- Dữ liệu cần trao đổi của bạn quan trọng đến đâu?
- Dữ liệu của bạn được truyền tải bằng hình thức nào (FTP, Email, HTTP…)?
- Dung lượng file trao đổi như thế nào? Có cần nén không?
- Các file hiện tại có cần được mã hóa trước khi truyền tải không? Hay cần mã hóa chính đường truyền?
- Các sản phẩm mã hóa được các nhà cung cấp hỗ trợ có sẵn trên thị trường là gì?

Nhà cung cấp sẽ là người tư vấn chuẩn xác nhất về giải pháp ứng dụng, thí dụ một số ngân hàng yêu cầu phải dùng OpendPGP để mã hóa file thông tin khách hàng, trong khi một doanh nghiệp lớn có thể lựa chon Prim'X để bảo vệ toàn diện. Hãy thử trả lời những câu hỏi dưới đây để chúng tôi có thể tư vấn cho bạn:

- Bảo vệ dữ liệu lưu trữ (Data at reste) trên máy local, server, San, Nas?
- Bảo vệ dữ liệu lưu trữ trên nền tảng Cloud của bên thứ 3 (One drive, Google drive, Dropbox…)?
- Bảo vệ dữ liệu chia sẻ trên Sharepoint (on premise)?
- Bảo vệ trao đổi thông tin như Mail Exchange (gửi mail nội bộ và ra ngoài)? Trao đổi copy qua USB, ổ cứng rời…?
- Bảo vệ vật lý các ổ đĩa rời, laptop chống mất trộm, mã hóa ổ đĩa…?
- Quy mô sơ bộ hạ tầng của doanh nghiệp như thế nào? Số lượng PC, máy ảo, kết nối DC, cách thức triển khai các chính sách hiện tại như thế nào?

Như đã nói ở trên, Prim'X là giải pháp bảo vệ hạ tầng CNTT truyền thống, bổ sung cho các giải pháp trong xu thế phòng thủ chủ động hiện tại, giúp doanh nghiệp quản lý an toàn thông tin hiệu quả giữa lúc quá trình số hóa và chuyển đổi số đang diễn ra mạnh mẽ ở Việt Nam./.

(MK Group)

PRIMX
MAKE ENCRYPTION HAPPEN

FIDO mang lại sự tiện lợi và an toàn cho quy trình xác thực

Tiêu chuẩn Nhận dạng Trực trực tuyến Nhanh (FIDO) là các giao thức xác thực đáp ứng nhu cầu nâng cao mức độ bảo mật và trải nghiệm người dùng.

Tiêu chuẩn FIDO - được hiệp hội FIDO Alliance phát triển - mang lại khả năng bảo mật cao hơn so với mật khẩu thông thường hoặc mật khẩu dùng 1 lần (OTP), cũng như cho phép xác thực nhanh, an toàn và mạnh mẽ hơn. Tiêu chuẩn này bao gồm một số kỹ thuật xác thực như quét sinh trắc học, quét mống mắt, nhận dạng giọng nói hoặc nhận dạng khuôn mặt. FIDO cũng hỗ trợ các giải pháp xác thực hiện có như token bảo mật, xác thực thẻ thông minh, giao tiếp tầm gần (NFC)…

Đáng thú vị là nguồn gốc ngôn ngữ của tên gọi FIDO bắt nguồn từ một từ Latin “fido” - có nghĩa là “sự tin tưởng” theo định nghĩa trong từ điển tiếng Latin của Đại học Notre Dame, và chính là từ viết tắt thích hợp dành cho môi trường bảo mật - nơi mà sự tin tưởng đóng vai trò tối quan trọng.

Sứ mệnh của FIDO Alliance là “giảm sự phụ thuộc của thế giới vào mật khẩu”. Tầm nhìn của PayPal và Validity Sensors bắt đầu từ năm 2009 về một tiêu chuẩn ngành cho phép sử dụng thông tin sinh trắc học để xác định người dùng trực tuyến, thay vì mật khẩu, giờ đây đã xác lập được vị trí vững vàng.

Hiện nay, thành viên của FIDO Alliance bao gồm những tập đoàn toàn cầu hàng đầu trong lĩnh vực công nghệ, thanh toán, viễn thông, chính phủ, y tế và có dự tham gia của cả những gã siêu khổng lồ công nghệ như Amazon, Alibaba, Facebook và Google. Các trang web và ứng dụng hỗ trợ FIDO đang thu hút được hơn 3 tỷ người dùng thương mại.

fido™ ALLIANCE | simpler stronger authentication

Tiêu chuẩn FIDO là gì ?

