EN (English)

Mitel SIP-DECT base stations RFP 44/45/47/47RDC/48 – description of operating system and voice encryption capabilities

Mitel RFP 44/45/47/47RDC/48 base stations uses software based on the Marvell Linux BSP 17 for ARMADA 37xx, which is built around Linux kernel 4.4, and open source libSRTP stack.

The operating system kernel-related software includes the following drivers:

- Audio
- Chip driver
- DDR controller
- DMA
- Ethernet
- GPIO
- I2C
- LED
- RTC
- SD/MMC
- SPI
- Timers
- UART
- Watchdog

SIP Signaling traffic protection: TLS ciphers

AES128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA1
AES256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA1
CAMELLIA128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(128)	Mac=SHA1
CAMELLIA256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(256)	Mac=SHA1
DES-CBC3-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=3DES(168)	Mac=SHA1
DH-DSS-AES128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA1
DH-DSS-AES256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA1
DH-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(128)	Mac=SHA1
DH-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(256)	Mac=SHA1
DH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=3DES(168)	Mac=SHA1
DH-DSS-SEED-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=SEED(128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA1
DHE-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(128)	Mac=SHA1
DHE-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(256)	Mac=SHA1
DHE-DSS-SEED-SHA	SSLv3	Kx=DH	Au=DSS	Enc=SEED(128)	Mac=SHA1
DHE-RSA-AES128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA1
DHE-RSA-AES256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA1
DHE-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(128)	Mac=SHA1
DHE-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(256)	Mac=SHA1
DHE-RSA-SEED-SHA	SSLv3	Kx=DH	Au=RSA	Enc=SEED(128)	Mac=SHA1
DH-RSA-AES128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA1
DH-RSA-AES256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(256)	Mac=SHA1
DH-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(128)	Mac=SHA1
DH-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(256)	Mac=SHA1
DH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=3DES(168)	Mac=SHA1
DH-RSA-SEED-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=SEED(128)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH	Au=DSS	Enc=3DES(168)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH	Au=RSA	Enc=3DES(168)	Mac=SHA1
PSK-3DES-EDE-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=3DES(168)	Mac=SHA1
PSK-AES128-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(128)	Mac=SHA1
PSK-AES256-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(256)	Mac=SHA1
PSK-RC4-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=RC4(128)	Mac=SHA1
RC4-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1
SEED-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=SEED(128)	Mac=SHA1
SRP-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=3DES(168)	Mac=SHA1
SRP-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(128)	Mac=SHA1
SRP-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(256)	Mac=SHA1
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=3DES(168)	Mac=SHA1
SRP-DSS-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(128)	Mac=SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(256)	Mac=SHA1
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=3DES(168)	Mac=SHA1
SRP-RSA-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(128)	Mac=SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(256)	Mac=SHA1
AES128-GCM-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(128)	Mac=AEAD

AES128-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA256
AES256-GCM-SHA384	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
AES256-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA256
DH-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DH-DSS-AES128-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA256
DH-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(256)	Mac=AEAD
DH-DSS-AES256-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA256
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(128)	Mac=AEAD
DHE-DSS-AES128-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA256
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(256)	Mac=AEAD
DHE-DSS-AES256-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA256
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA256
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA256
DH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DH-RSA-AES128-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA256
DH-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(256)	Mac=AEAD
DH-RSA-AES256-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(256)	Mac=SHA256

LibSRPT package provides an implementation of the Secure Real-time Transport Protocol (SRTP), the Universal Security Transform (UST), and a supporting cryptographic kernel. LibSRTP, the Open Source Secure RTP library from Cisco Systems, Inc. RTP is the Real-time Transport Protocol, an IETF standard for the transport of real-time data such as telephony, audio, and video, defined by RFC 3550. Secure RTP (SRTP) is an RTP profile for providing confidentiality to RTP data and authentication to the RTP header and payload. SRTP is an IETF Standard, defined in RFC 3711, and was developed in the IETF Audio/Video Transport (AVT) Working Group (https://github.com/cisco/libsrtp).

The libSRTP stack supports standard cryptographic functions for SRTP voice encryption for secure communications:

- Encryption using AES CM 128 bit;
- Authentication using HMAC-SHA1 80 bit hash and 32 bit hash.

DECT Encryption:

- DECT Standard Cipher (DSC) as defined in ETSI EN 300 175-7; key length is 64 bit. It is possible to deactivate DECT encryption in the OMM for the whole system or for a portable device individually.
- DECT Standard Authentication Algorithm (DSAA) as defined in ETSI EN 300 175-7; key length is 128 bit.

