(12) **BẢN MÔ TẢ GIẢI PHÁP HỮU ÍCH THUỘC BẰNG ĐỘC QUYỀN GIẢI PHÁP HỮU ÍCH**

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **2-0003565**

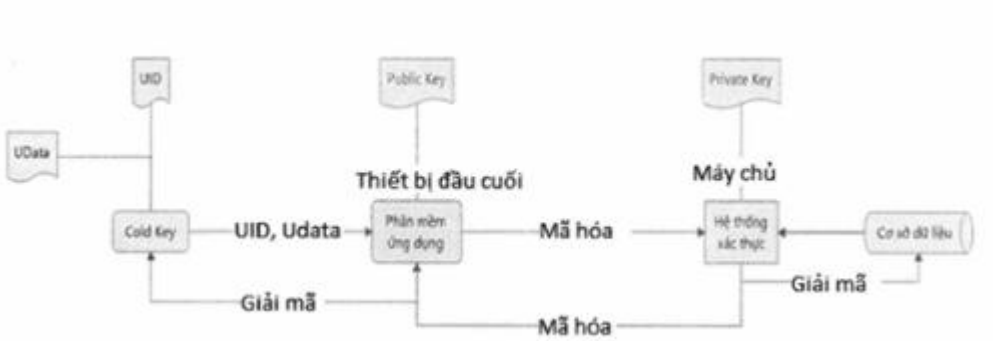
(51) **H04L 9/00**
2021.01

(13) **Y**

(21) 2-2022-00388
(22) 12/09/2022
(45) 25/04/2024 433
(43) 25/11/2022 416
(76) 1. Trần Minh Huy (VN)
134/97/5 Lý Chính Thắng, phường Võ Thị Sáu, quận 3, thành phố Hồ Chí Minh
2. Nguyễn Ngọc Tâm (VN)
E40, đường C3, phường Tân Thới Nhất, quận 12, thành phố Hồ Chí Minh

(54) QUY TRÌNH XÁC THỰC VÀ ĐỊNH DANH HỒ SƠ SỬ DỤNG CHỮ KÝ SỐ

(57) Sáng chế đề cập đến quy trình xác thực và định danh hồ sơ, tài liệu bằng thiết bị ký số với tính bảo mật và mức độ tiện dụng được cải thiện. Trong đó, thiết bị ký số theo sáng chế phải có một mã cố định là mã định danh duy nhất (Unique Identifier, UID) và một chuỗi dữ liệu biến đổi ngẫu nhiên không trùng lặp (Unique Data, UData). Thiết bị này có thể đọc được bởi các thiết bị đầu cuối di động như điện thoại thông minh mà không cần đến cổng giao tiếp USB. Quy trình theo sáng chế. Quy trình xác thực được thực hiện bởi một phần mềm hệ thống hỗ trợ, có tài khoản được cấp cho người dùng. Ngoài việc định danh bằng tài khoản và mật khẩu người dùng, mỗi người dùng được cấp một thiết bị định danh gọi là thiết bị ký số theo sáng chế. Với thông tin mô tả của thiết bị ký số theo sáng chế như UID không trùng lặp, không thay đổi và Udata là chuỗi dữ liệu có thể thay đổi thông tin tại mỗi lần sử dụng, cho ra chuỗi dữ liệu không trùng lặp và không thể làm giả, việc xác thực, định danh, số hóa hồ sơ, tài liệu, chứng từ được bảo mật tối đa.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến thiết bị điện tử để xác thực, định danh, và quy trình xác thực, định danh, số hóa các số hóa các loại hồ sơ, tài liệu, văn bản sử dụng thiết bị này.

Tình trạng kỹ thuật của sáng chế

Bước vào thời kỳ công nghệ số, việc ứng dụng khoa học công nghệ vào đời sống, hoạt động sản xuất kinh doanh là một xu hướng tất yếu. Điển hình nhất phải nhắc đến việc sử dụng chữ ký số, bởi chữ ký số đang được xem là giải pháp công nghệ thông minh và tiện ích trong các giao dịch điện tử.

Chữ ký số là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng, theo đó, người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác: việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa; sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

Hay có thể hiểu theo cách đơn giản hơn, chữ ký số (Token) chính là một loại thiết bị đã được mã hóa toàn bộ những thông tin, dữ liệu của một cá nhân, tổ chức hoặc doanh nghiệp. Chữ ký số sẽ có giá trị tương đương và dùng thay thế cho chữ ký tay tại các giao dịch trên môi trường thương mại điện tử.

Cấu tạo của chữ ký số

Chữ ký số được thiết lập dựa vào công nghệ mã hóa công khai RSA. Mỗi đơn vị kinh doanh khi được cung cấp và sử dụng chữ ký số sẽ có một khóa công khai (public key) và một khóa bí mật (private key).

Khóa bí mật (private key): một bộ phận không thể thiếu trong cặp khóa khi tạo chữ ký số. Khóa bí mật thuộc hệ thống mã hóa không đối xứng.

Khóa công khai (public key): loại khóa không thể thiếu trong cặp khóa khi kiểm tra chữ ký số. Khóa công khai nằm trong hệ thống mã không bí mật, và được tạo nên bởi khóa bí mật tương ứng trong cặp khóa.

