BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 1455/BTTTT-UDCNTT	*Hà Nội, ngày 21 tháng 5 năm 2013*
V/v lựa chọn hình thức xác thực điện tử người sử dụng dịch vụ công trực tuyến	

SỞ THÔNG TIN VÀ TRUYỀN THÔNG
ĐẾN Số:.....
Ngày: 28/5/2013
Chuyển:.....
Lưu hồ sơ số:.....

Kính gửi:

- Đơn vị chuyên trách về công nghệ thông tin của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương.

Xác thực điện tử là một công nghệ đảm bảo an toàn thông tin cho giao dịch điện tử cần thiết để triển khai Nghị định 43/2011/NĐ-CP của Chính phủ ngày 13/6/2011 về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang/cổng thông tin điện tử của cơ quan nhà nước và Quyết định 1605/QĐ-TTg của Thủ tướng Chính phủ ngày 27/8/2010 phê duyệt Chương trình quốc gia về ứng dụng CNTT trong hoạt động của cơ quan nhà nước giai đoạn 2011 - 2015.

Thực hiện Chỉ thị số 897/CT-TTg của Thủ tướng Chính phủ ngày 10/6/2011 về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số, với vai trò là cơ quan quản lý nhà nước chịu trách nhiệm phát triển hạ tầng công nghệ cho các hoạt động giao dịch điện tử, Bộ Thông tin và Truyền thông xây dựng Hướng dẫn lựa chọn hình thức xác thực điện tử người sử dụng dịch vụ công trực tuyến gửi kèm công văn này.

Trong quá trình thực hiện, nếu có ý kiến đóng góp hoặc kiến nghị, đề nghị gửi về Bộ Thông tin và Truyền thông (Cục Ứng dụng CNTT), 18 Nguyễn Du, Hà Nội.

Nơi nhận:
- Như trên;
- Bộ trưởng (để báo cáo);
- Thứ trưởng Nguyễn Minh Hồng (để báo cáo);
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Lưu: VT, UDCNTT.

TL. BỘ TRƯỞNG
CỤC TRƯỞNG CỤC ỨNG DỤNG CÔNG NGHỆ THÔNG TIN

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Phúc

HƯỚNG DẪN LỰA CHỌN CÁC HÌNH THỨC XÁC THỰC ĐIỆN TỬ NGƯỜI SỬ DỤNG DỊCH VỤ CÔNG TRỰC TUYẾN

(Ban hành kèm theo công văn số 1455/BTTTT-UDCNTT ngày 21 tháng 5 năm 2013 của Bộ Thông tin và Truyền thông)

Hướng dẫn này áp dụng cho các cơ quan, tổ chức cung cấp dịch vụ công trực tuyến trong việc lựa chọn các hình thức xác thực điện tử người sử dụng dịch vụ một cách phù hợp với yêu cầu đảm bảo an toàn thông tin của từng loại dịch vụ, qua đó giúp tiết kiệm thời gian triển khai và nâng cao hiệu quả đầu tư của các dự án triển khai dịch vụ công trực tuyến, giảm thiểu các rủi ro đối với các hệ thống cung cấp dịch vụ và tạo dựng niềm tin cho người sử dụng.

1. Các khái niệm cơ bản

Trong công văn này, các khái niệm dưới đây được hiểu như sau:

a. Dịch vụ công trực tuyến được hiểu theo định nghĩa tại Điều 3 Nghị định số 43/2011/NĐ-CP ngày 13/6/2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử của cơ quan nhà nước.

b. Người sử dụng dịch vụ công trực tuyến là các tổ chức, cá nhân trực tiếp sử dụng hoặc các đại lý được ủy quyền để giúp sử dụng dịch vụ công trực tuyến.

c. Xác thực điện tử

Xác thực điện tử (người sử dụng) là quy trình thiết lập sự tin tưởng đối với danh tính người dùng hiện diện điện tử trước một hệ thống thông tin.

