BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 269/BTTTT-UDCNTT	*Hà Nội, ngày 06 tháng 02 năm 2012*

V/v giải thích việc áp dụng các tiêu chuẩn kỹ thuật chính sử dụng cho hệ thống cổng thông tin điện tử và hệ thống thư điện tử

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

Ngày 04/01/2011, Bộ trưởng Bộ Thông tin và Truyền thông đã ban hành Thông tư số 01/2011/TT-BTTTT về việc Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

Thực hiện nội dung quy định tại Thông tư này, Bộ Thông tin và Truyền thông ban hành công văn giải thích việc áp dụng các tiêu chuẩn kỹ thuật chính sử dụng cho hệ thống cổng thông tin điện tử và hệ thống thư điện tử.

Trong quá trình thực hiện, nếu có vướng mắc, đề nghị Quý cơ quan phản ánh về Bộ Thông tin và Truyền thông để được hướng dẫn giải quyết.

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Minh Hồng (để b/c);
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Lưu: VT, UDCNTT.

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

Nguyễn Thành Phúc

GIẢI THÍCH VIỆC ÁP DỤNG CÁC TIÊU CHUẨN KỸ THUẬT CHÍNH SỬ DỤNG CHO HỆ THỐNG THƯ ĐIỆN TỬ

(Kèm theo Công văn số: 269 /BTTTT-UDCNTT ngày 06/02/2012 của Bộ Thông tin và Truyền thông)

1. Phạm vi và đối tượng áp dụng

1.1. Phạm vi áp dụng

Tài liệu này nhằm giải thích việc áp dụng các tiêu chuẩn kỹ thuật chính phần liên quan đến hệ thống thư điện tử công bố kèm theo Thông tư số 01/2011/TT-BTTTT ngày 04 tháng 01 năm 2011 của Bộ trưởng Bộ Thông tin và Truyền thông về việc Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

1.2. Đối tượng áp dụng

Đối tượng áp dụng bao gồm các các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

2. Giới thiệu về thư điện tử

2.1. Khái niệm

- Thư điện tử (electronic mail, viết tắt là email hay e-mail) là một phương thức trao đổi các thông điệp điện tử từ một nơi gửi tới một hay nhiều nơi nhận, thông qua mạng các máy vi tính hay mạng Internet;

- MUA (Mail User Agent): Chương trình được cài đặt trên trên máy vi tính của người sử dụng, hỗ trợ gửi/nhận thư còn gọi là email client, ví dụ Microsoft Outlook, Microsoft Outlook Express, hay Mozilla Thunderbird…;

- Web browser: Trình duyệt web được cài đặt trên trên máy vi tính của người sử dụng, hỗ trợ gửi/nhận thư, ví dụ Internet Explorer, Mozilla Firefox…;

- MTA (Mail Transfer Agent hay Message Transfer Agent): Phần mềm máy chủ thư điện tử có nhiệm vụ cung ứng các dịch vụ thư điện tử bao gồm gửi, nhận hoặc trung chuyển thư điện tử. MTA là đầu mối giao tiếp trực tiếp với các MUA, ví dụ postfix, qmail, sendmail…

2.2. Các chức năng tối thiểu hệ thống thư điện tử cần có

a) Chức năng của phần mềm thư điện tử

- Cho phép nhận, soạn thảo, lưu tạm và gửi thư, đính kèm tệp tin;

- Cho phép quản lý lịch làm việc cá nhân;

- Cho phép quản lý sổ địa chỉ;

- Cho phép tạo sổ tay để ghi chép, ghi nhớ các thông tin;

- Cung cấp công cụ tìm kiếm thư điện tử.

b) Chức năng của phần mềm trên máy chủ thư điện tử

- Cho phép tích hợp với dịch vụ thư mục để quản lý thông tin và tài khoản của người sử dụng;

- Cho phép người sử dụng truy cập máy chủ để đọc, lấy thư;

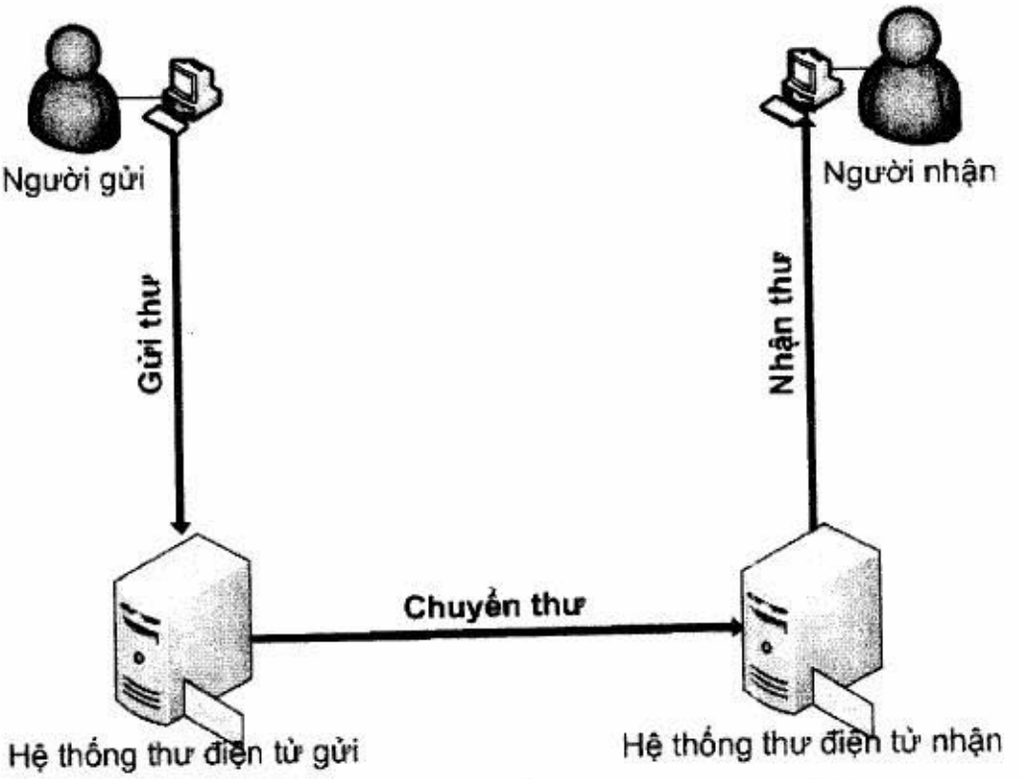
- Cho phép người gửi gửi thư cho người nhận qua máy chủ thư điện tử.

(Công văn số 1654/BTTTT-UDCNTT ngày 27/5/2008 và Công văn số 3386/BTTTT-UDCNTT ngày 23/10/2009 của Bộ Thông tin và Truyền thông)

3. Giải thích việc áp dụng các tiêu chuẩn

3.1. Mô hình trao đổi thư điện tử

Mô hình trao đổi thư điện tử đơn giản trong Hình 1 mô tả cách thức và đường đi của thư giữa hai hệ thống thư điện tử.



Hình 1. Mô hình trao đổi thư điện tử đơn giản

Trong mô hình trao đổi thư điện tử đơn giản:

- Người gửi gửi thư cho người nhận thông qua chương trình gửi/nhận thư hoặc trình duyệt web đã cài đặt trên máy vi tính, thư này được chuyển đến máy chủ thư điện tử của hệ thống thư điện tử gửi.

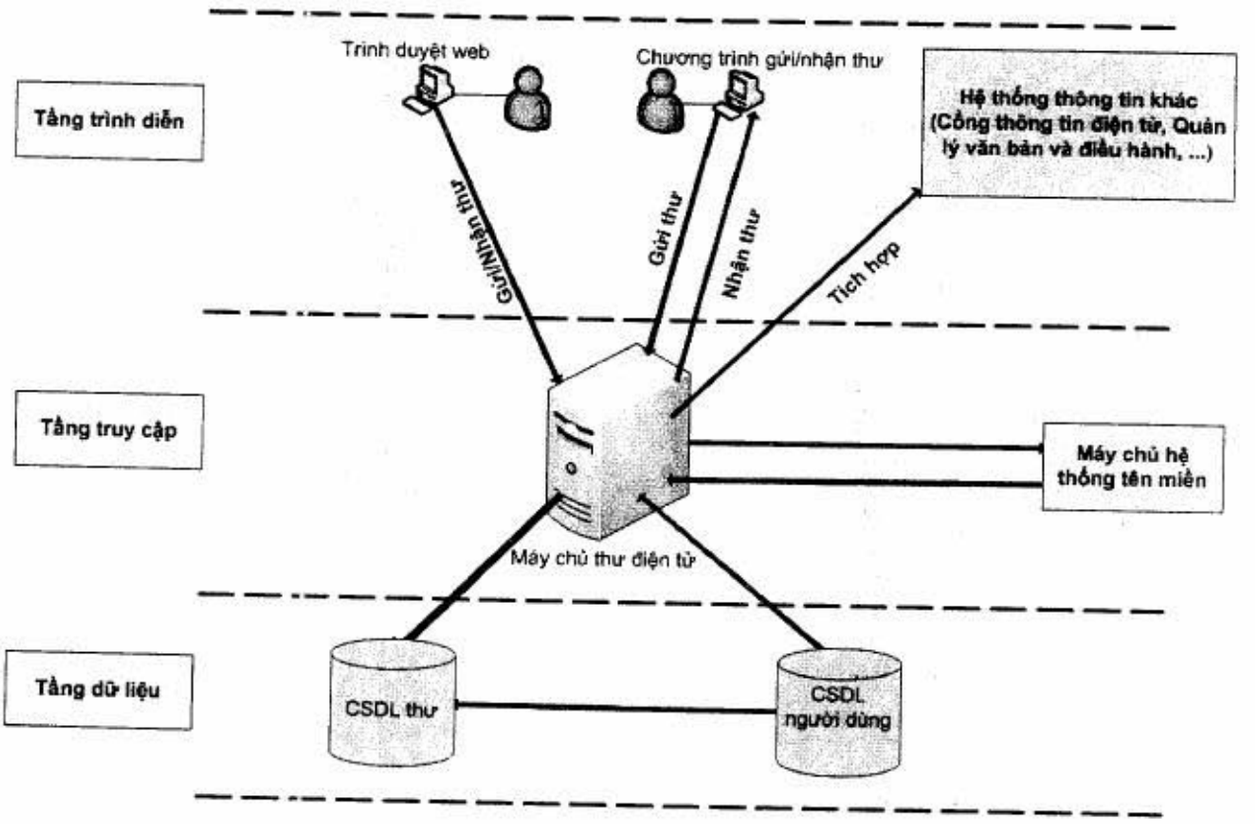
- Máy chủ thư điện tử tại nơi gửi sẽ đọc địa chỉ của người nhận, nếu là thư gửi sang một hệ thống khác, máy chủ sẽ chuyển thư này tới máy chủ thư điện tử trên hệ thống thư điện tử nhận.

