SIP-DECT – Important Product Information for Customer GDPR Compliance Initiatives

SIP-DECT Release 7.1

Version 1.1

June 2018

NOTICE

Trademarks

Contents

Introduction

1.1 Overview

This document is one in a series of product specific documents that discuss the product security controls and features available on Mitel products.

This particular document will be of interest to SIP-DECT customers that are putting security processes and security controls in place to comply with GDPR.

This document is intended to assist Mitel SIP-DECT customers with their GDPR compliance initiatives by:

- Identifying the types of personal data that are processed by SIP-DECT
- Listing the SIP-DECT Security Features that customers may require to achieve GDPR compliance
- Providing a description of the SIP-DECT Security Features
- Providing information on where the SIP-DECT Security Features are documented

This document is not intended to be a comprehensive product specific security guideline. For information on product security guidelines, product engineering guidelines or technical papers, refer to Mitel's Web Site.

1.2 What is GDPR?

The European Union (EU) General Data Protection Regulation (GDPR) effective on 25 May 2018 replaces the previous EU Data Protection Directive 95/46/EC.

The intent of GDPR is to harmonize data privacy laws across Europe so that the data privacy of EU citizens can be ensured. GDPR requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. GDPR also addresses the export of personal data outside of the EU. Any business that processes personal information about EU citizens within the EU must ensure that they comply with GDPR. Under GDPR, 'processes personal information' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

1.2.1 What do Businesses need to know about GDPR?

GDPR applies to businesses with a presence in any EU country, and, in certain circumstances, to businesses that process personal data of EU residents even if the businesses have no presence in any EU country.

In order to achieve GDPR compliance, businesses must understand what personal data is being processed within their organization and ensure that appropriate technical and organizational measures are used to appropriately safeguard such data. This document explains what personal data is processed by Mitel’s SIP-DECT and highlights available security features to safeguard such data.

The SIP-DECT system and application consists of the Open Mobility Manager (OMM), the administration tool OM Management Portal (OMP), the OM Configurator (OMC), the Multi OMM Manager (MOM), the SIP-DECT Phone, and the Open Mobility Locating and Alarming application (OML).

2 Personal Data Collected by SIP-DECT

During the course of installation, provisioning, operation and maintenance, the SIP-DECT collects data related to several types of users, including:

- End users of SIP-DECT – typically Mitel customer employees using Mitel SIP-DECT phones and collaboration tools.
- Customers of Mitel customers – for example the end user's personal contact lists may contain personal data of business contacts, short messages may contain personal content of both parties.
- System administrators and technical support personnel – logs and audit trails contain records of the activities of system administrators and technical support personnel.
- Other persons information contained in end user's short messages.

3 Personal Data Processed by SIP-DECT

SIP-DECT processes the following types of data:

- **Provisioning Data:**
  - The user's name, business extension phone number (office phone number), mobile phone number, user description like department, and SIP account data.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System and content backups, logs, diagnostic debug trace logs, and audit trails.
  - Voice quality logs and voice quality statistics.
- **User Activity Records:**
  - User's call status data, location data including date and time, and text message data.
- **User Personal Content:**
  - Voice mails, text messages, and personal contact lists.
- **User Personal Settings:**
  - Service settings (login password, PIN, display language and so on), and call forwarding destination and its modes.
- **User Device Related Data:**
  - User device login and device subscription data.

Personal data processed by the SIP-DECT is required for the delivery of communication services, technical support services or other customer business interests. For example, call billing and reporting services. There are no end user opt-in consent mechanisms implemented in the application.

4 Personal Data Transferred by SIP-DECT

The types of personal data transferred among the SIP-DECT and various applications and services will depend on the specific use requirements of those applications or services, for example:

- **Provisioning Data:**
  - The user's first name, last name, office phone number, user description like department, SIP account data, user account information, and any user device data.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System and content backups, logs, diagnostic debug trace logs, and audit trails.
  - Voice quality logs and voice quality statistics.
  - System management activity, such as login and logout, and activity audit logs may be transferred to secondary storage or to technical support personnel.
- **User Activity Records:**
  - User’s call status data, location data including date and time, and text message data including date and time. These data may be shared *globally* between (clustered) SIP-DECT systems connected to a SIP-DECT MOM, a call server, alarming and locating application, and management systems connected through Application XML Interface (AXI) synchronization protocol.
- **User Personal Content:**
  - Voice mails and personal contact lists.
  - Text message content may be shared *globally* between (clustered) SIP-DECT systems connected to a SIP-DECT MOM, a call server, alarming and locating application, and management systems connected through AXI synchronization protocol.
- **User Personal Settings:**
  - Service settings (login password, PIN, display language and so on), and call forwarding destination and its modes.
- **User Device Related Data:**
  - User device login and device subscription data.
- **User account information:**
  - SIP account data may be shared between SIP-DECT and connected call server through AXI synchronization protocol.

