|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN MÔN HỌC**

**BẢO MẬT THÔNG TIN**

**S/MIME EMAIL SECURITY**

Ngành: **CÔNG NGHỆ THÔNG TIN**

Sinh viên thực hiện : **NGUYỄN MAI TRƯỜNG PHÁT**

MSSV: 1811060560 Lớp: 18DTHB3

**PHẠM PHÚ LỢI**

MSSV: 1811061156 Lớp: 18DTHB3

**PHẠM PHI PHONG**

MSSV: 1811062517 Lớp: 18DTHB3

**Lời mở đầu**

Hiện nay, các cuộc tấn công lừa đảo đang gia tăng và hiện là nguyên nhân hàng đầu của các cuộc tấn công mạng. Một email đơn giản có thể tàn phá một công ty có quy mô bất kỳ bằng cách cung cấp cho hacker truy cập vào hệ thống của họ – bao gồm thông tin tài chính, thiết kế độc quyền, thông tin khách hàng và sao lưu dữ liệu – và cuối cùng, có thể khiến công ty đóng cửa vĩnh viễn.

Để giúp bảo mật thông tin liên lạc qua email của doanh nghiệp của họ, các công ty có thể xem xét các cách khác nhau mà họ có thể chọn để bảo mật email của mình – bộ lọc và plugin chống thư rác, Thư xác định khóa tên miền (DKIM), khung chính sách người gửi (SPF), mã hóa máy chủ email, v.v … Mặc dù sử dụng cách tiếp cận nhiều lớp là điều nên làm và cần thiết, sử dụng **chứng chỉ email S/MIME** là một trong những phương pháp quan trọng nhất.

Do chưa có nhiều kinh nghiệm nghiên cứu, thực hành nên đề tài thực hiện còn nhiều thiếu sót, chúng em mong nhận được đóng góp ý kiến của thầy để đề tài được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

Sinh viên thực hiện

**Nguyễn Mai Trường Phát**

**Phạm Phi Phong**

**Phạm Phú Lợi**

MỤC LỤC

Mục Lục

[CHƯƠNG 1. Tổng Quan Hệ Thống 4](#_Toc70421811)

[1.1. Tổng quan đề tài. 4](#_Toc70421812)

[1.1.1 Sỏ lược cách mã hóa email. 4](#_Toc70421813)

[1.1.1.1 Mã hóa kết nối. 5](#_Toc70421814)

[1.1.1.2. Mã hóa email gửi đi. 6](#_Toc70421815)

[1.1.1.3. Mã hóa email lưu trữ. 6](#_Toc70421816)

[1.1.1.4. Sơ lược về S/MIME 8](#_Toc70421817)

[1.2. Mục Tiêu. 9](#_Toc70421818)

[1.3. Cấu Trúc Đề Tài. 9](#_Toc70421819)

[CHƯƠNG 2. Cơ Sở Lý Thuyết. 11](#_Toc70421820)

[2.1 . S/MIME là gì? 11](#_Toc70421821)

[2.2 . Cấu trúc S/MIME. 11](#_Toc70421822)

[2.3 . Các thuật toán sử dụng trong S/MIME. 12](#_Toc70421823)

[2.4 . Chữ kí số. 12](#_Toc70421824)

[2.4.2 Không bác bỏ. 12](#_Toc70421825)

[2.4.3 Chuỗi tin cậy 13](#_Toc70421826)

[2.5 . Chức năng. 13](#_Toc70421827)

[2.6 . Hoạt động. 14](#_Toc70421828)

[CHƯƠNG 3. Kết Quả Thực Nghiệm. 17](#_Toc70421829)

[CHƯƠNG 4. Kết Luận. 17](#_Toc70421830)

[Trích dẫn tài liệu tham khảo. 17](#_Toc70421831)

# CHƯƠNG 1. Tổng Quan Hệ Thống

## Tổng quan đề tài.

### Sỏ lược cách mã hóa email.

Nếu không mã hóa, email của bạn có nguy cơ bị xâm nhập và đọc trộm bất cứ lúc nào, hoặc bạn có thể bị mất tài khoản. Bài viết này sẽ hướng dẫn tổng quát cách mã hóa email, giúp bạn hiểu và lựa chọn giải pháp mã hóa phù hợp.

Cho dù bạn chưa bao giờ gửi qua email những thông tin nhạy cảm - như thông tin tài khoản ngân hàng, bí mật kinh doanh - bạn cũng nên nghĩ đến việc sử dụng mã hóa. Bên cạnh việc "chặn bắt" nội dung email và các tập tin đính kèm, những kẻ lừa đảo còn có thể chiếm lấy toàn bộ tài khoản email nếu bạn không có cách bảo mật hợp lý.

Để bảo mật email của bạn hiệu quả, bạn nên mã hóa 3 thứ: đó là mã hóa kết nối từ nhà cung cấp dịch vụ email của bạn, mã hóa nội dung email gửi đi và mã hóa nội dung email được lưu trữ. Nếu bạn không mã hóa kết nối từ nhà cung cấp dịch vụ email đến máy tính của bạn hay thiết bị khác trong lúc kiểm tra hay gửi tin nhắn thì người dùng khác trong mạng của bạn có thể dễ dàng “chộp” tài khoản đăng nhập hay bất cứ nội dung bạn gửi hay nhận.

Điều nguy hiểm thường xảy ra khi bạn truy cập mạng nơi công cộng (chẳng hạn truy cập Wi-Fi ở quán cà phê), nhưng việc kết nối không mã hóa cũng có thể khiến bạn gặp vấn đề trong công việc hay khi dùng mạng riêng. Nội dung email vừa gửi của bạn có thể dễ bị xâm nhập khi chúng ở trên Internet, sau khi thông điệp vừa “rời khỏi” máy chủ của nhà cung cấp dịch vụ email. Kẻ xấu có thể chặn một thông điệp khi nó vừa chuyển từ máy chủ này sang máy chủ khác trên Internet.

Do đó, mã hóa nội dung trước khi gửi sẽ giúp kẻ gian không thể đọc được, kể từ thời điểm nội dung bắt đầu “dạo” trên Internet cho đến lúc đến tay người nhận để mở thông điệp. Nếu bạn lưu hay sao lưu email (từ một ứng dụng email như Microsoft Outlook) trên máy tính hay thiết bị của bạn, thì tin tặc cũng có thể “đánh hơi” để truy cập vào nội dung đó, ngay cả khi bạn đã đặt mật khẩu bảo vệ trên chương trình email và trên tài khoản Windows hay thiết bị di động. Một lần nữa, việc mã hóa khiến kẻ tấn công không thể đọc được nội dung email.

#### 1.1.1.1 Mã hóa kết nối.

Để bảo đảm việc kết nối giữa nhà cung cấp dịch vụ email với máy tính hay thiết bị khác, bạn cần cài đặt mã hóa giao thức SSL (Secure Socket Layer) và TLS (Transport Layer Security) – tương tự như cách thức bảo vệ mà bạn dùng khi kiểm tra tài khoản ngân hàng hay thực hiện giao dịch trực tuyến.

Nếu bạn kiểm tra email qua trình duyệt web (cho dù ở trên máy tính để bàn, máy tính xách tay, điện thoại thông minh hay máy tính bảng), cần mất một chút thời gian để chắc rằng việc mã hóa giao thức SSL/TLS được kích hoạt. Nếu thực hiện đúng, địa chỉ website sẽ bắt đầu bằng https thay vì là http. Tùy vào trình duyệt, bạn sẽ thấy một số dấu hiệu bổ sung, ví dụ như một thông báo bên cạnh thanh địa chỉ hay biểu tượng ổ khóa màu vàng trên thanh trạng thái ở phía dưới cùng của cửa sổ trình duyệt.

Nếu bạn không thấy địa chỉ https và những chỉ dấu khác sau khi đăng nhập vào chương trình email trên web, hãy gõ thêm một chữ s vào cuối của ‘http’ và nhấn Enter. Nếu nhà cung cấp dịch vụ email hỗ trợ giao thức SSL/TLS, cách này sẽ giúp mã hóa kết nối hiện tại của bạn. Sau đó, bạn duyệt thiết lập cài đặt tài khoản của mình để xem liệu có thể kích hoạt mã hóa theo mặc định, hoặc liệu có thể sửa bookmark hay tạo shortcut tới webmail dùng địa chỉ ‘https’. Nếu bạn không thể “ép” mã hóa, hãy kiểm tra nhà cung cấp dịch vụ email vì có thể họ không hỗ trợ giao thức SSL/TLS.