Xác thực điện tử đa yếu tố là phương thức xác thực điện tử sử dụng kết hợp của hai hay nhiều yếu tố xác thực độc lập, đem lại phương án đảm bảo an toàn thông tin cao hơn.

d. Các mức đảm bảo độ tin cậy

Mức đảm bảo độ tin cậy (tiếng Anh là Assurance Level, sau đây gọi tắt là AS) của người sử dụng dịch vụ là mức độ hệ thống cung cấp dịch vụ yêu cầu đối với tính xác thực của người sử dụng dịch vụ. Mỗi dịch vụ công trực tuyến có thể yêu cầu mức AS khác nhau.

Xác minh thông tin đăng ký là một trong các yếu tố ảnh hưởng đến mức AS. Có 04 mức AS dành cho người sử dụng dịch vụ với hình thức xác minh thông tin dưới đây:

- Mức AS-1: Mức đảm bảo độ tin cậy thấp. Không yêu cầu xác minh thông tin đăng ký của người sử dụng dịch vụ.

- Mức AS-2: Mức đảm bảo độ tin cậy trung bình. Người sử dụng dịch vụ được phép đăng ký tài khoản qua mạng và tự cung cấp một số thông tin cơ bản như số chứng minh thư nhân dân, họ và tên, năm sinh,... Thông tin này không cần đối chiếu và xác thực.

- Mức AS-3: Mức đảm bảo độ tin cậy khá. Người sử dụng dịch vụ được phép đăng ký qua mạng và phải cung cấp một số thông tin cá nhân. Thông tin cung cấp sẽ được đối chiếu và xác minh (có thể được thực hiện qua bên thứ ba có thẩm quyền, hoặc qua đường bưu điện, SMS, hoặc bằng tài khoản ngân hàng được cung cấp,...). Sau đó, tài khoản hoặc thiết bị xác thực sẽ được cung cấp cho người sử dụng.

- Mức AS-4: Mức đảm bảo độ tin cậy cao. Người sử dụng dịch vụ đến nộp trực tiếp các thông tin được yêu cầu với các giấy tờ có công chứng để được cấp tài khoản, thiết bị xác thực hoặc làm các thủ tục nhận dạng sinh học (ví dụ như xác nhận vân tay, giọng nói,...). Sau khi thông tin được đối chiếu, thông tin nhận dạng cá nhân được xác nhận qua cơ quan có thẩm quyền, tài khoản hoặc thiết bị xác thực sẽ được cung cấp cho người sử dụng.

e. Các thuật ngữ được sử dụng

- Xác thực bằng danh tính/mật khẩu (ID/Password): Trong hình thức xác thực điện tử này, danh tính được sử dụng nhằm xác định tính duy nhất của người sử dụng dịch vụ trong giao dịch điện tử. Danh tính của người sử dụng dịch vụ được kết hợp với mật khẩu (được thể hiện dưới dạng chuỗi các ký tự bí mật được người sử dụng dịch vụ giữ) để sử dụng cho mỗi lần đăng nhập.

- Cơ chế xác thực qua nhiều kênh (out-of-band authentication): Mỗi lần xác thực, mật khẩu hay thông tin xác thực ngẫu nhiên được gửi qua một kênh an toàn khác như điện thoại, SMS, thư điện tử,... đến người sử dụng dịch vụ để yêu cầu xác thực.

- FIPS (Federal Information Processing Standards) là tập hợp các chuẩn được ban hành bởi Viện Tiêu chuẩn và Công nghệ quốc gia Mỹ (NIST) về xử lý tài liệu, thuật toán mã hóa và các chuẩn CNTT khác. Chuẩn này đã được đề cập trong Quyết định số 59/2008/QĐ-BTTTT ngày 31/12/2008 của Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.

FIPS 140-2 là chuẩn về các yêu cầu bảo mật cho các thành phần mã hóa, bao gồm nhiều khía cạnh như tài liệu đặc tả, cổng giao tiếp, vai trò, dịch vụ và xác thực, mô hình trạng thái, bảo mật vật lý, môi trường vận hành, quản lý khóa mã hóa, tương thích điện từ trường, khả năng tự kiểm tra, đảm bảo thiết kế và phát hiện tấn công. FIPS 140-2 định nghĩa bốn mức độ bảo mật 1, 2, 3 và 4. (Tham khảo tại Bảng 1 và Bảng 2 của tài liệu FIPS 140-2 Security Requirements for Crytographic Module).