- Máy chủ thư điện tử tại nơi nhận sẽ chuyển thư của người gửi đến hộp thư của người nhận. Cũng thông qua chương trình gửi/nhận thư hoặc trình duyệt web đã được cài đặt trên máy vi tính, người nhận sẽ nhận thư gửi đến.

Để hiểu và áp dụng các tiêu chuẩn hoặc giao thức trong hệ thống thư điện tử, phần 3.3 mô tả chi tiết cách thức người sử dụng gửi/nhận thư thông qua một hệ thống thư điện tử đơn giản.

3.2. Kiến trúc của một hệ thống thư điện tử đơn giản

Hình 2 mô tả về kiến trúc của một hệ thống thư điện tử đơn giản và cách thức người sử dụng tương tác với hệ thống trong ba tầng truyền dữ liệu.



Hình 2. Kiến trúc một hệ thống thư điện tử đơn giản

Các thành phần trong kiến trúc hệ thống thư điện tử đơn giản ở ba tầng:

- Tầng trình diễn:

+ Chương trình gửi/nhận thư và trình duyệt web: Được cài đặt trên máy vi tính của người sử dụng;

+ Hệ thống thông tin khác: Tích hợp hệ thống thư điện tử với các hệ thống thông tin khác như cổng thông tin điện tử, quản lý văn bản và điều hành…

- Tầng truy cập:

+ Máy chủ thư điện tử: Nhận, định tuyến, truyền thư sử dụng giao thức SMTP đến một hộp thư cùng hệ thống hay đến một hệ thống thư điện tử khác;

+ Máy chủ hệ thống tên miền: Phân giải tên miền thành địa chỉ IP.

- Tầng dữ liệu:

+ CSDL (Cơ sở dữ liệu) thư: Lưu trữ, nhận và thao tác thư đối với chương trình đọc thư trên máy khách. Có thể nhận thư bằng các giao thức POP, IMAP, hay HTTP. POP tải thư về trên máy khách để đọc và lưu trữ còn IMAP và HTTP đọc và lưu trữ thư trên máy chủ;

+ CSDL người dùng: Lưu trữ, nhận và truyền thông tin thư mục cho thành phần máy chủ thư điện tử, bao gồm thông tin định tuyến về người dùng, danh sách truyền tin, và các thông tin khác hỗ trợ cho việc truyền và truy cập thư. CSDL người dùng cũng lưu trữ mật khẩu và các thông tin cần thiết phục vụ cho máy chủ thư điện tử hay CSDL thư để xác thực người dùng.

3.3. Phương thức truyền dữ liệu giữa các tầng

Sau đây giải thích chi tiết phương thức truyền dữ liệu giữa các tầng và các tiêu chuẩn hoặc giao thức được áp dụng trong hệ thống thư điện tử đơn giản.

a) Ở tầng trình diễn:

- Để gửi thư điện tử, người sử dụng có thể sử dụng máy vi tính có cài đặt chương trình gửi/nhận thư thông qua giao thức SMTP hoặc truy cập từ web thông qua trình duyệt web sử dụng giao thức HTTP, thư này được chuyển đến máy chủ thư điện tử ở tầng truy cập. Thông qua giao thức MIME, ngoài thông tin dạng văn bản, người sử dụng có thể gửi các tập tin đính kèm như hình ảnh, âm thanh, phim ảnh hay chương trình máy vi tính…

- Để nhận thư điện tử, người sử dụng có thể sử dụng máy vi tính có cài đặt chương trình gửi/nhận thư thông qua giao thức POP hoặc giao thức IMAP hoặc truy cập vào web thông qua trình duyệt web sử dụng giao thức HTTP từ máy chủ thư điện tử ở tầng truy cập.

- Có thể kết hợp giao thức SMTP với một trong hai giao thức SSL hoặc TLS để đảm bảo an toàn trên đường truyền khi gửi thư; kết hợp giao thức POP

hoặc giao thức IMAP với một trong hai giao thức SSL hoặc TLS để đảm bảo an toàn trên đường truyền khi nhận thư; hoặc kết hợp giao thức HTTP với một trong hai giao thức SSL hoặc TLS để đảm bảo an toàn trên đường truyền khi gửi/nhận thư.

- Trường hợp sử dụng chữ ký số trong gửi/nhận thư điện tử, giao thức S/MIME thường được tích hợp trong các chương trình gửi/nhận thư để hỗ trợ mã hóa và xác thực.

- Hệ thống thư điện tử có thể được tích hợp với các hệ thống thông tin khác như cổng thông tin điện tử, quản lý văn bản và điều hành...

- Ở tầng trình diễn, các tiêu chuẩn hoặc giao thức chính sau được áp dụng:

+ SMTP (Simple Mail Transfer Protocol): Là giao thức chuẩn đảm nhận truyền các thư từ máy chủ thư điện tử của người gửi đến máy chủ thư điện tử của người nhận. Quy định tất cả các máy chủ thư điện tử bắt buộc phải áp dụng và hỗ trợ giao thức SMTP đảm bảo thống nhất trao đổi dữ liệu;

+ MIME (Multipurpose Internet Mail): Là giao thức bổ sung thêm cho SMTP để cho phép gắn kèm các thông điệp đa phương tiện (không phải là văn bản) bên trong thông điệp SMTP chuẩn. Quy định tất cả các máy chủ thư điện tử bắt buộc phải áp dụng và hỗ trợ giao thức MIME đảm bảo thống nhất trao đổi dữ liệu;

+ POP (Post Office Protocol): Là giao thức chuẩn cho phép truy cập vào hộp thư và tất cả thư điện tử sẽ được tải từ máy chủ thư điện tử về máy vi tính, ngoài ra có thể chọn để lại một bản sao của mỗi thư lại máy chủ thư điện tử;

+ IMAP (Internet Message Access Protocol): Là giao thức chuẩn cho phép truy cập vào hộp thư, trong đó các thư điện tử được nhận về và giữ lại trên máy chủ thư điện tử. Khi có yêu cầu đọc một thư điện tử cụ thể, nội dung thư mới được tải xuống từ máy chủ.

Quy định tất cả các máy chủ thư điện tử bắt buộc phải áp dụng và hỗ trợ hoặc giao thức POP hoặc giao thức IMAP hoặc bắt buộc áp dụng và hỗ trợ đồng thời cả hai giao thức POP và IMAP để đảm bảo thống nhất trao đổi dữ liệu.

+ HTTP (HyperText Transfer Protocol): Là giao thức chuẩn truyền tải dữ liệu từ một máy chủ vào một trình duyệt web để người dùng có thể xem một trang tin. Quy định tất cả các máy chủ cung cấp dịch vụ bắt buộc phải áp dụng và hỗ trợ giao thức HTTP;

+ SSL (Secure Sockets Layer), TLS (Transport Layer Security): Là các giao thức đảm bảo an toàn trên đường truyền bằng cách mã hóa các gói kết nối.

Trong trường hợp muốn đảm bảo an toàn trên đường truyền, quy định các ứng dụng (ví dụ trình duyệt web) và các máy chủ cung cấp dịch vụ bắt buộc phải áp dụng và hỗ trợ các giao thức SSL/TLS.

b) Ở tầng truy cập:

- Sau khi nhận thư từ người dùng gửi đi từ tầng trình diễn, máy chủ thư điện tử sẽ đọc địa chỉ của người nhận và dựa vào phần tên miền, nó sẽ phân giải địa chỉ của tên miền này qua máy chủ hệ thống tên miền sử dụng giao thức DNS để xác định máy chủ sẽ nhận thư gửi đến. Máy chủ hệ thống tên miền sẽ trả lại một bản ghi trao đổi thư, đây là bản ghi chỉ ra cách thức làm thế nào định tuyến cho thư điện tử này. Nếu là thư gửi trong cùng một hệ thống, máy chủ thư điện tử sẽ chuyển thư này đến CSDL thư ở tầng dữ liệu, sau đó sẽ chuyển đến hộp thư của người nhận theo mô tả trong Hình 3 bên dưới. Ngược lại, sẽ gửi đến một máy chủ thư điện tử khác rồi mới chuyển đến hộp thư của người nhận (theo mô tả về mô hình trao đổi thư điện tử đơn giản trong mục 3.1) qua giao thức SMTP.

- Ngoài ra, có thể áp dụng tiêu chuẩn DNSSEC để tăng cường tính bảo mật cho máy chủ hệ thống tên miền.