Người ký: chủ thể của thuê bao sẽ dùng khóa bí mật đã được cung cấp để thực hiện ký số vào một thông điệp dữ liệu dưới tên mình.

Người nhận: tổ chức, doanh nghiệp hoặc một cá nhân sẽ nhận được thông điệp dữ liệu đã được ký số thông qua việc sử dụng các chứng thư số của người ký, kiểm tra lại chữ ký số ở thông điệp dữ liệu nhận được. Sau đó mới tiếp tục tiến hành các hoạt động, giao dịch liên quan.

Ký số: người sử dụng đưa khóa bí mật của mình vào phần mềm tự động tạo. Sau đó, gắn chữ ký số vào thông điệp dữ liệu cần ký.

Các loại chữ ký số được sử dụng phổ biến nhất hiện nay

Chữ ký số USB Token

USB Token là một trong các loại chữ ký số ra đời đầu tiên trên thị trường. Đây cũng chính là loại ký số được dùng thông dụng nhất hiện nay. Cho đến hiện tại, có rất nhiều cá nhân, tổ chức và doanh nghiệp lựa chọn sử dụng USB Token để ký công văn, hợp đồng, giao dịch hành chính công, v.v..

USB Token mang một đặc điểm đặc trưng của một thiết bị phần cứng đặc biệt an toàn. Nhìn bên ngoài, USB Token được thiết kế có hình dáng giống với một chiếc USB thông thường. Bạn cần cài đặt phần mềm ký số trên máy tính, sau đó cắm USB, đăng nhập vào chữ ký số bằng mã PIN của mình. Trong quá trình ký số, USB Token sẽ dùng các thuật toán được cài đặt sẵn để xác thực và ký số cho người dùng.

Toàn bộ thông tin của tổ chức, doanh nghiệp sẽ được mã hóa trong USB Token.Mỗi đơn vị khi đăng ký sử dụng chữ ký số sẽ có cặp khóa (key pairs) gồm một khóa bí mật (private key) và một khóa công khai (public key).

Khóa bí mật: bao gồm các thông tin bí mật của khách hàng. Đây là phần khóa tạo ra chữ ký số.

Khóa công khai: phần khóa chứa các thông tin công khai của khách hàng.

USB Token đã và đang được sử dụng vô cùng phổ biến bởi loại chữ ký số này có ưu điểm như sau: khả năng bảo mật cực kỳ cao, dễ dàng sử dụng, giá thành tốt, khả năng lưu trữ lớn, cập nhật nhanh, xử lý thông tin với tốc độ cao, có dữ liệu lên tới 32 bit.

Tuy nhiên, USB Token vẫn còn tồn tại một số nhược điểm: bắt buộc phải kết nối với máy tính mới có thể thực hiện được các thao tác ký số; nếu máy tính xảy ra lỗi, USB Token cũng không thể sử dụng được; phụ thuộc vào một token duy nhất, không thể phân quyền người dùng.

Chữ ký số HSM

HSM (viết tắt của từ tiếng Anh: Hardware Security Module) là một thiết bị bảo mật có chức năng quản trị và bảo vệ các cặp khóa, chứng thư số cho các ứng dụng xác thực mạnh và xử lý mật mã. HSM thường được sản xuất dưới dạng một card PCI cắm vào máy tính hoặc một thiết bị độc lập có kết nối mạng. Nhằm đáp ứng mọi nhu cầu sử dụng của các khách hàng trong ứng dụng công việc và nâng cao hiệu suất làm việc, HSM là một trong những loại chữ ký số sở hữu nhiều tính năng vượt trội nhất trên thị trường hiện nay. Chính vì vậy, so với những loại chữ ký số trước đó, HSM được nâng cấp với những đặc điểm nổi bật hơn cả: phần cứng của chữ ký số được dùng để thực hiện các thao tác quản lý và bảo vệ các cặp khóa điện tử để cải thiện tốc độ xác thực và mã hóa dữ liệu; thực hiện các tác vụ với tốc độ cao lên tới 1200 tác vụ trong một giây; chuyên dùng cho các doanh nghiệp phải ký số nhiều, nhu cầu hỗ trợ ký số tự động và tiến hành thao tác nhanh chóng; có thể sử dụng ký số HSM trực tuyến thông qua tài khoản online do chính HSM tạo ra; linh hoạt phân quyền sử dụng ký số HSM ở mọi lúc mọi nơi; bảo toàn sự toàn vẹn của các dữ liệu số, hợp đồng và tài liệu số trên môi trường điện tử.

Ưu điểm của chữ ký số HSM: khả năng xác thực các thông tin ký số nhanh chóng và chính xác; mang tính pháp lý cao; áp dụng với số lượng ký lớn

trong những giao dịch lớn; sử dụng ở mọi lúc mọi nơi, linh hoạt trong mọi trường hợp; tính bảo mật khá cao; đảm toàn sự nguyên vẹn của văn bản.

Nhược điểm của chữ ký số HSM: khó có thể kiểm soát được hết các luồng giao dịch khi sử dụng; lệ thuộc vào tài khoản (mã OTP, tên đăng nhập –mật khẩu (username – password), v.v..); có thời hạn sử dụng nhất định.