All system activity including provisioning data and user’s activity containing any data may be shared *globally* between (clustered) SIP-DECT systems connected to a SIP-DECT MOM, connected call server, applications, or maintenance systems through AXI synchronization protocol.

5 How SIP-DECT Security Features Relate to GDPR

SIP-DECT provides security-related features that allow customers to secure user data and telecommunications data and to prevent unauthorized access to the user's data

Table 1 summaries the security features Mitel customers can use when implementing both customer policy and technical and organizational measures the customer may require to achieve GDPR compliance.

Table 1: SIP-DECT Security Features that Customers May Require to Achieve GDPR Compliance

Security Feature	Relationship to GDPR	Where the Feature is Documented
System and Data Protection	Access to personal data is limited with administrative controls on accounts for both personnel and Application Programming Interfaces. The SIP-DECT OMM and MOM are not intended to allow standard telephony users to log in. OMM and MOM Administrators should configure additional accounts only for other administrators or for tools that need to log in. Access to the system is limited by allowing only authorised access that is authenticated using encrypted username/password login combination. Failed logins are logged but are not restricted to a maximum of attempts. Communications to the system are performed over authenticated, encrypted communications channels using HTTPS (TLS). A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls. In all cases, physical access to systems should be restricted by the customer.	For OMM, see the document SIP-DECT OM System Manual Administration Guide, Chapter 4.2 System Configuration. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter 2 Multi-OMM Manager and Installation > Managing MOM user accounts. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation and Configuration > Administration > Managing Users.
Communications Protection	All personal data transmissions use secure channels if configured. Unsecured channels are available; but the administrator has the choice to use only secure channels. **Voice Streaming** The administrator may configure SIP-DECT OMM to encrypt all IP voice media streams with AES.	For OMM, see the document SIP-DECT OM System Manual Administration Guide, Chapter 2.5 VoIP Encryption, Chapter 4.2 System Configuration, Chapter 5.4.1.2 DECT settings, Chapter 7.30 SRTP [for telephony], Chapter 7.31 SIP over TLS,

	Note that not all SIP providers and third-party SIP devices support encryption; if permitted, the communications will negotiate to no encryption. The DECT protocol uses the “DECT Standard Cipher” for encryption over air by default. **Voice Call Signaling** Only authenticated devices may connect to SIP-DECT. Call signaling between SIP-DECT and IP phones may be secured with TLS. The DECT protocol uses the “DECT Standard Cipher” for encryption over air by default. **Call Privacy** Only authenticated DECT devices can connect to Mitel SIP-DECT. The DECT protocol uses the “DECT Standard Authentication Algorithm” for authentication process. The user of a DECT device may secure their device with a PIN to protect device access. **Messaging** Messages sent between SIP-DECT OMM and the OML application are always encrypted using TLS. For system integrity and reliability, all provisioning interfaces use secure channels. Communications to the system are performed over authenticated, encrypted communications channels using HTTPS or SSH (TLS). The SIP-DECT OMM and MOM support two restriction levels: full access and read-only access. System provisioning needs full access. The SIP-DECT OML application supports only HTTP and not HTTPS protocol; but the application is installed on a Linux server, which may provide an HTTPS proxy to secure the network interface. When installing the HTTPS proxy on the same server on which the OML application is installed, the Linux administrator configures the server firewall to forward external OML HTTP requests to the HTTPS proxy from any network address other than the *localhost* address.	Chapter 7.31.5 Additional Security Considerations. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter 2 Multi-OMM Manager and Installation > Getting started with the Multi-OMM Manager > System requirements (firewall setting). For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation and Configuration > Administration > Managing Users.