Tiêu chuẩn FIDO cung cấp một loạt thông số kỹ thuật mở và có thể mở rộng như Khung Xác thực Phổ quát (UAF), Yếu tố Thứ 2 Phổ quát (U2F) và FIDO2, mang lại trải nghiệm xác thực người dùng thuận tiện và an toàn hơn.

FIDO giúp nhận dạng người dùng dễ dàng hơn với các hệ thống sinh trắc học, xác thực đa yếu tố (MFA) và những lựa chọn thay thế khác trên các trang web và ứng dụng. Tiêu chuẩn này nhấn mạnh mô hình lấy thiết bị làm trung tâm, trong đó sử dụng mật mã khóa công khai tiêu chuẩn, nơi người dùng được thử thách để chứng minh quyền sở hữu khóa cá nhân thông qua nhiều cách khác nhau.

FIDO hoạt động như thế nào?

Khi người dùng tạo tài khoản hoặc đăng ký trên một dịch vụ trực tuyến sử dụng tiêu chuẩn FIDO, thiết bị sẽ tạo một bộ khóa mật mã. Hệ thống đăng ký khóa công khai với các dịch vụ trực tuyến và lưu khóa cá nhân trên thiết bị.

Trong quá trình xác thực, hệ thống yêu cầu người dùng chứng minh quyền sở hữu khóa cá nhân. Bạn có thể thực hiện yêu cầu này thông qua những phương pháp xác thực hỗ trợ FIDO khác nhau, như xác thực sinh trắc học, nhận dạng khuôn mặt, xác thực đa yếu tố... Bạn có thể sử dụng khóa cá nhân trên thiết bị sau khi mở khóa bằng những phương pháp an toàn, bao gồm vuốt ngón tay, nói vào microphone, nhập mã PIN hoặc nhấn nút.

Các tiêu chuẩn FIDO

FIDO cung cấp những thông số dưới đây nhằm giảm bớt sự rườm rà khi phải ghi nhớ những mật khẩu phức tạp và giải quyết tình trạng thiếu khả năng tương tác giữa các thiết bị xác thực mạnh.

Khung Xác thực Phổ quát (UAF)

UAF được ra mắt vào năm 2014 nhằm mục đích tạo điều kiện thuận lợi cho xác thực bằng thông tin sinh trắc học mà không cần mật khẩu. Theo UAF, khi người dùng xác thực một dịch vụ hoặc ứng dụng, họ sẽ bị thách thức bởi một hoặc nhiều yếu tố bảo mật trên thiết bị số cá nhân. Khi vượt qua những hàng rào đó, một mã khóa cá nhân sẽ được kích hoạt để có thể giúp người dùng vượt qua thử thách do server FIDO UAF đặt ra.

Cơ chế được người dùng sử dụng để xác minh trên thiết bị có thể là sinh trắc học, sở hữu hoặc dựa trên kiến thức để có được khóa cá nhân và hoàn tất quá trình xác thực. UAF cũng hướng dẫn cách tạo lập và quản lý nhiều chính sách để xác minh giao dịch. Tiêu chuẩn FIDO này được một số tổ chức sử dụng để cải thiện khả năng bảo mật và mang lại trải nghiệm người dùng tích cực cho cả khách hàng và đội ngũ nhân viên.

Yếu tố Thứ 2 Phổ quát (U2F)

Tiêu chuẩn U2F đưa ra những hướng dẫn về tăng cường và đơn giản hóa xác thực 2 yếu tố (2FA) sử dụng các thiết bị NFC hoặc USB dựa trên công nghệ tương tự thẻ thông minh. Ban đầu, U2F được Yubico và Google phát triển với sự đóng góp của nhà sản xuất bán dẫn NXP.

Thiết kế của U2F phát triển xung quanh các thiết bị USB kết nối với hệ thống máy chủ sử dụng thiết bị giao diện con người (HID), vốn đơn giản là giả lập một bàn phím. U2F cho phép trình duyệt truy cập vào các tính năng bảo mật của thiết bị và loại bỏ nhu cầu cài đặt phần mềm trình điều khiển phần cứng cụ thể để đọc thiết bị USB.

