GIẢI PHÁP XÁC THỰC MỘT LẦN SỬ DỤNG GIỌNG NÓI (VOICE OTP) CHO VNPT

ThS. Vũ Tuấn Anh

Email: vtanh@ptit.edu.vn

Tóm tắt*: Bài báo giới thiệu giải pháp xác thực một lần sử dụng thông báo bằng giọng nói (Voice OTP) do Viện CDIT xây dựng cho Tập đoàn Bưu chính Viễn thông Việt Nam VNPT.*

Từ khóa*: VNPT, IP network, Voice OTP.*

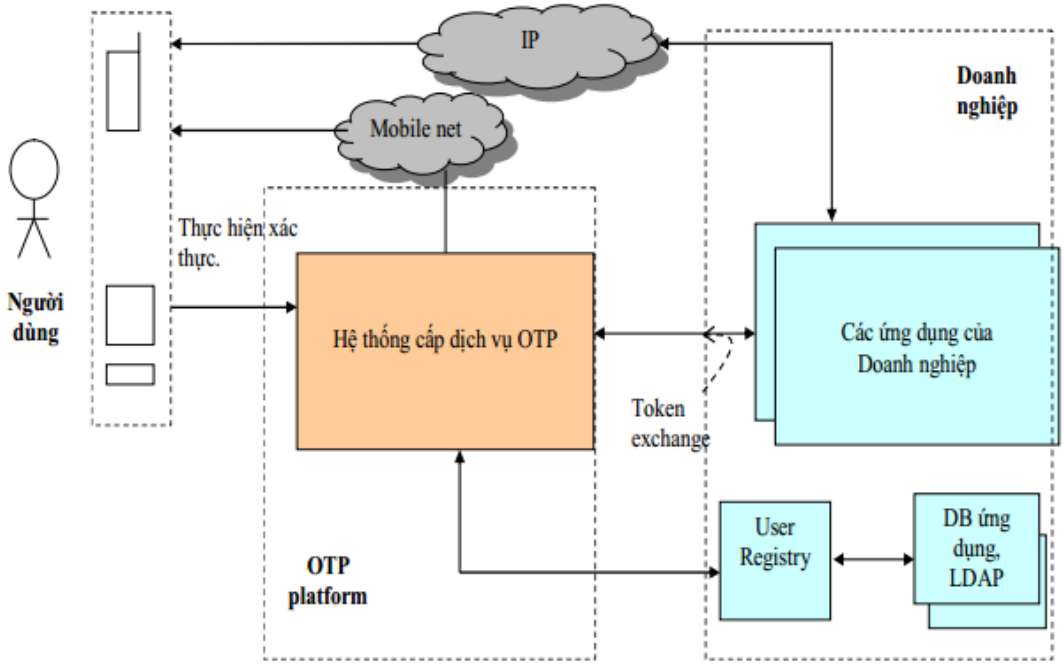
1. GIỚI THIỆU CHUNG

One Time Password (OTP) là dạng mật khẩu sử dụng một lần với một chuỗi số hoặc chuỗi kết hợp cả số với ký tự. Mã này có thể tồn tại trong một khoảng thời gian rất ngắn trước khi vô tác dụng và được thay thế bằng một mã mới.

Lợi ích của OTP là nó chống được tấn công phát lại, nghĩa là nếu có một ai đó có thể lấy được thông tin về OTP trong một phiên làm việc thì cũng không thể sử dụng nó để đăng nhập vào lần kế tiếp. Với lợi thế như vậy, OTP được sử dụng khá phổ biến như là lớp bảo vệ thứ hai cho các tài khoản ngân hàng điện tử, thanh toán trực tuyến, email hay mạng xã hội. Khi muốn chuyển tiền hay thực hiện một giao dịch trực tuyến, ngoài tên tài khoản và mật khẩu đăng nhập, người dùng còn phải thực hiện thao tác nhập đúng mã xác thực OTP để hoàn tất.

