

GIẢI PHÁP OTP (ONE TIME PASSWORD) TĂNG CƯỜNG AN TOÀN BẢO MẬT THÔNG TIN CHO DOANH NGHIỆP

KS. Nguyễn Minh Đức

Phòng NCPT Ứng dụng Viễn thông

Tóm tắt: Giải pháp OTP (One Time Password) hiện tại ở Việt Nam đang được ứng dụng khá mạnh ở lĩnh vực ngân hàng trong các khâu thanh toán, rút tiền. Ở một số lĩnh vực khác cũng áp dụng giải pháp OTP vào phục vụ chủ yếu cho các khâu liên quan đến giao dịch, xác thực. Giải pháp OTP của CDIT được phát triển dựa trên web-base, có khả năng tương thích với nhiều nền tảng phát triển phần mềm nổi tiếng hiện nay. Với cơ chế bảo mật có độ tin cậy cao đi kèm với giá thành rẻ, trong tương lai giải pháp OTP sẽ thay thế dần công nghệ RSA, một công nghệ bảo mật nổi tiếng nhưng khá tốn kém. Bài báo này sẽ giới thiệu về nền tảng công nghệ, giải pháp kỹ thuật và hướng triển khai cũng như ứng dụng thực tế.

1. GIỚI THIỆU

Nền tảng phát triển ứng dụng trên nền web đang phát triển không ngừng trong 10 năm trở lại đây, dần thay thế hoàn toàn các ứng dụng desktop với mô hình cổ điển client – server. Cũng từ đó mà mọi con mắt đều dồn về phía ứng dụng trên mạng với 2 mục đích chính: tìm mọi cách để phá hoại và lấy được thông tin, dữ liệu. Một trong những chìa khóa giúp hacker khai thác được dữ liệu của doanh nghiệp một cách dễ dàng nhất đó là vấn đề về Xác thực (Authentication), thường được sử dụng một cặp thông tin tài khoản truy cập và mật khẩu. Việc tấn công thường hướng đến những thành viên giữ vị trí chủ chốt, hay lãnh đạo trong tổ chức, doanh nghiệp là có nguy cơ bị tấn công nhiều nhất.

Giải pháp OTP do Viện Công nghệ Thông tin và Truyền thông cung cấp là giải pháp toàn diện dành cho tổ chức, doanh nghiệp. Giải pháp là sự kết hợp linh hoạt, mềm dẻo giữa 2 công nghệ tiên tiến hiện nay là OTP và SSO (Single Sign On), mang đến nhiều lợi ích cho tổ chức, doanh nghiệp như:

- Tăng cường khả năng an toàn bảo mật và đơn giản tối đa quá trình đăng nhập.
- Tiết kiệm chi phí rất nhiều so với các giải pháp OTP sử dụng token vật lý như RSA.
- Dễ dàng trong sử dụng cũng như quản trị vận hành.
- Đơn giản trong triển khai, tích hợp.

2. GIẢI PHÁP CÔNG NGHỆ

Đối với các doanh nghiệp lớn hiện nay việc ứng dụng công nghệ thông tin ngày một nhiều, đi kèm theo là nhu cầu bảo mật cho các ứng dụng đó cũng ngày một cấp thiết hơn. Hình dung chúng ta sẽ gặp rắc rối ra sao khi có tới 10 tài khoản cho 10 ứng dụng riêng biệt, rồi khi chúng ta lộ một trong những mật khẩu đó, nếu không có cách ngăn chặn kịp thời, hậu quả sẽ ra sao ?

Giải pháp OTP do Viện Công nghệ Thông tin và Truyền thông CDIT có thể giải quyết được những vấn đề nêu trên. Đây là một giải pháp an toàn bảo mật cho từng ứng dụng một cách tổng thể đem lại cho doanh nghiệp những lợi ích khi sử dụng như sau:

- Tập trung hóa các tài khoản trên các ứng dụng đơn lẻ, người dùng sẽ chỉ cần 01 tài khoản duy nhất để truy cập ứng dụng, dễ dàng cho việc quản lý người dùng cho Doanh nghiệp.
- Đem đến cho người dùng một tính năng vô cùng hữu dụng, đó là chỉ cần đăng nhập một lần (Single Sign On) là có thể khai thác toàn bộ các ứng dụng bên trong Doanh nghiệp, giải quyết triệt để bài toán quản lý quá nhiều tài khoản của người dùng.
- Để tăng cường bảo mật cho tài khoản duy nhất, ứng dụng OTP được trang bị giúp người dùng chủ động trong việc bảo vệ tài khoản của mình, tiết kiệm rất nhiều chi