Nếu bạn dùng chương trình email như Microsoft Outlook để nhận email hay một ứng dụng email trên điện thoại thông minh, máy tính bảng, bạn nên cố gắng sử dụng mã hóa SSL/TLS.

Tuy nhiên, trong những tình huống như vậy, sẽ khó khăn hơn trong việc xác thực hay thiết lập mã hóa. Để thực hiện, hãy mở chương trình email hay ứng dụng và tìm tới menu thiết lập; tại đó, tài khoản của bạn được “dán nhãn” POP/SMTP, IMAP/SMTP, HTTP hay tài khoản Exchange. Tìm tùy chọn để kích hoạt mã hóa, thường nằm trong các thiết lập nâng cao nơi bạn có thể chỉ định số cổng (port) cho kết nối đến và đi.

Nếu bạn dùng tài khoản email Exchange cho công việc, bạn sẽ thấy mục dành cho thiết lập bảo mật, nơi bạn có thể thấy rõ liệu mã hóa/bảo mật có được kích hoạt cho các kết nối đến và đi cũng như cho tài khoản Exchange của bạn hay không. Nếu nó không được kích hoạt, kiểm tra nhà cung cấp dịch vụ email để xem họ có hỗ trợ mã hóa này và có thể tìm kiếm nhà cung cấp nào khác có hỗ trợ mã hóa SSL/TLS.

#### 1.1.1.2. Mã hóa email gửi đi.

Bạn có thể mã hóa nội dung email cá nhân trong suốt quá trình email di chuyển, nhưng cả bạn và người nhận phải thực hiện một số thao tác để tính bảo mật được bảo đảm. Bạn có thể dùng các tính năng mã hóa tích hợp trong dịch vụ email hay bạn có thể tải phần mềm mã hóa hay các ứng dụng phụ trợ sử dụng phương thức OpenPGP.

Trong trường hợp cấp thiết, bạn có thể sử dụng dịch vụ email mã hóa dựa trên web như [Sendinc](https://www.sendinc.com/) hay [JumbleMe](http://www.jumbleme.com/), mặc dù bạn phải ủy thác cho bên thứ 3. Hầu hết các phương thức mã hóa nội dung email, gồm S/MIME (Secure/Multipurpose Internet Mail Extensions) và OpenPGP, yêu cầu bạn cài đặt một chứng nhận bảo mật trên máy tính và cung cấp địa chỉ liên lạc của bạn qua một chuỗi ký tự, được gọi là khóa công khai trước khi bạn nhận được nội dung được mã hóa. Tương tự, người nhận mail của bạn cũng phải cài đặt chứng nhận bảo mật trên máy tính của họ và người nhận sẽ cung cấp cho bạn khóa công khai của họ trước.

Việc hỗ trợ chuẩn S/MIME được tích hợp sẵn trong nhiều trình email, trong đó có Microsoft Outlook. Ngoài ra, các tiện ích trên trình duyệt web, như Gmail S/MIME dành cho Firefox cũng hỗ trợ cho các nhà cung cấp dịch vụ email nền web.

Chuẩn mã hóa email OpenPGP có một vài biến thể, gồm PGP và GNU Privacy Guard (GnuPG). Bạn có thể tìm thấy các phần mềm miễn phí hay thương mại và ứng dụng phụ trợ (add-on), như [Gpg4win](https://www.gpg4win.org/), [PGP Desktop Email](https://www.symantec.com/desktop-email) để hỗ trợ cho mã hóa theo chuẩn OpenPGP.

#### 1.1.1.3. Mã hóa email lưu trữ.

Nếu bạn thích sử dụng trình email trên máy tính hay ứng dụng trên thiết bị di động hơn là qua trình duyệt web, bạn nên chắc rằng dữ liệu email được lưu trữ đã mã hóa để những kẻ tấn công trên mạng không thể truy cập vào nội dung email đã lưu, nếu bạn lỡ mất hay bị ai đó đánh cắp thiết bị.

Cách tốt nhất là mã hóa toàn bộ nội dung trên laptop hay thiết bị di động, bởi vì các thiết bị di động thường rơi vào trường hợp đặc biệt là bị mất hay đánh cắp. Đối với các thiết bị di động, tốt nhất là dùng hệ điều hành cung cấp đầy đủ mã hóa trên thiết bị bằng cách thiết lập mã PIN hay mật khẩu để bảo vệ email và dữ liệu khác của bạn.

Các thiết bị BlackBerry và iOS (như iPhone, iPad và iPod Touch) đã cung cấp loại mã hóa này trong nhiều năm qua; Android hỗ trợ chỉ phiên bản 3.0 hay cao hơn. Các thiết bị Android cũ hơn, có thể dùng ứng dụng email của bên thứ 3, như [TouchDown](http://www.nitrodesk.com/TouchDown.aspx) cung cấp mã hóa dành cho các tài khoản Exchange.

Đối với máy tính để bàn và máy tính xách tay, bạn có thể mã hóa tập tin dữ liệu email nếu bạn không muốn mã hóa toàn bộ nội dung trên máy tính. Các chức năng mã hóa của mỗi trình email lại khác nhau, do đó nên kiểm tra tài liệu hướng dẫn đối với mỗi chương trình và phiên bản cụ thể. Nếu trình email của bạn không cung cấp mã hóa đáng tin cậy, hãy chọn lựa mã hóa theo thư mục nơi email của bạn được lưu trữ.

Ví dụ, nếu bạn dùng phiên bản Professional, Business hay Ultimate của Windows, bạn có thể mã hóa nội dung email, không phụ thuộc vào chương trình email bạn dùng, nhờ vào tính năng Encrypted File System (EFS) tích hợp sẵn trong Windows. Trước hết, tìm các dạng tập tin mà trình email của bạn sử dụng để lưu trữ các nội dung email; Microsoft Outlook dùng tập tin .PST để lưu nội dung, hay tập tin .OST dành cho các tài khoản Exchange.

Một khi đã xác định nơi trình email của bạn lưu dữ liệu, nhấn phải vào tập tin hay thư mục chứa nội dung đó, chọn Properties, nhấn Advanced và chọn Encrypt để mã hóa. Đó là tất cả những điều bạn cần làm. Tính năng EFS sẽ giúp mở tập tin và giải mã tự động khi bạn đăng nhập vào tài khoản Windows.

Hãy nhớ vô hiệu hóa mã hóa trước khi cài đặt lại Windows hay thay đổi tài khoản Windows của bạn nếu không bạn sẽ có nguy cơ không thể giải mã được các tập tin sau đó.

#### 1.1.1.4. Sơ lược về S/MIME

Tiêu chuẩn Secure/Multipurpose Internet Mail Extensions (S/MIME) - Tiêu chuẩn an toàn mở rộng thư Internet đa mục đích cung cấp một phương thức gửi/nhận thông điệp thư Internet đa mục đích một cách an toàn do Nhóm chuyên trách kỹ thuật Internet (Internet Engineering Task Force - IETF) phát hành dưới dạng RFC (RFC - Request for Comments, là những tài liệu kỹ thuật và tổ chức về Internet, bao gồm những tài liệu đặc tả kỹ thuật và chính sách được tổ chức IETF phát hành). S/MIME là một tiêu chuẩn cho mã hóa khóa công khai (tham khảo trong Giải thuật mã hóa công khai RSA) và ký dữ liệu mở rộng thư Internet đa mục đích [MIME](http://aita.gov.vn/tin-tuc/1377/tieu-chuan-ky-thuat-ve-udcntt-trong-cqnn-tieu-chuan-mime-giao-thuc-mo-rong-thu-dien-tu-internet-da-muc-dich-6).

Trước khi công bố tiêu chuẩn S/MIME, các nhà quản trị chỉ sử dụng Giao thức truyền thư đơn giản [SMTP](http://aita.gov.vn/tin-tuc/1378/tieu-chuan-ky-thuat-ve-udcntt-trong-cqnn-tieu-chuan-smtp-giao-thuc-truyen-thu-don-gian-5) được chấp nhận rộng rãi, tuy nhiên, giao thức này không đảm bảo an toàn hoặc có đảm bảo an toàn nhưng phải sử dụng các giải pháp mang tính độc quyền. Do đó, các nhà quản trị lựa chọn một giải pháp nhằm tăng cường tính an toàn và đảm bảo kết nối, S/MIME ra đời đã hỗ trợ giao thức SMTP chuyển sang một cấp độ tiếp theo là cho phép kết nối thư điện tử phổ biến rộng rãi mà vẫn đảm bảo an toàn.

