Certificate of Function

for

MobiCall

from

New Voice

with

SIP-DECT 7.1

Authors: New Voice Austria, Kapsch Austria, Mitel Germany

Date: 28.09.2018, Rev. 21.12.2018 (B. Jobes)

Doc Number : HO2989

Mitel
Powering connections

Mitel.com

CONTENTS

1 Management Summary 3
1.1 Purpose of the test 3
1.2 Result of the test 3
1.2.1 Summary of supported functionality 3
1.2.2 Summary of restrictions and limitations 3
1.2.3 Conclusion 3
1.3 Open Topics / Next Steps 3
2 General Information 4
2.1 Partner Company 4
2.2 Mitel Product Line / Mitel CSU 4
2.3 kapsch Business Com 5
3 Product information 6
3.1 Hardware Components 6
3.1.1 IP PBX system and Terminals 6
3.1.2 Partner Product Hardware Components 6
3.2 Software Components 6
3.3 Application Type 6
3.4 Language Support 6
3.5 Interfaces 6
4 Application overview 7
4.1 Brief Description of the Application 7
4.2 System Architecture of Application and Validation Environment 7
5 Installation and Configuration 8
5.1 Pre-conditions 8
5.2 Installation of the Application 8
5.3 Configuration of the Switch 8
5.4 Configuration of the Application 8
6 Test Execution 9
6.1 Alarming functionality 9
6.1.1 Integration with SIP-DECT 9
7 ANNEX: Support and Escalation Processes 12
7.1 Pre-Conditions 12
7.2 MQT Certified Products being sold by Partner Company 12
7.2.1 Support Responsibilities 12
7.2.2 Support Process 12

1 MANAGEMENT SUMMARY

1.1 PURPOSE OF THE TEST

The purpose is validating the interoperability of the MobiCall Alarm Server from New Voice and SIP-DECT

1.2 RESULT OF THE TEST

1.2.1 SUMMARY OF SUPPORTED FUNCTIONALITY

MobiCall functionality via SIP-DECT

1.2.2 SUMMARY OF RESTRICTIONS AND LIMITATIONS

No known restrictions

1.2.3 CONCLUSION

TEST RESULT	DECISION CRITERIA FOR CATEGORIZING THE TEST RESULT
☒ fully acceptable	
☐ acceptable with restrictions	
☐ not acceptable	

1.3 OPEN TOPICS / NEXT STEPS

No open topics

2 GENERAL INFORMATION

2.1 PARTNER COMPANY

COMPANY NAME:	**New Voice**
COMPANY ADDRESS:	Paschinger Straße 59/3 A-4060 Leonding
CONTACT PARTNER	
NAME	Johannes N. Jungreithmayr
TEL	+43 664 130 5440
E-MAIL	jungreithmayr@newvoice.at
ROLE	Head of Austria
CONTACT PARTNER	
NAME	Jürgen Blaha
TEL	+43 664 8861 3920
E-MAIL	blaha@newvoice.at
ROLE	Sales and Marketing
CONTACT PARTNER	
NAME	Ekrem Ajdinovic
TEL	
E-MAIL	ajdinovic@newvoice.ch
ROLE	Development
SUPPORT HOTLINE	
TEL:	+41 58 750 1111
E-MAIL:	support@newvoice.ch

2.2 MITEL PRODUCT LINE / MITEL CSU

COMPANY NAME:	**Mitel Deutschland GmbH**
COMPANY ADDRESS:	Zeughofstrasse1 10997 Berlin
CONTACT PARTNER	
NAME	Steffen Wenzlawek
TEL	+49 30 6104 3261
E-MAIL	steffen.wenzlawek@mitel.com
ROLE	Consultant Design DACH
SUPPORT HOTLINE	
TEL:	0900 111 315
E-MAIL:	

2.3 KAPSCH BUSINESS COM

COMPANY NAME:	**Kapsch Business COM (Austria)**
COMPANY ADDRESS:	Kornstrasse16 A-4060 Leonding
CONTACT PARTNER	
NAME	Robert Kneidinger
TEL	+43 50 811 7185
E-MAIL	Robert.Kneidinger@kapsch.net
ROLE	ICT Delivery Applications Salzburg & Upper Austria
SUPPORT HOTLINE	
TEL:	
E-MAIL:	

3 PRODUCT INFORMATION

3.1 HARDWARE COMPONENTS

3.1.1 IP PBX SYSTEM AND TERMINALS

MiVoice MX-ONE with SIP-DECT terminals 622 & 632 (Firmware 7.0 SP11)

3.1.2 PARTNER PRODUCT HARDWARE COMPONENTS

The Alarm server hardware is a HP DL380 Gen7 (Win Server 2016).