Sau khi đã đăng ký dịch vụ, mỗi lần muốn đăng nhập (log in), hay thực hiện bất kì thao tác sử dụng dịch vụ nào yêu cầu tính xác thực cao, người dùng sẽ được cung cấp một mật khẩu tạo ra bởi đầu đọc và thẻ thông minh hay thiết bị tạo mật khẩu dạng cầm tay (token) nhờ vào kết nối internet với máy chủ cung cấp dịch vụ OTP, hoặc cũng có thể thông qua thẻ OTP được tạo sẵn hay điện thoại di động. Mật khẩu này sẽ tự mất hiệu lực sau khi người dùng thực hiện tác vụ thành công hoặc sau một thời gian ngắn. Như vậy, nếu bị lộ mật khẩu thì người có được mật khẩu đó cũng không thể dùng được, và do đó giải pháp OTP có tính bảo mật cao.

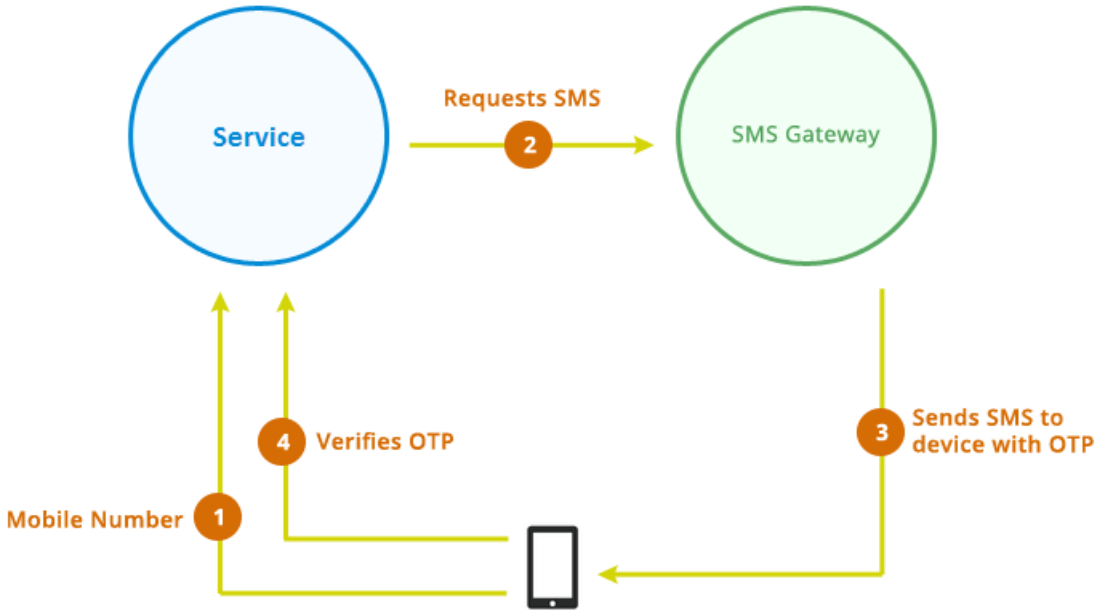
Quá trình tạo mật khẩu mới sẽ lặp lại mỗi lần người dùng đăng nhập vào hệ thống được bảo mật bằng OTP. Công nghệ OTP được dùng nhiều trong chứng thực trực tuyến (thương mại trực tuyến). Hiện nay người dùng các thiết bị cầm tay như iPhone, Blackberry cũng có thể tự cài đặt cơ chế bảo mật OTP bằng các chương trình như VeriSign, RSA SecureID hay SafeNet MobilePASS.



Hình 1: Mô hình tổng quan hệ thống OTP

1.1. Mật khẩu xác thực gửi qua tin nhắn SMS

Đây là hình thức phổ biến nhất hiện nay, hệ thống sẽ gửi một tin nhắn SMS chứa OTP tới số điện thoại mà người dùng đăng kí để xác nhận thao tác trên hệ thống là đúng của người đó.



Hình 2: Quá trình xác thực với OTP

Rất nhiều công ty và dịch vụ, ứng dụng đã áp dụng phương thức xác thực này vì nó tiện lợi với người sử dụng. Các tên tuổi nổi bật là Google, Facebook, Microsoft, Twitter, WhatsApp,...

Hình 3: Xác thực mật khẩu Facebook dùng SMS

Tuy nhiên, tin nhắn SMS có thể bị foward hoặc chặn xem bởi bên thứ ba, đây là một điểm yếu của giải pháp này, nhưng nhìn chung, SMS OTP vẫn được xem như một phương thức khá tiện lợi và an toàn trong xác thực truy cập hệ thống và dịch vụ.