Các phiên bản S/MIME gồm:

* Phiên bản đầu tiên của S/MIME được các nhà cung cấp về an toàn bảo mật phát triển năm 1995, tuy nhiên phiên bản này không được công bố chính thức.
* Phiên bản thứ hai là S/MIME v2 được IETF chính thức công bố vào tháng 3/1998 là một tiêu chuẩn Internet tại [RFC 2311](http://www.ietf.org/rfc/rfc2311.txt) (Đặc tả kỹ thuật thông điệp S/MIME phiên bản 2) và [RFC 2312](http://www.ietf.org/rfc/rfc2312.txt) (Xử lý chứng thư S/MIME phiên bản 2). Các RFC này đưa ra một khung dựa trên tiêu chuẩn Internet mà các nhà cung cấp có thể tuân theo khi cung cấp các giải pháp an toàn thông điệp có khả năng tương tác. Kể từ đó, S/MIME đã trở thành một trong những tiêu chuẩn hàng đầu về bảo mật thông điệp.
* Phiên bản thứ ba là S/MIME v3 được IETF đề xuất vào tháng 6/1999 nhằm tăng cường khả năng của S/MIME, bao gồm [RFC 2632](http://www.ietf.org/rfc/rfc2632.txt) (Xử lý chứng thư S/MIME phiên bản 3), [RFC 2633](http://www.ietf.org/rfc/rfc2633.txt) (Đặc tả kỹ thuật thông điệp S/MIME phiên bản 3) và [RFC 2634](http://www.ietf.org/rfc/rfc2634.txt) (Các dịch vụ an toàn mở rộng cho S/MIME). Sau đó RFC 2633 đã được cập nhật thành [RFC 3851](http://tools.ietf.org/html/rfc3851) (Đặc tả kỹ thuật thông điệp S/MIME phiên bản 3.1) vào tháng 6/2004 và được cập nhật mới đây nhất tại [RFC 5751](http://tools.ietf.org/html/rfc5751) (Đặc tả kỹ thuật thông điệp S/MIME phiên bản 3.2) vào tháng 1/2010.

## Mục Tiêu.

Khi bạn gửi email thông qua các nền tảng email thông thường như Outlook, Gmail hoặc Yahoo, thông tin có thể được hiển thị cho những người biết cách để nhìn lén. Email được gửi đi thông qua một loạt các máy chủ và trên internet. Như vậy, chúng không an toàn nếu không có mã hóa hoặc các cơ chế bảo vệ khác. Điều này có nghĩa là email hoàn toàn có thể bị đọc bởi các tin tặc, khiến dữ liệu nhạy cảm của công ty (và khách hàng) của bạn gặp rủi ro. Điều này không chỉ mở ra cho công ty của bạn các chi phí tài chính và uy tín liên quan đến vi phạm dữ liệu, mà còn bị phạt theo quy định cắt cổ do không tuân thủ.

Vì vậy, **chứng chỉ kỹ thuật số cho mã hóa email** cho phép bạn mã hóa nội dung của email trước khi nó rời khỏi tài khoản email của bạn.

## Cấu Trúc Đề Tài.

**Chương 1: Tổng quan**

* *Tổng quan về vấn đề được nghiên cứu:* Tóm tắt những lý thuyết, tài liệu có liên quan đến đề tài “S/MIME EMAIL SECURITY”.
* *Mục tiêu:* Lý do hình thành đề tài
* *Cấu trúc đề tài:* Trình bày cấu trúc của đề tài gồm các chương và tóm tắt từng chương.

**Chương 2: Cơ sở lý thuyết**

Khái niệm, làm rõ vấn đề nghiên cứu,cấu trúc, cách thức hoạt động,….

**Chương 3: Kết quả thực nghiệm**

3.1. Kịch bản thực nghiệm

3.2. Yêu cầu thực nghiệm

3.3. Công cụ sử dụng

3.4. Các bước thực hiện

3.5. Kết luận

**Chương 4: Kết luận**

Những kết luận chung và hướng phát triển

**Trích dẫn tài liệu tham khảo**

# CHƯƠNG 2. Cơ Sở Lý Thuyết.

## . S/MIME là gì?

S/MIME, hoặc Bảo mật / Tiện ích mở rộng Internet Mail đa năng (Secure/Multipurpose Internet Mail), là một công nghệ cho phép bạn mã hóa email của mình. S/MIME dựa trên [mật mã bất đối xứng](https://ssl.vn/su-khac-biet-giua-ma-hoa-bat-doi-xung-va-ma-hoa-doi-xung.html) để bảo vệ email của bạn khỏi sự truy cập không mong muốn. Nó cũng cho phép bạn ký điện tử các email của bạn để xác minh bạn là người gửi thư hợp pháp, biến nó thành vũ khí hiệu quả chống lại nhiều cuộc tấn công lừa đảo ngoài kia.

Ngoài ra, S / MIME (Secure / Multipurpose Internet Mail Extension) là phiên bản nâng cao bảo mật của định dạng e-mail internet MIME, được thành lập dựa trên công nghệ bảo mật dữ liệu RSA. MIME đã thay thế giao thức SMTP vì nó bị giới hạn ở chỉ văn bản, nơi chỉ có tin nhắn văn bản được phép truyền. Giao thức bị hạn chế SMTP không thể trao đổi các tệp đa phương tiện, tài liệu ở các định dạng tùy ý khác nhau vì nó sử dụng biểu diễn ASCII 7-bit của các ký tự trong email mà không thể biểu thị các ký tự đặc biệt có giá trị lớn hơn 127.

Do đó, nhu cầu quan trọng về một tiêu chuẩn cũng có thể trao đổi các tệp đa phương tiện. Đó là cách các tính năng của hệ thống email chính được mở rộng thông qua MIME.

## . Cấu trúc S/MIME.

Một email MIME bao gồm một tin nhắn văn bản cùng với một số tiêu đề đặc biệt và các phần văn bản được định dạng. Mỗi phần có thể chứa một phần dữ liệu được mã hóa ASCII và cả cơ chế giải mã dữ liệu ở đầu bên nhận. Tiêu đề MIME bao gồm đặc điểm kỹ thuật của - Phiên bản MIME, Loại nội dung, Mã hóa chuyển nội dung, ID nội dung, Mô tả nội dung.

## . Các thuật toán sử dụng trong S/MIME.

* Tiêu chuẩn chữ ký số (DSS) cho chữ ký điện tử
* Diffie-Hellman để mã hóa các khóa phiên đối xứng.
* RSA cho chữ ký điện tử hoặc để mã hóa các khóa phiên đối xứng
* DES-3 để mã hóa khóa đối xứng

## . Mã hóa bật đối xứng.

Giống như SSL /TLS giao thức, S/MIME sử dụng mật khẩu hóa công khai để mã hóa và giải mã dữ liệu tin nhắn và chữ ký số. Khóa riêng được giữ an toàn, trong khi khóa chung có thể được phân phối rộng rãi. Một mối quan hệ toán học đặc biệt giữa hai khóa tồn tại sao cho dữ liệu được mã hóa bằng một khóa chỉ có thể được giải mã bởi khóa kia. Nếu một tin nhắn được mã hóa bằng khóa chung của bạn, chỉ có khóa riêng của bạn mới có thể giải mã nó và nếu một tin nhắn được ký bằng khóa riêng của bạn, ai đó có khóa chung của bạn có thể xác minh thực tế đó.

(Bạn có thể chia sẻ khóa công khai của mình một cách an toàn bởi vì, với kích thước khóa đủ lớn, thực tế không thể sử dụng nó để lấy khóa riêng tương ứng của nó.)

## . Chữ kí số.

Khi bạn ký một email với S/MIME chứng chỉ, phần mềm ứng dụng email của bạn tạo ra một [băm](https://www.ssl.com/vi/faqs/H%C3%A0m-b%C4%83m-m%E1%BA%ADt-m%C3%A3-l%C3%A0-g%C3%AC/) hoặc thông báo có độ dài cố định của thư, sau đó mã hóa thư bằng khóa cá nhân của bạn để tạo chữ ký điện tử đi kèm với email. Khi người nhận nhận được thư, phần mềm email của họ sử dụng khóa công khai của bạn (cũng được bao gồm trong thư) để xác minh rằng email thực sự do bạn gửi và nội dung của nó không bị thay đổi khi chuyển tiếp. Nếu ai đó, bằng cách nào đó, quản lý để chặn tin nhắn và thay đổi văn bản, hàm băm do người nhận tính toán sẽ không khớp với hàm băm trong chữ ký. Hơn nữa, vì bản thân chữ ký chỉ có thể được tạo bằng khóa cá nhân của bạn, nên trên thực tế, ai đó không có khóa sẽ không thể tạo một chữ ký mới, hợp lệ để khớp với nội dung đã thay đổi hoặc thành công trong việc gửi tin nhắn có mục đích là từ bạn.