Chữ ký số SmartCard

Loại chữ ký số cũng đang được dùng khá thông dụng tại các doanh nghiệp, cá nhân hiện nay đó chính là SmartCard. Smartcard được thiết kế có hình dạng giống như một chiếc sim điện thoại do một số nhà mạng hay đơn vị dịch vụ cung cấp nghiên cứu và phát triển. Đặc điểm nổi bật nhất của loại chữ ký số này chính là được tích hợp với thẻ sim trên điện thoại di động hay bất kỳ thiết bị điện tử khác. Kể cả khi thiết bị của người sử dụng không có mạng Internet vẫn có thể tiến hành ký số bằng SmartCard.

Ưu điểm của chữ ký số SmartCard: sử dụng khá linh hoạt trong mọi trường hợp, mọi thiết bị; nhỏ gọn, tiện lợi bởi SmartCard đã được tích hợp cùng với sim điện thoại; chi phí sử dụng SmartCard khá thấp và hợp lý.

Nhược điểm của chữ ký số thẻ thông minh (SmartCard): tính bảo mật chưa cao; khi sử dụng SmartCard, khách hàng bắt buộc phải dùng cả sim của cùng một nhà mạng để tích hợp ký số do nhà mạng đó cung cấp; trong trường hợp khách hàng đang ở nước ngoài hoặc ngoài vùng phủ sóng thì việc ký số bằng SmartCard sẽ không thể thực hiện được.

Chữ ký số từ xa

Chữ ký số từ xa (remote signature) hay còn được gọi bằng những tên gọi khác như: chữ ký số online, chữ ký số di động, v.v., được phát triển dựa vào công nghệ của điện toán đám mây. Đặc điểm của loại chữ ký số này là không phải sử dụng đến thiết bị phần cứng mà vẫn có thể thực hiện việc ký số ở mọi thiết bị và mọi lúc mọi nơi. Không những vậy, chữ ký số từ xa được áp dụng thêm các tiêu chuẩn định danh, dịch vụ tin cậy và xác thực điện tử đạt chuẩn

Châu Âu *eIDAS*. Người dùng sẽ ủy thác quyền quản lý và xác thực khóa bí mật cho đơn vị cung cấp chữ ký số đã lựa chọn. Để xác thực được danh tính của người ký, mỗi nhà cung cấp sẽ có những cách thức bảo mật khác nhau, đảm bảo sự an toàn và nguyên vẹn cho các văn bản số tối ưu nhất.

Ưu điểm của chữ ký số từ xa: tốc độ ký nhanh, nhiều; đảm bảo tính an toàn, pháp lý; sử dụng linh hoạt ở mọi lúc mọi nơi; sử dụng không phụ thuộc vào các thiết bị phần cứng.

Nhược điểm của chữ ký số từ xa: tiềm ẩn một số rủi ro về việc bị đánh cắp các dữ liệu số.

Ngoài việc xác thực bằng chữ ký số như mô tả trên, có thể xác thực bằng ứng dụng sinh mã QRCode: là phương thức sử dụng ứng dụng để xác minh 2 bước. Trong đó, một trong những bước xác thực là mã QRCode được phát sinh từ ứng dụng đó. Bằng cách thiết lập ứng dụng trình xác thực để gửi thông báo cho thiết bị di động hoặc gửi cho người dùng mã xác minh dưới dạng phương pháp xác minh bảo mật.

Bản chất kỹ thuật của sáng chế

Vấn đề kỹ thuật cần giải quyết

Ứng dụng giải pháp để xác thực định danh trong các quy trình phê duyệt hồ sơ đòi hỏi có tính bảo mật và an toàn thông tin và xác định danh tính và phân quyền cấp phê duyệt. Đồng thời, quy trình ứng dụng trong xác thực, phê duyệt, định danh cần phải được thực hiện bằng phương thức trực tuyến (online) hoặc ngoại tuyến (offline) thông qua phần mềm quản lý hệ thống.

Mục đích kỹ thuật của sáng chế

Sáng chế được đề xuất để giải quyết các vấn đề đặt ra nêu trên. Cụ thể sáng chế đề xuất các phương án nhằm các mục đích như được trình bày sau đây.

Một mục đích của sáng chế là để ứng dụng trong việc xác nhận các loại chứng từ, giấy tờ, cần có xác nhận, định danh hồ sơ của một chủ thể có thẩm quyền có thể là cá nhân hoặc tổ chức.

Mục đích khác của sáng chế là ứng dụng giải pháp giúp thực hiện việc số hóa hồ sơ, tài liệu, loại trừ các yếu tố làm giả chữ ký trên hồ sơ, làm giả hồ sơ, xác định được người chịu trách nhiệm trên hồ sơ đó bằng phương thức xác thực thông qua thiết bị định danh, phân quyền khi hồ sơ được ký.

Mục đích khác của sáng chế nhằm giải quyết được các vấn đề trong nền tảng số hóa hồ sơ, giấy tờ, tài liệu. Giúp làm giảm áp lực lưu trữ hồ sơ bản giấy/cứng, ứng dụng trong các quản lý hồ sơ hành chính nhà nước, hồ sơ văn phòng, hợp đồng, thỏa thuận, hồ sơ công chứng, chứng thực, v.v..

Mục đích khác nữa của sáng chế là để ứng dụng trong xác thực, định danh hồ sơ, giấy tờ, giao dịch trên nền tảng online và offline một cách an toàn và nhanh chóng mà không nhất thiết phải sử dụng máy tính mà có thể ứng dụng thực hiện xác thực ngay trên điện thoại thông minh (smartphone).

