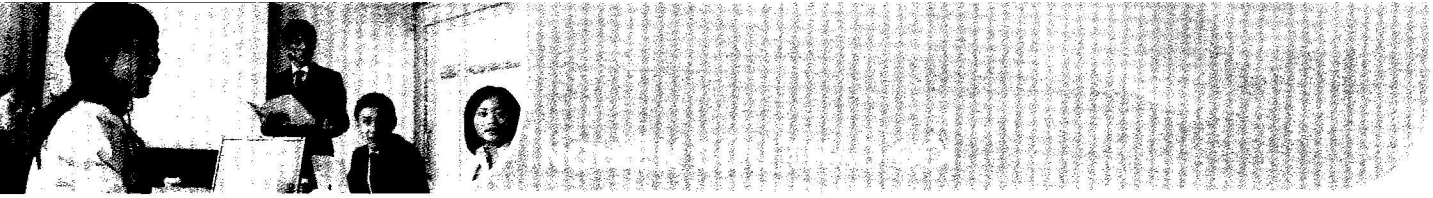

ÁP DỤNG BẢO MẬT BẰNG SINH TRẮC HỌC trong hoạt động nghiệp vụ Kho bạc Nhà nước

LÊ QUANG TÔN

Định hướng Chiến lược phát triển KBNN đến năm 2030 mở ra thời kỳ mới trong quá trình xây dựng, phát triển KBNN, trong đó tăng cường kết nối, chia sẻ dữ liệu để hình thành "hệ sinh thái" dịch vụ tài chính công mở đã đặt ra yêu cầu mới cho công tác bảo mật công nghệ thông tin để đảm bảo an toàn cao và phù hợp với xu hướng phát triển. Áp dụng bảo mật bằng sinh trắc học là hướng đi KBNN đang nghiên cứu, lựa chọn giải pháp phù hợp.

Từ khóa: Bảo mật sinh trắc học

The State Treasury's development strategy to 2030 triggers a new period in the development of State Treasury with the further connection and sharing of data to formulate an 'ecosystem' for public financial services, which sets out new requirements for information security and in line with the development trend. Application of security using biometrics is one of the options which State Treasury is exploring for a suitable solution.

Tag: Biometric security

Đến năm 2020, 100% đơn vị sử dụng ngân sách có quan hệ giao dịch với kho bạc đã triển khai dịch vụ công trực tuyến (DVCTT) với 98% giao dịch kiểm soát chi qua KBNN được thực hiện qua DVCTT, KBNN đã cơ bản hoàn thành triển khai kho bạc điện tử theo Chiến lược phát triển KBNN giai đoạn 2010 - 2020. Các phương thức giao dịch thủ công truyền thống được chuyển sang phương thức giao dịch điện tử. Theo định hướng Chiến lược phát triển đến năm 2030, KBNN tập trung vào liên thông dữ liệu số, đẩy mạnh chia sẻ dữ liệu mở, hình thành hệ sinh thái các dịch vụ mở trong lĩnh vực tài chính nhà nước; từ đó cung cấp thêm nhiều dịch vụ mới, đẩy mạnh việc tự động hóa các giao dịch, phân tích rủi ro, phân tích dự báo dựa trên dữ liệu lớn, công nghệ trí tuệ nhân tạo, hướng đến hình thành kho bạc số. Tốc độ phát triển và ứng dụng CNTT của KBNN đòi hỏi công tác đảm bảo an toàn bảo mật về CNTT cần phải được quan tâm nghiên cứu và áp dụng thêm các hình thức xác thực, bảo mật mới, phù hợp với xu hướng phát triển chung của xã hội.

Thực trạng công tác bảo mật ứng dụng trong hệ thống KBNN

Để đảm bảo an toàn thông tin tiền, tài sản của nhà nước, hệ thống KBNN áp dụng bảo mật nhiều lớp đối với các chương trình ứng dụng CNTT như: Bảo mật mạng, bảo mật hệ điều hành, bảo mật cơ sở dữ liệu, bảo mật ứng dụng. Trong đó, bảo mật ứng dụng đã áp dụng các hình thức: Tên và mật khẩu đăng nhập; mã hóa thông tin trên đường truyền bằng các thuật toán hiện đại; áp dụng chữ ký số trong các giao dịch thanh toán. Mật khẩu người dùng phải được thay đổi định kỳ và đảm bảo độ phức tạp nhất định. Một số vị trí kiểm soát, phê duyệt giao dịch quan trọng phải được xác thực bằng thiết bị bảo mật lưu chứng thư số.

