Ôn Tập An Toàn Thông Tin CUỐI KỲ (2021-2022)

An toàn thông tin (Trường Đại học Công nghiệp Thành phố Hồ Chí Minh)

Câu 1: Chữ ký điện tử là gì? Mục tiêu của chữ ký điện tử? Trình bày hiện trạng áp dụng chữ ký điện tử ở Việt Nam (gợi ý: Định nghĩa chữ ký điện tử: ứng dụng của mã hóa khóa công khai, người dùng có (PU_A, PR_A); Tạo chữ ký: $S_{AM}=E(M,PR_A)$ – giải thích; Thẩm tra chữ ký $D(S_{AM}, PU_A)$ -→ Yes/No – Giải thích; Mục tiêu của chữ ký số; Hiện trạng áp dụng chữ ký: 4 lĩnh vực đó là cơ quan Thuế, Bảo hiểm xã hội, Hải quan và Chứng khoán).

Chữ ký điện tử là gì?

Chữ ký điện tử được định nghĩa tương đối rộng và trừu tượng. Theo Luật GDĐT 2005, "chữ ký điện tử" có các đặc tính sau: (i) được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử; (ii) được gắn liền hoặc kết hợp một cách lô gic với hợp đồng điện tử (ví dụ, dưới định dạng PDF hoặc Word); và (iii) có khả năng xác nhận người ký hợp đồng điện tử và xác nhận sự chấp thuận của người đó đối với nội dung của hợp đồng điện tử được ký.Chữ ký điện tử có giá trị pháp lý nếu thỏa mãn các điều kiện về khả năng định danh và mức độ tin cậy, cụ thể là: phương pháp tạo chữ ký điện tử cho phép xác minh được người ký và chứng tỏ được sự chấp thuận của người ký đối với nội dung của hợp đồng và phương pháp tạo chữ ký điện tử là đủ tin cậy và phù hợp với mục đích mà hợp đồng được tạo ra và gửi đi.

Mục tiêu của chữ ký điện tử?

- Giúp xác minh chủ thể là ai: Tăng khả năng bảo mật, chống giả mạo, cho phép chủ thẻ xác minh danh tính của mình trên các hệ thống khác nhau như xe bus, thẻ rút tiền ATM, hộ chiếu điện tử tại các cửa khẩu, kiểm soát hải quan … Dùng để kê khai, nộp thuế trực tuyến, khai báo hải quan và thông quan trực tuyến mà không phải mất thời gian in các tờ khai, trình ký đóng dấu đỏ của công ty rồi đến cơ quan thuế xếp hàng và ngồi đợi để nộp tờ khai này sẽ thuận tiện hơn

Một số ứng dụng chữ ký số điện tử điển hình:

- Ứng dụng trong Chính phủ điện tử.+ *Ứng dụng của Bộ Tài chính+ Ứng dụng của Bộ Công thương*

+ Ứng dụng của Bộ KHCN, …

- Ứng dụng trong Thương mại điện tử.+ *Mua bán, đặt hàng trực tuyến+ Thanh toán trực tuyến, …*

- Ứng dụng trong giao dịch trực tuyến.+ *Giao dịch qua email*

- Hội nghị truyền hình và làm việc từ xa với Mega e-Meeting...

Làm thế nào để tạo ra một chữ ký điện tử?

Chữ ký điện tử yêu cầu phải sử dụng một mã hóa khóa công cộng (public key). Nếu muốn tạo chữ ký điện tử thì cần phải có thêm cả mã hóa khóa cá nhân (private key). Bạn dùng khóa cá nhân để ký - chỉ là một dạng mã - sau đó chỉ cung cấp khóa công cộng cho người cần xác nhận chữ ký đó (chẳng hạn như ngân hàng, nơi bạn vay tiền).

Một số ví dụ có liên quan đến chữ kí điện tử:

- Mặc dù chưa có bất kỳ án lệ nào của tòa án giải quyết cụ thể vấn đề về hiệu lực của các hợp đồng được ký bằng chữ ký điện tử, đã có các án lệ và bản án cho thấy các tòa án Việt Nam thiên về cách tiếp cận chú trọng nội dung (tức là xem xét ý chí thực sự của các bên trong giao dịch) hơn là hình thức thể hiện sự chấp thuận đối với nội dung đó (tức là xem xét hình thức hợp đồng và chữ ký). Trong một số án lệ và bản án, Tòa án nhân dân tối cao đã ra phán quyết rằng, hành vi của các bên trong quá trình giao kết và thực hiện hợp đồng có giá trị quan trọng để xác định ý chí của các bên trong hợp đồng và cho dù hợp đồng không được ký bởi các bên có liên quan, hợp đồng đó vẫn không bị vô hiệu.

- Án lệ số 07/2016/AL ngày 17/10/2016 về công nhận hợp đồng mua bán nhà được xác lập trước ngày 1 tháng 7 năm 1991(tranh chấp giữa Nguyễn Đình Sông, Nguyễn Thị Hồng, Nguyễn Thị Hương với Đỗ Trọng Thành, Đỗ Thị Nguyệt, Vương Chí Tường, Vương Chí Thắng, Vương Bích Vân, Vương Bích Hợp - Án lệ 07)

Câu 2: Đưa ra một hệ thống thông tin hoặc một trang web thực tế ở Việt Nam mà có sử dụng chữ ký điện tử? Nghiệp vụ nào trong hệ thống đó có sử dụng chữ ký số? Trình bày các bước cụ thể để người dùng trong hệ thống này thực hiện nghiệp vụ có sử dụng chữ ký số. (gợi ý: Website của cơ quan Thuế, Wibsite của cơ quan Hải quan, Website của cơ quan Bảo hiểm xã hội, ...)

Đưa ra một hệ thống thông tin hoặc một trang web thực tế ở Việt Nam mà có sử dụng chữ ký điện tử?

Website của cơ quan Hải quan, Website của cơ quan Bảo hiểm xã hội,...)