- Ở tầng truy cập, các tiêu chuẩn hoặc giao thức chính sau được áp dụng:

+ DNS (Domain Name System): Là giao thức chuẩn mục đích để phân giải địa chỉ, dùng để ánh xạ giữa tên miền (domain name) sang địa chỉ IP (Internet Protocol address viết tắt là IP address). Quy định tất cả các máy chủ hệ thống tên miền bắt buộc phải áp dụng và hỗ trợ giao thức DNS;

+ DNSSEC (Domain Name System Security Extensions): Là một tập các sửa đổi, bổ sung cho giao thức DNS để cung cấp tính xác thực, toàn vẹn. Các máy chủ hệ thống tên miền có thể tùy chọn áp dụng, nhưng khuyến nghị nên áp dụng để tăng cường bảo mật cho máy chủ hệ thống tên miền.

c) Ở tầng dữ liệu:

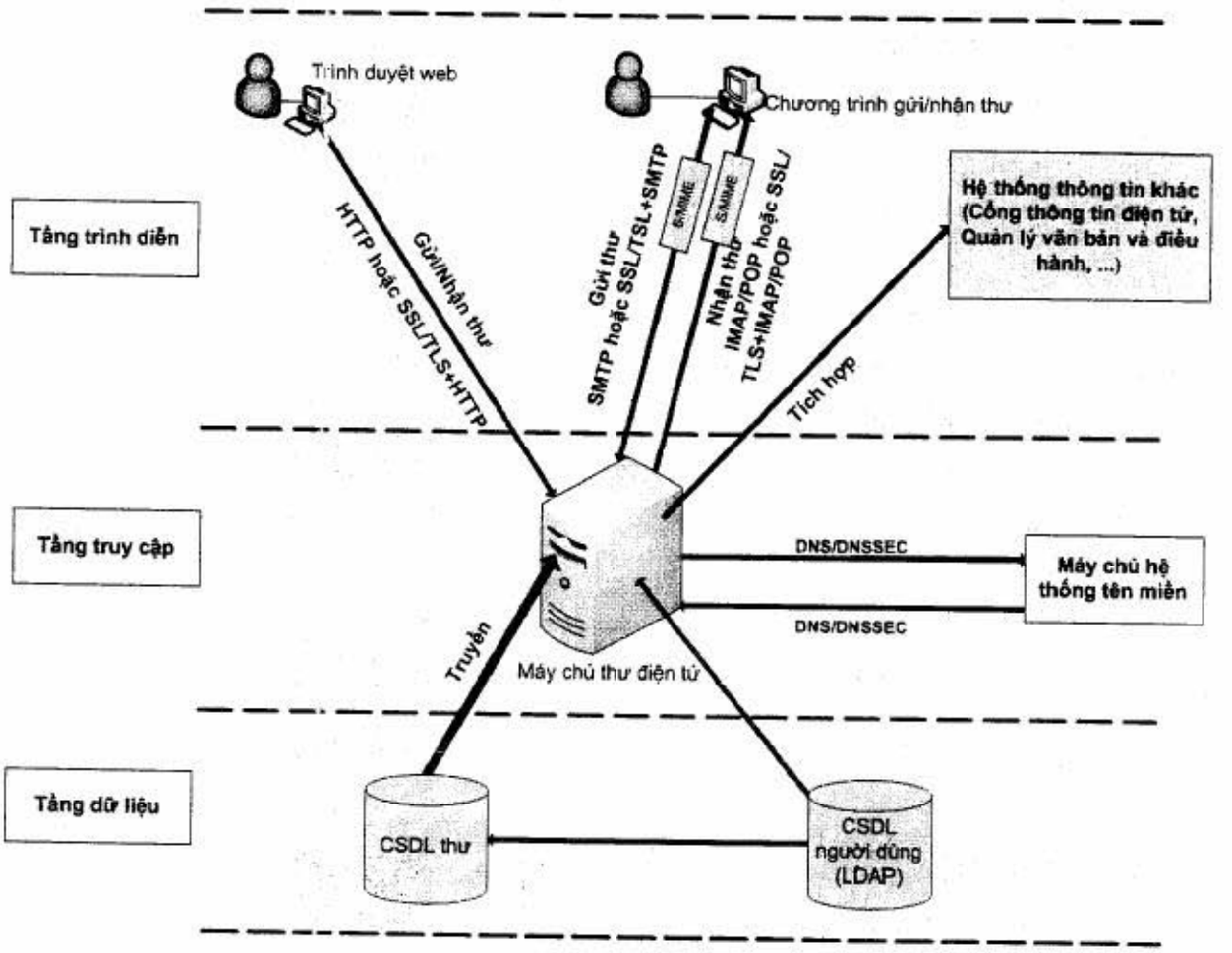
- Nếu là thư gửi trong cùng một hệ thống, máy chủ thư điện tử sẽ chuyển thư này đến CSDL thư ở tầng dữ liệu, sau đó sẽ chuyển đến hộp thư của người nhận. CSDL thư lưu thông tin về các thư gửi/nhận của người sử dụng. CSDL người dùng lưu các thông tin tài khoản người sử dụng, phục vụ cho máy chủ thư điện tử hay CSDL thư để xác thực người sử dụng và dựa trên giao thức chuẩn LDAP.

- Ở tầng dữ liệu, các tiêu chuẩn hoặc giao thức chính sau được áp dụng:

+ LDAP (Lightweight Directory Access Protocol): Là giao thức chuẩn dùng để truy nhập các dịch vụ thư mục, phục vụ tích hợp dữ liệu để từ đó có thể

dùng chung giữa các hệ thống khác nhau. Quy định tất cả các phần mềm máy chủ dịch vụ thư mục bắt buộc phải áp dụng và hỗ trợ giao thức LDAP.

Hình 3 minh họa các tiêu chuẩn hoặc giao thức chính được áp dụng trong hệ thống thư điện tử đơn giản.



Hình 3. Các tiêu chuẩn hoặc giao thức chính áp dụng trong hệ thống thư điện tử

Tất cả các luồng dữ liệu tương tác giữa người sử dụng với máy chủ thư điện tử hoặc trao đổi giữa các thành phần của máy chủ thư điện tử đều thực hiện trên môi trường mạng thông qua bộ giao thức Internet (Internet Protocol Suite). Trong đó:

+ TCP (Transmission Control Protocol): Là một trong các giao thức cốt lõi của bộ giao thức Internet. Giao thức này đảm bảo chuyển giao dữ liệu tới nơi nhận một cách đáng tin cậy và đúng thứ tự;

+ UDP (User Datagram Protocol): Là một trong các giao thức cốt lõi của bộ giao thức Internet. UDP không cung cấp sự tin cậy và thứ tự truyền nhận như TCP thực hiện, các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo;

+ IP (Internet Protocol): Là một trong các giao thức cốt lõi của bộ giao thức TCP/IP, IP là một giao thức hướng dữ liệu được sử dụng bởi các máy chủ nguồn và đích để truyền dữ liệu trong một liên mạng chuyển mạch gói. Để đảm bảo an toàn cho giao thức IP, có thể sử dụng IPsec (Internet Protocol Security) để xác thực và mã hóa từng gói IP của một phiên giao dịch và chỉ bắt buộc áp dụng khi muốn đảm bảo an toàn;

+ Quy định tất cả các mạng đều phải bắt buộc áp dụng và hỗ trợ các giao thức TCP, UDP, IP. Đối với giao thức IP, giao thức này đang trong quá trình chuyển đổi từ IPv4 (phiên bản 4) lên IPv6 (phiên bản 6).

4. Chi tiết các tiêu chuẩn hoặc giao thức

Đối chiếu với Danh mục tiêu chuẩn về ứng dụng công nghệ thông tin trong cơ quan nhà nước (Công bố kèm theo Thông tư số 01/2011/TT-BTTTT ngày 04 tháng 01 năm 2011 của Bộ trưởng Bộ Thông tin và Truyền thông), các tiêu chuẩn hoặc giao thức chính được sử dụng trong hệ thống thư điện tử bao gồm:

4.1. Giao thức truyền siêu văn bản HTTP

- Nguồn tài liệu:

+ HTTP v1.1 http://www.w3.org/Protocols/rfc2616/rfc2616.html

- Nội dung: HTTP là một trong năm giao thức chuẩn về mạng Internet, được dùng để giao tiếp giữa Máy cung cấp dịch vụ (Web server) và Máy sử dụng dịch vụ (Web client). Trong hệ thống thư điện tử, HTTP được dùng để giao tiếp giữa máy chủ thư điện tử và máy vi tính của người sử dụng. Trong Thông tư số 01/2011/TT-BTTTT, HTTP được quy định là bắt buộc áp dụng phiên bản 1.1 và được xếp vào phần Tiêu chuẩn về kết nối.

4.2. Giao thức gửi thư SMTP và MIME

- Nguồn tài liệu:

+ SMTP: http://tools.ietf.org/html/rfc5321

+ MIME:

http://tools.ietf.org/html/rfc2045, http://tools.ietf.org/html/rfc2046, http://tools.ietf.org/html/rfc2047, http://tools.ietf.org/html/rfc4289, http://tools.ietf.org/html/rfc4288

- Nội dung:

+ SMTP là giao thức chuẩn cho gửi thư điện tử thông qua môi trường mạng. SMTP sử dụng dịch vụ truyền dữ liệu tin cậy của TCP để truyền thư từ máy chủ thư điện tử của người gửi đến máy chủ thư điện tử của người nhận. SMTP có hai thành phần chính: phía máy khách, trên máy chủ thư điện tử của người gửi và phía máy chủ trên máy chủ thư điện tử của người nhận. Tất cả các máy chủ thư điện tử đều chạy cả hai phía khách và chủ của SMTP. Máy chủ thư điện tử đóng vai trò máy khách khi gửi thư, và đóng vai trò máy chủ khi nhận thư. Trong Thông tư số 01/2011/TT-BTTTT, SMTP được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về kết nối;

+ MIME là một giao thức truyền thông tin để truyền những dữ liệu theo nhiều kiểu khác nhau như: âm thanh, dạng nhị phân hoặc hình ảnh, video... MIME mã hoá những tập tin và chúng được giải mã trở lại dạng gốc tại điểm nhận. Thông tin đầu (Header) của MIME được thêm vào tập tin bao gồm kiểu nội dung dữ liệu và phương pháp dùng để mã hoá. Trong Thông tư số 01/2011/TT-BTTTT, MIME được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về kết nối.