3.2 SOFTWARE COMPONENTS

PRODUCT NAME	PRODUCT SW VERSION	COMMUNICATION SYSTEM NAME	COMMUNICATION SYSTEM SW VERSION
MobiCall	V8.2.2	MiVoice MX-ONE	R6.3 SP2
MobiCall AXI	3.4.7.1142	Mitel SIP DECT	7.1 CK14

3.3 APPLICATION TYPE

Alarm Server

3.4 LANGUAGE SUPPORT

LANGUAGE SUPPORT

☐ Brazilian	☐ Finnish	☒ Italian	☒ Spanish	☐
☐ Danish	☒ French	☐ Norwegian	☐ Swedish	☐
☒ Dutch	☒ German	☐ Portuguese	☐ <other>	☐
☒ English	☐ Greece	☐ Russian	☐	☐

3.5 INTERFACES

MIVOICE 5000	MIVOICE MX-ONE	MIVO 400	SIP-DECT
☐ CSTA II [1])	☐ CSTA III	☐ CSTA III	☐ SIP subscriber
☐ IAE	☐ AL / CSTA I	☐ FIAS (Hotel)	☐ SIP trunk
☐ LDAP	☐ AL / TAPI	☐ SNMP	☒ AXI/XML
☐ TAPI	☐ CPDM	☐ PC5	☐
☐ Tickets	☐ ISDN	☐ ISDN	
☐ Web Services	☐ SIP subscriber	☐ SIP subscriber	
☐ ISDN	☐ SIP trunk	☐ SIP trunk	
☐ SIP subscriber	☐ analogue	☐ ATAS	
☐ SIP trunk	☐	☐ analogue	
☐ analogue		☐	

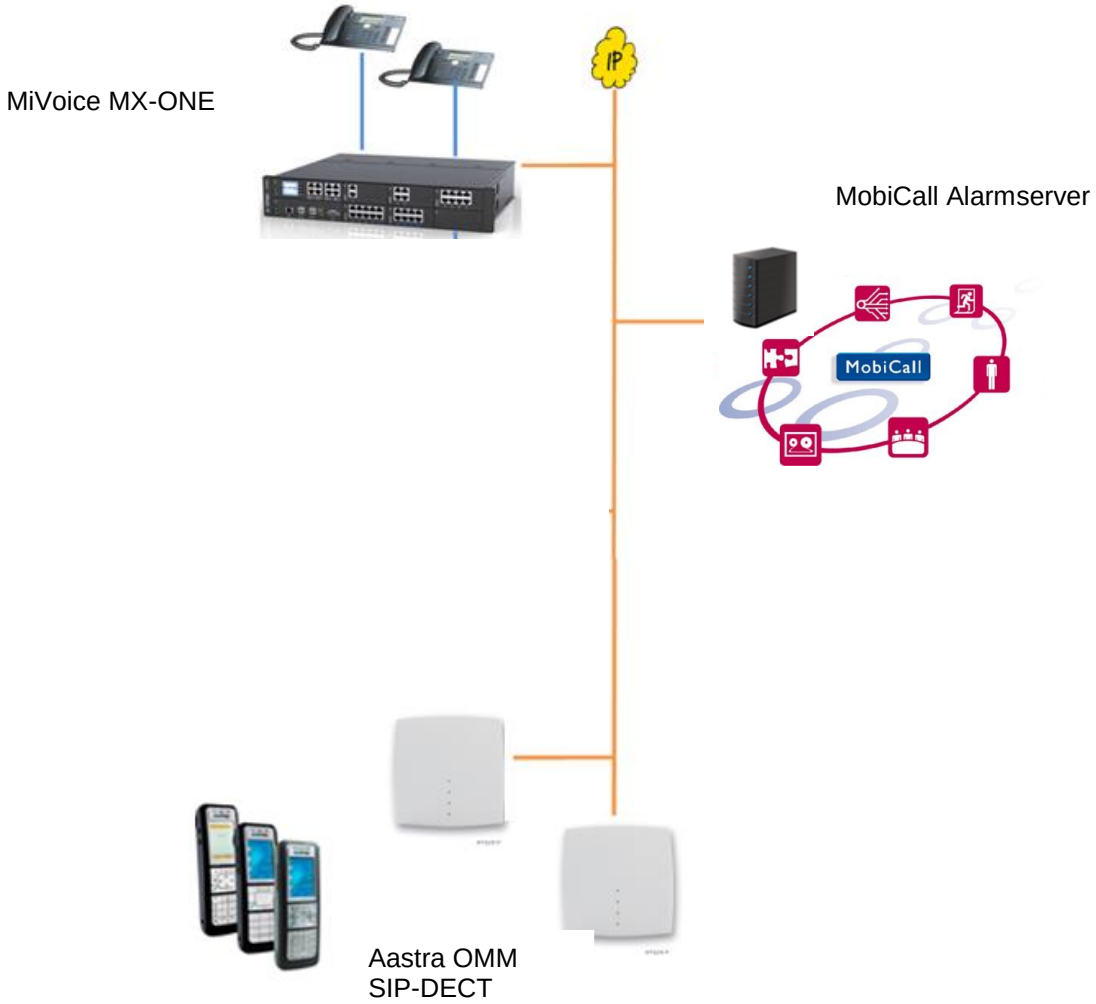
[1]) In case of connecting an application to MiVoice 5000 via CSTA one needs to include multiple CSTA servers, backup, redundancy and dual homing into account when testing the application integration

