MiVoice Office 400 Description of Security Measures for the SMBC Platform

Date: 2023-11-21
Doc no.: depl-2599 v1.1

REVISION INFORMATION

Version	Release Date	valid for
1.1	21.11.2023	Updated the contact information
1.0	03.12.2018	Mitel Office 400 SMBC platform

The information conveyed in this document is confidential and proprietary to Mitel® and is intended solely for Mitel employees and official trade control authorities who specifically have a need to know this information. If you are not a Mitel employee or an official trade control authorities, you are not the intended recipient of this information. Please delete or return any related material. Mitel will enforce its right to protect its confidential and proprietary information and failure to comply with the foregoing may result in legal action against you or your company.

Table of Contents

1 PURPOSE

This document describes the security measures on the MiVoice Office 400, focusing on the SMBC platform. It lists the security modules and the used mechanisms as well as the derivation of the security software modules.

2 SCOPE

The MiVoice Office 400 as of release R6.0 (09.2018). The MiVoice Office 400 refers in this document to the SMB Controller (SMBC) only.

The overview of the MiVoice Office 400 and the related security mechanisms are described in general in the document “MiVoice Office 400 Product Description” (depl-1623). This document is an add-on to the document mentioned above regarding the dependencies on the original manufacturers of the security software modules.

3 RELEASE INFORMATION

This document describes the SMBC platform and its firmware as of 09.2018.

In the MiVoice Office 400, the different security options are:

- Secure call control signaling by means of TLS, like SIP
- Secure media transport by means of SRTP
- Secure service control by means of TLS, like HTTPS and SMTP
- Secure service control by means of SSH, for remote access

The usage of the above security methods for the “call control signaling” and the “media transport” requires a specific security licence. For all other secure services this is available by default.

4 OPERATION SYSTEM INFORMATION

The operating system used for the SMBC is based on Linux. The Linux is a so called embedded Linux distribution which uses the standard Linux Kernel version 4.x. For the security functionality appropriate components were configured to the Linux system.

5 SECURITY MEASURES

The security measures for the SMBC can be separated into the services which belong to the signaling of the telephony services, the processing of voice data and the global services based on IP as an underlying layer.

5.1 SECURE SIGNALLING MEASURES

The measures for the signalling security for VoIP calls use the Transport Layer Security (TLS) layer on the SMBC.

5.1.1 USED SIGNALLING ENCRYPTION

For signaling encryption, the SMBC uses the TLS version 1.2 (TLSv1.2). For the Negotiation- and Record layer in TLS, the implementation uses the Signature Algorithm SHA512 with RSA. The Server key size is RSA 1024 bits, and the used fingerprint is done with SHA1/SHA256. The used ciphers are: AES256-GCM-SHA384, AES256-SHA256 AES256-SHA, CAMELLIA256-SHA, AES128-GCM-SHA256, AES128-SHA256, AES128-SHA, SEED-SHA and CAMELLIA128-SHA.
For the server certificate usage, the SMBC uses self- signed certificates which are generated by the internal CA (Certificate Authority).

5.1.2 SOFTWARE VENDOR DEPENDENCIES

The TLS functionality used in the SMBC is the open software called “OpenSSL” which is distributed by the “OpenSSL Software Foundation”. The OpenSSL library is linked within the operating system (OS) of the SMBC statically. All functionality of the TLS communication is used from the native OpenSSL library. The OpenSSL version used in the Release 6.0 GA on the SMBC is 1.0.2j.

5.2 SECURE MEDIA MEASURES

The measures for the media security for VoIP calls are implemented in the Digital Signalling Processor (DSP) which is located on the main board of the SMBC. In addition to this hardware, modules or cards where DSP chips are mounted can be plugged in on the main board of the SMBC. The used DSP is the C55x series from Texas Instruments. Note that secure VoIP channels need to be setup in the configuration. Additionally it is mandatory for all secure media streams that the secure signaling using TLS is activated.

5.2.1 USED MEDIA ENCRYPTION

The SRTP functionality uses the Advanced Encryption Standard (AES) for encryption with 128 bit master key and the authentication tag has either 32 or 80bit.