4.3. Giao thức truy cập hộp thư POP

- Nguồn tài liệu:

+ POP3 http://tools.ietf.org/html/rfc1939

- Nội dung: Giao thức POP cho phép người sử dụng đăng nhập vào máy chủ thư và lấy (tải về) các thư về hộp thư. Người sử dụng có thể truy xuất máy chủ POP từ bất cứ hệ thống nào trên mạng, bất cứ chương trình gửi/nhận thư nào hỗ trợ giao thức POP. Trong Thông tư số 01/2011/TT-BTTTT, POP được quy định là bắt buộc áp dụng phiên bản 3 và được xếp vào phần Tiêu chuẩn về kết nối.

4.4. Giao thức nhận thư IMAP

- Nguồn tài liệu:

+ IMAP4rev1 http://tools.ietf.org/html/rfc3501

- Nội dung: Giao thức IMAP cung cấp tất cả các tính năng của giao thức POP và có thể thay thế POP mà không phá vỡ hệ thống thư hiện hành. Giao thức này cho phép người dùng lưu trữ thư trên máy chủ thư, không cần phải tải về tất cả các thư về máy vi tính. Khả năng này đặc biệt có ích cho người dùng di động có thể đọc thư trên bất kỳ máy tính nào. Trong Thông tư số 01/2011/TT-BTTTT, IMAP được quy định là bắt buộc áp dụng phiên bản 4 sửa đổi lần 1 và

được xếp vào phần Tiêu chuẩn về kết nối.

4.5. Giao thức truy cập thư mục LDAP

- Nguồn tài liệu:

+ LDAPv3 http://www.ietf.org/rfc/rfc2251

- Nội dung: Giao thức LDAP thường phân chia theo O (Organisation - tổ chức) và các OU (Organisation Unit - phân bộ). Trong các OU có thể có những OU con và trong các OU có các CN (Common Name), những nhóm giá trị này thường được gọi là DN (Distinguished Name - tên gọi phân biệt). Mỗi giá trị chứa trong LDAP thuộc dạng tên: giá trị, thường được gọi là LDAP Attribute - thuộc tính LDAP (viết tắt là attr, mỗi attr được nhận diện như một LDAP Object - đối tượng LDAP). Những điểm ở trên hình thành nên lược đồ LDAP và có tiêu chuẩn thống nhất giữa các ứng dụng phát triển LDAP. Đây là lý do LDAP được lựa chọn cho việc lưu trữ và tích hợp với các tính năng xác thực; LDAP được dùng trong bất kỳ hệ thống nào hỗ trợ và tuân thủ đúng giao thức này. Trong Thông tư số 01/2011/TT-BTTTT, LDAP được quy định là bắt buộc áp dụng phiên bản 3 và được xếp vào phần Tiêu chuẩn về kết nối.

4.6. Giao thức dịch vụ tên miền DNS

- Nguồn tài liệu:

+ DNS http://tools.ietf.org/html/rfc1034, http://tools.ietf.org/html/rfc1035

- Nội dung: DNS là một giao thức cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền, nó chuyển tên miền có ý nghĩa thành số định danh (nhị phân), định vị và địa chỉ hóa các thiết bị khắp thế giới. Ví dụ, www.example.com dịch thành 208.77.188.166. Tên miền Internet dễ nhớ hơn các địa chỉ IP như là 208.77.188.166 (IPv4) hoặc 2001: db8: 1f70: 999: de8: 7648:6e8 (IPv6). Trong Thông tư số 01/2011/TT-BTTTT, DNS được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về kết nối.

4.7. Giao thức giao vận mạng có kết nối TCP

- Nguồn tài liệu:

+ TCP http://www.ietf.org/rfc/rfc793

- Nội dung: Giao thức TCP là một trong các giao thức cốt lõi của bộ giao thức Internet. Sử dụng TCP, các ứng dụng trên các máy chủ được nối mạng có thể tạo các kết nối với nhau, qua đó các ứng dụng có thể trao đổi dữ liệu hoặc các gói tin. Giao thức này đảm bảo chuyển giao dữ liệu tới nơi nhận một cách

đáng tin cậy và đúng thứ tự. TCP còn phân biệt giữa dữ liệu của nhiều ứng dụng (chẳng hạn, dịch vụ web và dịch vụ thư điện tử) đồng thời chạy trên cùng một máy chủ. Trong Thông tư số 01/2011/TT-BTTTT, TCP được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về kết nối.

4.8. Giao thức giao vận mạng không kết nối UDP

- Nguồn tài liệu:

+ UDP http://tools.ietf.org/html/rfc768

- Nội dung: UDP là một trong những giao thức cốt lõi của bộ giao thức Internet. Sử dụng giao thức UDP, chương trình trên mạng máy tính có thể gửi những dữ liệu ngắn được gọi là datagram tới máy khác. UDP không cung cấp sự tin cậy và thứ tự truyền nhận mà TCP cung cấp; các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên, UDP nhanh và hiệu quả hơn đối với các yêu cầu như kích thước nhỏ và yêu cầu khắt khe về thời gian. Do bản chất không trạng thái của nó nên UDP hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu. Trong Thông tư số 01/2011/TT-BTTTT, UDP được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về kết nối.

4.9. Giao thức liên mạng LAN/WAN IP

- Nguồn tài liệu:

+ IPv4 http://tools.ietf.org/html/rfc791

+ IPv6: http://tools.ietf.org/html/rfc2460

- Nội dung: Giao thức IP là một trong những giao thức cốt lõi của bộ giao thức Internet, được sử dụng bởi các máy chủ nguồn và đích để truyền dữ liệu trong một liên mạng chuyển mạch gói. Dữ liệu trong một liên mạng IP được gửi theo các khối được gọi là các gói (packet hoặc datagram). Cụ thể, IP không cần thiết lập các đường truyền trước khi một máy chủ gửi các gói tin cho một máy khác mà trước đó nó chưa từng liên lạc. Giao thức IP cung cấp một dịch vụ gửi dữ liệu không đảm bảo (còn gọi là cố gắng cao nhất), nghĩa là giao thức này hầu như không đảm bảo gì về gói dữ liệu. Gói dữ liệu có thể đến nơi mà không còn nguyên vẹn, gói dữ liệu có thể đến không theo thứ tự (so với các gói khác được gửi giữa hai máy nguồn và đích đó), gói dữ liệu có thể bị trùng lặp hoặc bị mất hoàn toàn. Trong Thông tư số 01/2011/TT-BTTTT, IP được quy định là bắt buộc áp dụng phiên bản 4 (IPv4), khuyến nghị áp dụng IP phiên bản 6 (IPv6) và

được xếp vào phần Tiêu chuẩn về kết nối. Hiện tại, IP đang trong quá trình chuyển đổi từ IPv4 lên IPv6.

4.10. Giao thức an toàn thư điện tử S/MIME

- Nguồn tài liệu:

+ S/MIME v3.2 http://tools.ietf.org/html/rfc5751

- Nội dung: Giao thức S/MIME là một tiêu chuẩn hỗ trợ an toàn, cụ thể là mã hóa cho giao thức MIME. S/MIME đưa vào hai phương pháp an ninh cho thư điện tử. Thứ nhất là xác thực, đảm bảo toàn vẹn, chống chối bỏ thông qua chữ ký số; thứ hai là đảm bảo bảo mật và an toàn dữ liệu bằng cách mã hóa. Trong Thông tư số 01/2011/TT-BTTTT, S/MIME được quy định là bắt buộc áp dụng phiên bản 3.2 và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.11. Giao thức an toàn tầng giao vận SSL/TLS

- Nguồn tài liệu:

+ SSL v3.0 http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00

+ TLS v1.2 http://tools.ietf.org/html/rfc5246

- Nội dung: SSL là giao thức được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước nhằm mã hoá toàn bộ thông tin đi/đến, ngày nay SSL được sử dụng rộng rãi cho giao dịch điện tử như truyền số hiệu thẻ tín dụng, mật khẩu, số bí mật cá nhân (PIN) trên Internet. Giao thức TLS được phát triển dựa trên SSL. Hai giao thức này được sử dụng tùy theo từng trường hợp cụ thể. Trong Thông tư số 01/2011/TT-BTTTT, SSL và TLS được quy định bắt buộc áp dụng phiên bản 3.0 và phiên bản 1.2 tương ứng, và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.12. Giao thức an toàn truyền siêu văn bản HTTPS

- Nguồn tài liệu:

+ HTTPS http://tools.ietf.org/html/rfc2818

- Nội dung: HTTPS là giao thức dựa trên HTTP và SSL/TLS để bảo mật trong quá trình giao tiếp giữa Máy cung cấp dịch vụ và Máy sử dụng dịch vụ. Trong Thông tư 01/2011/TT-BTTTT, HTTPS được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.13. Giao thức an toàn truyền thư điện tử SMTPS

- Nguồn tài liệu:

+ SMTPS http://www.ietf.org/rfc/rfc2487, http://www.ietf.org/rfc/rfc1425

- Nội dung: SMTPS là kết hợp của giao thức SMTP với một trong hai giao thức SSL hoặc TLS. SMTPS là một phương thức đảm bảo an toàn cho giao thức SMTP trên đường truyền, cung cấp tính năng xác thực, toàn vẹn dữ liệu và bảo mật. Trong Thông tư số 01/2011/TT-BTTTT, SMTPS được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.14. Giao thức an toàn truy cập hộp thư POPS

- Nguồn tài liệu:

+ POPS http://tools.ietf.org/html/rfc2595, http://tools.ietf.org/html/draft-melnikov-pop3-over-tls-00