Sáng chế đề xuất quy trình xác thực hồ sơ theo thẩm quyền, chức năng có thể thay cho công nghệ token xác thực (chữ ký số) hiện có trên thị trường, đảm bảo tính bảo mật và an toàn cao trong giao dịch, xác thực, cần tính định danh danh tính cao.

Sáng chế đề ra được xem như là lớp bảo mật bổ sung, tích hợp đi kèm với các phương thức bảo mật, xác thực hiện có, là biện pháp hỗ trợ bảo mật, xác thực trong các giao dịch trực tuyến và xác thực của phần mềm ứng dụng. Đề phòng trường hợp hacker tấn công mạng, dữ liệu phần mềm gây ra các tổn thất không đáng có vì lí do bảo mật, xác thực.

Theo một phương án, sáng chế đề xuất giải pháp giúp thực hiện việc số hóa hồ sơ, tài liệu, loại bỏ các yếu tố làm giả chữ ký trên hồ sơ, làm giả hồ sơ, xác định được người chịu trách nhiệm trên hồ sơ đó bằng phương thức xác thực thông qua thiết bị định danh, phân quyền khi hồ sơ được ký, lưu trữ được các thông tin thay đổi, chỉnh sửa hồ sơ trước thời điểm chốt nội dung văn bản (làm trực tiếp tại một hệ thống ghi nhận thay cho hình thức gửi mail trao đổi thông tin một cách thủ công). Ngoài ra, với việc số hóa hồ sơ tài liệu, giải pháp giải quyết được các vấn đề còn tồn đọng trong hoạt động lưu trữ giấy tờ, hồ sơ, xác minh

hồ sơ thật giả hay xác định danh tính người chịu trách nhiệm ký hồ sơ, giấy tờ và trách nhiệm pháp lý của nó. Với các phương pháp để thực hiện việc số hóa hồ sơ, hệ thống hiện chưa có, chưa đáp ứng được nhu cầu lưu trữ, bảo quản hồ sơ văn phòng. Tính ứng dụng, kiểm tra đối chiếu thông tin hệ thống đối với các hình thức số hóa hồ sơ không cao, không ứng dụng được trong những trường hợp sử dụng hồ sơ số hóa (hồ sơ lưu trữ hệ thống online/phần mềm quản lý) để thực hiện việc sao y, chứng thực giấy tờ.

Do vậy, một phương án của sáng chế đề xuất giải pháp xác thực (mà trong bản mô tả này, có thể được gọi dưới tên giải pháp "*TrueVerified*") có thể thực hiện được điều đó mà đảm bảo được tối đa việc làm giả hồ sơ tài liệu và xác định được chủ thể, đối tượng có trách nhiệm đối với hồ sơ, tài liệu đó căn cứ vào thông tin ký số của thiết bị ký số (trong sáng chế này, thiết bị ký số có thể được gọi dưới tên "*ColdKey*") được cấp định danh cho từng đối tượng phù hợp.

Theo một phương án ưu tiên, với phương thức xác thực, ký số bằng thiết bị ký số "*ColdKey*", thông tin dùng để xác thực được lưu trữ offline và được mã hóa bằng thuật toán RSA (Rivest – Shamir – Adleman). Điều này giúp bảo mật an toàn thông tin xác thực và hầu như không thể bị người khác tấn công hoặc sao chép được trừ khi chính người sở hữu tự làm lộ thông tin.

Ngoài việc chống giả, giải pháp còn giúp cho việc hoạt động và làm việc online và tập thể, nhóm được diễn ra một cách dễ dàng bằng phương thức lưu trữ thông tin liên quan đến việc chỉnh sửa, góp ý, v.v., người thực hiện đối với hồ sơ trực tiếp trên hệ thống lưu trữ hồ sơ.

Theo phương án của sáng chế, quy trình xác thực được thực hiện trực tuyến (online) hoặc ngoại tuyến (offline) tùy từng trường hợp ứng dụng, xác thực, có thể xem hồ sơ xác thực bằng phương thức offline và online một cách linh động, dễ dàng. Thay vì các phương thức xác thực khác như token đều phải nhờ vào máy tính để ký xác thực, người dùng có thể sử dụng điện thoại thông minh (smartphone) để trực tiếp thực hiện việc xác thực này.

Theo sự triển khai phương án của sáng chế, tốc độ thực hiện xác thực sẽ nhanh hơn nhiều do không cần phải chờ đợi hệ thống xác thực trả về mã xác thực và người dùng phải nhập mã xác thực để gửi lại lên hệ thống để xác thực như các phương thức khác.

Mô tả vắn tắt các hình vẽ

Hình 1: Sơ đồ khối hệ thống triển khai quy trình xác thực, định danh hồ sơ theo một phương án của sáng chế;

Hình 2: Sơ đồ so sánh quy trình xác thực theo tình trạng kỹ thuật hiện có và theo phương án của sáng chế;

Hình 3: Sơ đồ quy trình xác thực theo một phương án cụ thể của sáng chế.