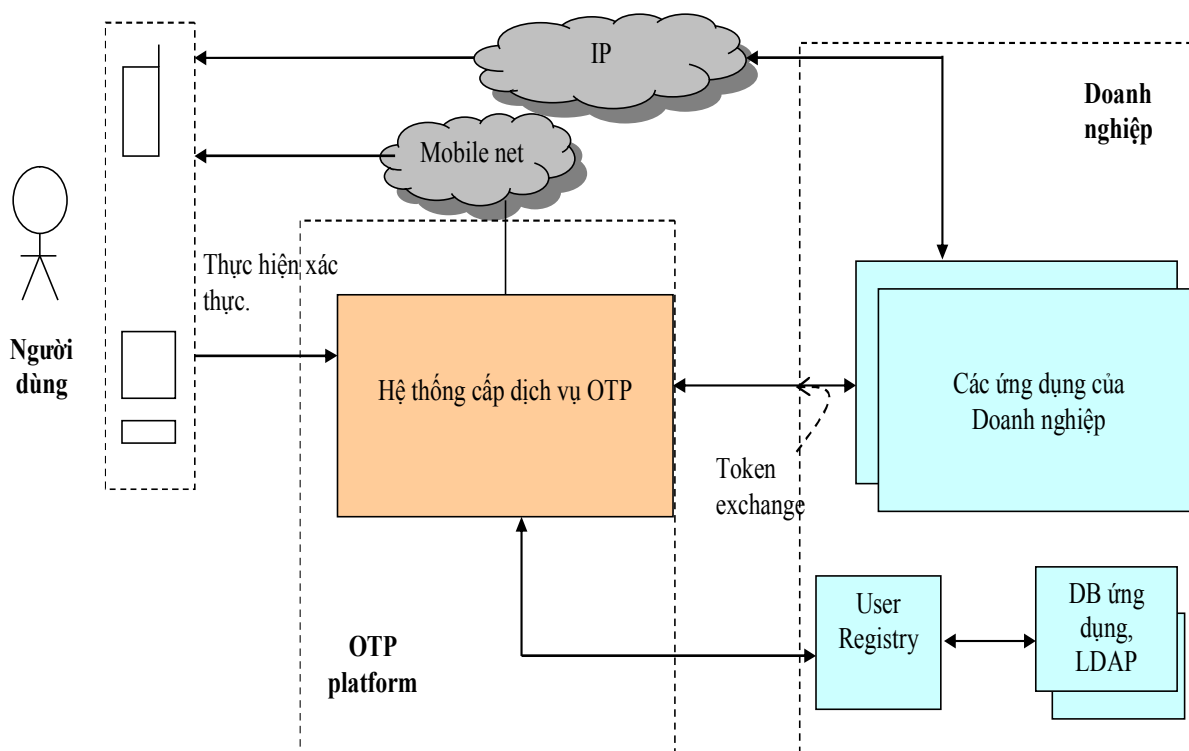
phí phần cứng cho doanh nghiệp so với nhiều giải pháp khác.

- Tăng cường khả năng bảo mật với hai cơ chế bảo mật đồng thời: đăng nhập bằng mật khẩu thông thường (có mã hóa dữ liệu trên đường truyền SSL) và cơ chế mật khẩu một lần (OTP), nghĩa là mật khẩu được sinh ra tại thời điểm người dùng login vào hệ thống thông qua SMS
- Cung cấp địa chỉ xác thực duy nhất và an toàn nhất trên toàn bộ hệ thống điều hành SXKD cũng như cung cấp dịch vụ khách hàng của đối tác.
- Hệ thống OTP được xây dựng trên nền tảng J2EE, hỗ trợ các công nghệ mã hóa và xác thực như sau:
 - Hỗ trợ Kerberos v5.
 - Hỗ trợ SSL v3.

- Hỗ trợ LDAP v3.
- Hỗ trợ SAML 2.0.
- Hỗ trợ SMPP 5.0.
- Jvm 1.7.
- Webservices.
- Hỗ trợ tích hợp nhiều ứng dụng nền tảng ngoài J2EE như: .NET, PHP, Flex...