- Nội dung: POPS là kết hợp của giao thức POP (phiên bản 3) với một trong hai giao thức SSL hoặc TLS để đảm bảo an toàn trên đường truyền. Trong Thông tư số 01/2011/TT-BTTTT, POPS được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.15. Giao thức an toàn truy cập hộp thư IMAPS

- Nguồn tài liệu:

+ IMAPS http://tools.ietf.org/html/rfc2595

- Nội dung: IMAPS là kết hợp của giao thức IMAP với một trong hai giao thức SSL hoặc TLS để đảm bảo an toàn trên đường truyền. Trong Thông tư số 01/2011/TT-BTTTT, IMAPS được quy định bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.16. Giao thức an toàn dịch vụ DNS DNSSEC

- Nguồn tài liệu:

+ DNSSEC http://tools.ietf.org/html/rfc2535

- Nội dung: DNSSEC là một tập các sửa đổi, bổ sung cho giao thức DNS để cung cấp tính xác thực, toàn vẹn. Trong Thông tư số 01/2011/TT-BTTTT, DNSSEC được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.17. Giao thức an toàn tầng mạng IPsec

- Nguồn tài liệu:

+ IPsec http://tools.ietf.org/html/rfc4301

- Nội dung: IPsec là một bộ giao thức để đảm bảo an toàn truyền dữ liệu giao thức IP bằng cách xác thực và mã hóa từng gói IP của một phiên giao dịch. Trong Thông tư số 01/2011/TT-BTTTT, IPsec được quy định là bắt buộc áp dụng và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

Dưới đây là bảng tổng kết về một số tiêu chuẩn hoặc giao thức chính sử dụng trong hệ thống thư điện tử được đề cập trong Thông tư số 01/2011/TT-BTTTT:

Số TT	Loại tiêu chuẩn	Tên đầy đủ (tiếng Anh)	Tên đầy đủ (tiếng Việt)	Ký hiệu tiêu chuẩn	Quy định áp dụng trong Thông tư 01/2011/TT-BTTTT
	Tiêu chuẩn về kết nối				
1		Hypertext Transfer Protocol	Giao thức truyền siêu văn bản	HTTP	Bắt buộc áp dụng phiên bản 1.1
2		Simple Mail Transfer Protocol/Mult-ipurpose Internet Mail Extensions	Giao thức truyền thư điện tử	SMTP/MIME	Bắt buộc áp dụng
3		Post Office Protocol	Giao thức truy cập hộp thư	POP	Bắt buộc áp dụng cả hai tiêu chuẩn đối với máy chủ: POP phiên bản 3, IMAP phiên bản 4 sửa đổi lần 1
		Internet Message Access Protocol		IMAP	
4		Lightweight Directory Access Protocol	Giao thức truy cập thư mục	LDAP	Bắt buộc áp dụng phiên bản 3
5		Domain Name System	Giao thức hệ thống tên miền	DNS	Bắt buộc áp dụng
6		Transmission Control	Giao thức giao vận	TCP	Bắt buộc áp dụng

Số TT	Loại tiêu chuẩn	Tên đầy đủ (tiếng Anh)	Tên đầy đủ (tiếng Việt)	Ký hiệu tiêu chuẩn	Quy định áp dụng trong Thông tư 01/2011/TT-BTTTT
		Protocol	mạng có kết nối		
7		User Datagram Protocol	Giao thức giao vận mạng không kết nối	UDP	Bắt buộc áp dụng
8		Internet Protocol	Giao thức liên mạng LAN/WAN		Bắt buộc áp dụng phiên bản 4 Khuyến nghị áp dụng phiên bản 6
	Tiêu chuẩn về an toàn thông tin				
9		Secure Multi-purpose Internet Mail Extensions	Giao thức an toàn thư điện tử	S/MIME	Bắt buộc áp dụng phiên bản 3.2
10		Secure Socket Layer	Giao thức an toàn tầng giao vận	SSL	Bắt buộc áp dụng một trong hai tiêu chuẩn: SSL phiên bản 3.0, TLS phiên bản 1.2
		Transport Layer Security		TLS	
11		Hypertext Transfer Protocol over Secure Socket Layer	Giao thức an toàn truyền siêu văn bản	HTTPS	Bắt buộc áp dụng
12		Simple Mail Transfer Protocol over Secure Socket Layer	Giao thức an toàn truyền thư điện tử	SMTPS	Bắt buộc áp dụng
13		Post Office	Giao thức an	POPS	Bắt buộc áp dụng một

Số TT	Loại tiêu chuẩn	Tên đầy đủ (tiếng Anh)	Tên đầy đủ (tiếng Việt)	Ký hiệu tiêu chuẩn	Quy định áp dụng trong Thông tư 01/2011/TT-BTTTT
		Protocol over Secure Socket Layer	toàn dịch vụ truy cập hộp thư		hoặc cả hai tiêu chuẩn
		Internet Message Access Protocol over Secure Socket Layer		IMAPS	
14		Domain Name System Security Extension	Giao thức an toàn dịch vụ DNS	DNSSEC	Khuyến nghị áp dụng
15		Internet Protocol security	Giao thức an toàn tầng mạng	IPsec	Bắt buộc áp dụng

GIẢI THÍCH VIỆC ÁP DỤNG CÁC TIÊU CHUẨN KỸ THUẬT CHÍNH SỬ DỤNG CHO CỔNG THÔNG TIN ĐIỆN TỬ

(Kèm theo Công văn số: 269 /BTTTT-UDCNTT ngày 06/02/2012 của Bộ Thông tin và Truyền thông)

190. b8 x124

1. Phạm vi và đối tượng áp dụng

1.1 Phạm vi áp dụng

Tài liệu này nhằm giải thích việc áp dụng các tiêu chuẩn kỹ thuật chính phần liên quan đến cổng thông tin điện tử công bố kèm theo Thông tư số 01/2011/TT-BTTTT ngày 04 tháng 01 năm 2011 của Bộ trưởng Bộ Thông tin và Truyền thông về việc Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

1.2 Đối tượng áp dụng

Đối tượng áp dụng bao gồm các các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

2. Tổng quan về cổng thông tin điện tử

2.1 Khái niệm

Cổng thông tin điện tử là điểm truy cập duy nhất trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

(Khoản 2, Điều 3, Thông tư số 25/2010/TT-BTTTT ngày 15 tháng 11 năm 2010 của Bộ trưởng Bộ Thông tin và Truyền thông quy định việc thu thập, sử dụng, chia sẻ, đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước).

2.2 Các chức năng cần có của cổng thông tin điện tử

Các chức năng cần có của cổng thông tin điện tử theo Công văn số 1654/BTTTT-UDCNTT ngày 27/5/2008 và Công văn số 3386/BTTTT-UDCNTT ngày 23/10/2009 của Bộ Thông tin và Truyền thông gồm những nhóm chức năng chính như sau:

Nhóm chức năng của phần mềm cổng lõi: Nhóm chức năng này có các chức năng con như Cá nhân hóa và tùy biến; Đăng nhập một lần, xác thực và phân quyền; Quản lý cổng thông tin và trang thông tin; Quản lý cấu hình; Tích hợp các kênh thông tin; Chức năng tìm kiếm thông tin; Quản trị người sử dụng; Thu thập và xuất bản thông tin; Sao lưu và phục hồi dữ liệu; Nhật ký theo dõi; An toàn, bảo mật cổng thông tin.

Nhóm chức năng cung cấp dịch vụ tương tác ứng dụng quản lý hành chính công: Nhóm chức năng này có các chức năng con như quản trị và biên tập nội dung (CMS); Cung cấp các dịch vụ ứng dụng (dịch vụ hành chính công); Biểu mẫu điện tử.

Nhóm chức năng cung cấp dịch vụ tương tác trực tuyến, tiện ích: Nhóm chức năng này có các chức năng con như Thư điện tử; Giao lưu trực tuyến; Hỏi đáp trực tuyến; Góp ý trực tuyến.

3. Giải thích việc áp dụng các tiêu chuẩn

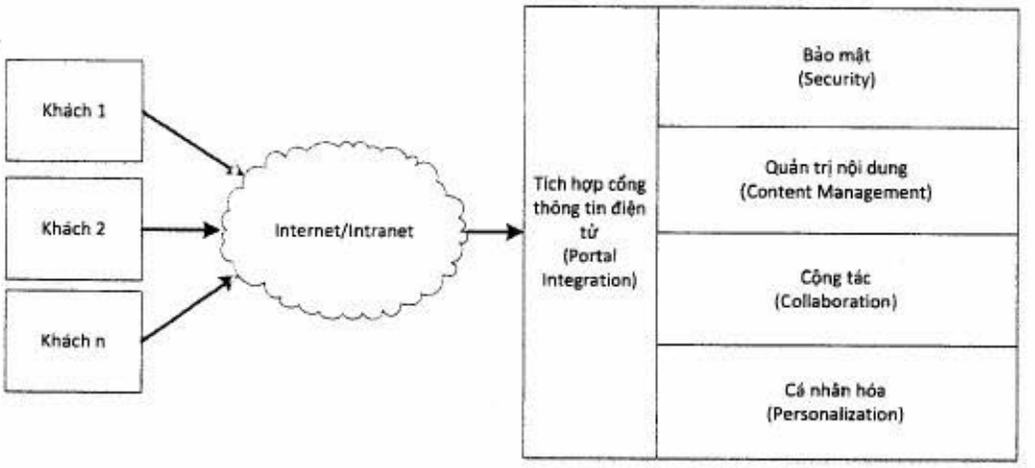
3.1 Đặc trưng cơ bản của cổng thông tin điện tử so với trang thông tin điện tử

Một trang thông tin điện tử tĩnh có đặc điểm là giao diện và nội dung được dựng sẵn do vậy gặp khó khăn trong vấn đề cập nhật thông tin, còn trang thông tin điện tử động là những trang mà các nội dung của chúng được cập nhật, truy xuất và hiển thị tùy theo yêu cầu người dùng, ví dụ cùng một trang *xem.aspx* nhưng lúc này thì hiển thị nội dung này lúc khác thì hiển thị nội dung khác tùy theo người dùng kích vào liên kết nào. Còn đối với cổng thông tin điện tử thì không chỉ có động về nội dung mà còn động về cấu trúc và vì thế nên ta có thể dễ dàng tùy biến, áp dụng cho nhiều lĩnh vực khác nhau mà phần điều chỉnh là ít nhất vì các thành phần đều ở dạng tương đối độc lập.