Trình bày các bước cụ thể để người dùng trong hệ thống này thực hiện nghiệp vụ có sử dụng chữ ký số?

Hướng dẫn cá nhân, doanh nghiệp sử dụng chữ ký số để nộp thuế điện tử

Bước1: Đăng nhập vào Trang thông tin điện tử của Tổng cục Thuế tại http://thuedientu.gdt.gov.vn

***Bước2*:** Lập giấy nộp tiền

- Sau khi đăng nhập thành công, doanh nghiệp lập giấy nộp tiền theo các bước dưới đây:

- Tại mục "Nộp thuế" nhấn chọn "Lập giấy nộp tiền"

- Lựa chọn "Ngân hàng nộp thuế" và nhấn "Tiếp tục"

Bước 3: Khai báo thông tin trên tờ khai

- Trong quá trình hoàn tất thủ tục nộp thuế điện tử, doanh nghiệp cần khai báo đầy đủ và chính xác những nội dung sau trong tờ khai thuế:

+ Thông tin loại tiền: Chọn "VND" nếu đơn vị thuộc diện nộp thuế bằng đồng Việt Nam, trường hợp thuộc diện nộp thuế ngoại tệ thì đơn vị chọn đúng loại ngoại tệ mình sử dụng.

+ Thông tin ngân hàng: Chọn ngân hàng và số tài khoản để trích tiền.

+ Thông tin cơ quan quản lý thu: Chính là thông tin cơ quan thuế quản lý đơn vị.

+ Thông tin nơi phát sinh khoản thu: Điền địa chỉ nơi phát sinh khoản thu theo quy định của từng Cục Thuế hoặc Chi cục thuế địa phương.

+ Thông tin kho bạc nhận tiền.

+ Loại thuế: Chọn tương ứng theo mục đích nộp thuế của đơn vị.

- Tại mục "Nội dung các khoản nộp NSNN" bạn tích chọn vào ô vuông 3 chấm để chọn loại thuế muốn nộp

- Tại mục Nội dung các khoản nộp danh sách: Nhập mã NDKT

***Lưu ý*:**

+ Căn cứ vào vốn điều lệ ghi trong Giấy Đăng ký kinh doanh. Trường hợp không có vốn điều lệ thì căn cứ vào vốn đầu tư ghi trong giấy chứng nhận đăng ý đầu tư.

+ Đối với công ty, doanh nghiệp, tổ chức mới thành lập cần nộp Thuế môn bài: Nếu được cấp đăng ký thuế và mã số thuế, mã số doanh nghiệp trong thời gian của 6 tháng đầu năm thì nộp mức lệ phí môn bài cả năm; Nếu thành lập, được cấp đăng ký thuế và mã số thuế, mã số doanh nghiệp trong

thời gian 6 tháng cuối năm (từ ngày 1/7 đến 31/12) thì nộp 50% mức lệ phí môn bài cho năm đầu tiên.

- Sau khi nhập xong giá trị vào ô Mã "NDKT", hệ thống sẽ tự sinh các thông tin tương ứng theo quy định của pháp luật.

- Người dùng khai báo thông tin đầy đủ và chính xác, nhấn "Hoàn thành" để tạo lập xong tờ khai.

Bước 4: Ký số

- Bước cuối cùng để hoàn thành thủ tục nộp thuế điện tử là ký số. Doanh nghiệp cần kiểm tra lại thông tin vừa khai báo trong Giấy nộp tiền vào ngân sách nhà nước. Nếu thông tin đã chính xác, người dùng cắm chữ ký số của doanh nghiệp và tiếp tục nhấn "Ký và nộp".

- Sau đó, nhập mã PIN và nhấn "OK".

Như vậy, doanh nghiệp đã hoàn thành xong việc nộp tiền một mục thuế, trường hợp cần nộp nhiều mục thì đơn vị thực hiện lặp lại từ bước Lập giấy nộp tin

Câu 3: Chứng thư số là gì? Mục tiêu của chứng thư số? Hiện nay Việt Nam đã có các đơn vị nào có thể cung cập dịch vụ chứng thư số?

Chứng thư số là gì?

Căn cứ theo quy định luật giao dịch điện tử 2005, chứng thư số là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Nhằm cung cấp thông tin định danh cho khóa công khai của một cơ quan, tổ chức, cá nhân. Từ đó xác nhận cơ quan, tổ chức, cá nhân là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng.

Chứng thư số có thể được coi là "chứng minh thư" để sử dụng trong môi trường của máy tính và internet. Chứng thư số được sử dụng để nhận diện một cá nhân, một máy chủ, hay là một vài đối tượng khác. Và gắn định danh của đối tượng đó với một public key (khóa công khai). Được cấp bởi những tổ chức có thẩm quyền xác định nhận danh và cấp chứng thư số.

Hiện nay Việt Nam đã có các đơn vị nào có thể cung cấp dịch vụ chứng thư số?

Hiện nay trên thị trường có gần 20 đơn vị cung cấp chữ ký số điện tử, khiến doanh nghiệp tuy có nhiều sự lựa chọn đa dạng hơn nhưng lại gặp khó khăn trong việc đưa ra quyết định mua của đơn vị nào. Có thể kể đến một vài loại chữ ký số được các doanh nghiệp tin dùng hiện nay như:

1. Chữ ký số điện tử MISA eSign của nhà cung cấp MISA
2. Chữ ký số Viettel – CA của nhà cung cấp Viettel
3. Chữ ký số VNPT – CA của nhà cung cấp VNPT
4. Chữ ký số BKAV – CA của nhà cung cấp BKAV

Câu 4: Chứng thư số là gì? Nội dung có trong chứng thư số là gồm những nội dung gì?