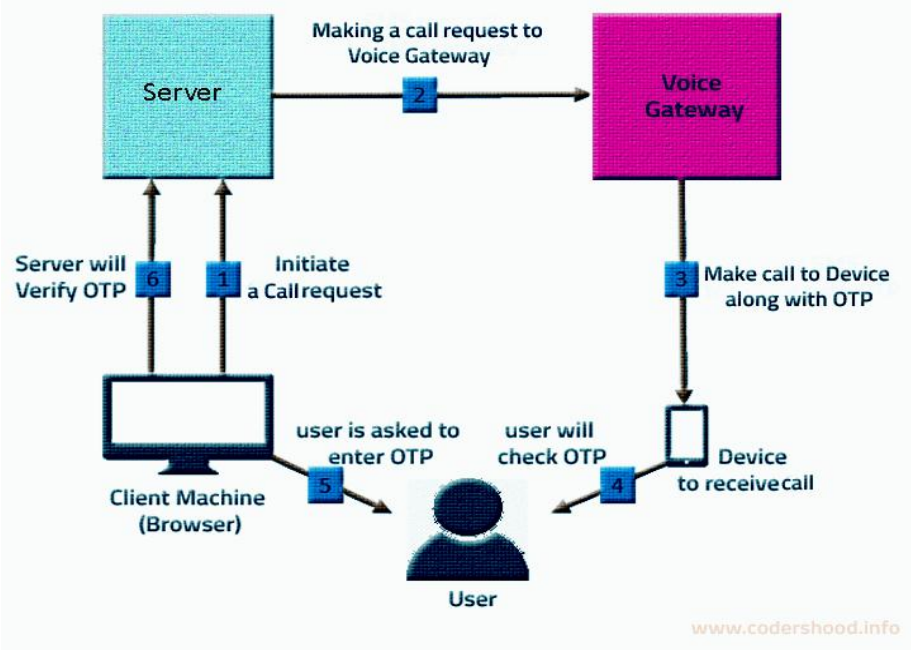
1.2. Mật khẩu xác thực gửi bằng giọng nói qua kênh thoại (Voice OTP)

Giải pháp Voice OTP ra đời góp phần mở rộng khả năng xác thực OTP, ở đây, mật khẩu xác thực được chuyển thành giọng nói và gửi qua mạng thoại.

Voice OTP đã được khá nhiều nhà cung cấp dịch vụ trên thế giới sử dụng cho hệ thống của mình, các tên tuổi nổi bật có thể kể đến là Google, Facebook, Microsoft,... nhưng tại Việt Nam, giải pháp này còn khá mới mẻ, chưa thực sự phổ biến. Các ngân hàng, các tổ chức tín dụng là những đơn vị thường xuyên sử dụng giải pháp xác thực OTP như: Ngân hàng Á Châu, Vietcom Bank, DongA Bank, Techcombank,… hiện đang gửi mã OTP đến khách hàng của mình chủ yếu thông qua kênh SMS.

Giải pháp gửi mật khẩu qua SMS gần đây liên tiếp xảy ra các vụ lùm xùm xoay quanh vấn đề bảo mật được truyền thông đưa tin, nhiều khách hàng bị rút tiền trong tài khoản mà không hề hay biết cho đến khi kiểm tra số dư trong thẻ. Hacker có thể lấy được mã OTP của khách hàng sử dụng SMS OTP chỉ với vài thủ thuật: đầu tiên, kẻ gian sẽ cài mã độc dưới một ứng dụng hấp dẫn cho người dùng tải về, yêu cầu quyền được đọc/xóa tin nhắn. Tiếp đó, ứng dụng sẽ đánh cắp dữ liệu của người dùng. Sau khi có được tài khoản đăng nhập, hacker sẽ thực hiện chuyển tiền qua Internet Banking. Tất nhiên lúc này một SMS OTP sẽ được gửi về smartphone của người dùng. Một lần nữa, ứng dụng kia sẽ đọc OTP và gửi lại cho hacker, đồng thời xóa SMS OTP kia. Đây cũng là một lợi thế của Voice khi mà hacker không thể đọc OTP từ cuộc gọi khi chúng không phải người nghe máy.