- Mật khẩu đăng nhập một lần (One-time password hay OTP): Công nghệ tạo mật khẩu, thường chỉ có hiệu lực trong một thời điểm ngắn, được sử dụng một lần như thông tin xác thực.

- Thiết bị tạo mật khẩu sử dụng một lần đơn yếu tố (single-factor OTP device): Thiết bị này cho phép tạo ra mật khẩu là mã ngẫu nhiên và được sử dụng một lần để xác thực.

- Thiết bị tạo mật khẩu sử dụng một lần đa yếu tố (multi-factor OTP device): Thiết bị này cho phép tạo ra mật khẩu xác thực là mã ngẫu nhiên và được sử dụng như thiết bị tạo mật khẩu sử dụng một lần đơn yếu tố. Tuy nhiên, yêu cầu mỗi lần xác thực cần sử dụng yếu tố xác thực thứ hai như mật khẩu, vân tay,... để kích hoạt sử dụng. Thành phần mã hóa (bao gồm nhiều yêu cầu như: tài liệu đặc tả, cổng giao tiếp, vai trò, dịch vụ và xác thực,..) phải đạt chuẩn FIPS 140-2 mức 2 trở lên nhưng mức bảo mật vật lý phải đạt chuẩn FIPS 140-2 mức 3 trở lên.

- Thiết bị mã hóa bảo mật đa yếu tố (multi-factor cryptographic device) như PKI token: Thiết bị chứa khóa mật mã khi được kích hoạt phải yêu cầu yếu tố xác thực thứ hai như mật khẩu hoặc vân tay và không cho phép truy xuất khóa xác thực từ thành phần mã hóa. Thành phần mã hóa này phải đạt chuẩn FIPS 140-2 mức 2 trở lên nhưng mức bảo mật vật lý phải đạt chuẩn FIPS 140-2 mức 3 trở lên.

- CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart): là một kỹ thuật kiểm thử dạng hỏi/đáp được máy tính đưa ra để xác định xem câu trả lời có phải là con người tạo ra hay không (trước khi cấp quyền thực thi tác vụ).

2. Lựa chọn hình thức xác thực điện tử người sử dụng dịch vụ

Hình thức xác thực điện tử người sử dụng dịch vụ được xác định từ các mức độ dịch vụ công trực tuyến thông qua một khái niệm trung gian gọi là *mức đảm bảo độ tin cậy*.

Đối với dịch vụ công trực tuyến đơn giản (mức độ 1 đến 3), mức AS được quy định tường minh. Đối với các dạng dịch vụ công trực tuyến phức tạp (mức độ 4, cho phép thanh toán và trả kết quả trực tuyến), cơ quan, tổ chức cung cấp dịch vụ cần căn cứ vào đặc điểm của dịch vụ để xác định mức AS phù hợp theo phương pháp được trình bày tương ứng tại Phần 3.

Sau đó, sử dụng Bảng 3 tại Phần 4 để xác định các hình thức xác thực điện tử người sử dụng dịch vụ tương ứng với mức AS.

Yêu cầu tối thiểu về việc sử dụng các hình thức xác thực điện tử theo mức dịch vụ công trực tuyến từ 1 đến 4 được trình bày tại Phần 5 của Phụ lục này.

3. Hướng dẫn xác định mức AS

Đối với các dạng dịch vụ công trực tuyến phức tạp, việc tính toán mức AS của người sử dụng dịch vụ được tiến hành theo các bước sau:

a. Bước 1: Đánh giá rủi ro của hệ thống cung cấp dịch vụ

Các nguy cơ, rủi ro khi có lỗi xác thực xảy ra được phân loại như sau:

c. Bước 3: Tính mức AS phù hợp

Tổng hợp kết quả tham chiếu từ các nguy cơ, rủi ro khi xảy ra lỗi xác thực tương ứng với 6 loại tiêu chí có thể suy ra mức AS phù hợp dựa trên quy tắc sau:

Mức AS phù hợp bằng mức AS cao nhất trong số các mức AS tương ứng với các loại nguy cơ, rủi ro.