Chứng thư số là: Chứng thư số là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Chứng thư số có thể được xem như là "chứng minh thư" để sử dụng trong môi trường của máy tính và Internet. Chứng thư số được sử dụng để nhận diện một cá nhân, một máy chủ, hay là một vài đối tượng khác và gắn định danh của đối tượng đó với một public key, được cấp bởi những tổ chức có thẩm quyền xác định nhận danh và cấp chứng thư số. Chứng thu số được tạo bởi nhà cung cấp dịch vụ chứng thực trong đó chứa public key và các thông tin của người dùng theo chuẩn X.509. Khóa bí mật của chữ ký số bắt buộc phải lưu trữ trong một thiết bị phần cứng chuyên dụng là USB Token hoặc SmartCard được cung cấp bởi nhà cung cấp. Các thiết bị này đảm bảo khóa bí mật không bị copy hay bị virus phá hỏng.

Chứng thư số chứa những nội dung gì?

1. Tên của thuê bao.
2. Số hiệu của chứng thư số (số seri)
3. Thời hạn có hiệu lực của chứng thư số
4. Tên của tổ chức chứng thực chữ ký số (Ví du: VIETTEL CA)
5. Chữ ký số của tổ chức chứng thực chữ ký số.
6. Các thư hạn chế về mục đích, phạm vi sử dụng của chứng số.
7. Các hạn chế về trách nhiệm của tổ chức cung cấp dịch vụ chứng thực chữ ký số.
8. Các nội dung cần thiết khác theo quy định của Bộ Thông Tin Truyền Thông.

9. Chứng thư số là cặp khóa đã được mã hóa dữ liệu gồm thông tin công ty & mã số thuế của DN, dùng để ký thay cho chữ ký thông thường , được ký trên các loại văn bản và tài liệu số như : word, excel, pdf….., những tài liệu này dùng để nộp thuế qua mạng, khai hải quan điện tử và thực hiện các giao dịch điện tử khác.

Câu 5: Chứng thực thực thể là gì? Trình này 2 phương pháp mà bạn biết mà có thể cài đặt để chứng thực thực thể?

Chứng thực thực thể: là một kỹ thuật được thiết kế cho phép một bên chứng minh sự nhận dạng của một bên khác.

Các phương pháp Chứng thực thực thể :

Chứng thực bằng Passwords

Chứng thực bằng sinh trắc học Biometrics

- Hiện nay phương pháp chứng thực bằng Passwords được sử dụng chủ yếu, tuy nhiên, công nghệ ngày càng phát triển, việc chứng thực bằng sinh trắc học đang dần được sử dụng nhiều mang lại hiệu quả cao hơn.

Vì: Nhận dạng sinh trắc học (vân tay, móng mắt/võng mạc, DNA…) là những điểm đặc trưng nhận dạng của mỗi người, có thể nói không thể trùng nhau nên việc chứng thực sẽ có độ chính xác cao, tin cậy, thời gian chứng thực nhanh (dưới 1s) trong các trường hợp có thể đụng độ nhưng khả năng hầu như rất thấp và không đáng kể và vì cần phải sử dụng các thiết bị công nghệ cao nên giá thành đắt đó là nhược điểm lớn làm cho phương pháp này thực sự chưa phổ biến bằng phương pháp chứng thực truyền thống.

* Mô tả:

Phương pháp chứng thực bằng vân tay, võng mac/móng mắt

+ Sử dụng các thiết bị thu nhận (quét) và lưu trữ các đặc tính sinh trắc học.

+ Quét các đặc tính sinh trắc của chủ thể (đặc điểm vân tay, móng mắt, ..) đưa về dạng dữ liệu biểu diễn dưới dạng các bit và lưu trữ trong cơ sở dữ liệu.

+ Chứng thực: Chủ thể muốn giao dịch cần phải chứng thực danh tính/định danh cần tiến hành quét lại các thông tin bảo mật lưu trước đó qua các thiết bị quét như vân tay, móng mắt, sau khi quét, tiến hành đưa về chuỗi các bit và so sánh trong cơ sở dữ liệu:

Nếu đúng (trùng với dữ liệu đã lưu)→Xác thực thành công

Nếu không trùng với dữ liệu trước đó, hệ thống từ chối giao dịch đến khi chủ thể chứng thực thành công.

+ Chứng thực thực thể bằng sinh trắc học (biometrics) là gì, nêu ưu điểm và nhược điểm của phương pháp này, phương pháp này thường được áp dụng ở đâu.

Chứng thực thực thể bằng sinh trắc học (Biometrics) là sử dụng các phép đo lường về các đặc tính sinh lí học hoặc hành vi học mà nhận dạng một con người, các đặc thù của sinh trắc học không thể đoán , ăn cắp hay chia sẻ. ví dụ như vân tay, vân lòng bàn tay, võng mạc, móng mắt, khuôn mặt, giọng nói…

- Ưu điểm:

+ Có độ chính xác cao

+ Thời gian chứng thực rất nhanh (nhỏ hơn 1s)

+ Sự tác động của người dùng thấp

+ Có sự kết hợp nhiều yếu tố: vân tay, võng mạc, giọng nói.

- Nhược điểm:

+ Giá thành: triển khai hệ thống sinh trắc học đòi hỏi chi phí cao cho cả phần cứng (thiết bị thu/quét, và nhận dạng) với các phần mềm hiện đại.

+ có thể nhận diện sai: do hư hỏng phần cứng, lỗi phần mềm làm cho hệ thống từ chối người dùng mặc dù đúng người.

- Hiện nay: công nghệ chứng thực bằng sinh trắc học được áp dụng rộng rãi hơn ở những ngân hang, các công ty (dùng chấm công, điểm danh) hay thực hiện bảo mật dữ liệu cá nhân trên các thiết bị di động cao cấp ...

Câu 6: Điều khiển truy cập là gì? Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin?

6.1. Điều khiển truy cập là gì?