Mô hình xác thực OTP sử dụng Voice thay cho SMS như hình 3.

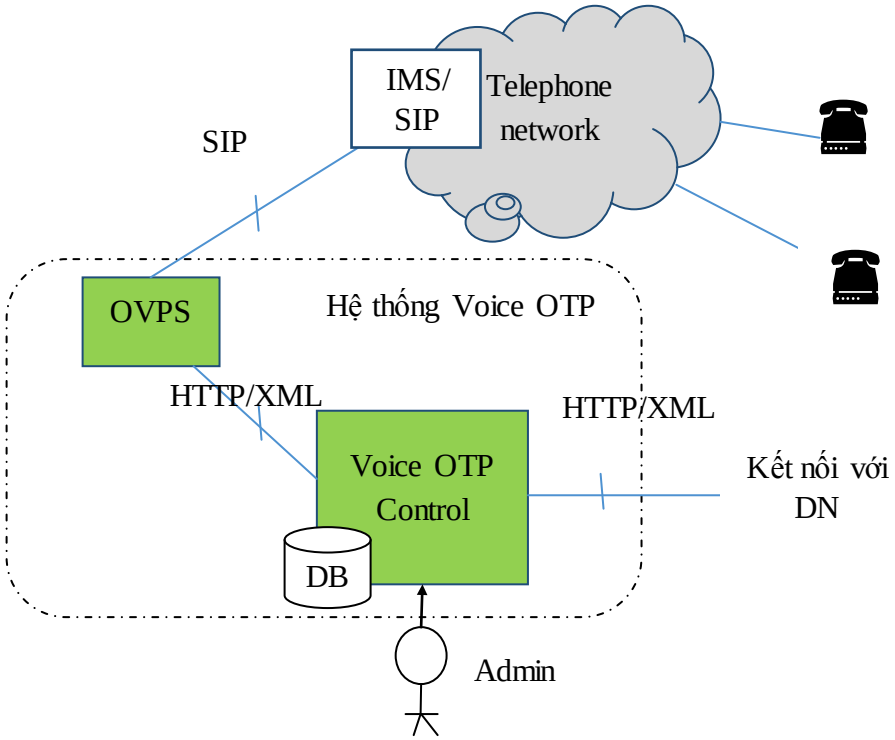


Hình 4: Mô hình tổng quan hệ thống Voice OTP

2. GIẢI PHÁP Voice OTP CỦA CDIT

2.1. Mô tả giải pháp

a) Kiến trúc giải pháp



Hình 5: Mô hình kiến trúc giải pháp

Giải pháp Voice OTP của CDIT gồm 2 thành phần: OVPS (OTP Voice Play Server) và Voice OTP Control.

OVPS là thực thể thực hiện chức năng VoIP Gateway, có chức năng tạo cuộc gọi Voice tới mạng thoại, chuyển mật khẩu từ kí tự hay số sang giọng nói. OVPS có 2 giao diện:

- Giao diện với mạng Voice sử dụng báo hiệu SIP và kết nối với hệ thống IMS hiện tại do các nhà mạng quản lý.
- Giao diện với hệ thống Voice OTP Control, sử dụng webservice,

Voice OTP Control: Thực hiện các chức năng cấu hình và điều khiển các hoạt động xác thực Voice. Thành phần này có 2 giao diện:

- Giao diện cấu hình/điều khiển OVPS và
- Giao diện giao tiếp với các doanh nghiệp/các hệ thống khác để nhận yêu cầu khởi động phiên xác thực Voice OTP,

Lưu đồ hoạt động:

- Các doanh nghiệp đăng kí sử dụng dịch vụ sẽ được cung cấp tài khoản riêng, khi người dùng cuối thực hiện chức năng đăng nhập hay giao dịch, hệ thống của doanh nghiệp sẽ gửi thông tin về tài khoản được cấp, cũng như số điện thoại và đoạn mã code đến hệ thống Voice OTP control.
- Khi nhận được yêu cầu, hệ thống Voice OTP control sẽ kiểm tra thông tin doanh nghiệp có hợp lệ không từ cơ sở dữ liệu. Nếu hợp lệ, hệ thống sẽ thực hiện gửi mã và số điện thoại đến OVPS để play Voice.
- Sau khi OVPS thực hiện cuộc gọi ra đến thuê bao và tùy theo kết quả sẽ trả về kết quả báo cho Voice OTP control biết có cần retry hay không.
- Nếu cuộc gọi thành công, khách hàng của doanh nghiệp sẽ nhập lại chuỗi mã vừa được nghe để xác thực giao dịch trên hệ thống của doanh nghiệp (thường là trang web).