### Không bác bỏ.

Vì tính xác thực và tính toàn vẹn của email được ký điện tử được đảm bảo, người nhận có thể chứng minh rằng một người cụ thể (hoặc ít nhất là một người sở hữu khóa riêng của họ) đã gửi một tin nhắn cụ thể. Ngược lại, rất khó để người gửi từ chối một cách chính đáng rằng họ đã gửi cùng một tin nhắn. Thuộc tính này của email được ký điện tử được gọi là không bác bỏvà tương tự như khái niệm với một bức thư hoặc tài liệu pháp lý mang chữ ký vật lý của một người bằng mực.

### Chuỗi tin cậy

Khi bạn yêu cầu một S/MIME chứng chỉ từ SSL.com, chúng tôi xác minh quyền kiểm soát của bạn đối với một địa chỉ email cụ thể và có thể (tùy thuộc vào loại chứng chỉ cụ thể được yêu cầu) thông tin nhận dạng bổ sung trước khi ký và gửi cho bạn. Chứng chỉ đã ký của bạn sau đó là một phần của chuỗi tín thác dẫn trở lại chứng chỉ gốc của SSL.com, được bao gồm trong tất cả các kho lưu trữ chứng chỉ gốc của hệ điều hành và trình duyệt web chính hiện nay. Sau khi cài đặt chứng chỉ và sử dụng nó để ký email, phần mềm của người nhận của bạn có thể xác minh rằng chứng chỉ của bạn đã được ký bởi tổ chức phát hành chứng chỉ (CA) mà nó hoàn toàn tin tưởng để cung cấp thông tin nhận dạng hợp lệ.

## . Chức năng.

S / MIME cung cấp các dịch vụ bảo mật mật mã sau cho các ứng dụng nhắn tin điện tử:

* Xác thực
* Tính toàn vẹn của thư
* Không thoái thác nguồn gốc (sử dụng chữ ký số )
* Quyền riêng tư
* Bảo mật dữ liệu (sử dụng mã hóa)

S / MIME chỉ định kiểu MIME application / pkcs7-mime (smime-type "wraed-data" ) để bao bọc dữ liệu (mã hóa) trong đó toàn bộ thực thể MIME (đã chuẩn bị) được bao bọc được mã hóa và đóng gói vào một đối tượng mà sau đó được chèn vào một thực thể MIME ứng dụng / pkcs7-mime.Wikipedia site:vi.nipponkaigi.net.

## . Hoạt động.

Tóm lại, **chứng chỉ email** S / MIME cho phép bạn:

* Mã hóa email của bạn để chỉ người nhận dự định của bạn có thể truy cập nội dung của tin nhắn.
* Ký điện tử vào email của bạn để người nhận có thể xác minh rằng trên thực tế, email đó được gửi bởi bạn chứ không phải là một kẻ lừa đảo giả như bạn.

Cách mà **chứng chỉ mã hóa email** hoạt động là sử dụng [mã hóa bất đối xứng](https://ssl.vn/su-khac-biet-giua-ma-hoa-bat-doi-xung-va-ma-hoa-doi-xung.html). Nó sử dụng khóa chung để mã hóa email và gửi nó để người nhận, người có khóa riêng phù hợp, có thể tự động giải mã toàn bộ tin nhắn (và mọi tệp đính kèm). Mã hóa bất đối xứng cũng là những gì đứng đằng sau giao thức SSL / TLS cũng như tiền điện tử.

Giả sử bạn cần gửi email cho đồng nghiệp về dữ liệu tài chính của công ty. Đây là một email về cách quá trình này hoạt động khi gửi email mà không có và với một **chứng chỉ email** :

|  |  |
| --- | --- |
| NẾU KHÔNG CÓ CHỨNG CHỈ EMAIL S / MIME ĐƯỢC CÀI ĐẶT | VỚI CHỨNG CHỈ EMAIL S / MIME ĐƯỢC CÀI ĐẶT |
| • Bạn tạo một email mới trong Outlook.  • Bạn phác thảo nội dung của email và đính kèm bảng tính Excel.  • Bạn nhấn vào Gửi Send Send để gửi email văn bản gốc từ Outlook.  • Email được gửi từ nền tảng email của bạn đến máy chủ email thông qua kênh không được mã hóa.  • Nội dung email (và tệp đính kèm bảng tính) được gửi từ máy chủ email đến internet.  • Dữ liệu email sau đó được gửi từ internet đến máy chủ email của người nhận.  • Người nhận nhận được một email chưa được ký, không được mã hóa từ bạn, một người gửi chưa được xác minh. Họ mở email và đọc tin nhắn văn bản gốc của nó và truy cập bảng tính Excel văn bản gốc của nó. | • Bạn tạo một email mới trong Outlook.  • Bạn phác thảo nội dung của email và đính kèm bảng tính Excel.  • Bạn nhấn vào Gửi Send Send để gửi email văn bản gốc từ Outlook.  • Trước khi tin nhắn rời khỏi Outlook, chứng chỉ email S / MIME sẽ tự động:  1. ký điện tử email để xác minh danh tính của bạn là người gửi.  2. mã hóa dữ liệu email văn bản bằng cách sử dụng mã hóa bất đối xứng (khóa công khai).  • Email an toàn, được mã hóa di chuyển từ nền tảng email của bạn đến máy chủ thông qua kênh không được mã hóa.  • Nội dung email được đính kèm và tệp đính kèm được gửi từ máy chủ email đến internet.  • Dữ liệu email sau đó được gửi từ internet đến máy chủ email của người nhận.  • Người nhận nhận được email được mã hóa, được ký điện tử để xác minh danh tính của bạn là người gửi.  • Khi họ mở email, khóa riêng sẽ tự động giải mã nội dung và tệp đính kèm email để họ có thể đọc nó trong bản rõ. |

Trong trường hợp đầu tiên thiếu **chứng chỉ mã hóa email**, người gửi gửi một bản rõ, email không được mã hóa đến người nhận thông qua một máy chủ không được mã hóa và internet. Điều này khiến tin nhắn và các tệp đính kèm của nó dễ bị chặn bởi các tin tặc, những người có thể đọc dữ liệu trên mạng và dịch nó sang bản rõ. Trong kịch bản thứ hai mà người gửi sử dụng chứng chỉ bảo mật email, người gửi viết một email văn bản gốc được mã hóa trước khi chuyển đến máy chủ không được mã hóa và internet. Điều này có nghĩa là ngay cả khi tin tặc quản lý để chặn tin nhắn, họ sẽ không thể giải mã dữ liệu vì họ sẽ không có khóa riêng. Ngay cả khi email đến tay người nhận, nó vẫn được mã hóa trong khi nó đang ngồi trên máy tính của họ. Quá trình mã hóa email này giúp bảo vệ dữ liệu của bạn cả khi nó ở trạng thái nghỉ và quá cảnh.

# CHƯƠNG 3. Kết Quả Thực Nghiệm.

## 3.1. Mã hóa và xác thực bằng S/MIME

* Các chức năng của MIME:
  + Enveloped data: mã hóa thư
  + Signed data: xác thực thư, có chuyển mã
  + Clear-signed data: xác thực không chuyển mã
  + Signed and enveloped data: mã hóa và xác thực đồng thời
* MIME\_Mã hóa nội dung thư:
  + Tạo khóa ngẫu nhiên tương ứng với thuật toán mã đối xứng được chọn
  + Mã hóa bằng khóa công khai của người nhận (RSA)
  + Mã hóa nội dung thư với khóa ngẫu nhiên vừa tạo
* MIME\_Xác thực:
  + Chọn một hàm băm tương ứng với khả năng của người nhận
  + Áp dụng hàm băm lên nội dung thư
  + Mã hóa hàm băm bằng khóa riêng (PR) của người gửi

## 3.2. Ứng dụng S/MIME

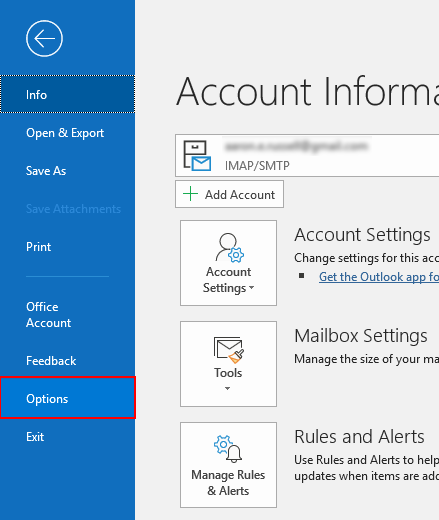
Những hướng dẫn này chi tiết cách cài đặt [S/MIME](https://www.ssl.com/vi/b%C3%A0i-vi%E1%BA%BFt-/g%E1%BB%ADi-email-an-to%C3%A0n-v%E1%BB%9Bi-sime/) chứng chỉ và gửi thư email an toàn với Microsoft Outlook trên PC chạy Windows. Thử nghiệm đã được thực hiện trong Outlook phiên bản 1902 trên Windows 10 Enterprise.