4. Lựa chọn hình thức xác thực điện tử dựa trên mức AS

Các hình thức xác thực điện tử đáp ứng các mức AS khác nhau. Mỗi mức AS tương ứng với một hay một số hình thức xác thực điện tử như sau:

Mức AS	Hình thức xác thực điện tử cho người sử dụng tương ứng
AS-1	Xác thực bằng danh tính/mật khẩu trong đó mật khẩu gồm ít nhất 06 ký tự.
AS-2	Sử dụng một trong số các hình thức xác thực điện tử sau: - Xác thực bằng danh tính/mật khẩu trong đó mật khẩu gồm ít nhất 08 ký tự và đạt yêu cầu về độ phức tạp (mật khẩu mạnh). - Cơ chế xác thực qua nhiều kênh. - Thiết bị tạo mật khẩu sử dụng một lần đơn yếu tố.
AS-3	Xác thực 2 yếu tố sử dụng kết hợp các cơ chế xác thực sau: danh tính/mật khẩu, cơ chế xác thực qua nhiều kênh, hoặc thiết bị tạo mật khẩu sử dụng một lần đơn yếu tố.
AS-4	Xác thực điện tử đa yếu tố có sử dụng một trong số các hình thức xác thực điện tử sau: - Thiết bị tạo mật khẩu sử dụng một lần đa yếu tố. - Thiết bị mã hóa bảo mật đa yếu tố, ví dụ thiết bị lưu trữ khóa bí mật để ký số.

Bảng 3: Đối chiếu mức AS và hình thức xác thực điện tử

5. Các bước lựa chọn các hình thức xác thực điện tử người sử dụng dịch vụ công trực tuyến

Các mức độ dịch vụ công trực tuyến có yêu cầu về mức AS đối với người sử dụng dịch vụ *tối thiểu* như sau:

a. Dịch vụ công trực tuyến mức độ 1 và 2

Do thông tin ở các dịch vụ công trực tuyến mức độ 1 và mức độ 2 thường được công bố rộng rãi cho mọi đối tượng nên không yêu cầu xác định danh tính của người truy cập.

- *Mức AS được yêu cầu tối thiểu*: Không.
- *Hình thức xác thực điện tử*: Không.

- *Khuyến cáo:* Tuy nhiên, nhằm phòng tránh tấn công dạng từ chối dịch vụ bằng cách kích hoạt yêu cầu tự động tải mẫu đơn hàng loạt, nhà cung cấp dịch vụ công trực tuyến mức độ 2 được khuyến cáo áp dụng kỹ thuật CAPTCHA với người sử dụng dịch vụ khi tải tệp tin từ máy chủ.

b. Dịch vụ công trực tuyến mức độ 3

Do người sử dụng dịch vụ có thể gửi hồ sơ qua mạng nên cần xác định chính xác danh tính của người gửi nhằm hạn chế giả mạo để nộp hồ sơ.

-Mức AS được yêu cầu tối thiểu: tối thiểu ở mức AS-2, tuy nhiên quy trình xác thực thông tin đăng ký phải đảm bảo ở mức AS-3 (thông tin danh tính cần xác thực bởi một tổ chức có thẩm quyền).

Nếu yêu cầu cao về tính chính xác và độ tin cậy về của danh tính của người sử dụng dịch vụ trong giao dịch, khuyến cáo sử dụng ít nhất ở mức AS-3. Nếu yêu cầu về tính toàn vẹn, chống chối bỏ của hồ sơ trong giao dịch, khuyến cáo áp dụng mức AS-4.

- *Hình thức xác thực điện tử:* Đơn vị triển khai dịch vụ công trực tuyến lựa chọn hình thức xác thực điện tử tương ứng với mức AS theo Bảng 3 tại Phần 4.

c. Dịch vụ công trực tuyến mức độ 4

- *Mức AS được yêu cầu tối thiểu*: Phụ thuộc vào đặc trưng riêng của từng dịch vụ công trực tuyến mức độ 4, đơn vị triển khai xác định mức AS phù hợp với dịch vụ công đang triển khai theo hướng dẫn tại Phần 3. Do dịch vụ công mức độ 4 yêu cầu trả kết quả trực tuyến, có nguy cơ rò rỉ thông tin, vì vậy mức AS không nhỏ hơn mức AS-2.