Thuật ngữ điều khiển truy cập (*access control*) ám chỉ đến các thi hành nhằm hạn chế sự thâm nhập vào một cơ sở, một tòa nhà, hoặc một phòng làm việc, chỉ cho phép những người đã được ủy quyền tiếp cận mà thôi. An ninh trên hiện trường có thể thực hiện được bằng sức người - chẳng hạn dùng người canh gác, người gác cổng thuê (*bouncer*), hoặc một người tiếp tân - hoặc bằng sức máy - khóa và chìa khóa - hay bằng việc áp dụng khoa học kỹ thuật như việc sử dụng một hệ thống truy cập dùng thẻ.

6.2. Phương pháp có thể cài đặt điều khiển truy cập một hệ thống thông tin

Điều khiển truy cập bắt buộc MAC

- Điều khiển truy cập bắt buộc (Mandatory Access Control - MAC)

Là mô hình điều khiển truy cập nghiêm ngặt nhất
Thường bắt gặp trong các thiết lập của quân đội
Hai thành phần: Nhãn và Cấp độ
- Mô hình MAC cấp quyền bằng cách đổi chiều nhân của đối tượng với nhân của chủ thể
Nhãn cho biết cấp độ quyền hạn
- Để xác định có mở một file hay không:

So sánh nhân của đối tượng với nhân của chủ thể
Chủ thể phải có cấp độ tương đương hoặc cao hơn: đối tượng được cấp phép truy cập
- Hai mô hình thực thi của MAC

Mô hình mạng lưới (Lattice model)
Mô hình Bell-LaPadula
- Mô hình mạng lưới

Các chủ thể và đối tượng được gán một "cấp bậc" trong mạng lưới
Nhiều mạng lưới có thể được đặt cạnh nhau
- Mô hình Bell-LaPadula

Tương tự mô hình mạng lưới
Các chủ thể không thể tạo một đối tượng mới hay thực hiện một số chức năng nhất định đối với các đối tượng có cấp thấp hơn
- Ví dụ về việc thực thi mô hình MAC

Windows 7/Vista có bốn cấp bảo mật

Các thao tác cụ thể của một chủ thể đối với phân hạng thấp hơn phải được sự phê duyệt của quản trị viên

- Hộp thoại User Account Control (UAC) trong Windows

Điều khiển truy cập tùy ý (DAC)

- Điều khiển truy cập tùy ý (DAC)

Mô hình ít hạn chế nhất

Mọi đối tượng đều có một chủ sở hữu

Chủ sở hữu có toàn quyền điều khiển đối với đối tượng của họ

Chủ sở hữu có thể cấp quyền đối với đối tượng của mình cho một chủ thể khác

Được sử dụng trên các hệ điều hành như Microsoft Windows và hầu hết các hệ điều hành UNIX

- Nhược điểm của DAC

Phụ thuộc vào quyết định của người dùng để thiết lập cấp độ bảo mật phù hợp

Việc cấp quyền có thể không chính xác

Quyền của chủ thể sẽ được "thừa kế" bởi các chương trình mà chủ thể thực thi

Trojan là một vấn đề đặc biệt của DAC

Điều khiển truy cập dựa trên vai trò (RBAC)

- Điều khiển truy cập dựa trên vai trò (Role Based Access Control - RBAC)

Còn được gọi là Điều khiển Truy cập không tùy ý

Quyền truy cập dựa trên chức năng công việc

- RBAC gần các quyền cho các vai trò cụ thể trong tổ chức

Các vai trò sau đó được gắn cho người dùng

Điều khiển truy cập dựa trên quy tắc (RBAC)

- Điều khiển truy cập dựa trên quy tắc (Rule Based Access Control - RBAC)

- Tự động gán vai trò cho các chủ thể dựa trên một tập quy tắc do người giám sát xác định

- Mỗi đối tượng tài nguyên chứa các thuộc tính truy cập dựa trên quy tắc

- Khi người dùng truy cập tới tài nguyên, hệ thống sẽ kiểm tra các quy tắc của đối tượng để xác định quyền truy cập

- Thường được sử dụng để quản lý truy cập người dùng tới một hoặc nhiều hệ thống

Những thay đổi trong doanh nghiệp có thể làm cho việc áp dụng các quy tắc thay đổi

Câu 7: Mật khẩu (password) là gì? Mật khẩu cố định (fixed password) và mật khẩu dùng một lần (one time password) khác nhau như thế nào? Trình bày điểm mạnh và điểm yếu của 2 loại mật khẩu?

Password (mật khẩu) là gì?

Mật khẩu (tiếng Anh: Password) thường là một xâu, chuỗi, loạt các ký tự mà dịch vụ internet phần mềm hệ thống máy tính yêu cầu người sử dụng nhập vào bằng bàn phím trước khi có thể tiếp tục sử dụng một số tính năng nhất định.

Khác nhau giữa mật khẩu cố định và mật khẩu dùng một lần:

Mật khẩu cố định	**Mật khẩu dùng một lần**
Được dùng lặp đi lặp lại.	Chỉ dùng được 1 lần và không sử dụng lại.
Dễ tấn công.	Khó tấn công.
Tính bảo mật thấp	Tính bảo mật cao

Điểm mạnh và điểm yếu của mật khẩu cố định và mật khẩu dùng một lần:

- Mật khẩu cố định:

+ Điểm mạnh: khi sử dụng những mật khẩu mạnh có thể tạo một lớp bảo mật chắc chắn.

+ Điểm yếu: người dùng sử dụng những mật khẩu quá phổ biến, mật khẩu chứa thông tin cá nhân, … điều này tạo ra lỗ hỏng bảo mật.

- Mật khẩu dùng một lần:

+ Điểm mạnh: khó bị tấn công, có tính bảo mật rất cao, nhận được mật khẩu nhanh chóng, tiện lợi, được yêu cầu lấy mật khẩu nhiều lần, chi phí thấp. Thẻ thông minh hay thiết bị tạo mật khẩu cầm tay (token) nhờ vào kết nối internet với máy chủ của dịch vụ cung cấp OTP hoặc cũng có thể thông qua thẻ OTP in sẵn thay điện thoại di động mà không cần đến kết nối internet

+ Điểm yếu: hạn chế thời gian hiệu lực, không thể sử dụng những nơi không có sóng di động đối với OTP SMS.