3. KIẾN TRÚC HỆ THỐNG

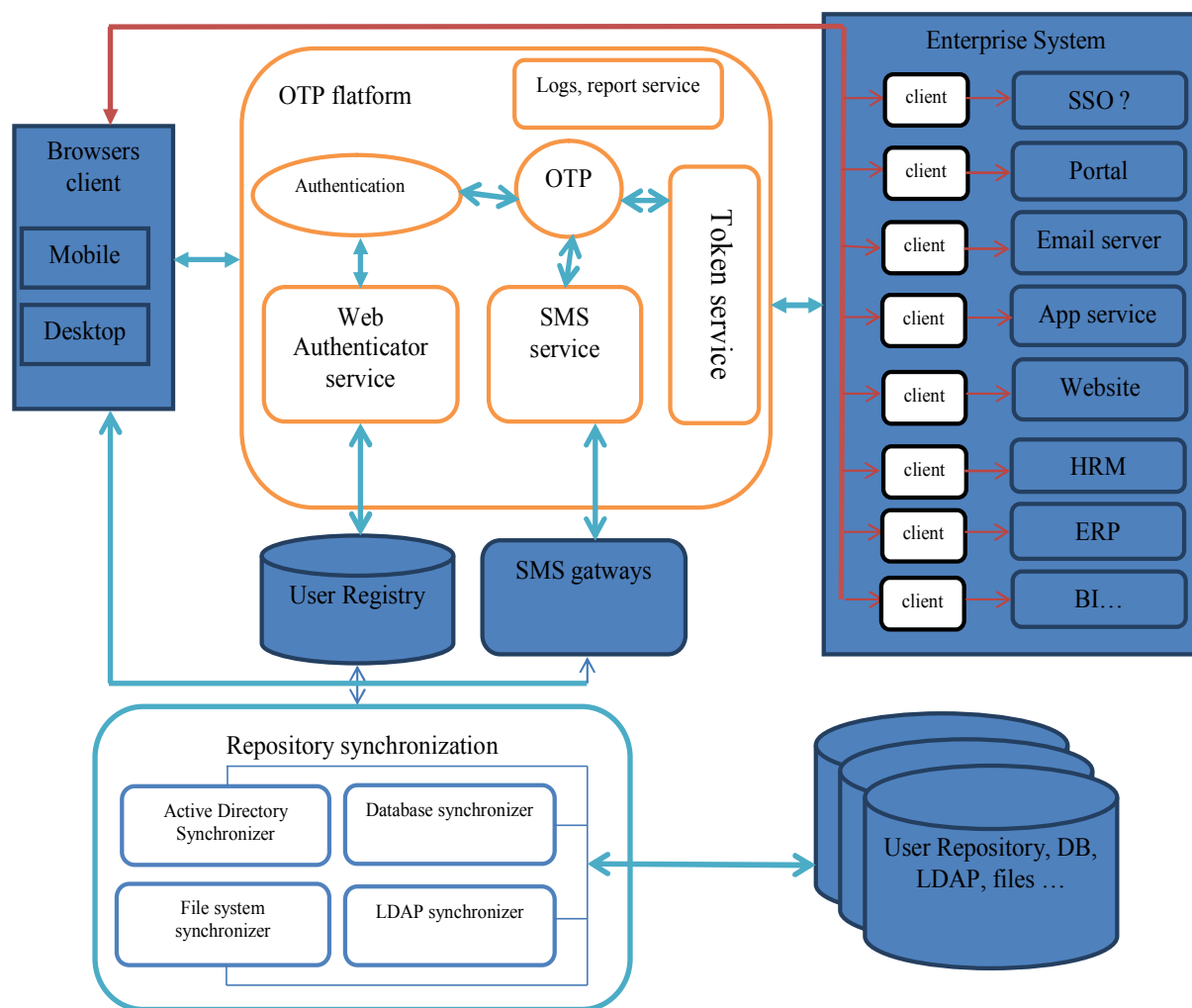
Về kiến trúc hệ thống, hệ thống OTP sẽ thay thế hoàn toàn phần xác thực (Authentication) của các ứng dụng được tích hợp, trở thành một cổng duy nhất cho mọi ứng dụng phía sau:



Hình 1. Mô hình tổng quan hệ thống OTP

Mô hình chi tiết kỹ thuật phía dưới sẽ mô tả rõ các thành phần của hệ thống khi triển khai trên mạng Doanh nghiệp, bao gồm phần lõi là hệ thống xác thực tập trung (SSO) và phần mềm OTP sẽ được CDIT xây dựng,

đồng bộ hóa các tài khoản người dùng, tích hợp các ứng dụng. Ngoài ra tất cả mọi giao dịch qua web đều phải được mã hóa SSL (sẽ đồng bộ với certificate của Doanh nghiệp):



Hình 2. Mô hình chi tiết kỹ thuật hệ thống OTP

Các chức năng chính của Hệ thống:

3.1. Chức năng SSO:

Được xây dựng dựa trên nền tảng CAS của đại học Yale Hoa Kỳ (sau này được chuyển giao cho tổ chức Jasig quản lý vào năm 2005) cung cấp khả năng bảo mật lần thứ nhất với chức năng đăng nhập một lần với một mật khẩu duy nhất, người dùng có thể khai thác toàn bộ các hệ thống được tích hợp trên hệ thống OTP. Tính năng SSO của hệ thống hoàn toàn độc lập với nền tảng ứng dụng và không hạn chế số lượng ứng dụng và lượng người truy cập. Một số lưu ý với chức năng SSO của hệ thống như sau:

- Hệ thống SSO hiện tại hỗ trợ ứng dụng nền tảng webbase.
- Hệ thống SSO có thể chạy ở các chế độ Load Balancing, High Availability tùy thuộc vào phần cứng.

- Hệ thống SSO yêu cầu người dùng phải cho phép sử dụng cookie trên trình duyệt.

3.2. Chức năng OTP:

Hệ thống cung cấp khả năng bảo mật lần hai với chức năng kiểm tra mật khẩu một lần, do hệ thống tạo ra và gửi tới máy di động của người dùng qua kỹ thuật OTT. Người dùng sẽ đăng nhập vào hệ thống sau khi hoàn tất việc xác thực mật khẩu một lần. Một số lưu ý với chức năng OTP như sau:

- Hệ thống OTP tự động tạo mật khẩu một lần và gửi tới máy điện thoại di động của người dùng, do vậy không giới hạn client, số máy và có thể tùy biến chuỗi mật khẩu tùy nhu cầu bảo mật và mức độ tiện dụng cho người dùng.
- Hệ thống OTP yêu cầu người dùng có máy điện thoại di động, có thể tùy biến

nhấn tin tới các nhà mạng tùy vào nhu cầu sử dụng và bảo mật thông tin.

3.3. Công cụ hỗ trợ các nhà quản trị

- Đóng mở việc xác thực OTP cho người dùng, lưu vết truy cập người dùng.
- Báo cáo thống kê truy cập.
- Đồng bộ dữ liệu người dùng với hệ thống cơ sở dữ liệu người dùng tập trung của doanh nghiệp.

4. QUY MÔ TRIỂN KHAI

Với khả năng xác thực kép tối ưu hóa quá trình xác thực, đơn giản nhưng rất an toàn, dễ sử dụng và quan trọng là tiết kiệm được nhiều chi phí so với các giải pháp sử dụng khóa token như RSA hay Chữ ký số... Hệ thống OTP còn mang đến khả năng triển khai mềm dẻo, quy mô hỗ trợ từ doanh nghiệp vừa và nhỏ cho tới những doanh nghiệp có quy mô ứng dụng Công nghệ thông tin lớn. Cụ thể áp dụng có các phương pháp triển khai cho từng dạng Doanh nghiệp khác nhau:

- Triển khai trọn gói trên hạ tầng Công nghệ thông tin của Doanh nghiệp, mô hình này dành cho các Doanh nghiệp vừa và lớn, triển khai tùy biến cả OTP và SSO.
- Cung cấp riêng dịch vụ OTP (không có dịch vụ SSO) dành cho các doanh nghiệp muốn tăng thêm khả năng bảo mật cho ứng dụng của mình nhưng không muốn đầu tư hạ tầng, nhân lực để vận hành hệ thống. Ngoài ra, các doanh nghiệp nhỏ thường chỉ cần thiết bảo mật cho một hay một số ứng dụng cần thiết.

5. ỨNG DỤNG THỰC TẾ

Đến nay, Viện công nghệ Thông tin & Truyền thông đã tiến hành triển khai thành công giải pháp OTP (One Time Password) cho các Tổ chức, Doanh nghiệp lớn, tiêu biểu là:

- Tập đoàn Bưu chính Viễn thông Việt nam: với hơn 30 ngàn thành viên truy cập hàng ngày. Hệ thống luôn sẵn sàng đáp ứng mọi yêu cầu gia tăng về lượng người cũng như tần suất của truy cập Tập đoàn khi cần. Ngoài ra còn rất nhiều các ứng

dụng nền tảng khác nhau được tích hợp phục vụ Tập đoàn.

- Văn phòng Quốc hội: với hơn 2000 thành viên quốc hội truy cập hàng ngày thì việc bảo mật cho từng thành viên là hết sức quan trọng.
- Công ty Thông tin Di động VMS: hiện đang triển khai cho hơn 20 ngàn thành viên của cơ quan, đơn vị thuộc công ty và rất nhiều các đại lý trên toàn quốc truy cập và khai thác các ứng dụng sản xuất kinh doanh.