1. **Tải xuống chứng chỉ của bạn.**

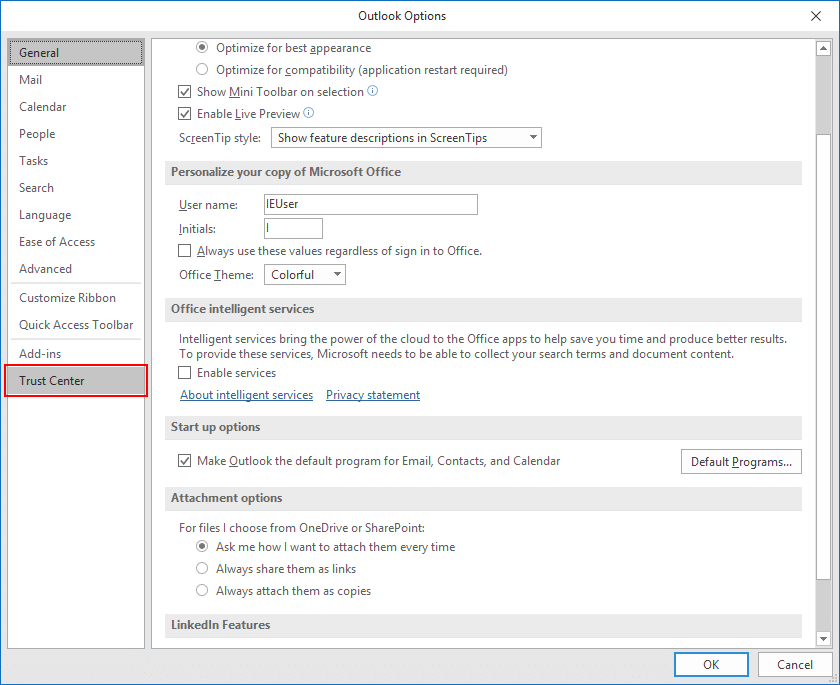
Tải xuống tệp PKCS # 12 cùng với chứng chỉ của bạn từ tài khoản SSL.com của bạn bằng cách nhấp vào liên kết được cung cấp trong email Liên kết kích hoạt chứng chỉ của bạn và làm theo hướng dẫn trên màn hình trong trình duyệt web của bạn. Bạn sẽ được nhắc tạo mật khẩu trước khi tải xuống tệp. (Giữ mật khẩu này an toàn - bạn sẽ cần nó sau này.) **Đảm bảo theo dõi nơi bạn đã lưu tệp PKCS # 12 của mình và không làm mất tệp đó.** Nếu bạn mất khóa riêng, bạn sẽ không thể đọc các tin nhắn được mã hóa bằng khóa chung của bạn.  
  
**Lưu ý:** khi tải xuống chứng chỉ của bạn, có thể chọn giữa các thuật toán RSA và ECDSA thông qua **Thuật toán** trình đơn thả xuống. Tuy nhiên, không thể sử dụng khóa ECDSA để mã hóa email, vì vậy tốt nhất bạn nên để bộ này thành **RSA**.

1. **Mở Tùy chọn Outlook.**

Trong Outlook, hãy chọn **Tập tin** từ menu chính, sau đó nhấp **Các lựa chọn**.

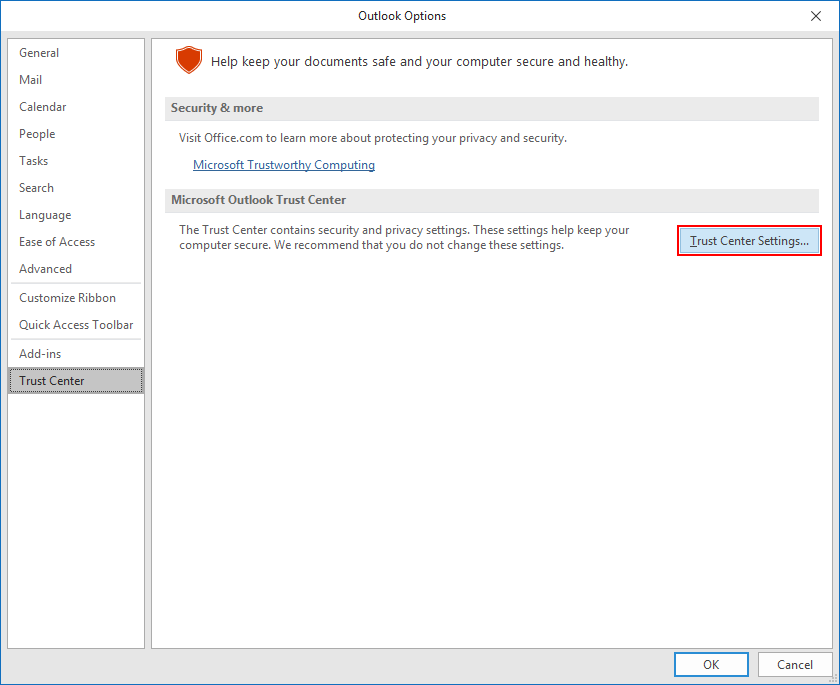
1. **Mở Trung tâm Tin cậy.** 

Chọn **Trung tâm tin tưởng** ở dưới cùng của menu ở bên trái của **Tùy chọn Outlook** cửa sổ.



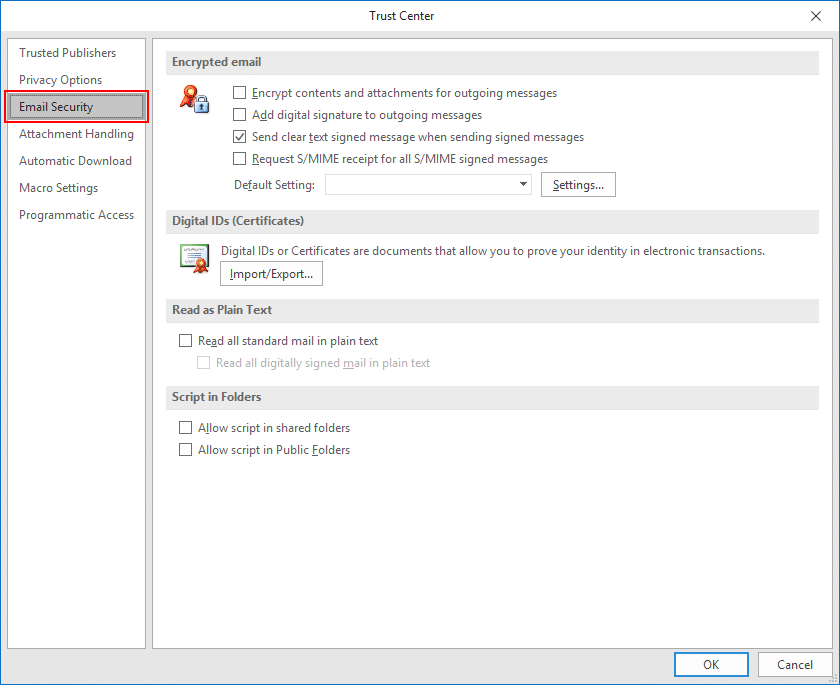
1. **Mở Cài đặt Trung tâm Tin cậy.**

Nhấn vào **Cài đặt Trung tâm Niềm tin** .