Câu 8: Trình bày các loại mã OPT, nêu ưu điểm và nhược điểm của từng loại?

Các hình thức cung cấp mã OTP và ưu nhược điểm

Hiện nay có 3 hình thức cung cấp mã OTP chủ yếu. Bao gồm:

1) SMS OTP

Đây là hình thức cung cấp mã OTP phổ biến nhất hiện nay. Mã OTP sẽ được gửi bằng tin nhắn SMS về số điện thoại đã đăng ký. Để thực hiện được giao dịch bạn cần phải nhập mã OTP được gửi về số điện thoại đã đăng ký. Đa số các ngân hàng tại Việt Nam hiện nay đều có sử dụng mã OTP theo hình thức này.

Hình thức này không chỉ được các ngân hàng sử dụng mà cả các công ty công nghệ lớn trên thế giới như Google, Facebook cũng áp dụng để tạo lớp bảo mật thứ hai cho tài khoản của bạn. Và lớp bảo vệ này sẽ xuất hiện khi phát hiện bất kỳ hoạt động không rõ ràng nào từ tài khoản của bạn.

Ưu điểm:

- Thời gian tích hợp dịch SMS OTP nhanh chóng, chỉ từ 30 – 60 phút.
- Hỗ trợ đăng ký nhanh thương hiệu riêng (SMS Brand) cho từng doanh nghiệp để gửi SMS OTP và chăm sóc khách hàng.
- Hệ thống ổn định trên nền tảng Cloud.
- Hỗ trợ cả HTTP và SMPP và App.
- Hỗ trợ API, code mẫu và tài liệu hướng dẫn tích hợp miễn phí.
- Cách sử dụng đơn giản, dễ hiểu, tiện lợi. (Người dùng có thể copy mã OTP trực tiếp từ tin nhắn sang mục OTP trong tài khoản để thực hiện giao dịch.)
- Mức phí dịch vụ thấp.
- Phổ biến trong nhiều hình thức xác minh chủ thể như giao dịch ngân hàng, tạo tài khoản mạng xã hội, tạo tài khoản email…
- Tốc độ gửi SMS OTP nhanh (từ 5-10s/SMS).
- Ưu điểm lớn nhất chính là khả năng bổ sung thêm lớp bảo mật cho tài khoản thanh toán.

Nhược điểm:

- Người dùng không thể sử dụng được ở nơi không có sóng di động hoặc di chuyển ra nước ngoài

2) Token Key – Tokey Card

Hiện này thì Token có hai loại: hard token và soft token :

- Hard token: Là một máy cầm tay dạng như USB để bạn mang theo và sử dụng khi cần.

- Soft token: Là các phần mềm được tích hợp vào máy tính hoặc điện thoại của người sử dụng để cung cấp mã số khi cần thiết.

Token là một thiết bị điện tử mà chủ tài khoản được cấp khi mở tài khoản thanh toán tại Ngân hang, có thể tự động sinh ra mã OTP mà không cần đến kết nối mạng.

Bạn muốn sử dụng hình thức này sẽ phải trả thêm phí làm máy Token.

Một số ngân hàng áp dụng hình thức bảo mật Token như ACB, HSBC, Sacombank,…

Mỗi tài khoản cần đăng ký Tokey Key riêng cho mỗi tài khoản, và sau một thời gian quy định thì ngân hàng sẽ đổi Tokey Key của bạn.

Ưu điểm:

- Máy Token là một thiết bị rời có kích thước khá là nhỏ gọn, giúp bạn dễ dàng mang theo bên người cũng như dễ dàng cho vào chùm chìa khóa cá nhân.
- Giúp bảo vệ các giao dịch của khách hàng, Tránh bị kẻ gian hack thông tin cũng như sử dụng những thông tin để thực hiện giao dịch.
- Nếu chẳng may bị lộ mã OTP đã sử dụng thì khách hàng cũng không cần quá lo lằng bởi mã đó chỉ có hiệu lực duy nhất một lần.
- Các sử dụng thiết bị Token khá là đơn giản phù hợp cho rất nhiều đối tượng.

Nhược điểm:

- Để sử dụng, bạn bỏ ra chi phí mua máy Token từ 200.000-400.000đ.

- Mã Token thường chỉ có hiệu lực trong 60 giây.

- Bắt buộc phải có máy Token thì bạn mới có thể giao dịch được.

- Đây là một thiết bị rời , nhỏ gọn cho nên luôn luôn mang theo bên mình. Tuy nhiên cần bảo quản cẩn thận vì nó dễ bị mất

3) Smart OTP – Smart Token

Smart OTP là đang nói đến một ứng dụng tạo mã OTP có thể cài trên điện thoại/máy tính bảng có hệ điều hành Android hay iOS.

Sau khi đăng kí tài khoản trên ứng dụng và kích hoạt thành công thì ứng dụng này cũng sẽ hoạt động tương tự như Token.

Smart OTP là phương thức xác thực sử dụng công nghệ tiên tiến, bảo mật, thuận tiện cho Doanh nghiệp khi sử dụng các tiện ích của F@st EBank. Nó được coi là hình thức kết hợp hoàn hảo giữa SMS OTP và Token Key. Smart OTP sẽ được gửi về ứng dụng khi xuất hiện yêu cầu giao dịch.

Tại Việt Nam các ngân hàng: Vietcombank và TPBank đang sử dụng hình thức xác thực bằng Smart OTP hoạt động song song SMS OTP.

Để sử dụng Smart OTP người dùng cần phải đăng ký với ngân hàng hoặc các nhà cung cấp dịch vụ. Đặc biệt nên nhớ không thể có nhiều thiết bị sử dụng chung một ứng dụng tạo ra mã OTP.