Một đặc điểm nổi bật của cổng thông tin điện tử là khả năng cho phép xây dựng nội dung thông tin từ nhiều nguồn cho nhiều đối tượng sử dụng và thiết đặt các thông tin khác nhau cho các loại đối tượng sử dụng khác nhau theo yêu cầu, hỗ trợ nhiều môi trường hiển thị thông tin của cùng một nội dung, chẳng hạn cùng một nội dung nhưng hiển thị trên máy tính thì sử dụng HTML, hiển thị trên PDA thì sử dụng WML, ngoài ra khả năng đăng nhập một lần và quản trị (bao gồm quản trị cổng thông tin và quản trị người dùng) cũng là một đặc điểm quan trọng của cổng thông tin điện tử so với trang thông tin điện tử.

3.2 Kiến trúc cơ bản của cổng thông tin điện tử

Với mỗi hãng phát triển cổng thông tin điện tử sẽ có một dòng sản phẩm liên quan và ứng với đó là kiến trúc đi kèm, tuy nhiên tựu chung lại kiến trúc cơ bản của cổng thông tin điện tử được thể hiện như Hình 1, Khách ở đây có thể là người dùng cuối, các hệ thống hỗ trợ nội dung, cổng WAP, cổng thoại. Các Khách thông qua Internet/Intranet giao tiếp với phần lõi của cổng thông tin điện tử, phần lõi này có thể là thành phần tích hợp, bảo mật, quản trị nội dung, cộng tác và cá nhân hóa. Chi tiết hơn các thành phần như sau:



Hình 1. Kiến trúc cơ bản của cổng thông tin điện tử

Bảo mật: Đây là vấn đề sống còn đối với một cổng thông tin điện tử. Các cổng thông tin điện tử cần cung cấp một cơ chế xác thực và kiểm soát người sử dụng truy cập vào thông tin và các ứng dụng, ngoài ra cung cấp cơ chế lưu trữ và trao đổi thông tin với các phương pháp khác nhau chẳng hạn như mã hóa.

Quản trị nội dung: Cổng thông tin điện tử chứa thông tin từ các nguồn khác nhau và thông tin này phải được cập nhật thường xuyên, do vậy cổng thông tin cần cho phép thay đổi dễ dàng nội dung, đồng thời được tự động hóa mức cao nhất có thể bằng các công cụ cập nhật đến từng người dùng cũng như triển khai thực hiện tự động các dịch vụ thu thập thông tin từ xa.

Cộng tác: Mục tiêu chính của cộng tác là cung cấp một tập hợp các chức năng để giao tiếp giữa người sử dụng của cổng thông tin điện tử như các danh sách thảo luận, trò chuyện và nhóm tin.

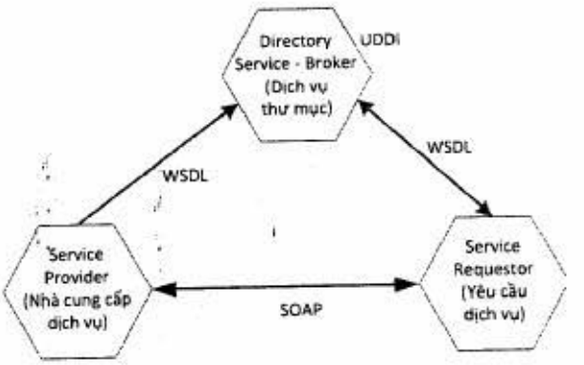
Cá nhân hóa: Mục tiêu chính của cá nhân hóa là hỗ trợ người dùng hiện các thông tin theo mong muốn của mình, cho phép thiết lập các thông tin khác nhau, trình bày theo các cách khác nhau, phục vụ cho các loại đối tượng sử dụng khác nhau theo các yêu cầu cá nhân như sở thích, thói quen, yêu cầu đa dạng của người dùng. Cho phép người dùng tự định nghĩa các tính năng cá nhân của riêng mình, hiển thị các dịch vụ mà người dùng muốn, cho phép người dùng có thể tự cấu hình lại giao diện liên quan đến vị trí, màu sắc của các thành phần (như các trang, các khung, các liên kết…).

Ngoài các thành phần của kiến trúc đã được liệt kê ở trên, các thành phần sau cũng thường được đề cập đến như là một phần của kiến trúc cổng thông tin điện tử như khả năng tích hợp, xuất bản nội dung, khả năng tìm kiếm, đăng nhập một lần, quản trị, hỗ trợ nhiều môi trường hiển thị thông tin. Một cổng thông tin điện tử không nhất thiết phải có đầy đủ các thành phần trên, tùy vào điều kiện thực

tế khi xây dựng cổng thông tin điện tử chúng ta lựa chọn các thành phần cho phù hợp.

3.3 Cổng thông tin điện tử và dịch vụ web

Trên thị trường với mỗi dòng sản phẩm sẽ có nhiều hãng tham gia với nhiều giải pháp công nghệ khác nhau, câu hỏi đặt ra là làm thế nào để các sản phẩm cổng thông tin điện tử xây dựng dựa trên các công nghệ khác nhau này có thể giao tiếp với nhau, dịch vụ web là một giải pháp cho vấn đề này, dịch vụ web cho phép các máy giao tiếp với nhau ngay cả trong môi trường khác nhau. Hình 2 mô tả mô hình dịch vụ web với ba thành phần cơ bản:



Hình 2. Mô hình dịch vụ web

Nhà cung cấp dịch vụ: Gửi các dịch vụ mà mình có thể cung cấp lên Dịch vụ thư mục, ứng với mỗi dịch vụ gửi lên có một bản mô tả dịch vụ được viết bằng ngôn ngữ định nghĩa dịch vụ web (Web Services Definition Language, WSDL).

Ngôn ngữ định nghĩa dịch vụ web (Web Services Definition Language, WSDL) *là một ngôn ngữ dựa trên XML dùng để xác định vị trí và mô tả các dịch vụ web, WSDL là một tiêu chuẩn của W3C.*

Dịch vụ thư mục (còn gọi là dịch vụ trung gian): Lưu trữ thông tin về các dịch vụ được cung cấp bởi các Nhà cung cấp dịch vụ bằng tiêu chuẩn Tích hợp, Khám phá và Mô tả toàn cầu (Universal Discovery, Description, and Integration, UDDI).

Tiêu chuẩn Tích hợp, Khám phá và Mô tả toàn cầu (Universal Discovery, Description, and Integration, UDDI) *là một dịch vụ thư mục mà ở đó có thể đăng ký và tìm kiếm các dịch vụ web, UDDI lưu trữ thông tin liên quan đến các dịch vụ web với giao diện được miêu tả bằng WSDL và giao tiếp với nhau qua SOAP, UDDI là một chuẩn của OASIS.*

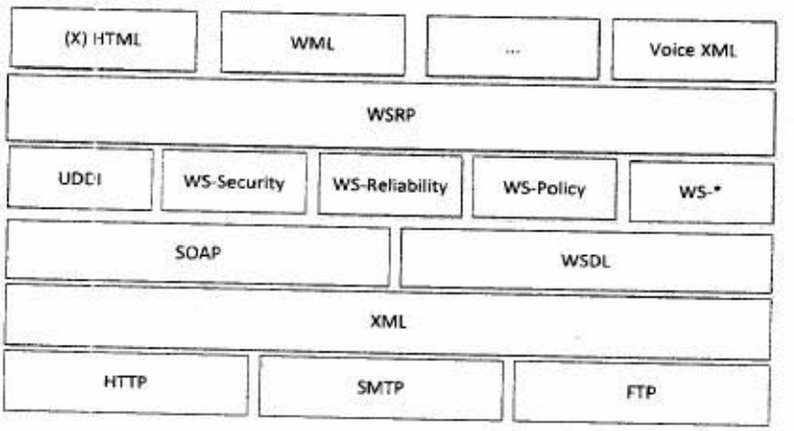
Yêu cầu dịch vụ: Khi một khách hàng có yêu cầu sử dụng một dịch vụ nào đấy, Yêu cầu dịch vụ sẽ dùng WSDL để mô tả nhu cầu sử dụng của mình và gửi cho Dịch vụ thư mục, sau đó giữa phía Yêu cầu dịch vụ và Nhà cung cấp dịch vụ

giao tiếp với nhau dựa trên ngôn ngữ đánh dấu mở rộng (eXtensible Markup Language, XML) và thông qua giao thức truy cập đối tượng đơn giản (Simple Object Access Protocol, SOAP).

Giao thức truy cập đối tượng đơn giản (Simple Object Access Protocol, SOAP) *là giao thức dựa trên XML dùng để trao đổi thông tin giữa các ứng dụng* thông qua HTTP, SOAP là một tiêu chuẩn của W3C.

Ngôn ngữ đánh dấu mở rộng (eXtensible Markup Language, XML) *là ngôn ngữ được thiết kế để vận chuyển và lưu trữ dữ liệu do người dùng tự định nghĩa, XML là một tiêu chuẩn của W3C.*

Vì dịch vụ web dựa trên một tập hợp các tiêu chuẩn và công nghệ phục vụ cho khả năng tương thích giữa nhiều ngôn ngữ với nhiều nền tảng phát triển khác nhau và cổng thông tin điện tử cũng được tiếp cận theo dịch vụ web nên nếu đặt trong mối quan hệ với dịch vụ web ta có các tiêu chuẩn/giao thức chính của cổng thông tin điện tử được thể hiện như Hình 3.