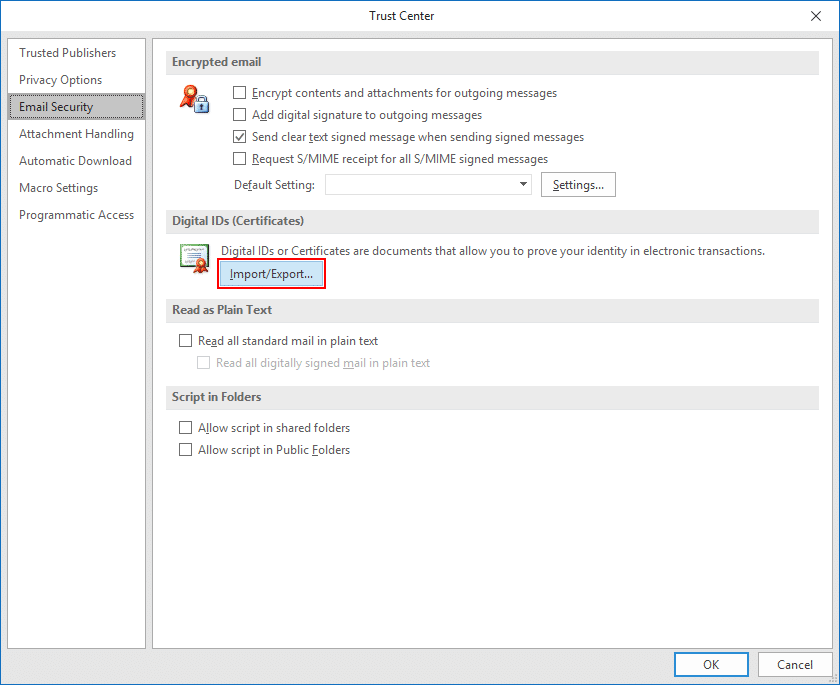
1. **Chọn Bảo mật Email.**

Chọn **Bảo mật Email** từ menu bên trái của **Trung tâm tin tưởng** cửa sổ.

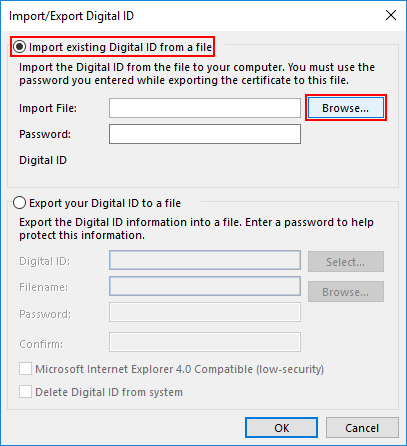


1. **Nhấp vào Nhập / Xuất.**

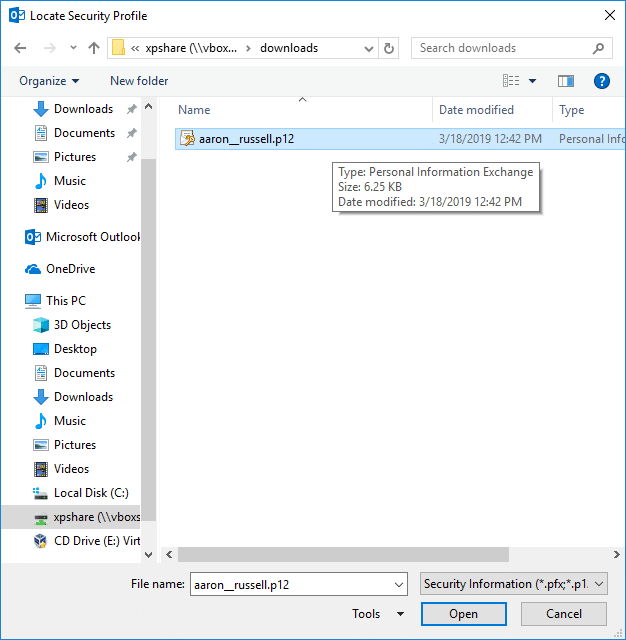
Nhấn vào **Import / Export** nút, dưới **ID kỹ thuật số (Chứng chỉ)**.



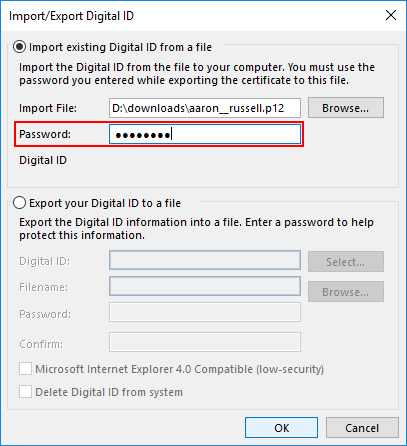
1. **Duyệt tìm tệp.**

Hãy chắc chắn **Nhập ID kỹ thuật số hiện có từ một tệp tin** được kiểm tra, sau đó nhấp **Duyệt qua ...**  


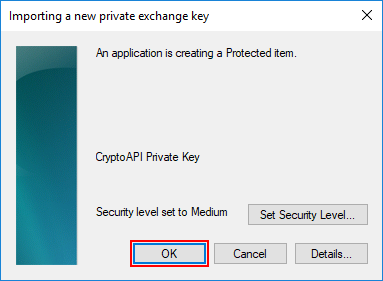
1. **Mở tệp.**

Điều hướng đến tệp PKCS # 12, sau đó nhấp vào **Mở**. Phần mở rộng tên tệp phải là .p12.  


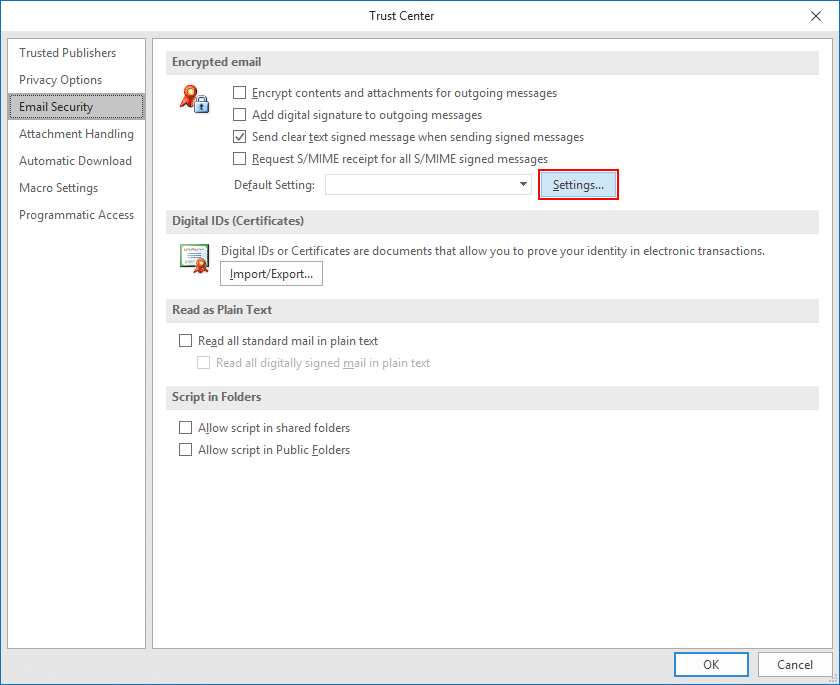
1. **Nhập mật khẩu PKCS # 12.**

Nhập mật khẩu bạn đã sử dụng khi tải xuống tệp PKCS # 12, sau đó nhấp vào **OK**.  


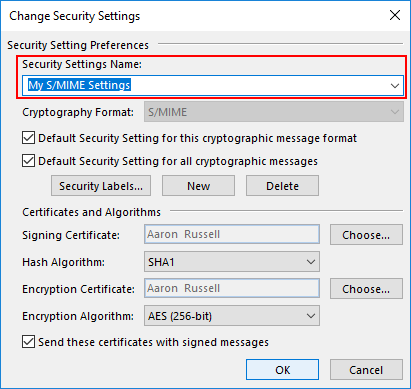
1. **Nhấp vào OK.**

Nhấp chuột **OK** trên hộp thoại bảo mật bật lên.  


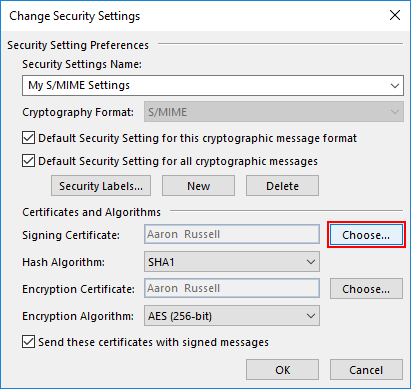
1. **Mở cài đặt email được mã hóa.**

Nhấn vào **Cài đặt** nút, dưới **Email được mã hóa**.  


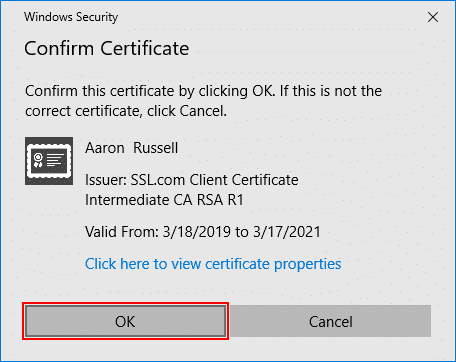
1. **Đặt tên cho cài đặt bảo mật.**

Nhập tên cho cài đặt bảo mật của bạn.  