Ưu điểm:

- Ứng dụng cung cấp mã OTP nên khách hàng sẽ chủ động lấy khi có nhu cầu giao dịch điện tử.
- Được sinh ra ngay trên điện thoại của khách hàng và được mã hóa với hệ thống bảo vệ nhiều lớp phức tạp và khó có thể can thiệp được.
- Thiết bị di động cài đặt Smart OTP cũng không yêu cầu phải kết nối internet hay kết nối mạng viễn thông sau khi đã kích hoạt. (Khách hàng không phải roaming khi đi nước ngoài như nhận OTP qua SMS).
- Là giải pháp có mức độ bảo mật cao nhất hiện nay (so với nhận OTP qua SMS/email truyền thống).
- Chủ động lấy OTP bằng việc nhập mã PIN 4 số của Smart OTP
- Mã OTP sẽ tự động hiển thị vào ô xác thực giao dịch sau khi điền mã PIN (để đăng nhập phần mềm Smart OTP) thành công. Vì thế, quý khách tuyệt đối không chia sẻ mã PIN đăng nhập Smart OTP cho bất kỳ ai, bao gồm người "tự xưng" là nhân viên ngân hàng hay cơ quan chức năng.

Nhược điểm:

- Để sử dụng Smart OTP người dùng cần phải đăng ký với ngân hang hoặc các nhà đăng ký dịch vụ. Ngoài ra , không thể có nhiều thiết bị sử dụng chung một ứng dụng tạo mã OTP

Câu 9: Đưa ra một hệ thống mà bạn biết có sử dụng mật khẩu cố định (fixed password) và mô tả các bước thực hiện để bạn có thể được chứng thực người dùng trong hệ thống đó. Nêu mục tiêu của việc chứng thực này.

Hệ thống có sử dụng mật khẩu cố định (fixed password)

- Teamviewer

Các bước thực hiện

Bước 1:

Tại giao diện trên Teamviewer, người dùng nhấn chọn vào mục Extras bên trên rồi chọn tiếp Options.

Bước 2:

Chuyển sang giao diện mới nhấn vào mục quản lý Security ở góc bên trái màn hình. Nhìn sang bên phải phần Personal password (For unattended access), hãy nhập mật khẩu muốn đặt cho Teamviewer vào. Nhấn OK để lưu lại mật khẩu là xong.

Ngoài ra trong phần Random password người dùng cũng có thể điều chỉnh độ dài mật khẩu từ 4 ký tự sang 6, 8, 10 ký tự. Disabled để vô hiệu hóa mật khẩu khi cần kết nối 2 máy tính.

Bây giờ, bạn sẽ sử dụng mật khẩu mình vừa tạo để tạo kết nối cho người khác. Cách này rất tiện nếu bạn thường xuyên nhờ một người, họ sẽ ghi nhớ ID và mật khẩu cho lần trợ giúp tiếp theo mà không cần hỏi lại mật khẩu đăng nhập. Tuy nhiên, nếu để kẻ gian phát hiện và lợi dụng, đây sẽ là mối nguy hiểm lớn cho tài khoản của người dùng. Vì vậy, hãy cân nhắc thật kỹ trước khi tiến hành sử dụng, bởi mỗi mật khẩu đều có những ưu - nhược điểm riêng.

* Mục tiêu của chứng thực

- Tăng cường an toàn cho hệ xác thực dựa trên mật khẩu

- Xây dựng giao thức an toàn

- Đảm bảo nội dung thông tin trao đổi giữa các thực thể là chính xác không bị thêm, sửa, xóa hay phát lại (đảm bảo tính toàn vẹn về nội dung)

- Đảm bảo đối tượng tạo ra thông tin (nguồn gốc thông tin) đúng là đối tượng hợp lệ đã được khai báo (đảm bảo tính toàn vẹn về nguồn gốc thông tin)

- Đảm bảo an toàn đối với thông tin xác thực (tên đặng nhập và mật khẩu không được truyền đi trực tiếp trên mạng)

- Xác thực ai đang giao dịch

- Đảm bảo bảo mật thông tin (không thẩm quyền => không đọc được)

- Đảm bảo tính toàn vẹn

- Chống thoái thoát

- Sử dụng thay cho bản chính trong các giấy tờ

- Chứng minh người yêu cầu chứng thực đã ký chữ ký đó và là căn cứ để xác định trách nhiệm của người ký giấy tờ, văn bản.

- Chứng minh về thời gian, địa điểm các bên đã ký kết hợp đồng, giao dịch; năng lực hành vi dân sự, ý chí tự nguyện, chữ ký hoặc dấu điểm chỉ của các bên tham gia hợp đồng, giao dịch.

Câu 10: Đưa ra một hệ thống mà bạn biết có sử dụng mật khẩu dùng một lần (one time password) và mô tả tình huống mà bạn có sử dụng mật khẩu để chứng thực người dùng/giao dịch. Nêu mục tiêu của việc chứng thực này.

Câu 11: Sinh trắc học (biometric) là gì? Nêu các lĩnh vực mà có thể áp dụng sinh trắc học?

Câu 12: Nêu ưu điểm và nhược điểm của việc áp dụng chứng thực bằng sinh trắc học.

Câu 13. Hệ thống quản lí an toàn thông tin là gì ? Mục tiêu của hệ thông an toàn thông tin?

- Khái niệm

-ISMS là từ viết tắt của information security management system. Đây là hệ thống quản lí an ninh thông tin, là khái niệm được sử dụng nhiều trong những Doang Nghiệp công nghệ thông tin và những đơn vị có ứng dụng hệ thống CNTT vào quản lí sản xuất

-Hệ thống quản lí an toàn thông tin là một phần của hệ thống quản lí toàn diện, dựa trên các rủi ro có thể xuất hiện trong doang nghiệp để xây dựng, điều hành, triển khai, soát xét, duy trì và cải tiến thông tin.

