White Paper
mPollux CallSign Authentication

Fujitsu's strong authentication service based on mobile phones.

Contents

1 Introduction to mPollux™ CallSign

In the context of digitalization of services, securing of transactions is of ever-growing importance. Several different schemes exist for authentication of the user safeguarding transaction confidentiality.

User of e-business services benefits greatly from an authentication solution that

- Is easy to use
- Operates with any mobile phone
- Is secure

A strong authentication mechanism that enables several security levels makes authentication easy leading to customer satisfaction and trust in accessing valuable and critical services.

By definition, strong authentication means authentication that is based on at least two of the following factors:

- **Something that the user knows** (for example, password or PIN code)
- **Something that the user possesses** (for example, a smart card)
- **Something that the user is** (biometrics, for example palm vein diagram)

CallSign is Fujitsu Finland's answer to these needs. CallSign is an easy to use authentication service that provides trustworthy authentication to services. CallSign fulfils the requirement for strong authentication by two authentication factors with the phone as the "something user possesses" factor and the PIN number as "something that the user knows" factor. CallSign supports standards including SIP and SAML v.2.0.

2 mPollux™ CallSign service

CallSign relies on different mPollux™ components forming a comprehensive authentication solution. Once a user registers CallSign service to him, the phone number of his mobile phone and selected PIN number are stored into mPollux™ Server database. This database is often MS Active Directory, but can also be a SQL database or a LDAP based directory, and is often customer's own database. A hash value of the PIN is stored into a database and it is possible for users to change their PIN codes when wanted.

As a user wants to access a service, his request is redirected to mPollux™ WebFront proxy and mPollux™ Login application. At Login application user can choose an authentication option for the authentication if several options are available, otherwise user is redirected for authenticating using the default option in use.

As he chooses CallSign, the user is requested to enter a user ID to the service. The user ID can be name, email-address, or his phone number. Based on the user ID a search is made to check if the ID exists in the database and user's PIN is retrieved from the database.

After this a call from mPollux™ Server is made utilizing a VoIP server to the user. A voice prompt is played requesting the user to enter his PIN. As the user enters the pin from his handset keyboard, DTMF tones are sent to the mPollux™ VoIP server that detects them and passes to CallSign application for checking. If the PIN is correct an access granted prompt is played. If the PIN is not correct, an access denied prompt is played.

Once the user has entered correct PIN, user credentials are passed to the application through WebFront interface using cookies or http header fields. In addition, SAML 2.0 and mPollux Service API interfaces can be used.

CallSign's features include different dialing options, which provide a wide area of usage possibilities:

Authentication using dial-out

CallSign dials out to remote telephone number specified by the client application. Connected call is processed according to profile settings and may result authentication.

Authentication using dial-in to dynamically allocated phone number

CallSign server selects and returns a telephone number from configured telephone number pool to the client application. Only a call from a client (any or specific specified by the client application) to the reserved telephone number may result authentication.

Authentication using dial-in to fixed phone number

An incoming call to fixed telephone number reserved for the authentication request may result authentication.

Call notifications

Call notifications are relayed to the subscribing application and are used to determine whether authentication has occurred.

3 mPollux™ CallSign Authentication options

Security code option

CallSign can be further protected against spam with use of security codes. In this context spam means that someone who knows other person's user ID could try to make authentications generating authentication calls to the owner of the particular user ID.

In order to use a security code option, user registers a security code to his use. With all authentication attempts, he enters the user ID and the security code to a separate field specified for the security code. This code is verified against stored value before a call is made to user's phone.

One time pin

One time pin is an optional feature that can be used with CallSign authentication method for verifying that used phone number is registered. It is commonly used with reset and registration.

4 Key benefits of mPollux™ CallSign Authentication

The key business benefits of CallSign authentication service:

- Is easy to use
  - The service is easy to use and does not require training or user manuals to be utilized.
- Operates independent of mobile data connectivity
  - In many places, the mobile data connectivity may be weak, the network is congested or not available at all, but voice calls can be made.
- Operates with any mobile phone
  - People can use just plain phones without any phone-based applications common in smart phones. Also if a phone is lost the user requires just to get any working phone and SIM to get authentication capability.
- Relies on impossibility to forge phone's phone number
  - With two-factor authentication, the phone is used as the "something the user possesses" factor. The SIM and consequently the phone B-number is extremely difficult to copy leading to security.
- Does not require any applications in the phone
  - With CallSign no applications are employed, freeing the authentication service provider from the need to produce and manage different versions of phone applications. In addition, this makes life easier for the user and eliminates one possible security attack vector from authentication service.
- Provider as options selectable levels of security
  - CallSign employs several options to balance ease of use and authentication security levels. These options can be utilized enhance the already high security level of standard CallSign service to even higher levels.

5 Example use cases for mPollux™ CallSign Authentication

Authenticating to Extranet and Intranet services

Authenticating to Extranet and Intranet services user is required to remember only his PIN code for authenticating as the phone number is already configured to client applications number pool.

Similarly connecting to VPN using CallSign is also possible and requires user to remember only the personal PIN code.

For Intranet CallSign authentication can be used for replacing authentication with username and password. This can help in avoiding locked user accounts and DoS attacks.

Self-service for password reset using mPollux™ CallSign

CallSign can also be used for authenticating to password reset service. A self-service for password reset is also available as a service provided by Fujitsu.

Authentication using dial-out

Applications for CallSign authentication using dial out, thus where user enters his user ID or phone number for login service when wanting to authenticate and then service calls the user, are useful for:

- establishing a VPN connection
- authentication to web services
- recording of phone calls

Authentication services can also call directly to the user for authentication when user has been registered for the service and the service receives a trigger for beginning the authentication process. Such use cases can include the following:

- Authentication to mobile devices or applications – authentication service receives a notification that user is requesting to use the device or application and calls the user. This makes authentication easier as only PIN code is needed for authentication.

Authentication using dial-in

When authenticating using dial-in, user calls the authentication service and the service asks user to enter his PIN code. Possible use cases:

- Access control for physical places, e.g. car park
- Authentication to a voting machine
- Recording of phone calls

Call notifications

Call notifications can be used for determining whether authentication has occurred. User may call the authentication service for permission and the service checks if user is a registered user, no PIN code is asked. Possible use cases include the following:

- Access control for physical places, e.g. car park
- Authentication to a voting machine

6 Operating Environment

The Fujitsu mPollux™ product family runs on any standard Java Application Server platform. It requires a standard Java Virtual Machine and a user database. CallSign server software requires Red Hat Enterprise Linux operating system. Any Intel x86-based PC hardware is supported by the operating system. Fujitsu also offers the whole package as a service.

For more information, please contact:

Fujitsu Finland Oy
mPollux-Sales@fi.fujitsu.com

- https://www.fujitsu.com/fi/services/security/