Các giải pháp kỹ thuật nêu trên cơ bản đã đảm bảo yếu tố bảo mật thông tin, không thể chối bỏ, không thể dò tìm bằng phương thức thủ công cũng như các công cụ dò tìm chuyên nghiệp. Tuy nhiên, trong thực tế hoạt động nghiệp vụ kho bạc, các hình thức bảo mật đã sử

Hoạt động nghiệp vụ tại Cục Công nghệ thông tin, KBNN *Ảnh: TL*

dụng vẫn chưa ngăn ngừa được tình trạng vô ý hoặc cố ý thực hiện sai nguyên tắc nghiệp vụ. Tình trạng công chức cho đồng nghiệp mượn tài khoản, mật khẩu đăng nhập; cho mượn thiết bị ký chữ ký số để nhờ người không có thẩm quyền thực hiện thay công việc của mình... tiềm ẩn nhiều nguy cơ rủi ro.

Bảo mật bằng sinh trắc học

Bảo mật trong ứng dụng CNTT luôn là vấn đề được tất cả các cơ quan, tổ chức quan tâm. Theo thời gian, công nghệ bảo mật trong CNTT được phát triển từ đơn giản đến phức tạp, từ bảo mật một yếu tố bằng tên truy cập và mật khẩu đến bảo mật đa nhân tố (như once time password qua SMS, email, thiết bị token...), bảo mật bằng các yếu tố sinh trắc học. Trong vòng một thập kỷ trở lại đây, công nghệ nhận dạng sinh trắc học đã có những bước tiến vượt bậc về kỹ thuật cũng như giá thành, vì vậy được ứng dụng ngày càng rộng rãi trong CNTT, truyền thông. Ví dụ: Nhận dạng vân tay, nhận dạng khuôn mặt đã ứng dụng phổ biến trong rất nhiều dòng máy điện thoại thông minh, máy tính xách tay, các hệ thống ngân hàng số. Vậy sinh trắc học là gì?

Theo Wikipedia, sinh trắc học là môn khoa học ứng dụng phân tích toán học xác suất thống kê để nghiên cứu các hiện tượng sinh học hoặc các chỉ tiêu sinh học có thể đo lường được. Trong khuôn khổ bài viết, chúng tôi chỉ đề cập tới kỹ thuật sinh trắc học là công nghệ sử dụng những thuộc tính vật lý, đặc điểm sinh học riêng của mỗi cá nhân như vân tay, mống mắt, khuôn mặt... để nhận diện. Sinh trắc học từ lâu đã được xem như phương pháp bảo mật đầy hứa hẹn trong tương lai, thay vì sử dụng các kiểu bảo mật truyền thống như mật khẩu, mã PIN, hình vẽ.... sinh trắc học là sử dụng "chính con người" để làm "chìa khóa". Đã có nhiều cách tiếp cận bảo mật dạng này được giới thiệu nhưng cho đến hiện nay, phổ biến nhất vẫn là các giải pháp bảo mật sinh trắc học dựa trên dấu vân tay, khuôn mặt và mống mắt để xác định danh tính.

Áp dụng công nghệ sinh trắc học trong hoạt động nghiệp vụ KBNN

Sự phát triển của công nghệ trí tuệ nhân tạo, cùng với công nghệ dữ liệu lớn đã tạo điều kiện cho bảo mật dùng sinh trắc học ngày càng hoàn thiện về độ chính xác, khả năng triển khai, tích hợp cũng như giá thành ngày càng rẻ. Một số công nghệ điển hình có thể kể đến như nhận dạng vân tay, nhận dạng khuôn mặt, mống mắt, tĩnh mạch lòng bàn tay, nhận diện vành tai, nhận diện qua cử chỉ, hành động... Trong rất nhiều công nghệ sinh trắc học, KBNN cần đánh giá, lựa chọn giải pháp để vừa đảm bảo yêu cầu về bảo mật trong thời gian nhanh nhất, vừa đảm bảo tuân thủ quy trình đầu tư ứng dụng CNTT sử dụng vốn NSNN rất chặt chẽ. Một số tiêu chí lựa chọn giải pháp của KBNN được đưa ra: Công nghệ hiện đại, tương thích với các hệ thống ứng dụng CNTT của KBNN; nhanh chóng tích hợp với các hệ thống CNTT của KBNN; đảm bảo tuân thủ quy trình đầu tư CNTT.