Mô tả chi tiết sáng chế

Giải pháp được cấu thành từ mô hình hoạt động kết hợp thiết bị ký số theo sáng chế, thiết bị đọc thiết bị ký số theo sáng chế, phần mềm ứng dụng (ứng dụng di động mobile app, ứng dụng desktop, website), hệ thống phần mềm máy chủ chịu trách nhiệm xác thực thông tin. Trong đó:

Thiết bị ký số theo sáng chế phải có một mã cố định là mã định danh duy nhất (Unique Identifier, UID) và một chuỗi dữ liệu biến đổi ngẫu nhiên không trùng lặp (Unique Data, UData).

Thiết bị đọc thiết bị ký số theo sáng chế là những thiết bị có thể đọc được dữ liệu trong thiết bị ký số theo sáng chế. Theo một phương án của sáng chế, các thiết bị đầu cuối người dùng có tích hợp chức năng để đọc được dữ liệu lưu trogn thiết bị ký số đã nêu.

Phần mềm ứng dụng có nhiệm vụ đấu nối với thiết bị đọc thiết bị ký số theo sáng chế để đọc và ghi dữ liệu vào thiết bị ký số theo sáng chế và giao tiếp với phần mềm trên máy chủ để xác thực dữ liệu thông tin.

Phần mềm máy chủ có nhiệm vụ nhận dữ liệu thông tin từ phần mềm ứng dụng để xử lý (giải mã hoặc không) và xác thực dữ liệu có hợp lệ. Đồng thời khi

xác thực thành công thì trả về dữ liệu (mã hóa hoặc không) cho ứng dụng di động và thông qua thiết bị đọc để cập nhật dữ liệu vào vùng UData của thiết bị ký số theo sáng chế.

Khi thông tin thiết bị ký số theo sáng chế được xác thực thành công thì hệ thống sẽ tiến hành ký định danh UID (hoặc ký số mã hóa RSA) lên tài liệu.

Tham khảo đến Hình 1, sơ đồ hệ thống thực hiện quy trình xác thực theo một phương án của sáng chế sẽ được mô tả chi tiết như dưới đây.

Thiết bị ký số theo sáng chế: là thiết bị hoặc vật phẩm có lưu trữ hai thông tin UID và Udata, theo một phương án ưu tiên là loại chip RFID, hoặc loại tương tự.

UID: Một chuỗi mã không trùng lặp, không thay đổi của thiết bị ký số theo sáng chế.

UData: lưu trữ thông tin dữ liệu không trùng lặp và có thể thay đổi của Thiết bị ký số theo sáng chế.

Phần mềm ứng dụng: phần mềm ứng dụng di động trên các nền tảng điện thoại thông minh (smartphone), hoặc website, hoặc phần mềm ứng dụng trên máy bàn (desktop); hoặc điện thoại thông minh được thiết kế hoặc tích hợp phương thức giao tiếp với thiết bị ký số theo sáng chế và hệ thống xác thực. Phần mềm ứng dụng sẽ lưu trữ một khóa công khai gọi là Public Key để mã hóa dữ liệu.

Hệ thống xác thực: là hệ thống phần mềm máy chủ có tích hợp chức năng xác thực, trên hệ thống này sẽ lưu trữ khóa bí mật Private Key tương ứng với khóa công khai Public Key trên phần mềm ứng dụng.

Public Key: là khóa công khai trong thuật toán mã hóa RSA, khóa này chỉ có thể được dùng để mã hóa mà không thể dùng để giải mã.

Private Key: là khóa riêng tư (bí mật) trong thuật toán mã hóa RSA, khóa này được sử dụng để giải mã chuỗi thông tin được mã hóa bởi Public Key tương ứng.

Cơ sở dữ liệu: là nơi lưu trữ các thông tin dữ liệu của hệ thống.

Hình 2 chỉ ra hai phương thức xác thực, một phương án ác thực toàn bộ trực tuyến (online) theo tình trạng kỹ thuật và có khả năng bị tin tặc xâm nhập, một phương án theo sáng chế như được phân tích sau đây.

Phương thức xác thực được kết hợp song song bởi hai nền tảng trực tuyến và ngoại tuyến (online và offline). Phương thức xác nhận bởi thiết bị offline là điều kiện bắt buộc trong quy trình xác thực để đảm bảo giao dịch được diễn ra thành công. Bởi nguyên lý tin tặc (hacker) xâm nhập hệ thống chỉ có thể tấn công hệ thống bảo mật online, mà không thể tấn công, can thiệp vào phương thức bảo mật online thông qua mã xác thực của thiết bị ký số theo sáng chế offline trừ trường hợp người dùng tự làm lộ thông tin hoặc bảo quản không tốt thiết bị ký số theo sáng chế.

Với việc cấp mã xác thực trực tuyến theo hình thức truyền thống như mã xác nhận qua điện thoại hoặc mã Smart OTP rất không an toàn, dễ bị tấn công để lấy dữ liệu. Không đảm bảo được an toàn trong giao dịch.

Tham chiếu đến Hình 3, quy trình xác thực và định danh hồ sơ sẽ được trình bày chi tiết như dưới đây.