- Mục tiêu

Gồm 3 mục tiêu chính:

-Confidentiality: Đảm bảo tính bí mật của thông tin, tức là thông tin chỉ được phép truy cập (đọc) bởi những đối tượng (người, chương trình máy tính…) được cấp phép.

Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng. Sau đây là một số cách thức như vậy:

+Khóa kín và niêm phong thiết bị.

+Yêu cầu đối tượng cung cấp credential, ví dụ, cặp username + password hay đặc điểm về sinh trắc để xác thực.

+Sử dụng firewall hoặc ACL trên router để ngăn chặn truy cập trái phép.

+Mã hóa thông tin sử dụng các giao thức và thuật toán mạnh như SSL/TLS, AES, v.v..

-Integrity: Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi. Về điểm này, nhiều người thường hay nghĩ tính "integrity" đơn giản chỉ là đảm bảo thông tin không bị thay đổi (modify) là chưa đầy đủ.

Ngoài ra, một giải pháp "data integrity" có thể bao gồm thêm việc xác thực nguồn gốc của thông tin này (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy và ta gọi đó là tính "authenticity" của thông tin.

Sau đây là một số trường hợp tính "integrity" của thông tin bị phá vỡ:

+Thay đổi giao diện trang chủ của một website.

+Chặn đứng và thay đổi gói tin được gửi qua mạng.

+Chỉnh sửa trái phép các file được lưu trữ trên máy tính.

+Do có sự cố trên đường truyền mà tín hiệu bị nhiễu hoặc suy hao dẫn đến thông tin bị sai lệch.

-Availability: Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn. Ví dụ, nếu một server chỉ bị ngưng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng của nó là 99,999%.

Ví dụ sau cho thấy hacker có thể cản trở tính sẵn sàng của hệ thống như thế nào: Máy của hacker sẽ gửi hàng loạt các gói tin có các MAC nguồn giả tạo đến switch làm bộ nhớ lưu trữ MAC address table của switch nhanh chóng bị đầy khiến switch không thể hoạt động bình thường được nữa. Đây cũng thuộc hình thức tấn công từ chối dịch vụ (DoS).

Để tăng khả năng chống trọi với các cuộc tấn công cũng như duy trì độ sẵn sàng của hệ thống ta có thể áp dụng một số kỹ thuật như: Load Balancing, Clustering, Redudancy, Failover…

Như vậy, vấn đề bảo mật thông tin không chỉ đơn thuần là việc chống lại các cuộc tấn công từ hacker, ngăn chặn malware để đảm bảo thông tin không bị phá hủy hoặc bị tiết lộ ra ngoài… Hiểu rõ 3 mục tiêu của bảo mật ở trên là bước căn bản đầu tiên trong quá trình xây dựng một hệ thống thông tin an toàn nhất có thể. Ba mục tiêu này còn được gọi là tam giác bảo mật C-I-A**.**

TÌNH HUỐNG

Tình huống 1:

Để phục vụ cho nhu cầu học tập và tra cứu của cán bộ, giảng viên và sinh viên của trường, nhà trường đã xây dựng một hệ thống thư viện trực tuyến ***www.thuviendientu.iuh.edu.vn***, hệ thống giúp độc giả (cán bộ, giảng viên và sinh viên của trường) có thể tìm kiếm các loại sách, báo, tạp chí,… Đối với tài liệu điện tử thì độc giả có thể đọc trực tuyến hoặc tải về, đối với sách trong thư viện thì độc giả có thể đăng ký mượn. Độc giả cũng có thể yêu cầu mua các loại tài liệu điện tử và thanh toán phí mua trực tuyến. Hệ thống cũng giúp cho các thủ thư có thể quản lý thông tin mượn và trả sách của độc giả, hệ thống còn có tính năng thông báo nhắc nhở đến hạn trả sách bằng email, tạo báo cáo, thống kê.

Yêu cầu: Với tình huống đã cho, bạn hãy

1. Chỉ ra ít nhất 2 loại thông tin/dữ liệu/chức năng nào cần nâng cao tính an toàn và nêu lý do tại sao?

2. Đưa ra giải pháp nào (chữ ký số, xác thực và điều khiểu truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngơi,…)) để cài đặt nâng cao tính an toàn cho từng loại thông tin/dữ liệu/chức năng ở trên và nêu lý do tại sao phương pháp pháp này là hữu hiệu nhất.

Tình huống 2:

Để phục vụ nhu cầu học tập và nghiên cứu của cán bộ, giảng viên và sinh viên của trường (gọi chung là độc giả), nhà trường đã trang bị một ***phòng đọc sách*** cho các độc giả. Phòng này có trang bị máy lạnh, bàn ghế, wifi, và 100 chiếc máy tính để bàn. Sinh viên có thể tự vào ra phòng đọc sách trong khoảng thời gian thư viện mở để ngồi đọc sách, học tập nghiên cứu và dùng các máy tính. Các máy tính chỉ dùng để học tập/nghiên cứu chứ không cho phép chơi game.

Yêu cầu:

1. Theo bạn để có thể kiểm soát, chứng thực và theo dõi sự vào ra phòng đọc sách của các độc giả một cách tự động thì chúng ta có thể dùng phương pháp nào (chữ ký số, xác thực và điều khiển truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngươi,…)) để kiểm soát và nêu lý do tại sao phương pháp này là hữu hiệu nhất?
2. Theo bạn để có thể chứng thức, kiểm soát và theo dõi việc sử dụng wifi và thiết bị máy móc ở phòng đọc sách thì chúng ta dùng những phương pháp nào (chữ ký số, xác thực và điều khiển truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngươi,…)) và nêu lý do tại sao phương pháp này là hữu hiệu
nhất?