Sau khi máy tính chủ đọc thiết bị USB và kết nối được thiết lập, khâu xác thực phản hồi sẽ được tiến hành khi thiết bị sử dụng các kỹ thuật mật mã khóa công khai và một khóa thiết bị duy nhất. Các trình duyệt như Google Chrome, Opera, Firefox, Safari và Thunderbird hỗ trợ các tiêu chuẩn U2F bằng cách sử dụng khóa bảo mật U2F trong vai trò của một phương pháp bổ sung cho xác minh 2 bước trên các dịch vụ trực tuyến.

Thiết bị khóa bảo mật FIDO Keypass S1 hiện của MK Group đã có thể hỗ trợ được cả tiêu chuẩn FIDO U2F và FIDO2

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

Giao thức xác thực ứng dụng khách (CTAP)

CTAP trao quyền cho trình xác thực mật mã chuyển vùng như điện thoại di động hoặc khóa bảo mật phần cứng để đảm bảo khả năng tương tác với thiết bị khách như máy tính xách tay. CTAP bổ sung cho tiêu chuẩn WebAuthentication (WebAuthn) do tổ chức World Wide Web (W3C) phát hành.

CTAP dựa trên tiêu chuẩn xác thực U2F của FIDO Alliance. U2F và WebAuth là nền tảng cho sự phát triển của tiêu chuẩn FIDO 2.0. CTAP đề cập đến 2 giao thức CTAP1 và CTAP2. CTAP 1 - tên mới của giao thức FIDO U2F - hướng dẫn cách thiết lập trình xác thực hỗ trợ FIDO U2F giao tiếp, các trình duyệt và như hệ điều hành hỗ trợ FIDO2 để kích hoạt 2FA. Trong khi đó, CTAP 2 xác định những cách thức để hệ điều hành và các trình duyệt hỗ trợ FIDO2 có thể giao tiếp với các trình xác thực bên ngoài như thiết bị di động hoặc khóa bảo mật FIDO nhằm tạo điều kiện thuận lợi cho xác thực không cần mật khẩu, 2FA hoặc MFA.

FIDO2

Mục đích của FIDO2 là cho phép xác thực không cần mật khẩu. FIDO2 được xây dựng trên U2F và một phiên bản mở rộng của CTAP. Tiêu chuẩn này cho phép xác thực không cần mật khẩu bằng cách tận dụng giao diện lập trình ứng dụng cho máy chủ web hoặc trình duyệt web (Web API) - WebAuthn.

FIDO2 loại bỏ rủi ro xuất phát từ việc quản lý không tốt mật khẩu, bởi vì các thông tin đăng nhập mã hóa của tiêu chuẩn này là duy nhất cho mọi trang web, chúng không được lưu trữ trên máy chủ mà được lưu trữ ngay trên thiết bị của người dùng.

Luồng giao tiếp được FIDO2 xác định là: (1) Kết nối được thiết lập giữa ứng dụng (hoặc trình duyệt) và trình xác thực; (2) Ứng dụng nhận ra các khả năng của trình xác thực và lấy thông tin về nó bằng cách sử dụng lệnh authenticatorGetInfo; (3) Lệnh hoạt động sẽ được ứng dụng gửi tới trình xác thực nếu thấy có khả năng; (4) Trình xác thực gửi dữ liệu phản hồi hoặc thông báo lỗi.

Trước khi thực hiện giao thức này, điều quan trọng là trình xác thực bên ngoài và máy chủ lưu trữ phải thiết lập một kênh truyền dữ liệu an toàn và được xác thực từ cả 2 phía.

Các đối tượng sử dụng FIDO

FIDO giúp các tổ chức hạn chế những rủi ro nghiêm trọng xuất phát từ một vụ rò rỉ dữ liệu do mật khẩu yếu hoặc quản lý mật khẩu yếu kém. FIDO cho phép công ty của bạn tiết kiệm chi phí liên quan đến hoạt động cung cấp thiết bị, đặt lại mật khẩu, hỗ trợ khách hàng và hơn thế nữa, đồng thời mang lại trải nghiệm liền mạch cho người dùng.

Do những lợi ích như vậy và nhiều ưu điểm khác, nên rất nhiều tổ chức và cơ quan đang tích cực sử dụng FIDO.

Chăm sóc y tế và bảo hiểm

Trong lĩnh vực chăm sóc sức khỏe, xác thực FIDO giúp bảo vệ các dữ liệu của bệnh nhân như hồ sơ y tế, thông tin cá nhân và các dữ liệu nhạy cảm khác mà chỉ họ mới có thể truy cập được ngoài các nhà cung cấp đáng tin cậy.