Hình 3. Các lớp giao thức/tiêu chuẩn chính của cổng thông tin điện tử

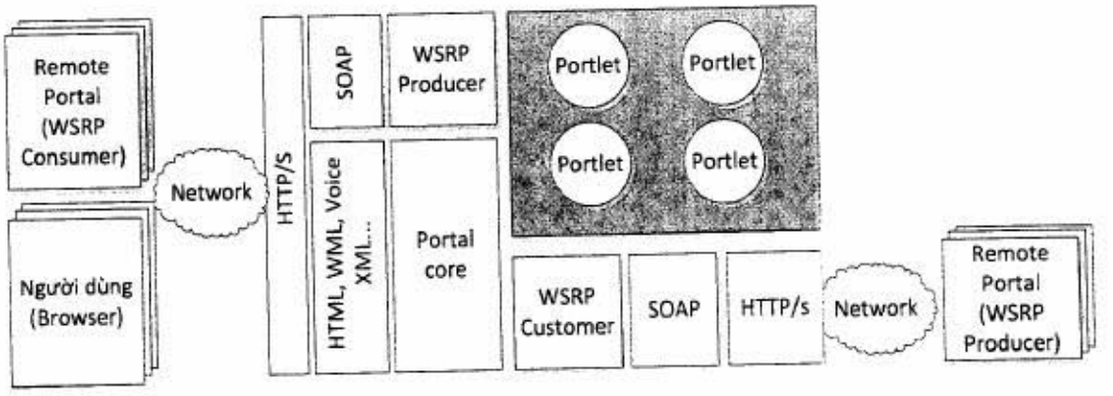
Dịch vụ web liên kết và tương tác với các ứng dụng qua Internet, chính vì vậy bảo mật là một vấn đề quan trọng, đặc biệt đối với những dịch vụ liên quan đến trao đổi tiền tệ, chứng khoán hay thương mại điện tử. Để an toàn dịch vụ web trong cổng thông tin điện tử chúng ta có thể thực hiện bảo mật bằng cách sử dụng tiêu chuẩn **An toàn dịch vụ web (Web Services Security, WS-Security).**

An toàn dịch vụ web (Web Services Security, WS-Security) *là một tiêu chuẩn nhằm bổ sung thêm cho việc bảo đảm an toàn dịch vụ web SOAP, WS-Security do OASIS công bố.*

Đối với cổng thông tin điện tử thì vấn đề giao tiếp giữa phần ứng dụng (portal application hay portlet) với phần nền tảng (portal framework hay portal server) là hết sức quan trọng, với mỗi hãng khác nhau thì phần ứng dụng sẽ có các giao diện lập trình ứng dụng (portlet API) khác nhau (ví dụ một số portlet API như:

JetSpeed API, uPortal API, JSR 168/286 và Web parts), hiện nay JSR168 (Java Specification Requests 168) là tiêu chuẩn cho portlet API dựa trên nền tảng J2EE được dùng phổ biến trên thế giới, mặt khác khi cổng thông tin điện tử giao tiếp với ứng dụng từ xa thì dịch vụ web cho ứng dụng từ xa (*Web Services for Remote Portlet, WSRP)* được sử dụng.

Tiêu chuẩn JSR 168 (Java Specification Requests 168) *là một portlet API chỉ ra cách tương tác giữa phần ứng dụng với phần nền tảng, các ứng dụng tuân thủ tiêu chuẩn này sẽ có thể hoạt động được ở tất cả các phần nền tảng tuân thủ/hỗ trợ tiêu chuẩn JSR168, JSR168 dựa trên nền tảng J2EE do Java Community Process công bố.*



Hình 4. Mối quan hệ giữa portlet API (JSR168) và WSRP

Tiêu chuẩn dịch vụ web cho ứng dụng từ xa (Web Services for Remote Portlet, WSRP)*, tiêu chuẩn WSRP chỉ ra cách thức giao tiếp giữa một hệ thống nền tảng với một hệ thống ứng dụng từ xa thông qua dịch vụ web, các hệ thống ứng dụng tuân thủ tiêu chuẩn này có thể chạy trên bất kỳ một hệ thống nền tảng nào áp dụng tiêu chuẩn WSRP mà không cần quan tâm đến việc ứng dụng hay hệ thống nền tảng được xây dựng trên công nghệ/ngôn ngữ nào.*

Hình 4 mô tả quan hệ cơ bản giữa các phần chính của cổng thông tin điện tử, khi người dùng hoặc một ứng dụng từ xa có yêu cầu thì yêu cầu đó sẽ được mô tả bằng các ngôn ngữ như WML, ebXML, HTML và sử dụng giao thức truyền siêu văn bản (HyperText Transfer Protocol, HTTP) hoặc giao thức an toàn truyền siêu văn bản (Hypertext Transfer Protocol over Secure Socket Layer, HTTPS) rồi gửi yêu cầu đến hệ thống nền tảng, hệ thống nền tảng này giao tiếp với các portlet thông qua portlet API (JSR168 chẳng hạn) để tìm kiếm các thông tin và phản hồi kết quả, ngược lại, nếu cổng thông tin điện tử đóng vai trò là một ứng dụng từ xa thì cổng sẽ gửi yêu cầu của mình qua HTTPS để đi đến hệ thống cần tìm thông qua mạng.

Giao thức truyền siêu văn bản (HyperText Transfer Protocol, HTTP), *được dùng để giao tiếp giữa Máy cung cấp dịch vụ (Web server) và Máy sử dụng dịch vụ (Web client), đây là giao thức cơ bản trên mạng Internet.*

Giao thức an toàn truyền siêu văn bản (HyperText Transfer Protocol over Secure Socket Layer, HTTPS), *HTTPS là giao thức kết hợp giữa HTTP và SSL/TSL để bảo mật thông tin cho quá trình truyền dữ liệu.*

4. Chi tiết các tiêu chuẩn chính sử dụng cho cổng thông tin điện tử có đề cập ở Thông tư 01/2011/TT-BTTTT

4.1 Ngôn ngữ đánh dấu mở rộng (eXtensible Markup Language, XML)

Nguồn tài liệu:

XML 1.1: www.w3.org/TR/2006/REC-xml11-20060816/;

XML 1.0: www.w3.org/TR/2008/REC-xml-20081126/.

Nội dung: Là ngôn ngữ tương tự như HTML nhưng trong khi HTML được thiết kế để biểu diễn dữ liệu thì XML được thiết kế để vận chuyển và lưu trữ dữ liệu do người dùng tự định nghĩa, từ XML ta có thể xây dựng các ngôn ngữ khác như RDF, RSS, SOAP, WSDL, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 1.0 và phiên bản 1.1 và được xếp vào phần Tiêu chuẩn tích hợp dữ liệu.

4.2 Giao thức truy cập đối tượng đơn giản (Simple Object Access Protocol, SOAP)

Nguồn tài liệu:

SOAP phiên bản 1.1: www.w3.org/TR/2000/NOTE-SOAP-20000508/;

SOAP phiên bản 1.2: www.w3.org/TR/soap/.

Nội dung: SOAP bản chất là XML kết hợp với một giao thức trên Internet chẳng hạn như HTTP, FTP. Vai trò của SOAP dùng để gửi thông tin giữa các ứng dụng thông qua việc gửi/nhận các thông điệp được gói dưới dạng XML, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 1.2 và được xếp vào phần Tiêu chuẩn về kết nối.

4.3 Ngôn ngữ định nghĩa dịch vụ web (Web Services Definition Language, WSDL)

Nguồn tài liệu:

WSDL phiên bản 1.1: www.w3.org/TR/2001/NOTE-wsdl-20010315;

WSDL 2.0: www.w3.org/TR/wsdl20/.

Nội dung: WSDL được viết dựa trên ngôn ngữ XML để mô tả và xác định vị trí dịch vụ web. Khi ta cần sử dụng dịch vụ, ta sẽ sử dụng WSDL để tìm ra vị trí của dịch vụ, các lời gọi hàm và cách thức truy cập chúng, sau đó ta sử dụng thông tin ở WSDL để tạo nên một yêu cầu SOAP, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 1.1 và được xếp vào phần Tiêu chuẩn về kết nối.

4.4 Tiêu chuẩn Tích hợp, Khám phá và Mô tả toàn cầu (Universal Description & Discovery Interface, UDDI)

Nguồn tài liệu:

www.oasis-open.org/committees/uddi-spec/doc/ tcspecs.htm.

Nội dung: UDDI lưu trữ thông tin liên quan đến các dịch vụ web với giao diện được miêu tả bằng WSDL và giao tiếp với nhau qua SOAP, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 1.3 và được xếp vào phần Tiêu chuẩn về kết nối.

4.5 Tiêu chuẩn an ninh dịch vụ web (Web Services Security, WS-Security)

Nguồn tài liệu:

WS-Security phiên bản 1.0: www.oasis-open.org/standards#wssv1.0;

WS-Security phiên bản 1.1: www.oasis-open.org/standards #wssv1.1.

Nội dung: Là một tiêu chuẩn nhằm bổ sung thêm cho việc bảo đảm an toàn dịch vụ web SOAP, trong Thông tư 01/2011/TT-BTTTT khuyến nghị áp dụng phiên bản 1.1 và được xếp vào phần Tiêu chuẩn về an toàn thông tin. Lý do khuyến nghị áp dụng là bởi vì nếu không có WS-Security thì chúng ta cũng có thể bảo mật kênh truyền dữ liệu thông qua HTTPS, ngoài ra WS-Security chỉ là một trong những lớp bảo mật cho dịch vụ web (xem Hình 3), có thể có thêm các thành phần khác tham gia vào bảo mật dịch vụ web như WS-Trust, WS-Policy, WS-Authentication, WS-Secure.

