Mobile ID
Citrix Netscaler/Web interface

Solution guide

Version: 1.0

swisscom

Contents

1 Introduction

The purpose of this document is to provide clarifications **how** to interface Mobile ID with Citrix NetScaler to authenticate a user with Mobile while using a Citrix Application.

This manual assumes that you are familiar with Citrix NetScaler and Swisscom Mobile ID.

More details about Mobile ID can be found in the Mobile ID SOAP client reference guide [1].

Terms and abbreviations

Abbreviation	Definition
ⓘ	Please note:
⚠	Be careful, important:
AP	Application Provider
DataToBeDisplayed DTBD	Data to be displayed
DataToBeSigned DTBS	Data to be signed
MSSP	Mobile Signature Service Provider
M-ID or MID	Mobile ID platform providing the mobile signature service
MSISDN	Number uniquely identifying a subscription in a GSM/UMTS mobile network
SOAP	Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured information in the implementation of Web Services relying on Extensible Markup Language (XML)
WS	A Web service (WS) is a method of communication between two electronic devices over the Web (Internet).

1.1 Referenced documents

[1] SOAP Client Reference Guide
[2] RADIUS Integration Guide
[3] Citrix NetScaler Gateway 10.1 - Configuring RADIUS Authentication
http://support.citrix.com/proddocs/topic/netscaler-gateway-101/ng-radius-configuration-tsk.html
[4] Citrix NetScaler Gateway 10.1 - RADIUS Authentication Policies
http://support.citrix.com/proddocs/topic/ns-security-10-1-map/ns-aaa-setup-policies-auth-radius-tsk.html
[5] Citrix Web Interface 5.4 - Enabling RADIUS Authentication
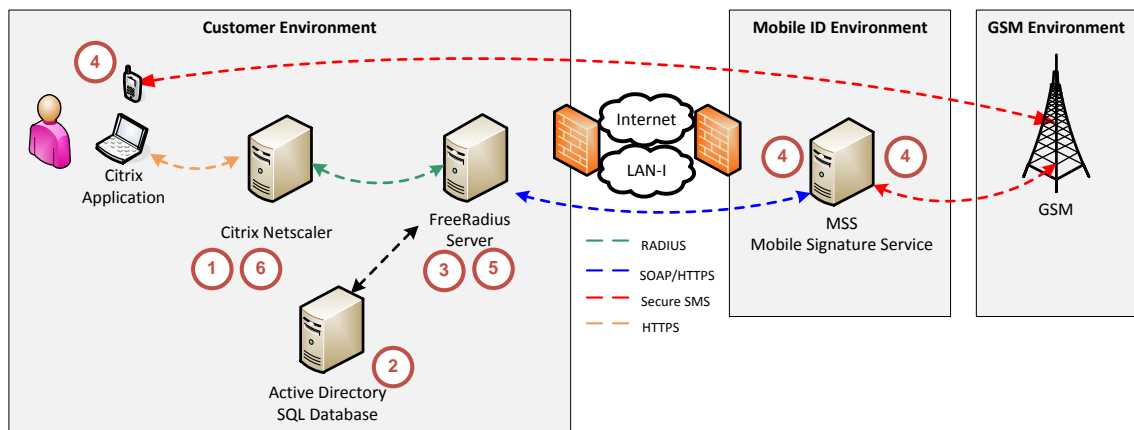http://support.citrix.com/proddocs/topic/web-interface-impington/wi-enable-radius-authentication-gransden.html

2   Overview and main scenario

This chapter describes a possible solution to "interface" a Citrix Netscaler product with Mobile ID.

The solution detailed in this guide is based on the available Radius interface at the Citrix NetScaler side. This interface communicates with a Radius server, in our case an on premise FreeRADIUS server. Basically it can be done with any Radius server that is extensible and would allow the integration of the Mobile ID. We documented such a Mobile ID integrated server based on FreeRADIUS in [2].

Scenario - Strong Authentication with Citrix NetScaler:

Before entering into more technical details, let's have a short look at the main solution:

This picture shows a Citrix application that request authentication to the Citrix Netscaler. Netscaler then sends the RADIUS requests to the FreeRADIUS server to authenticate the application user. FreeRADIUS will invoke the Swisscom Mobile ID service over SOAP and provide the answer back to the RADIUS client interface of NetScaler. FreeRADIUS server may also be connected to an external user store, like Microsoft Active Directory, where the end users details like phone number or credentials are stored.

Here the authentication dataflow:

1. When a Citrix application wants to authenticate its user against Citrix Netscaler, Netscaler makes a request to the defined FreeRADIUS server to authenticate the end user with Mobile ID.

2. FreeRADIUS server, optionally, verifies the user credentials against internal user stores and/or maps to a valid mobile phone user

3. FreeRADIUS server (which enabled the Mobile ID plugin) calls the Mobile ID service

4. The Mobile ID platform ensures that the end-user signature request is allowed and forwards the signature request to the end-user's mobile phone

5. The end-user answer will be processed by the Mobile ID platform and provided to FreeRADIUS server

6. After verification of Mobile ID response by FreeRADIUS server, the answer will be forwarded to Netscaler (over its Radius client interface). This answer will be processed by Netscaler to grant or reject the Citrix Application authentication requests.

3   Configuration and Best Practices

In this reference guide we assume that:

1. The preconditions defined in [1] are met.

2. The customer has built an intermediate protocol gateway like the FreeRADIUS server described in [2] (with the Mobile ID plugin).

3.1   Configuration of FreeRADIUS on Citrix NetScaler

To allow Netscaler to perform a Mobile ID authentication, Netscaler authentication must be configured to reroute the authentication requests towards the FreeRADIUS server. The configuration of NetScaler must be performed as described by Citrix in [3] and in [4].

Basically, the NetScaler must define a new NAS server as such:

1. Under "Server", in "IP Address", type the IP address of your "on premise" FreeRADIUS server.

2. Under "Time-out", type 90sec in order to give enough time to Mobile ID to handle the authentication requests.

3. Under "Port", type the authentication port that you defined in your "on premise" FreeRADIUS server.

4. Under Details, in Secret Key and Confirm Secret Key, type the FreeRADIUS shared secret that you defined in your "on premise" FreeRADIUS server.

3.2   Radius Gateway and end-users details

The document [2] describes as well how to inter-connect an external user store to the FreeRADIUS server, like Microsoft Active Directory (where the end users details like phone number or credentials are stored).

3.3   Mobile ID and Citrix Web Interface – XenApp & XenDesktop

Since Citrix Web Interface offers as well a RADIUS client interface, the solution describes above for NetScaler applies as well for Citrix Web Interface. See [5] how to configure Citrix Web Interface.