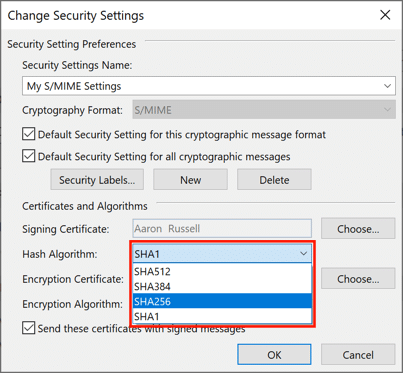
1. **Chọn chứng chỉ ký.**

Nhấp chuột **Chọn**, kế bên **Giấy chứng nhận ký**.  


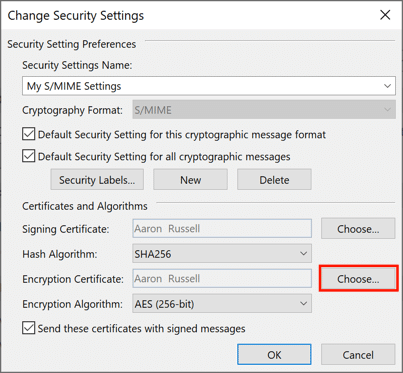
1. **Xác nhận hoặc chọn chứng chỉ.**

Nếu bạn chỉ cài đặt một chứng chỉ (như được hiển thị ở đây), bạn có thể nhấp vào **OK** trên **Xác nhận Giấy chứng nhận** hộp thoại bật lên. Nếu không, bạn sẽ phải chọn một trong danh sách các chứng chỉ đã cài đặt.  


1. **Đặt thuật toán băm.**

Đặt **Thuật toán băm** đến **SHA256.**  


1. **Chọn chứng chỉ mã hóa.**

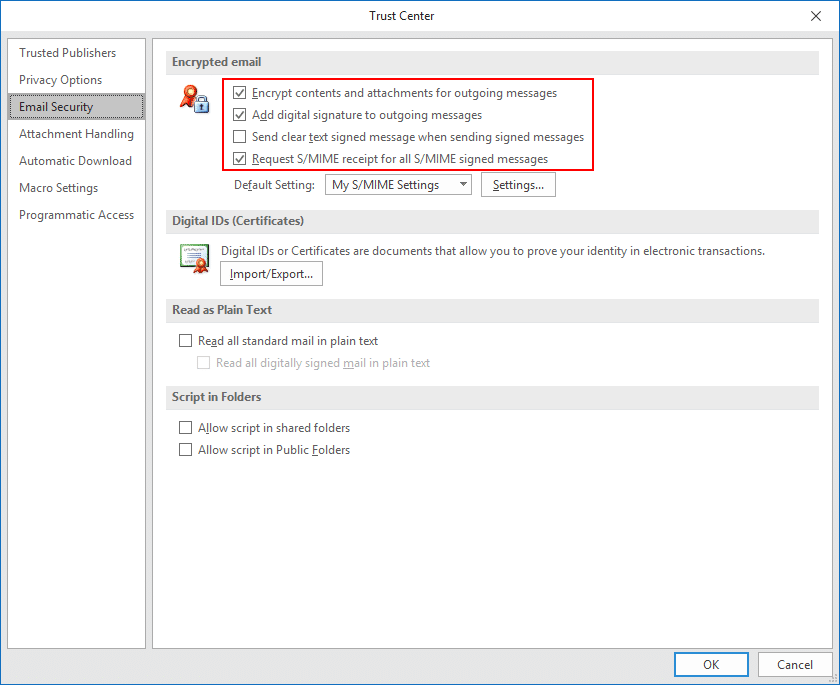
Nhấp chuột **Chọn**, kế bên **Chứng chỉ mã hóa**, Và nhấp vào **OK** trên **Xác nhận Giấy chứng nhận** hộp thoại. Một lần nữa, nếu bạn có nhiều chứng chỉ, hãy chọn cùng một chứng chỉ bạn đã chọn cho **Giấy chứng nhận ký**.  


1. **Đóng cửa sổ.**

Nhấp chuột **OK** để đóng **Thay đổi cài đặt bảo mật** cửa sổ.

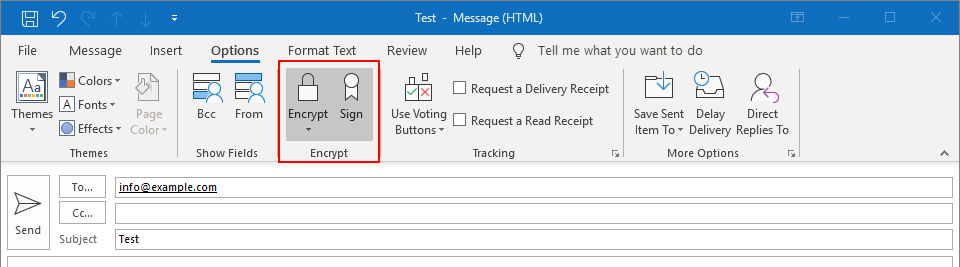
1. **Thiết lập S/MIME mặc định**

Đặt các tùy chọn mặc định mong muốn của bạn cho S/MIME email qua bốn hộp kiểm bên dưới **Email được mã hóa**, sau đó nhấn vào **OK** để đóng **Trung tâm tin tưởng** Cửa sổ.

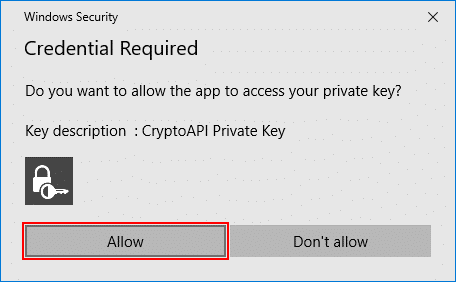


1. **Thiết lập S/MIME tùy chọn trong một tin nhắn mới.**

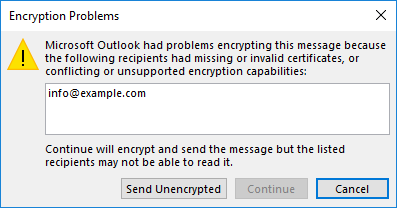
Bây giờ là của bạn S/MIME chứng chỉ được cài đặt và cấu hình, bạn có thể bắt đầu gửi tin nhắn đã ký và mã hóa. Bắt đầu bằng cách tạo một thư email mới trong Outlook. Dưới **Các lựa chọn**, bạn có thể chuyển đổi mã hóa và / hoặc cài đặt chữ ký số cho tin nhắn.



1. **Cho phép Outlook sử dụng khóa cá nhân của bạn.**

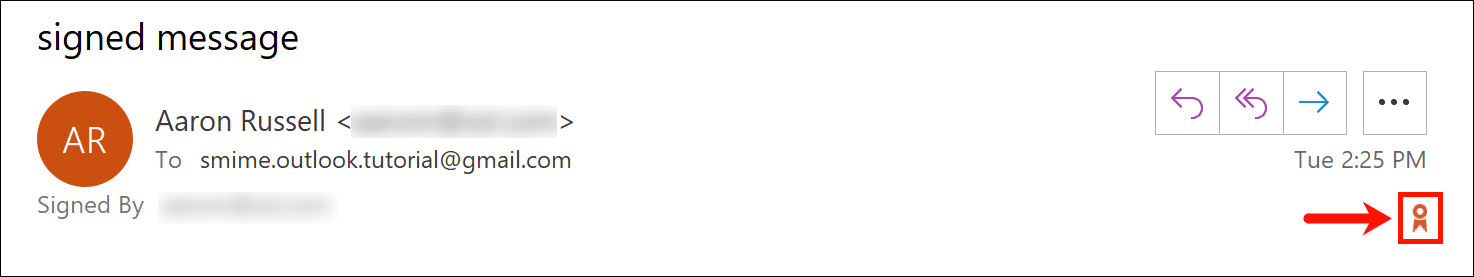
Sau khi gửi, nhấp vào **Cho phép** trong **Windows Security** hộp thoại xuất hiện, cho phép Outlook sử dụng khóa riêng của bạn.  


1. **Sự cố tiềm ẩn với mã hóa.**

Lưu ý rằng nếu bạn cố gắng gửi email được mã hóa và không có khóa công khai của người nhận, bạn sẽ nhận được thông báo lỗi cung cấp tùy chọn gửi thư không được mã hóa. Bạn có thể giải quyết vấn đề này bằng cách yêu cầu họ gửi cho bạn một email đã ký, sau đó thêm họ làm địa chỉ liên hệ trong Outlook.  