4.6 Tiêu chuẩn dịch vụ web cho ứng dụng từ xa (Web Services for Remote Portlets, WSRP)

Nguồn tài liệu:

WSRP phiên bản 1.0: www.oasis-open.org/ standards#wsrpv1.0;

WSRP phiên bản 2.0: www.oasis-open.org/ standards#wsrpv2.0.

Nội dung: WSRP chỉ ra cách thức giao tiếp giữa một hệ thống nền tảng với một hệ thống ứng dụng từ xa thông qua dịch vụ web, các hệ thống ứng dụng tuân thủ tiêu chuẩn này có thể chạy trên bất kỳ một hệ thống nền tảng nào áp dụng tiêu chuẩn WSRP mà không cần quan tâm đến việc ứng dụng hay hệ thống nền tảng

được xây dựng trên công nghệ/ngôn ngữ nào, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 1.0, khuyến nghị áp dụng phiên bản 2.0 và được xếp vào phần Tiêu chuẩn về truy cập thông tin. Lý do bắt buộc áp dụng phiên bản 1.0 và khuyến nghị áp dụng phiên bản 2.0 là vì một số sản phẩm về cổng thông tin điện tử chưa hỗ trợ phiên bản 2.0.

4.7 Tiêu chuẩn JSR 168 (Java Specification Requests 168)

Nguồn tài liệu:

JSR168: www.jcp.org/ja/jsr/detail?id=168;

JSR268: www.jcp.org/en/jsr/detail?id=268.

Nội dung: JSR168 chỉ ra cách tương tác giữa phần ứng dụng với phần nền tảng, các ứng dụng tuân thủ tiêu chuẩn này sẽ có thể hoạt động được ở tất cả các nền tảng tuân thủ/hỗ trợ tiêu chuẩn JSR168. Ví dụ: một ứng dụng nghiệp vụ do hãng A phát triển tuân thủ theo tiêu chuẩn JSR168 thì có thể chạy trên nền tảng của hãng B mà không phải biên dịch lại hoặc sửa đổi mã cho tương thích, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng JSR168, khuyến nghị áp dụng JSR268 và được xếp vào phần Tiêu chuẩn về truy cập thông tin. Lý do bắt buộc áp dụng JSR168 và khuyến nghị áp dụng JSR286 là vì một số sản phẩm về cổng thông tin điện tử chưa hỗ trợ phiên bản JSR268.

4.8 Giao thức truyền siêu văn bản (HyperText Transfer Protocol, HTTP)

Nguồn tài liệu:

www.w3.org/Protocols/rfc2616/rfc2616.html

Nội dung: HTTP là một trong năm giao thức cơ bản trong mạng Internet, nó cho phép xác định phương pháp định dạng và truyền tải các thông điệp (như các tệp văn bản, hình ảnh, âm thanh...) trong môi trường mạng, đối với hệ thống cổng thông tin điện tử HTTP được dùng để giao tiếp giữa Máy cung cấp dịch vụ (Web server) và Máy sử dụng dịch vụ (Web client), trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 1.1 và được xếp vào phần Tiêu chuẩn về kết nối.

4.9 Giao thức an toàn truyền siêu văn bản (HyperText Transfer Protocol over Secure Socket Layer, HTTPS)

Nguồn tài liệu:

www.ietf.org/rfc/rfc2818.txt

Nội dung: HTTPS là giao thức dựa trên HTTP và SSL/TLS để bảo mật trong quá trình giao tiếp giữa Máy cung cấp dịch vụ và Máy sử dụng dịch vụ, trong

Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng HTTPS và được xếp vào phần Tiêu chuẩn về an toàn thông tin.

4.10 Ngôn ngữ đánh dấu mở rộng cho giao dịch điện tử (Electronic Business using eXtensible Markup Language, ebXML)

Nguồn tài liệu:

www.ebxml.org/

Nội dung: ebXML có vai trò trong việc quy định việc định dạng văn bản cho giao dịch điện tử, đây là tiêu chuẩn được đề nghị bởi OASIS và UN/CEFACT, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 2.0 và được xếp vào phần Tiêu chuẩn tích hợp dữ liệu, ebXML cũng được Bộ Khoa học và Công nghệ công bố thành tiêu chuẩn Việt Nam tại Quyết định số 1670/QĐ-BKHCN ngày 14 tháng 8 năm 2007.

4.11 Ngôn ngữ đánh dấu không dây (Wireless Markup Language, WML)

Nguồn tài liệu:

www.openmobilealliance.org/Technical/wapindex.aspx

Nội dung: WML là một ngôn ngữ dựa trên XML được thiết kế dành riêng cho mục đích tạo ra những ứng dụng gửi lên mạng không dây đến những thiết bị nhỏ gọn như điện thoại di động, trong Thông tư 01/2011/TT-BTTTT bắt buộc áp dụng phiên bản 2.0 và được xếp vào phần Tiêu chuẩn về truy cập thông tin.

Dưới đây là bảng tổng kết về một số tiêu chuẩn hoặc giao thức chính sử dụng trong hệ thống cổng thông tin điện tử được đề cập trong Thông tư số 01/2011/TT-BTTTT ngày 04 tháng 01 năm 2011 của Bộ Thông tin và Truyền thông về việc Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước, việc tuân thủ các tiêu chuẩn này sẽ góp phần thúc đẩy sự phát triển của chính phủ điện tử nói chung và cổng thông tin điện tử nói riêng.

Loại tiêu chuẩn	STT	Tên tiêu chuẩn đầy đủ (Tiếng Anh)	Viết tắt	Tên tiêu chuẩn (Tiếng Việt)	Quy định áp dung trong Thông tư 01/2011/TT-BTTTT
Tiêu chuẩn về truy cập thông tin	1	Java Specification Requests 168/268	JSR 168/268	Tiêu chuẩn portlet API	Bắt buộc áp dụng phiên bản JSR 168 Khuyến nghị áp dụng phiên bản JSR 268
	2	Wireless Markup Language	WML	Ngôn ngữ đánh dấu	Bắt buộc áp dụng phiên bản 2.0

Loại tiêu chuẩn	STT	Tên tiêu chuẩn đầy đủ (Tiếng Anh)	Viết tắt	Tên tiêu chuẩn (Tiếng Việt)	Quy định áp dụng trong Thông tư 01/2011/TT-BTTTT
				không dây	
	3	Web Services for Remote Portlets	WSRP	Tiêu chuẩn dịch vụ web cho ứng dụng từ xa	Bắt buộc áp dụng phiên bản 1.0 Khuyến nghị áp dụng phiên bản 2.0
Tiêu chuẩn tích hợp dữ liệu	1	eXtensible Markup Language	XML	Ngôn ngữ đánh dấu mở rộng	Bắt buộc áp dụng phiên bản 1.0 và phiên bản 1.1
	2	Electronic Business using eXtensible Markup Language	ebXML	Ngôn ngữ đánh dấu mở rộng cho giao dịch điện tử	Bắt buộc áp dụng phiên bản 2.0
Tiêu chuẩn về an toàn thông tin	1	Web Services-Security	WS-Security	Tiêu chuẩn an ninh dịch vụ web	Khuyến nghị áp dụng phiên bản 1.1
	2	HyperText Transfer Protocol over Secure Socket Layer	HTTPS	Giao thức an toàn truyền siêu văn bản	Bắt buộc áp dụng
Tiêu chuẩn về kết nối	1	Universal Description & Discovery Interface	UDDI	Tiêu chuẩn Tích hợp, Khám phá và Mô tả Toàn cầu	Bắt buộc áp dụng phiên bản 1.3
	2	Web Services Definition Language	WSDL	Ngôn ngữ định nghĩa dịch vụ web	Bắt buộc áp dụng phiên bản 1.1
	3	Simple Object Access Protocol	SOAP	Giao thức truy cập đối tượng đơn giản	Bắt buộc nghị áp dụng phiên bản 1.2
	4	HyperText Transfer Protocol	HTTP	Giao thức truyền siêu văn bản	Bắt buộc áp dụng phiên bản 1.1

Giải thích thuật ngữ

Tiếng Anh	Tiếng Việt
Application Programing Interface (API)	Giao diện lập trình ứng dụng
Backend systems	Hệ thống phụ trợ
Client	Máy khách
Collaboration	Cộng tác
Content dynamic	Động về nội dung
Content management	Quản trị nội dung
Content providers	Nhà cung cấp nội dung
Content syndication	Xuất bản nội dung
ERP (Enterprise Resource Planning)	Hoạch định nguồn lực doanh nghiệp
Java Community Process	Tiến trình cộng đồng java (là một cơ chế chính thức cho phép các bên quan tâm phát triển các đặc tả tiêu chuẩn kỹ thuật công nghệ java)
JSR (Java Specification Request)	Yêu cầu đặc tả Java
OASIS (Organization for the Advancement of Structured Information Standards)	Tổ chức tiêu chuẩn về nâng cao thông tin có cấu trúc
PDA (Personal Digital Assistant)	Thiết bị số cá nhân
Personalization	Cá nhân hóa
Portal application /portlet	Thành phần ứng dụng
Portal architecture	Kiến trúc cổng thông tin điện tử
Portal framework/portal server	Thành phần nền tảng
Portal Topology	Sơ đồ cổng thông tin điện tử
Remote portlet	Hệ thống ứng dụng từ xa
Security	Bảo mật
Server	Máy chủ/máy phục vụ
Structure dynamic	Động về cấu trúc
UN/CEFACT (United Nations Centre for Trade facilitation and Electronic Business)	Tổ chức liên hiệp quốc về thương mại điện tử
Voice gateway	Cổng thoại
WAP gateway	Cổng WAP
Web portal	Cổng thông tin điện tử
Web Services	Dịch vụ web
World Wide Web Consortium (W3C)	Liên minh web toàn cầu