4 APPLICATION OVERVIEW

4.1 BRIEF DESCRIPTION OF THE APPLICATION

The Alarm Management server MobiCall centralizes the processing of all events seized by external sources (building/process control, fire alarm, network management, nurse call, etc.) and notifies the alarm organization based on the respective scenario through different communication media by SMS, phone call (VOIP), email, SNMP traps, Paging or text messages on cordless handsets (DECT/WLAN/ GSM).

4.2 SYSTEM ARCHITECTURE OF APPLICATION AND VALIDATION ENVIRONMENT



5 INSTALLATION AND CONFIGURATION

Any details on installation and/or configuration could be provided in a separate document.

5.1 PRE-CONDITIONS

The application is installed on the following operating systems:

APPLICATION	OPERATING SYSTEM	REMARKS
Server application	Windows Server 2016	

5.2 INSTALLATION OF THE APPLICATION

5.3 CONFIGURATION OF THE SWITCH

5.4 CONFIGURATION OF THE APPLICATION

6 TEST EXECUTION

6.1 ALARMING FUNCTIONALITY

6.1.1 INTEGRATION WITH SIP-DECT

Activity	Result	Remarks
Pre-requirement for SIP-DECT setup: setup a SIP-DECT system with basic parameters. In addition, make sure that - dynamic, unbound and fixed users are present in the configuration - some users and user attributes include special characters (&<>') - the OMAXI user password should include a "&" have an omaxi lograw trace running in the OMM at all time to validate I/O signals. Check for errors detected by the OMM and unexpected OMAXI connection interrupts. save the log and a sysdump after testing.	OK	
connect the application to a SIP-DECT system with a 2nd OMM (standby) configured. verify that ☒ The link recovers when the active OMM fail and the 2nd OMM become active ☒ An initial connection to the standby OMM is handled by failover to the active OMM. ☒ The connection recover if the network connection is interrupted for 1 and 7 minutes. ☒ disconnect power on the active OMM ☒ disconnect / reconnect power on both OMMs send messages to verify proper function. If subscriptions are initiated verify that the application initiate subscriptions with each failover.	OK	
send message to single and multiple handsets (AXI: SendMessage) verify the following parameters: ☒ sender information (name, number) ☒ callback information (if provided) ☒ message priority ☒ time and date are in the local time zone ☒ additional parameters (tone, color, …)	OK	
send message to a handset with a full inbox (15 messages received and overwrite off). Verify that the Alarm Server detects and handle this error appropriate. (AXI: SendMessageResp)	OK	
send multiple messages to one handset at the same time. So the handset queue is full and the application retry when queue is empty. (AXI: EventMessageQueueEmpty) (take handset out of coverage to force a delivery delay)	OK	