	All URI destination configurations in SIP-DECT should be configured to use secure connections for example HTTPS (TLS). A customer can further limit access over the network using standard network security techniques such as VLANs and firewalls.	
Identity and Authentication	Access to SIP-DECT is restricted by a login password. The SIP-DECT OMM and MOM are not intended to allow telephony users to log in. Administrators shall configure additional accounts only for other administrators or for machine APIs that need to log in. Access to the system is limited by allowing only authorised access that is authenticated using username/password login combination. Failed logins are logged but are not restricted to a maximum of attempts. Communications to the system are performed over authenticated, encrypted communications channels using HTTPS (TLS). The user of a DECT phone should secure their device with a PIN to protect the access. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls.	For OMM, see the document SIP-DECT OM System Manual Administration Guide, Chapter 1.6 Logins and Passwords, Chapter 5.1 Login (through web service), Chapter 6.1 Login (through OMP), Chapter 6.5.6.1 Creating New User Accounts. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter 1 Multi-OMM Manager functionality > MOM Interface [login area], Chapter 2 Multi-OMM Manager and Installation > Managing MOM user accounts, Chapter 2 Multi-OMM Manager and Installation > Getting started with the Multi-OMM Manager > Logging in and setting the system name. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Application Quick User Guide > Login / Logout.
Access and Authorization	All personal data processing is protected with access and authorization controls, this includes personal data processing by data subjects, administrators, technical support, and machine APIs. All system data processing and all access to databases, files, and operating systems, are protected with encrypted access and authorization controls.	For OMM, see the document SIP-DECT OM System Manual Administration Guide, Chapter 1.6 Logins and Passwords, Chapter 5.1 Login (through web service), Chapter 6.1 Login (through OMP), Chapter 6.5.6.1 Creating New User Accounts. For MOM, see document SIP-DECT Multi-OMM Manager Administration Guide,

	SIP-DECT OMM defines different permissions to an administrative account to allow limited access to the system. The administrator can have full access or read-only access. The administrator must also define permissions for machine API logging in.	Chapter 1 Multi-OMM Manager functionality > MOM Interface [login area], Chapter 2 Multi-OMM Manager and Installation > Managing MOM user accounts, Chapter 2 Multi-OMM Manager and Installation > Getting started with the Multi-OMM Manager > Logging in and setting the system name. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Application Quick User Guide > Login / Logout.
Data Deletion	The system provides an administrator with the ability to erase the end user's personal data. **Deleting a User and Phone Services** SIP-DECT allows the administrator to delete an end user and all of the end user's associated phone services. **Deleting Logs** Certain types of logs cannot be deleted on a per user basis such as messaging logs, error logs and debug trace logs. However, SIP-DECT provides the administrator with the ability to delete the entire contents from all logs. The system administrator can, once authenticated, log in to the shell, locate, and delete the entire file. **Note**: Some logs such as messaging data or debug trace logs are transferred outside of the SIP-DECT system. There is no control of the SIP-DECT system on who traces and how logs are treated outside the system. Logs that are transferred to external or third-party systems are not deleted by this step. For information on how to delete logs from these systems refer to the vendor's documentation. **Deleting short message content** The SIP-DECT OML application generates and stores end user’s short message content. This content cannot be erased in the OML application.	For OMM, see the document SIP-DECT OM System Manual Administration Guide, Chapter 6.5.6.4 Deleting User Accounts, Chapter 6.10.2 “Users” Menu. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter 2 Multi-OMM Manager Installation and Configuration > Managing MOM user accounts, Chapter 2 Multi-OMM Manager Installation and Configuration > Centralized user and device data management > Modifying user and DECT phone data sets > Deleting a user or DECT phone record. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation, and Configuration > Administration > Managing Users.

	The content must be erased by deleting the user record in the connected SIP-DECT OMM. The administrator may erase the end user's data through web interface or SIP-DECT OMP administration tool. SIP-DECT does not store any voicemail data. The administrator must erase any voicemail data in the originating call server system.	
Audit	Audit trails are supported to maintain records of administrator login for a limited time. Records of data processing activities are not collected in the system, but may be collected by external applications.	For OMM, see the document SIP-DECT OM System Manual Administration Guide, Chapter 5.4.8 Event Log Menu. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide. For OML, see the document SIP-DECT OM Locating Application Administration Guide.
End Customer Guidelines	SIP-DECT security configuration information is available to assist with installation, upgrades, and maintenance in the guides noted in the Where the Feature is Documented column.	For OMM, see the document SIP-DECT OM System Manual Administration Guide, Chapter 4.2 System Configuration, Chapter 7.30 SRTP [for telephony], Chapter 7.31 SIP over TLS, Chapter 7.31.5 Additional Security Considerations. For MOM, see the document SIP-DECT Multi-OMM Manager Administration Guide, Chapter 2 Multi-OMM Manager and Installation > Managing MOM user accounts. For OML, see the document SIP-DECT OM Locating Application Administration Guide, Chapter OM Locating Installation, and Configuration > Overview > Notes on Operating Conditions.

6 Product Security Information

6.1 Mitel Product Security Vulnerabilities

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:
www.mitel.com/support/security-advisories/mitel-product-security-policy

6.2 Mitel Product Security Publications

Mitel Product Security Publications are available at:
www.mitel.com/support/security-advisories

7 Disclaimer

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of SIP-DECT and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.