Việc xác thực được thực hiện bởi một phần mềm hệ thống hỗ trợ, có tài khoản được cấp cho người dùng. Ngoài việc định danh bằng tài khoản và mật khẩu người dùng, mỗi người dùng được cấp một thiết bị định danh gọi là thiết bị ký số theo sáng chế. Với thông tin mô tả của thiết bị ký số theo sáng chế như UID không trùng lặp, không thay đổi và Udata là chuỗi dữ liệu có thể thay đổi thông tin tại mỗi lần sử dụng, cho ra chuỗi dữ liệu không trùng lặp và không thể làm giả, việc xác thực, định danh, số hóa hồ sơ, tài liệu, chứng từ được bảo mật hơn bao giờ hết.

Phương pháp này được ứng dụng một cách triệt để trong việc số hóa mỗi hồ sơ, tài liệu đính kèm. Hồ sơ được theo dõi, giám sát theo từng trang với những nội dung chi tiết, lưu lại, truy vết được quá trình, nội dung và người thực

hiện chỉnh sửa hồ sơ tài liệu. Sau khi chốt thông tin văn bản, hồ sơ được người có thẩm quyền phê duyệt ký số xác thực văn bản, kích hoạt hiệu lực pháp lý của văn bản ký số.

Hồ sơ được lưu trữ hoàn toàn online/lưu trữ trên hệ thống phần mềm, đối với việc muốn lưu trữ văn bản offline hoặc sử dụng văn bản đã được ký số (lưu trữ hệ thống phần mềm, không có file giấy được ký sống, đóng dấu bởi các bên), giải pháp đưa đến một quy trình tích hợp bổ sung để đảm bảo tính pháp lý phù hợp đối với nhu cầu sử dụng hồ sơ giấy. Đảm bảo quy trình số hóa hoạt động công chứng, chứng thực hồ sơ đều phải được diễn ra một cách song song và đồng bộ. Công chứng viên có trách nhiệm kiểm tra, đánh giá, xác thực nội dung, hình thức hồ sơ từ dữ liệu hệ thống. Thực hiện việc công chứng hồ sơ, đảm bảo hồ sơ giấy (bản công chứng) cũng được ứng dụng giải pháp *TrueVerified* theo sáng chế để thực hiện việc số hóa hồ sơ quản lý hệ thống và gắn chip RFID để theo dõi, xác thực hồ sơ công chứng.

Quy trình nguyên lý xác thực hồ sơ theo một phương án cụ thể của sáng chế được mô tả như sau.

Bước 1: thông qua thiết bị đầu cuối người dùng, tại giao diện của phần mềm ứng dụng, người dùng (user) đăng nhập bằng tài khoản hệ thống, sau đó thiết bị đầu cuối sẽ thực hiện quét thiết bị ký số theo sáng chế để xác thực danh tính của người dùng.

Bước 2: người dùng đính kèm file tài liệu cần thỏa thuận, cần được kiểm tra, ký xác thực bởi người có thẩm quyền.

Bước 3: (các) người dùng kiểm tra hồ sơ, gửi tài liệu chỉnh sửa hoặc đính kèm nội dung chỉnh sửa lên hệ thống. Thông tin chỉnh sửa, ý kiến, v.v. đều được hệ thống ghi nhận và là một phần không tách rời của hồ sơ khi được chốt nội dung và được người có thẩm quyền phê duyệt, xác thực, ký số hồ sơ.

Bước 4: hồ sơ sau khi được ký xác thực sẽ được niêm phong, không cho phép chỉnh sửa trực tiếp. Trong luồng dữ liệu liên quan sẽ được lưu trữ các văn

bản, chứng từ có liên quan đến hồ sơ chính với hình thức đính kèm, chỉnh sửa tương tự.

Bước 5: xác định giá trị hồ sơ số hóa. Hồ sơ được lưu trữ trên hệ thống ở dạng file PDF được mã hóa, không chỉnh sửa, có thể xem trực tiếp trên hệ thống hoặc tải về và cho phép in ra. Tuy nhiên, tùy thuộc vào điều kiện và yêu cầu pháp lý xác thực của hồ sơ, trường hợp hồ sơ được người dùng tự ý in trực tiếp sẽ không đảm bảo tính pháp lý về độ thật giả của hồ sơ.

Đảm bảo hành lang an toàn pháp lý, công chứng viên có trách nhiệm kiểm tra, đối chiếu và xác thực nội dung, hình thức giấy tờ đối với bản giấy photo từ hồ sơ hệ thống với thông tin hồ sơ cụ thể tại hệ thống. Hồ sơ công chứng cần được gắn chip để theo dõi và số hóa hồ sơ của công chứng, chứng thực.

Quy trình xác thực bằng thiết bị ký số (*Coldkey*) theo sáng chế sẽ được trình bày chi tiết dưới dạng giải pháp kỹ thuật như dưới đây.

Bước 1: đọc thông tin mã định danh duy nhất (Unique Identifier, UID) và dữ liệu dạng chuỗi duy nhất không trùng lặp (Unique Data, UData) trên thiết bị ký số theo sáng chế bởi thiết bị đầu cuối người dùng và hiển thị thông qua phần mềm ứng dụng, để xác định danh tính người sử dụng (người giữ vai trò xác thực viên).

Bước 2: mã hóa các thông tin UID, UData và dữ liệu khác bằng thuật toán RSA thành một chuỗi mã hóa bởi thiết bị đầu cuối người dùng sử dụng phần mềm ứng dụng chứa khóa công khai public key.