- *Hình thức xác thực điện tử*: Đơn vị triển khai dịch vụ công trực tuyến lựa chọn hình thức xác thực điện tử tương ứng với mức AS theo *Bảng 3* tại Phần 4.

6. Một số quy định khác

a. Kiểm tra thông số kỹ thuật của thiết bị xác thực cung cấp bởi bên thứ ba

Đối với thiết bị xác thực do bên thứ ba cung cấp, trước khi được cấp tài khoản sử dụng dịch vụ, người sử dụng cần cung cấp giấy tờ chứng minh thiết bị đáp ứng yêu cầu kỹ thuật.

b. Sử dụng một hình thức xác thực điện tử cho nhiều dịch vụ công trực tuyến

Người sử dụng dịch vụ có thể dùng một hình thức xác thực điện tử (ví dụ thiết bị xác thực) cho nhiều dịch vụ công trực tuyến nếu đáp ứng được mức AS yêu cầu cho dịch vụ đó.

c. Khai thác dịch vụ thông qua đại lý được ủy quyền

Khi không có điều kiện, người sử dụng dịch vụ có thể ủy quyền cho các đại lý khai thác dịch vụ được thành lập theo quy định của pháp luật.

Đại lý khi thay mặt người sử dụng dịch vụ phải gửi cho cơ quan, tổ chức cung cấp dịch vụ Giấy ủy quyền của người sử dụng cho phép đại diện khai thác dịch vụ công trực tuyến.

7. Ví dụ minh họa hướng dẫn

Phần này trình bày cách xác định hình thức xác thực điện tử của một số dịch vụ công trực tuyến cụ thể để minh họa cho hướng dẫn này:

Ví dụ 1: Dịch vụ hành chính công trực tuyến cho phép người dân và doanh nghiệp tải các mẫu biểu để phục vụ cho việc cấp giấy đăng ký kinh doanh. Đây là một dịch vụ công trực tuyến mức độ 2, căn cứ vào hướng dẫn tại Phần 5 có thể xác định:

- Mức AS: Không.

- Hình thức xác thực điện tử: Không, nhưng khuyến cáo sử dụng công nghệ CAPTCHA để giảm nguy cơ bị tấn công từ chối dịch vụ.

Ví dụ 2: Dịch vụ hành chính công trực tuyến cho phép ứng viên điền vào biểu mẫu trực tuyến để nộp hồ sơ đăng ký thi tuyển cán bộ, công chức, viên chức nhà nước. Đây là một dịch vụ công trực tuyến mức độ 3, căn cứ vào hướng dẫn tại Phần 5 có thể xác định:

- Mức AS: Do ứng viên có thể điền thông tin vào biểu mẫu điện tử có sẵn và gửi hồ sơ đăng ký trực tuyến, mức AS tối thiểu là AS-2. Để đảm bảo xác định chính xác danh tính, người nộp hồ sơ phải sử dụng tài khoản được cấp phát sau khi được xác minh thông tin.

- Hình thức xác thực điện tử: Căn cứ vào mức AS-2 được xác định ở trên, cơ quan, tổ chức cung cấp dịch vụ công trực tuyến theo hướng dẫn tại Bảng 3 sử dụng một trong số các hình thức xác thực điện tử cho người sử dụng dịch vụ sau: xác thực bằng danh tính/mật khẩu mạnh; cơ chế xác thực qua nhiều kênh; thiết bị tạo mật khẩu sử dụng một lần đơn yếu tố.

Ví dụ 3: Dịch vụ hành chính công trực tuyến tại địa phương cho phép người dân và doanh nghiệp đăng ký nhập khẩu vật liệu đặc biệt (ví dụ như như thuốc nổ), có trả lệ phí qua mạng và kết quả được trả lại trực tuyến. Đây là một dịch vụ công trực tuyến mức độ 4. Cơ quan, đơn vị triển khai dịch vụ xác định mức AS phù hợp theo hướng dẫn tại Phần 3.