KBNN đã tìm hiểu, nghiên cứu nhiều giải pháp khác nhau. Năm 2017, KBNN đã thử nghiệm tích hợp giải pháp nhận diện tĩnh mạch lòng bàn tay của hãng Fujitsu. Đầu năm 2021, KBNN đã thử nghiệm giải pháp nhận dạng khuôn mặt trong ứng dụng DVCTT với phân hệ dành cho công chức KBNN với một số đối tác. Kết quả thử nghiệm cho thấy mỗi giải pháp đều có ưu,

nhược điểm khác nhau về sự tiện dụng, về trang thiết bị phần cứng, nhưng đều đảm bảo được tính bảo mật, chống giả mạo bằng chính yếu tố đặc trưng của mỗi con người cụ thể. Trong thời gian tới, KBNN sẽ tiếp tục đánh giá thêm một số giải pháp khác, từ đó lựa chọn công nghệ phù hợp nhất với điều kiện thực tiễn của KBNN.

Trên cơ sở đó, dự kiến năm 2022, KBNN sẽ bước đầu triển khai giải pháp sinh trắc học trong các chương trình ứng dụng, áp dụng cho công chức kho bạc, đầu tiên là đối với nghiệp vụ kiểm soát chi NSNN, tăng cường bảo mật, định danh chính xác người thực hiện các hoạt động nghiệp vụ theo đúng thẩm quyền, từ đó góp phần nâng cao mức độ an toàn tiền, tài sản của Nhà nước.

Giai đoạn 2025 - 2030, cùng với sự tiến bộ về công nghệ, cũng như sự hoàn thiện hành lang pháp lý về định danh điện tử, KBNN sẽ tiếp tục nghiên cứu, ứng dụng eKYC cho toàn bộ khách hàng của KBNN.

Định danh khách hàng

Để khắc phục nhược điểm của phương pháp bảo mật đã áp dụng, công tác đảm bảo an toàn thông tin ngày càng phải được cải tiến theo hướng ứng dụng các công nghệ hiện đại để ngăn ngừa các hành vi lợi dụng tín nhiệm, trong đó các công nghệ xác định được chính xác cá nhân, đơn vị (định danh) giao dịch với KBNN cần được quan tâm, nghiên cứu, áp dụng.

Định danh khách hàng là một thủ tục để xác định và xác minh danh tính khách hàng đúng với những gì họ đã khai báo, đảm bảo tính hợp pháp và tuân thủ luật, quy định hiện hành. Yêu cầu của ứng dụng CNTT trong các hoạt động giao dịch ngân hàng (một lĩnh vực gần gũi với lĩnh vực tài chính) đòi hỏi ngày càng kịp thời, chính xác, an toàn, tiện lợi. Vì vậy, định danh khách hàng trong lĩnh vực ngân hàng (know your customer - KYC) ngày càng trở nên quan trọng.

Các thủ tục KYC thường được áp dụng tại các ngân hàng, tổ chức tài chính để đánh giá, giám sát rủi ro, ngăn ngừa gian lận, tránh các hoạt động rửa tiền, tài trợ khủng bố và các chương trình tham nhũng bất hợp pháp khác. Quá trình thực hiện bao gồm các bước kiểm tra được tiến hành trong giai đoạn đầu doanh nghiệp tiếp xúc với khách hàng, để xác minh rằng khách hàng là thật, thông qua so sánh sự trùng khớp giữa các tài liệu xác định danh tính (chứng minh thư, thẻ căn cước, bằng lái xe...) và khuôn mặt, thông qua sự hiện diện của khách hàng.