Bước 3: gửi chuỗi mã hóa kèm khóa công khai public key lên hệ thống xác thực thông qua phần mềm ứng dụng bởi thiết bị đầu cuối người dùng.

Bước 4: giải mã chuỗi mã hóa thành UID, UData và dữ liệu khác bởi máy chủ trong hệ thống xác thực sử dụng khóa bí mật private key tương ứng với khóa công khai public key được gửi kèm ở bước trên.

Bước 5: kiểm tra tính hợp lệ của UID, UData bởi máy chủ trong hệ thống xác thực sẽ; nếu kết quả hợp lệ thì hệ thống xác thực sẽ tạo một UData mới (duy nhất và không trùng lặp) và gửi trả về phần mềm ứng dụng.

Bước 6: cập nhật UData mới cho thiết bị ký số theo sáng chế bởi thiết bị đầu cuối người dùng thông qua phần mềm ứng dụng.

Hiệu quả đạt được của sáng chế

Giải pháp thiết bị ký số theo sáng chế mang đến cho người sử dụng sự an toàn bảo mật gần như tuyệt đối.

Đảm bảo các giao dịch được thực hiện một cách an toàn.

Giữ toàn bộ thông tin dùng để giao dịch nằm ngoài tầm với của những kẻ tấn công.

Phương thức số hóa tài liệu, ứng dụng trong hoạt động quản lý văn phòng, hành chính.

Khả năng ứng dụng trong công nghiệp

Giao dịch được ứng dụng trong hoạt động số hóa hồ sơ văn phòng, quyết định, văn bản, hợp đồng, hồ sơ cần được lưu trữ. Thay vì phải làm việc trực tiếp và lưu trữ hồ sơ offline với khối lượng hồ sơ rất lớn gây khó khăn cho nhiều cá nhân thực hiện kiểm soát và lưu trữ hồ sơ.

Hồ sơ có thể kiểm tra nội dung online và lưu trữ một cách thuận tiện cho người dùng.

Các hệ thống và kỹ thuật được mô tả ở đây có thể được triển khai trong một hệ thống máy tính bao gồm thành phần đầu cuối phía sau (ví dụ: máy chủ dữ liệu) hoặc bao gồm thành phần phần sụn (ví dụ: máy chủ ứng dụng) hoặc bao gồm thành phần giao diện người dùng (ví dụ: máy khách có giao diện người dùng đồ họa hoặc trình duyệt Web mà qua đó người dùng có thể tương tác với việc triển khai các hệ thống và kỹ thuật được mô tả ở đây), hoặc bất kỳ sự kết hợp nào của các thành phần đầu cuối phía sau, phần sụn, đầu cuối phía trước đó.

Các thành phần của hệ thống có thể được kết nối với nhau bằng bất kỳ hình thức hoặc phương tiện truyền thông dữ liệu kỹ thuật số nào (ví dụ: mạng truyền thông). Ví dụ về mạng truyền thông bao gồm mạng cục bộ (LAN), mạng diện rộng (WAN) và Internet.

Hệ thống máy tính có thể bao gồm các máy khách và máy chủ. Máy khách và máy chủ thường cách xa nhau và thường tương tác thông qua mạng truyền thông. Mối quan hệ của máy khách và máy chủ phát sinh do các chương trình máy tính chạy trên các máy tính tương ứng và có mối quan hệ máy khách-máy chủ với nhau.

Mặc dù các cách triển khai khác nhau đã được mô tả chi tiết ở trên, nhưng vẫn có thể thực hiện được các sửa đổi khác. Ngoài ra, các luồng logic được mô tả trong các hình không yêu cầu thứ tự cụ thể được hiển thị, hoặc thứ tự tuần tự, để đạt được kết quả mong muốn. Ngoài ra, các bước khác có thể được cung cấp hoặc các bước có thể bị loại bỏ khỏi quy trình được mô tả và các thành phần khác có thể được thêm vào hoặc loại bỏ khỏi hệ thống được mô tả. Theo đó, các triển khai khác nằm trong phạm vi của các điểm yêu cầu bảo hộ sau.

YÊU CẦU BẢO HỘ

1. Quy trình xác thực và định danh hồ sơ sử dụng chữ ký số, quy trình này bao gồm các bước:

cho phép người dùng đăng nhập vào thiết bị đầu cuối người dùng thông qua phần mềm ứng dụng với mã định danh và mật khẩu được lưu trữ trong cơ sở dữ liệu của hệ thống;

đọc thông tin được lưu trữ trong thiết bị ký số theo sáng chế bởi thiết bị đầu cuối người dùng, để xác định danh tính người sử dụng (người giữ vai trò xác thực viên); trong đó thiết bị ký số được tạo cấu hình để có ít nhất một vùng chứa mã định danh duy nhất (unique identifier, UID) và một vùng chứa chuỗi mã dữ liệu thay đổi ngẫu nhiên không trùng lặp (unique data, Udata);

mã hóa các thông tin UID, UData và dữ liệu khác bằng thuật toán RSA thành chuỗi mã hóa bởi thiết bị đầu cuối người dùng sử dụng phần mềm ứng dụng chứa khóa công khai public key;