b) Chức năng của giải pháp

Các chức năng chính của giải pháp:

- Quản lý cấu hình cho thực thể OVPS,
- Quản trị tài khoản
- Quản lý cuộc gọi
- Quản trị thông báo OTP
- Giới hạn số lần query/s
- Quản lý log cuộc gọi và log hệ thống
- Điều khiển OVPS
  - Khởi tạo cuộc gọi: yêu cầu play thông báo OTP
  - Dừng cuộc gọi: Yêu cầu dừng thông báo OTP

- Kiểm tra trạng thái hiện tại của cuộc gọi

– Báo cáo định kỳ và đột xuất

– Quản lý blacklist.

c) API giao tiếp giữa hệ thống Voice OTP control và OVPS

– API #1-Tạo cuộc gọi (makeCall): Bản tin được thực hiện để yêu cầu SIPGW thực hiện cuộc gọi đến 1 thuê bao và play file audio với mã code mong muốn.

– API #2-Tra cứu trạng thái cuộc gọi (callStatus): Bản tin tra cứu thông tin hiện tại cuộc gọi.

– API #3-Ngắt cuộc gọi (dropCall): Bản tin yêu cầu SIPGW thực hiện ngắt cuộc gọi đang diễn ra.

– API #4-Thông báo kết quả cuộc gọi (callNotification): Bản tin thông báo kết quả cuộc gọi được SIPGW chủ động gửi sang Webservice của hệ thống mở rộng nhằm thông về kết quả cuộc gọi ra và hệ thống mở rộng đã tạo ra trước đó.

– API #5-Cấu hình hệ thống: Bản tin yêu cầu SIPGW thực hiện thay đổi tham số cấu hình hệ thống.

d) Một số đặc điểm khác của hệ thống

Hệ thống Voice OTP của CDIT hỗ trợ:

– Sử dụng SIP làm giao thức kết nối với mạng thoại, tương thích với báo hiệu SIP Trunk của hệ thống IMS của các nhà mạng ở Việt nam.

– Có khả năng thực hiện 50 cuộc gọi ra đồng thời,

– Có khả năng play các số từ 0..9 và các ký tự từ a..z.

– Giao tiếp với các doanh nghiệp/hệ thống thông tin khác dùng webservice

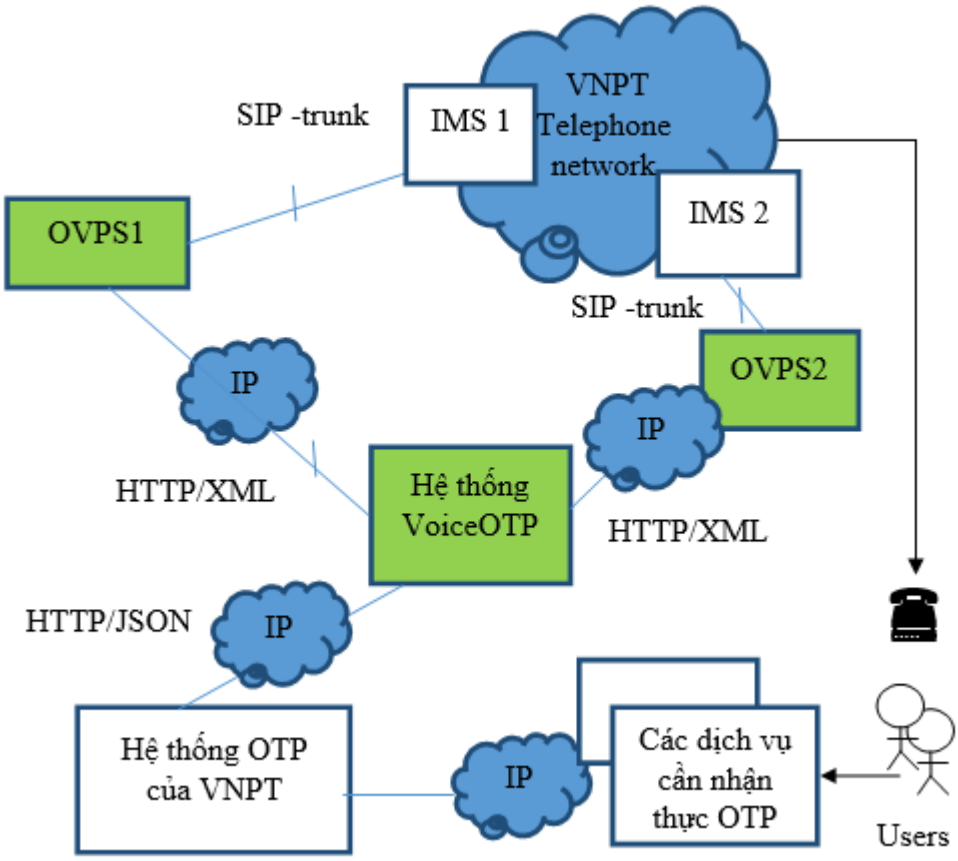
2.2. Triển khai giải pháp Voice OTP cho VNPT