FIDO đảm bảo với bệnh nhân rằng thông tin của họ được lưu trữ tại những cơ quan quản lý đáng tin cậy, nơi tuân thủ các tiêu chuẩn như Đạo luật về Trách nhiệm giải trình và Cung cấp Bảo hiểm Y tế (HIPAA) của Mỹ. Nó bảo vệ các hệ thống y tế và cơ sở chăm sóc sức khỏe bằng một lớp bảo mật mạnh mẽ để ngăn chặn những cuộc tấn công mạng.

Các công ty bảo hiểm xác thực bằng cách sử dụng các giao thức FIDO để đảm bảo họ luôn sẵn có khả năng xác thực mạnh.

Tổ chức doanh nghiệp

Tại các doanh nghiệp, FIDO đơn giản hóa quá trình xác thực của người dùng bằng cách làm cho quá trình này trở nên nhanh chóng và thuận tiện. FIDO thường được sử dụng để hỗ trợ xác thực người dùng trong thời gian hoạt động tại một tổ chức. Nó cho phép người dùng thực hiện các giao dịch thanh toán an toàn và duy trì một lớp bảo mật xung quanh chữ ký số của họ.

Trong những môi trường được gắn với các tiêu chuẩn xác thực FIDO, người dùng có thể cùng lúc sở hữu các trình xác thực khác nhau, chẳng hạn như một trình xác thực cho máy tính xách tay và một trình xác thực khác cho thiết bị di động. Tại thời điểm đăng ký người dùng, thông tin xác thực FIDO được ghi lại trên một trình xác thực cục bộ và được liên kết với một tài khoản người dùng cụ thể để sử dụng trong quá trình xác thực.

Thí dụ, khi người dùng bị mất thiết bị xác thực, các tiêu chuẩn FIDO cho phép quản trị viên thu hồi và xóa thông tin đăng nhập, vốn có thể được tạo ra trên một thiết bị khác bằng cách thực hiện theo quy trình đăng ký. Trong trường hợp thông tin đăng nhập FIDO cần được gia hạn, quản trị viên đảm bảo rằng mức độ bảo mật tương tự được áp dụng như trong quy trình đăng ký. Trên thực tế, tiêu chuẩn FIDO không hỗ trợ khái niệm gia hạn thông tin đăng nhập, vì vậy, bất kỳ quy trình gia hạn nào sẽ đều phải được thiết kế trong hệ thống hỗ trợ xác thực FIDO.

Dịch vụ tài chính

Các nhà cung cấp dịch vụ ngân hàng và tài chính đã mở rộng phạm vi hoạt động để tiếp cận khách hàng ở bất kỳ đâu. Với ngân hàng trực tuyến và di động, khách hàng có thể sử dụng các dịch vụ tài chính ngoài những chi nhánh được chỉ định, dẫn đến nhu cầu ngày càng cao về bảo mật xác thực mạnh mẽ.

Các giao thức FIDO giải quyết nhu cầu trên bằng cách cung cấp những tiêu chuẩn xác thực an toàn cho các ngân hàng và tổ chức tài chính, nơi người dùng hài lòng với trải nghiệm ngân hàng tiện lợi và đơn giản.

Chính phủ

Các cơ quan chính phủ có thể sử dụng FIDO để cung cấp MFA hoặc xác thực dựa trên thiết bị di động nhanh chóng và an toàn cho các dịch vụ trực tuyến. FIDO hỗ trợ thông tin xác thực danh tính cá nhân (PIV) có nguồn gốc, cho phép phát hành thông tin xác thực cơ sở hạ tầng khóa công khai (PKI) dựa trên việc sở hữu thẻ thông minh PIV. FIDO cho phép người dùng truy cập nhanh chóng và an toàn vào những thông tin và ứng dụng quan trọng./.

(G2)

MK® group

Smart Digital Security

www.mkgroup.com.vn | contact@mkgroup.com.vn | www.facebook.com.vn/mkgroup1999

Hà Nội: Tòa nhà The Vista, số 4 ngõ 15 Duy Tân, Quận Cầu Giấy, Hà Nội | Tel: (+84-24) 6266 2703

Tp. Hồ Chí Minh: Tầng 7 Thiên Sơn Building, 5 Nguyễn Gia Thiều, Quận 3, Tp.HCM | Tel: (+84-28) 3930 5023