6. KẾT LUẬN

Hệ thống OTP của Viện công nghệ Thông tin & Truyền thông là một trong những giải pháp độc đáo và khá thiết thực đối với các doanh nghiệp của Việt Nam tại thời điểm hiện tại và tương lai sắp tới. Hệ thống tập trung vào hai vấn đề khá cấp thiết hiện nay là tích hợp (SSO) và bảo mật (OTP). Doanh nghiệp, tổ chức đang phát triển không ngừng các ứng dụng CNTT trong quản lý và sản xuất hay người sử dụng dịch vụ cũng đã và đang ý thức hơn về dữ liệu của mình điển hình là khi sử dụng các dịch vụ internet banking, ví điện tử, game online... Tỉ lệ thuận với sự phát triển đó là sự dư thừa về dữ liệu người dùng, phức tạp trong bảo mật thông tin xác thực, qua đó rủi ro trong việc mất mát dữ liệu cũng sẽ ngày một gia tăng.

Hệ thống OTP của Viện công nghệ Thông tin & Truyền thông khi đưa ra bài toán tích hợp đã nhìn thấy trước được vấn đề này ở các doanh nghiệp Việt Nam. Hiện tại Hệ thống OTP đưa ra giải pháp kết nối (tích hợp) các ứng dụng hệ thống công nghệ thông tin của doanh nghiệp lại với nhau để thuận tiện cho người sử dụng hệ thống. Song song sẽ là việc quản lý người dùng tập trung cho toàn bộ hệ thống công nghệ thông tin, dần tới sẽ dễ dàng hơn nhiều trong vấn đề quản lý, bảo mật cũng như khắc phục các trường hợp dư thừa dữ liệu. Ngoài ra, hệ thống OTP còn giúp cho các sản phẩm công nghệ thông tin vốn đang rời rạc của doanh nghiệp trở thành một thể thống nhất, thuận tiện hơn cho doanh nghiệp trong vấn đề quản lý khai thác và phân tích dữ liệu.

Về phần bảo mật (OTP) thì như chúng ta đã biết, giải pháp OTP (One Time Password) hiện tại cũng không phải là mới mẻ khi nhiều ngân hàng và các doanh nghiệp tổ chức đã ứng dụng OTP vào nhằm bảo mật các hệ thống công nghệ thông tin của mình. Giải pháp OTP với các tính năng ưu việt của nó đã đang dần thay thế các công nghệ RSA. Hệ thống OTP của Viện công nghệ Thông tin & Truyền thông kế thừa tính ưu việt của giải pháp OTP và xây dựng hệ thống ứng dụng các công nghệ tiên tiến nhất và hỗ trợ nhiều công nghệ mã hóa xác thực như đã nói ở trên.

Trong thời gian tới, Hệ thống sẽ được nâng cấp hoạt động trên nền Cloud Computing, hỗ trợ đa thiết bị đặc biệt là Hệ thống sẽ ứng dụng thêm giải pháp xác thực vân tay, nhân dạng... để trở thành nhà cung cấp dịch vụ về bảo mật ứng dụng số một ở Việt nam dành cho mọi tổ chức, doanh nghiệp.

7. TÀI LIỆU THAM KHẢO:

1. Tìm hiểu giao thức Kerberos:
[http://en.wikipedia.org/wiki/Kerberos_\(protocol\)](http://en.wikipedia.org/wiki/Kerberos_(protocol))
2. Tìm hiểu giải pháp CAS:
<http://www.jasig.org/cas>,
<http://www.yale.edu/tp/auth/cas20.html>
3. Tìm hiểu giải pháp OTP:
http://en.wikipedia.org/wiki/One-time_password
4. Giải pháp OTP của McAfee:
<http://www.mcafee.com/us/products/one-time-password.aspx>

Thông tin tác giả:



Nguyễn Minh Đức

Sinh năm: 1980

Lý lịch khoa học:

- Tốt nghiệp Đại học chuyên ngành Điện tử Thông tin tại Viện Đại học Mở Hà Nội.
- Hiện đang công tác tại Phòng NCPT Ứng dụng Viễn thông thuộc Viện công nghệ Thông tin và Truyền thông – CDIT, Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu hiện nay: Bigdata, Data Mining, Authentication Protocols, System Information Architecture, Solutions Software for Enterprise.

Email: ducnm@ptit.edu.vn