Trong lĩnh vực KBNN, các thủ tục hành chính liên quan đến mở, sử dụng tài khoản, đối chiếu, tất toán số dư cũng như kiểm soát chi NSNN rất cần sử dụng đến định danh khách hàng giao dịch. Hiện tại, thủ tục hành chính lĩnh vực kho bạc sử dụng phương thức xác thực trực tiếp (mở, sử dụng tài khoản), xác thực bằng tên và mật khẩu đăng nhập DVCTT, chứng thư số của Ban cơ yếu Chính phủ, cũng như của các nhà cung cấp dịch vụ chứng thực số công cộng. Các phương thức nêu trên đã đảm bảo được khả năng quy trách nhiệm cho cá nhân, đơn vị, nhưng chưa ngăn chặn được việc cố tình thực hiện sai nguyên tắc nghiệp vụ, và vì vậy vẫn tiềm ẩn rủi ro về tiền, tài sản của nhà nước.

Định danh khách hàng trực tuyến

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, quy trình định danh khách hàng trực tuyến (electronic know your customer - eKYC) được các tổ chức tài chính và ngân hàng áp dụng để nâng cao năng lực cạnh tranh và thu hút khách hàng. eKYC được dựa trên quy trình KYC với sự hỗ trợ từ video call và các công nghệ trí tuệ nhân tạo như: Xác thực khuôn mặt (face-matching) để so khớp khuôn mặt với ảnh trên giấy tờ tùy thân; nhận diện ký tự (OCR) để đọc và trích xuất các thông tin trên giấy tờ, đối chiếu thông tin cá nhân tức thời với cơ sở dữ liệu tập trung về danh tính người dùng... Khách hàng không cần gặp mặt, tới trực tiếp chi nhánh của ngân hàng mà có thể thực hiện quy trình định danh ở bất cứ đâu, thông qua cuộc gọi có hình (video call).

eKYC giúp tổ chức, cơ quan, doanh nghiệp tự động hóa quy trình điền thông tin, rút ngắn thời gian xác thực khách hàng và đơn giản hóa quy trình tiếp nhận khách hàng, từ đó tiết kiệm được chi phí và mang lại sự hài lòng cho khách hàng.

Điểm qua một số xu hướng của eKYC nêu trên để cho thấy, có tiềm năng ứng dụng cho lĩnh vực hoạt động nghiệp vụ KBNN cả trong ngắn hạn và trong dài hạn nhằm ngăn ngừa các vi phạm do vô ý hoặc cố ý lợi dụng, gây mất an toàn tiền, tài sản của nhà nước. Trước mắt, KBNN sẽ nghiên cứu ứng dụng eKYC ở mức độ cơ bản như áp dụng bảo mật bằng sinh trắc học đối với công chức của KBNN nhằm ngăn chặn các hành vi lợi dụng kẽ hở của quy trình nghiệp vụ trên máy khi chuyển đổi từ hình thức giao dịch trực tiếp sang giao dịch qua DVCTT, từ in chứng từ phục hồi sang sử dụng hồ sơ, chứng từ điện tử thay thế giấy. Một trong những ứng dụng cơ bản của eKYC là bảo mật bằng sinh trắc học mà chúng ta có thể nghiên cứu, áp dụng sớm trong thời gian tới.

Về lâu dài, khi hành lang pháp lý về định danh, xác thực điện tử hoàn thiện hơn, hạ tầng định danh xác thực điện tử của xã hội phát triển, KBNN sẽ nghiên cứu, ứng dụng eKYC ở mức độ đầy đủ, nhằm định danh được khách hàng giao dịch với KBNN. Việc ứng dụng eKYC cũng giúp tạo điều kiện cho cải tiến quy trình nghiệp vụ, tăng cường tính tự chủ cho đơn vị, chuyển đổi KBNN dần sang thực hiện hậu kiểm, phù hợp với các thông lệ quốc tế. ■

TÀI LIỆU THAM KHẢO

1. An toàn dữ liệu - Mã hóa bảo mật thông tin,an ninh cơ sở dữ liệu và an ninh mạng. Lê Đắc Nhường, NXB Đại học Quốc gia;

2. An toàn thông tin, Lê Văn Phùng, NXB Thông tin và truyền thông;

3. Mật mã và an toàn thông tin - Lý thuyết và ứng dụng.Hồ Văn Can - Lê Danh Cường. NXB Thông tin và truyền thông.

Ngày nhận bài: 26/3/2021
Ngày đưa phản biện: 26/3/2021
Ngày chấp nhận đăng: 08/3/2021
Email: tonlq@vst.gov.vn