- Bước 1: Đánh giá rủi ro của hệ thống cung cấp dịch vụ

Tham chiếu Bảng 1: *Mức độ của nguy cơ, rủi ro xảy ra khi có lỗi xác thực* để đánh giá, phân tích rủi ro của hệ thống cung cấp dịch vụ. Sai sót trong việc xác thực người sử dụng dịch vụ trong quá trình xin đăng ký nhập khẩu vật liệu đặc biệt dẫn đến các nguy cơ sau:

- *Nguy cơ, rủi ro cho uy tín của cá nhân, tổ chức* ở mức Trung bình do thường không gây hệ quả đặc biệt.

- *Nguy cơ, rủi ro về tài chính* ở mức Khá do đây là các vật liệu thường có giá trị và yêu cầu bảo quản đặc biệt.

- *Nguy cơ, rủi ro cho hoạt động, nghiệp vụ của cơ quan, tổ chức hoặc lợi ích xã hội* ở mức Khá do các vật liệu đặc biệt dùng cho các nghiệp vụ quan trọng.

- *Nguy cơ, rủi ro về rò rỉ thông tin* là Trung bình, không gây hệ quả lớn.

- *Nguy cơ, rủi ro dẫn đến mất an toàn cá nhân* ở mức Cao do các vật liệu đặc biệt có thể gây ảnh hưởng lớn đến an toàn cá nhân và xã hội.

- *Nguy cơ, rủi ro có tính chất tội phạm* ở mức Khá do việc nhầm lẫn đối tượng được nhập khẩu vật liệu đặc biệt có thể dẫn đến việc lợi dụng vì mục đích xấu, gây ra các vi phạm về dân sự hoặc hình sự, có thể phải áp dụng các biện pháp pháp luật.

- Bước 2: Tham chiếu các rủi ro với các mức AS

Sau khi đánh giá các mức độ rủi ro, sử dụng Bảng 2 để tham chiếu các rủi ro với mức đảm bảo độ tin cậy, cụ thể như sau:

Các nguy cơ, rủi ro xảy ra khi lỗi xác thực	**Các mức đảm bảo độ tin cậy**			
	AS-1	**AS-2**	**AS-3**	**AS-4**
Nguy cơ, rủi ro cho uy tín của cá nhân, tổ chức	Trung bình			↑
Nguy cơ, rủi ro về tài chính			Khá	⋮
Nguy cơ, rủi ro cho hoạt động, nghiệp vụ của cơ quan, tổ chức hoặc lợi ích xã hội			Khá	⋮
Nguy cơ, rủi ro về việc rò rỉ thông tin	Trung bình			⋮
Nguy cơ, rủi ro dẫn đến mất an toàn cá nhân	- - -	- - -	- - -	→ Cao
.Nguy cơ, rủi ro có tính chất tội phạm			Khá	

Bảng 4: Đánh giá rủi ro của dịch vụ đăng ký nhập khẩu vật liệu đặc biệt

- Bước 3: Tính mức AS phù hợp

Mức AS được tính bằng mức AS-4 cao nhất trong số AS-1, AS-3, AS-3, AS-1, AS-4, AS-3. Mức này đáp ứng yêu cầu không nhỏ hơn AS-2.

- Bước 4: Lựa chọn hình thức xác thực điện tử tương ứng phù hợp

Căn cứ vào mức AS-4 được xác định ở trên, đơn vị triển khai dịch vụ công trực tuyến lựa chọn hình thức xác thực điện tử người sử dụng dịch vụ dạng đa yếu tố có sử dụng thiết bị tạo mật khẩu sử dụng một lần đa yếu tố hoặc thiết bị mã hóa bảo mật đa yếu tố. Hiện nay, dịch vụ chứng thực chữ ký số công cộng đã được triển khai rộng rãi. Người dùng có thể sử dụng chữ ký số với khóa bí mật được lưu trong thiết bị bảo mật (token) có mã PIN bảo vệ để thực hiện mã hóa bảo mật.