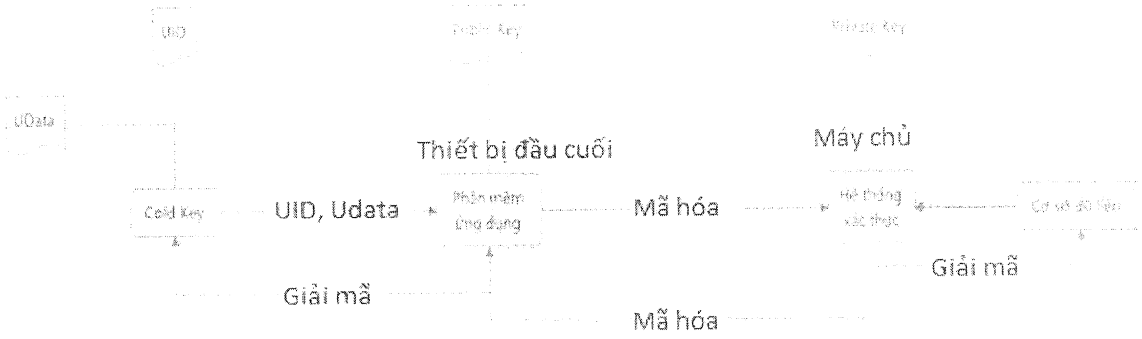
gửi chuỗi mã hóa kèm khóa công khai public key lên hệ thống xác thực thông qua phần mềm ứng dụng bởi thiết bị đầu cuối người dùng;

giải mã chuỗi mã hóa thành UID, UData và dữ liệu khác bởi máy chủ trong hệ thống xác thực sử dụng khóa bí mật private key tương ứng với khóa công khai public key được gửi kèm ở bước trên;

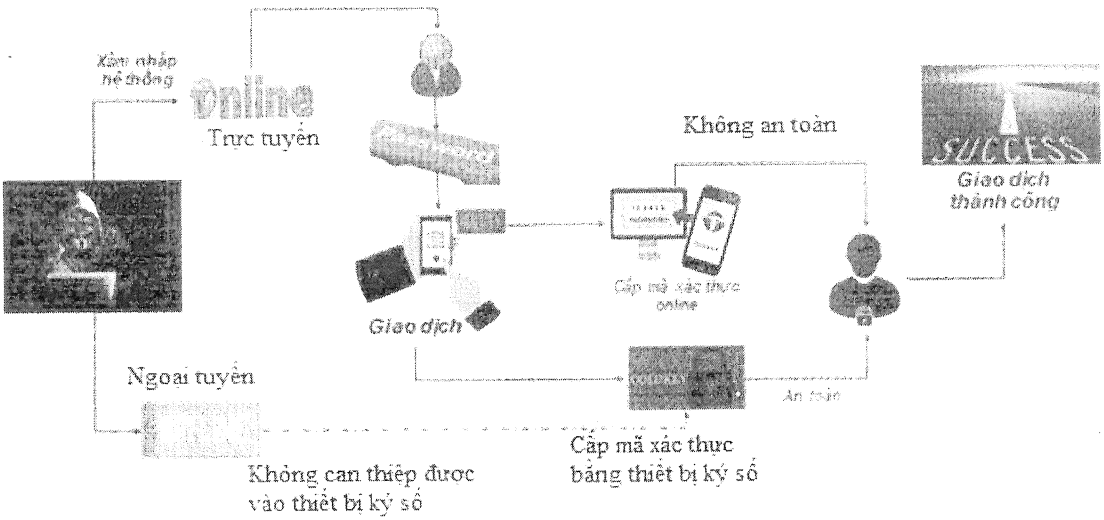
kiểm tra tính hợp lệ của UID, UData bởi máy chủ trong hệ thống xác thực sẽ; nếu kết quả hợp lệ thì hệ thống xác thực sẽ tạo một UData mới (duy nhất và không trùng lặp) và gửi trả về phần mềm ứng dụng;

cập nhật UData mới cho thiết bị ký số theo sáng chế bởi thiết bị đầu cuối người dùng thông qua phần mềm ứng dụng;

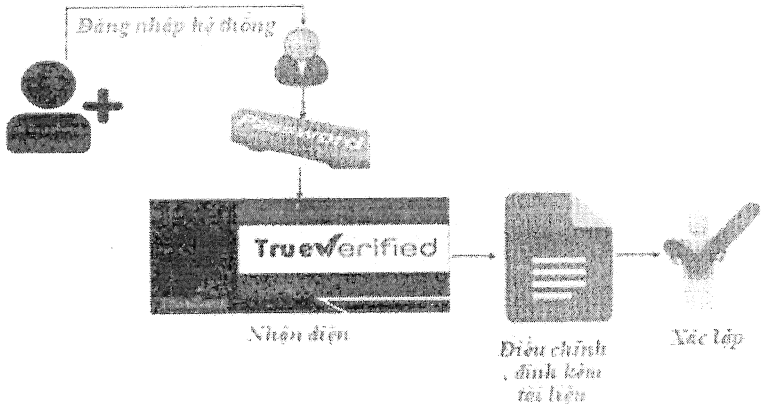
trong đó, thiết bị chữ ký số là loại tích hợp chip RFID (Radio Frequency Identification, nhận dạng bằng sóng vô tuyến) và có thể được đọc bởi bất kỳ thiết bị đầu cuối người dùng có tích hợp chức năng đọc RFID mà không cần giao tiếp qua cổng USB.



Hình 1



Hình 2



Hình 3