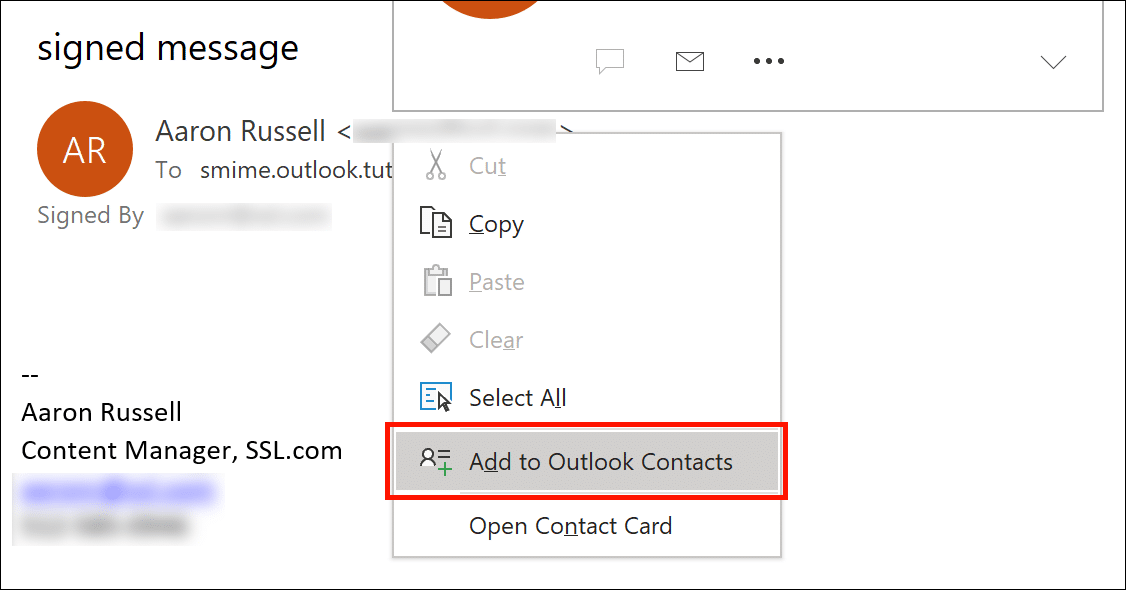
1. **Xác nhận chữ ký.**

Khi người liên hệ của bạn gửi cho bạn một email đã ký, bạn sẽ thấy một biểu tượng dải băng nhỏ ở góc trên bên phải của thư. Bạn có thể xác nhận thông tin chi tiết của chứng chỉ bằng cách nhấp vào biểu tượng.

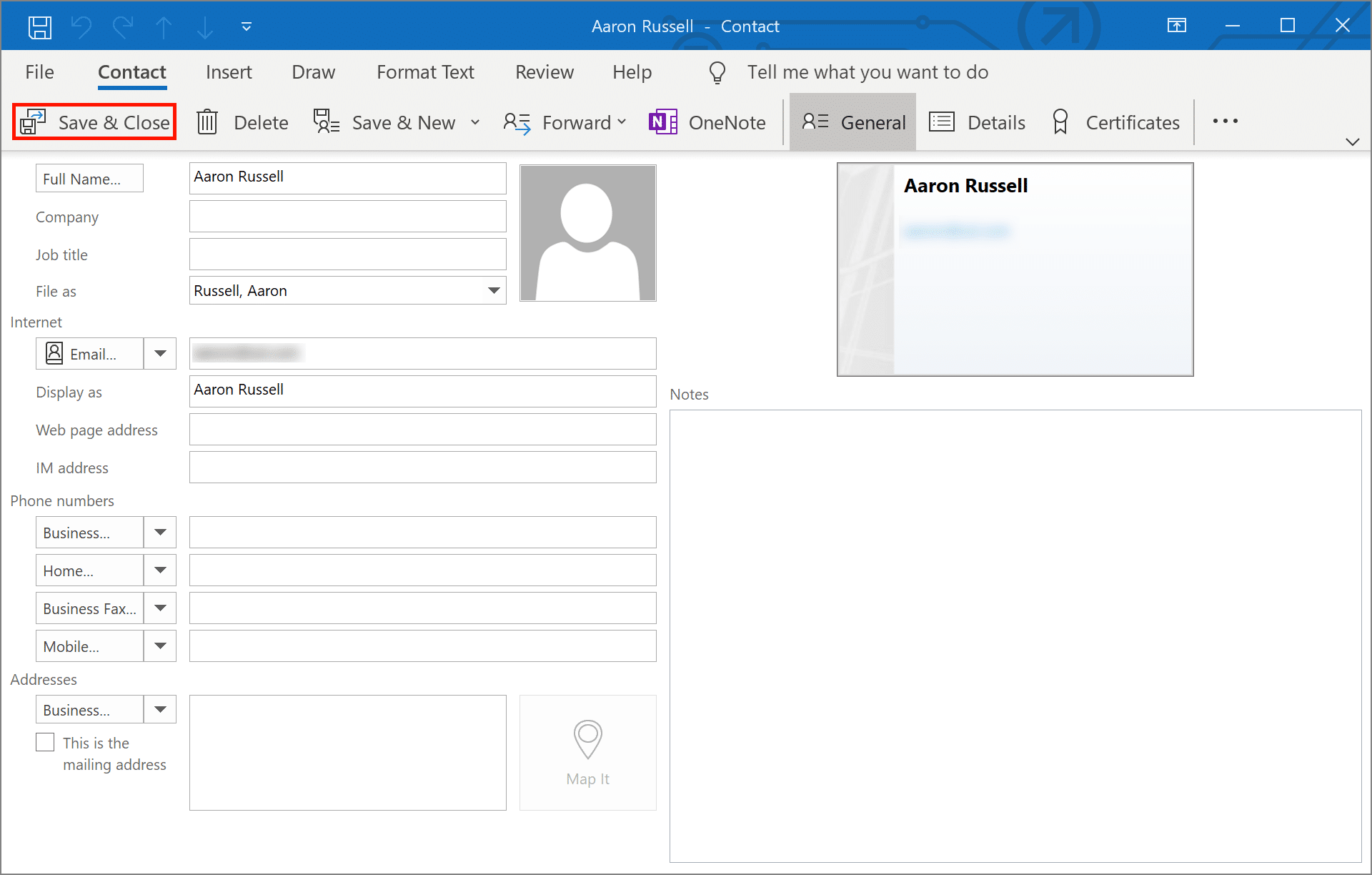


1. **Thêm liên hệ (bước 1).**

Nhấp chuột phải vào tên người gửi và chọn **Thêm vào Outlook Contacts**.



1. **Thêm liên hệ (bước 2)**
2. Nhấp chuột **Lưu và Đóng** để lưu số liên lạc của bạn. Bây giờ bạn sẽ có thể gửi email được mã hóa cho người nhận này.



# CHƯƠNG 4. Kết Luận.

Dựa trên tiêu chuẩn Mở rộng thư Internet đa mục đích MIME, S/MIME cung cấp các dịch vụ an toàn cho các ứng dụng truyền thông điệp điện tử như: xác thực, toàn vẹn, chống chối bỏ (sử dụng chữ ký số) và tính riêng tư, bảo mật của dữ liệu (sử dụng mã hóa). S/MIME có thể được sử dụng bởi người dùng thư điện tử truyền thống để bổ sung các dịch vụ an toàn mật mã cho các thư được gửi và thông dịch các dịch vụ an toàn trong thư nhận được. Tuy nhiên, S/MIME không bị giới hạn với thư điện tử, nó có thể được sử dụng với các cơ chế chuyển vận dữ liệu kiểu MIME khác, chẳng hạn như giao thức truyền siêu văn bản [HTTP](http://aita.gov.vn/tin-tuc/1352/tieu-chuan-ky-thuat-ve-udcntt-trong-cqnn-tieu-chuan-http-giao-thuc-truyen-sieu-van-ban-1).. Trong [Thông tư số 01/2011/TT-BTTTT](http://mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/DispForm.aspx?ID=7734) ngày 04/01/2011 của Bộ Thông tin và Truyền thông Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước quy định **Bắt buộc áp dụng** tiêu chuẩn S/MIME v3.2 và được xếp vào nhóm **Tiêu chuẩn về an toàn thông tin**.

# Trích dẫn tài liệu tham khảo.

https://www.ssl.com/vi/how-to/installing-s-mime-certificate-sending-secure-email-outlook-windows-10/

https://www.viendongtelecom.com.vn/Vien-Thong-Chi-Tiet-217-cach\_thuc\_ma\_hoa\_email.aspx