VNPT hiện đã sử dụng hệ thống xác thực 1 lần dùng SMS (cũng do CDIT cung cấp trước đây). Giải pháp được yêu cầu ở đây nhằm mở rộng khả năng xác thực OTP hiện nay lên hỗ trợ Voice mà điển hình là mục tiêu thông báo mã OTP qua mạng điện thoại. Yêu cầu hệ thống Voice OTP cần tương thích với báo hiệu SIP Trunk của VNPT IMS,

Căn cứ vào tổ chức mạng kết nối thoại của VNPT, CDIT đề xuất kết nối thực thể này vào mạng hiện nay của VNPT như hình 5:

– Thực hiện phương án dự phòng chia tải trên 2 hệ thống OVPS1 và OVPS2. Các OVPS1 và OVPS1 2 nối vào các IMS1 (Hà nội) và IMS2 (TPHCM) tương ứng và hoạt động ở chế độ Call-out.

– Giao diện kết nối với hệ thống OTP SMS cũ của VNPT để nhận lệnh yêu cầu xác thực Voice



Hình 2: Kết nối giải pháp vào mạng VNPT

Từ năm 2017, Tập đoàn VNPT đã đưa hệ thống vào sử dụng chính thức cung cấp tiện ích xác thực cho người dùng truy nhập các hệ thống thông tin của VNPT

3. KẾT LUẬN

Giải pháp Voice OTP do CDIT xây dựng và triển khai cho VNPT góp phần làm tăng tiện ích hỗ trợ xác thực một lần và tăng cường mức độ bảo mật cho hình thức xác thực này. Giải pháp này có thể xây dựng thành dịch vụ độc lập cung cấp cho các doanh nghiệp khác như một tiện ích nâng cao độ bảo mật trong truy cập các hệ thống nội bộ.

TÀI LIỆU THAM KHẢO

Tài liệu tiếng Việt

1. *Bảo mật trong giao dịch sử dụng công nghệ xác thực OTP*

   http://antoanthongtin.vn/Detail.aspx?CatID=b30679c6-ff8f-416f-a7b1-90921f26aea3&NewsID=9829cca2-5155-43b1-9beb-aab7d5c085ce

2. *Mã xác thực OTP và những rủi ro tiềm ẩn*

   https://thanhnien.vn/cong-nghe/ma-xac-thuc-otp-va-nhung-rui-ro-tiem-an-734020.html

3. *Thành trì bảo mật cuối cùng mang tên OTP có thể bị vượt qua như thế nào?*

http://genk.vn/hacker-co-the-lam-the-nao-de-vuot-qua-thanh-tri-bao-mat-cuoi-cung-mang-ten-otp-sau-do-an-cap-tien-cua-nan-nhan-20160812174328337.chn

Tài liệu tiếng Anh

4. *Authentication system using one-time passwords*

https://www.google.com/patents/US5661807

5. *Symantec™ Voice OTP Authentication Service Description*

https://www.symantec.com/content/en/us/about/media/repository/voice-otp-service-description.pdf