- Thẻ từ là hữu hiệu nhất
+ Số lượng thẻ từ quản lý được cực kỳ lớn tương ứng số người quản lý. Chúng cực kỳ hợp ở môi trường có số người ra vào lớn, nhà trường đông sinh viên
+ Thông thường thời gian đọc thẻ chỉ diễn ra trong chưa đến 1s/ lượt quẹt thẻ. Tốc độ này nhanh hơn nhiều so với việc dùng vân tay hay khuôn mặt. Nhờ đó nếu như số người tập chung ra vào lớn trong cùng một thời điểm sẽ không phải xếp hàng chờ đợi lâu
+ Chỉ cần dùng thẻ để quẹt mỗi khi đến nơi làm việc hoặc vào ra. Những thẻ sử dụng hoàn toàn không bị ảnh hưởng do môi trường hay thời tiết. Đây là một trong những điểm hạn chế của công nghệ nhận diện vân tay
+ Mỗi thẻ có một ID riêng không trùng lặp nhau. Khi mất thẻ thì những thẻ này sẽ bị vô hiệu quá lập tức nên không cần lo lắng nếu kẻ xấu nhặt được
- Camera :
+ Quản lý quyền truy cập và sử dụng phần mềm
+ Quản lý toàn bộ thông tin sinh viên

+ Theo dõi các thời gian của sinh viên nhanh chóng

- Sinh trắc học:

Tăng hiệu quả bằng cách loại bỏ các lỗi hệ thống.

Tăng cường trách nhiệm của sinh viên

Cung cấp khả năng đồng hóa hạng nhất.

Cho phép xác thực đa yếu tố bằng giọng nói cũng như nhận dạng khuôn mặt.

Xác minh đa phương thức với nhiều thông tin tuyển sinh.

Tình huống 3:

Giả sử khoa Kế toán của trường IUH trang bị một 'Phòng mô phỏng và thực hành quy trình nghiệp vụ Kế toán – Tài chính – Tín dụng' (gồm 30 máy tính) dùng để phục vụ cho việc học tập và nghiên cứu của các thành viên trong câu lạc bộ Kế_Tài_Ngân_Club. Phòng máy này gồm một máy chủ (server), nhiều máy trạm (work station) và một máy in (printer) được cài đặt các phần mềm về kế toán, tài chính & ngân hàng để cho các thành viên trong câu lạc bộ vào sử dụng để nghiên cứu và học tập. Khoa mong muốn phòng máy được cài đặt và cấu hình làm sao mà các thành viên có thể ra vào và sử dụng cái tài nguyên một cách thuận tiện nhưng vẫn có cơ chế theo dõi một cách tự động.

1. Theo bạn, phòng máy nên dùng phương pháp nào (chữ ký số, xác thực và điều khiển truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngươi,…)) mà các thành viên có thể vào ra một cách thuận tiện nhưng vẫn kiểm soát được khi cần thiết. Bạn hãy mô tả giải pháp một cách chi tiết nhất và nêu lý do tại sao đây là giải pháp hợp lý nhất.

- Theo em phòng máy nên dùng phương pháp sinh trắc học vân tay để các thành viên có thể ra vào một cách thuận tiện nhưng vẫn kiểm soát được khi cần thiết .

Nguyên lý hoạt động của giải pháp ứng dụng công nghệ tĩnh mạch ngón tay:

Ánh sáng hồng ngoại chiếu xuyên qua ngón tay, hồng huyết cầu hấp thu ánh sáng này, camera chụp lại cấu trúc mạng tĩnh mạch và số hóa nó, lưu lại và so sánh với mã hồ sơ định danh đã lưu trên hệ thống để nhận diện.

Với nguyên lý trên, công nghệ này có tính bảo mật và độ chính xác cao nhất trong bảo mật xác thực danh tính hiện nay. Một so sánh cụ thể, phương pháp xác thực định danh qua tĩnh mạch có chỉ số FAR, False Acceptance Rate: tỷ lệ nhận diện sai cỡ < 0,0001%, FR, False Rejection Rate: tỷ lệ từ

chối sai cỡ 0.01% trong khi đó, phương pháp phổ biến hiện nay, nhận diện qua vân tay có chỉ số FAR cỡ 3~4%.

Công nghệ tĩnh mạch ngón tay đạt yêu cầu chống giả mạo, nhờ phương pháp sinh trắc học vô hình dưới những điều kiện đặc biệt. Nó đảm bảo các mạch máu sống hiện hữu, mà nhờ đó ngăn cản sự giả mạo. Các kiểu dạng mạch máu tĩnh mạch rất rõ ràng và đặc trưng, đã giải thích chính xác cho độ chính xác cao của giải pháp. Các nghiên cứu ghi nhận có sự khác biệt rất lớn giữa các mẫu hình về kiểu loại tĩnh mạch, làm cơ sở cho sự duy nhất và không trùng lặp của tĩnh mạch. Thêm vào đó kiểu dạng tĩnh mạch không thay đổi trong suốt thời gian sống kể từ khi con người trưởng thành.

2. Theo bạn, để có thể kiểm soát việc sử dụng thiết bị, ứng dụng được cài đặt trong phòng mô phỏng chúng ta thể dùng phương pháp nào (chữ ký số, xác thực và điều khiển truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, con ngơi,…)) và nêu lý do tại sao đây là giải pháp hợp lý nhất?

- Để có thể kiểm soát việc sử dụng tiết bị, ứng dụng được cài đặt trong phòng mô phỏng chúng ta có thể dùng phương pháp xác thực và điều khiển truy cập bằng mật khẩu.
- Đây là giải pháp hợp lí nhất vì Điều khiển truy nhập là quá trình mà trong đó người dùng được nhận dạng và trao quyền truy nhập đến các thông tin, các hệ thống và tài nguyên. Điều khiển truy cập tạo nên khả năng cho chúng ta có thể cấp phép hoặc từ chối một chủ thể - một thực thể chủ động, chẳng hạn như một người hay một quy trình nào đó - sử dụng một đối tượng - một thực thể thụ động, chẳng hạn như một hệ thống, một tập tin - nào đó trong hệ thống.