5.2.2 SOFTWARE VENDOR DEPENDENCIES

The SRTP functionality used by the DSP is provided by the company Snapfield Ltd. The source code containing the encryption functions is included in the compilation process of the DSP software build.

5.3 SECURE SERVICE CONTROL MEASURES

The measures for the service security are to use either the above mentioned Transport Layer Security (TLS) or the Secure Shell (SSH) to access the SMBC. The services which use the TLS as the security layer are general services like mail or web based configuration of the SMBC. The details regarding the TLS layer are the same as mentioned above. The subchapters below describe the details of the SSH service.
The SSH functionality used in the SMBC is the open secure shell software called “OpenSSH”, which is open source. Note that the secure shell support / access must be activated in the SMBC configuration before it can be used.

5.3.1 USED SERVICE ENCRYPTION

For the service encryption, the SMBC uses the SSH version 7.3 (OpenSSH 7.3). For the key exchange algorithms, the implementation uses the curve25519-sha256, variants of the ecdh-sha2-nistp algorithm, and variants of the diffie-hellman-group14/16/18 algorithm. The used host-key algorithms are the ssh-rsa, rsa-sha2-256, rsa-sha2-512, ssh-ed25519. The ciphers used are chacha20-poly1305, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm and aes256-gcm. The message authentication code algorithms used are umac-64-etm, umac-128-etm, hmac-sha2-256-etm, hmac-sha2-512-etm, hmac-sha1-etm.

5.3.2 SOFTWARE VENDOR DEPENDNCIES

The SSH functionality used in the SMBC is the open software called “OpenSSH”. The OpenSSH library is linked within the operating system (OS) of the SMBC statically. All functionality of the OpenSSH service is used from the native OpenSSH library. The OpenSSH version used in the Release 6.0 GA on the SMBC is 7.3.

5.4 SECURE AUTHENTICATION MEASURES

The authentication measures depend on the accessed service. The services (or protocols) provided by the SMBC which support authentication include in most cases the authentication procedure itself. The services which include such an authentication are, for example, the SIP registration or the access via HTTP(S) to the SMBC web server.

5.4.1 USED MECHANISM

The authentication mechanism used by the protocols mentioned above (SIP/HTTP) is the “Digest Authentication” method. This uses the MD5 hash calculation.
Furthermore the web server uses the RSA algorithm with a 1024 bit key for the login procedure to access web applications.

5.4.2 SOFTWARE VENDOR DEPENDENCIES

The functionality for the authentication mechanisms are part of the OpenSSL, for details see above.

5.5 SECURE MEASURES MISCELLANEOUS

The SMBC contains some data which are not related to the signalling nor to the media processing. Furthermore these data are not accessed by the service controls mentioned above. But the data may be provided to the customer e.g. in the form of a file. Such data is also protected in that
the data backup generated by the SMBC is in a container (zipped file) which contains the encrypted configuration database of the system.

5.5.1 USED MECHANISM

The mechanism which is used to encrypt the database content is the AES_CBC_256 algorithm.

5.5.2 SOFTWARE VENDOR DEPENDENCIES

The functionality for the encryption algorithm is part of the OpenSSL, for details see above.

6 MITEL PRODUCT IDENTIFICATION

	Comments	Mitel part number	Release date
SMB Controller	Basic system SMB Controller including CPU, OS and embedded IP Media Gateway;	50006942	Q3 2018

7 MARKETS/ DISTRIBUTION FORMS

The MiVoice Office 400 is addressing the global enterprise market.

The MiVoice Office 400 is sold via indirect distribution channels.

8 CONTACT

Department Name: Mitel Legal Department

E-mail: legal@mitel.com

The information conveyed in this document is confidential and proprietary to Mitel® and is intended solely for Mitel employees and official trade control authorities who specifically have a need to know this information. If you are not a Mitel employee or an official trade control authorities, you are not the intended recipient of this information. Please delete or return any related material. Mitel will enforce its right to protect its confidential and proprietary information and failure to comply with the foregoing may result in legal action against you or your company.