Activity	Result	Remarks
verify that the Alarm Server send periodic keep alive packets (AXI: Ping) to the OMM. (timeout 5min)	OK	
verify that the message progress is detected in the application. Send messages also to a group of handsets for this test. states: ☒ delivered (device did receive message) ☒ read (user confirmation) ☒ order (user confirmation) ☐ complete (user confirmation) (AXI: EventMessageProgress, EventMessageConfirmation) Verify also that negative or higher-level confirmations (complete instead of read) are handled by the application	OK NS	
delete message on handset by application (AXI: DeleteMessage)	OK	
send message with text “Support ‘@”ÄÜÖ&éèà” to validate encoding of message text in UTF-8	OK	
Verify that the application detects DECT handsets incl. messaging capabilities (e.g. capMessaging, trType) Only if appropriate for application flow. e.g. if the application show a list of handsets or if a message is send to all handsets	OK	
Use dynamic user login / logout after the application did connect to the OMM ☒ login a user on an unbound handset ☒ exchange two users between two devices Check that the users receive messages and that the right users receive the message.	OK	
verify that the application deletes messages after the alarm scenario did end especially if the handset was out of range. OMM queue message only for a limited time and do not queue delete message requests.	OK	
If the application can handle alarm triggers try predefined alarm triggers e.g. SOS, custom alarm triggers, user monitoring, …	OK	
verify that the application detects and handles silent charging if supported.	OK	
verify that a message confirmation is also handled in case the OMM did restart after the message was delivered on the handset	OK	
Further scenarios If the application support further OMAXI commands e.g. locating, user monitoring, … List all supported features in the comments. Try the features by best effort	NS	

Activity	Result	Remarks
support of message priority's by application ☒ info ☒ low ☒ normal ☒ high ☒ emergency ☒ locating alert verify that the application support at least one priority which do not require a messaging license e.g. normal	OK	
supported recipient address types ☒ tel: ☒ ppn: ☒ custom prefix	OK	
supported message confirmation's used by application ☒ delivered (device did receive message) ☒ read (user confirmation) ☒ order (user confirmation) ☐ complete (user confirmation)	OK NS	

7 ANNEX: SUPPORT AND ESCALATION PROCESSES

7.1 PRE-CONDITIONS

The following general rules are applicable for analyzing and solving customer problems with solutions provided by Mitel equipment in combination with 3rd party equipment:

- Only certified solutions are officially supported by Mitel.
- Certifications are based on MCT (Mitel Compatible Test), MQT (Mitel Qualified Test) or MAT (Mitel Approved Test) test results and are documented within a CG (Config Guide) or CoF (Certificate of Function). These documents describe
  - main functionality of Partner Company's product
  - interfaces used for integration
  - details of all involved components (including PCs and operating systems)
  - installation and configuration of Partner Company's product and the configuration of Mitel's equipment - as far as this is necessary for the interoperability
  - test use cases, which have been executed
  - and test results.
- CGs and CoFs are published on the InfoChannel MSA

7.2 MQT CERTIFIED PRODUCTS BEING SOLD BY PARTNER COMPANY

7.2.1 SUPPORT RESPONSIBILITIES

Mitel provides full support for the Mitel CS (Communication System) but does not take any support responsibilities for Partner Company's Product.

- 1st level support is provided by an Mitel Reseller
- 2nd level support is the responsibility of Mitel CSU (Country Sales Unit)

Partner Company provides full support for Partner Company's Product.

7.2.2 SUPPORT PROCESS

If a problem occurs at a Customer site where Mitel's CS is used in combination with Partner Company's Product, and if this problem cannot clearly be assigned to Mitel's CS, the Reseller shall open a Support Case at Partner Company.

If the problem cannot be solved within Partner Company's support, the Reseller must open a support case at Mitel's 2nd level support. To open a Support Case, Partner Company must

- First upgrade all HW, FW and SW to latest supported version
- deliver a detailed description of the problem, including the exact time when it occurred and how to reproduce it
- specify all components involved, both HW and FW
- provide all available log file information showing the reported problem and containing a reasonable time period before (and up to) the time when the problem occurred
- comply with the support case opening/handling process applicable within the relevant Mitel Country Sales Unit

Upon receiving all requisite information from Partner Company, Mitel's 2nd level Support will, jointly accompanied by Partner Company, provide analysis and technical support with respect to the identified problem. For MQTs, as agreed on within a Qualification Agreement, full support will be offered within a defined region, while for MCT, global support will be offered assuring that the customer deployment complies with the configuration documented in the CG.

Mitel does not take any commitment on providing a solution fixing problems to end-customers. Mitel 2nd level Support reserves the right to close the case, if the investigations made are insufficient, don't clearly show that the problem can be assigned to Mitel's equipment, don't contain all relevant data or do not exist.