RU (Русский)

Базовые станции Mitel SIP-DECT RFP 44/45/47/47RDC/48 – описание операционной системы с возможностей шифрования голоса

Базовые станции Mitel RFP 44/45/47/47RDC/48 используют программное обеспечение, основанное на дистрибутиве операционной системе Marvell Linux BSP 17.10 для ARMADA 37xx, и ядре Linux 4.4, и стека libSRTP с открытым исходным кодом.

Связанное с ядром операционной системы программное обеспечение включает в себя следующие драйверы:
- Аудио
- Драйвер чипа
- контроллер DDR
- DMA
- Ethernet
- GPIO
- I2C
- индикаторы LED
- RTC
- SD / MMC
- SPI
- Таймеры
- UART
- Watchdog

Защита сигнального трафика SIP: TLS ciphers

AES128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA1
AES256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA1
CAMELLIA128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(128)	Mac=SHA1
CAMELLIA256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(256)	Mac=SHA1
DES-CBC3-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=3DES(168)	Mac=SHA1
DH-DSS-AES128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA1
DH-DSS-AES256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA1
DH-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(128)	Mac=SHA1
DH-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=Camellia(256)	Mac=SHA1
DH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=3DES(168)	Mac=SHA1
DH-DSS-SEED-SHA	SSLv3	Kx=DH/DSS	Au=DH	Enc=SEED(128)	Mac=SHA1
DHE-DSS-AES128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA1
DHE-DSS-AES256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA1
DHE-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(128)	Mac=SHA1
DHE-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(256)	Mac=SHA1
DHE-DSS-SEED-SHA	SSLv3	Kx=DH	Au=DSS	Enc=SEED(128)	Mac=SHA1

DHE-RSA-AES128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA1
DHE-RSA-AES256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA1
DHE-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(128)	Mac=SHA1
DHE-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(256)	Mac=SHA1
DHE-RSA-SEED-SHA	SSLv3	Kx=DH	Au=RSA	Enc=SEED(128)	Mac=SHA1
DH-RSA-AES128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA1
DH-RSA-AES256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=AES(256)	Mac=SHA1
DH-RSA-CAMELLIA128-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(128)	Mac=SHA1
DH-RSA-CAMELLIA256-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=Camellia(256)	Mac=SHA1
DH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=3DES(168)	Mac=SHA1
DH-RSA-SEED-SHA	SSLv3	Kx=DH/RSA	Au=DH	Enc=SEED(128)	Mac=SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH	Au=DSS	Enc=3DES(168)	Mac=SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH	Au=RSA	Enc=3DES(168)	Mac=SHA1
PSK-3DES-EDE-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=3DES(168)	Mac=SHA1
PSK-AES128-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(128)	Mac=SHA1
PSK-AES256-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(256)	Mac=SHA1
PSK-RC4-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=RC4(128)	Mac=SHA1
RC4-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1
SEED-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=SEED(128)	Mac=SHA1
SRP-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=3DES(168)	Mac=SHA1
SRP-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(128)	Mac=SHA1
SRP-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(256)	Mac=SHA1
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=3DES(168)	Mac=SHA1
SRP-DSS-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(128)	Mac=SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(256)	Mac=SHA1
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=3DES(168)	Mac=SHA1
SRP-RSA-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(128)	Mac=SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(256)	Mac=SHA1
AES128-GCM-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
AES128-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA256
AES256-GCM-SHA384	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
AES256-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA256
DH-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DH-DSS-AES128-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(128)	Mac=SHA256
DH-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AESGCM(256)	Mac=AEAD
DH-DSS-AES256-SHA256	TLSv1.2	Kx=DH/DSS	Au=DH	Enc=AES(256)	Mac=SHA256
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(128)	Mac=AEAD
DHE-DSS-AES128-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA256
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(256)	Mac=AEAD
DHE-DSS-AES256-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA256
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA256
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA256
DH-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(128)	Mac=AEAD
DH-RSA-AES128-SHA256	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AES(128)	Mac=SHA256
DH-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH/RSA	Au=DH	Enc=AESGCM(256)	Mac=AEAD

DH-RSA-AES256-SHA256 TLSv1.2 Kx=DH/RSA Au=DH Enc=AES(256) Mac=SHA256

Программный пакет libSRPT обеспечивает реализацию безопасного транспортного протокола реального времени (SRTP), Universal Security Transform (UST) и поддержку криптографического ядра. LibSRTP - библиотека RTP с открытым исходным кодом от Cisco Systems, Inc. RTP - это протокол транспорта в реальном времени, стандарт IETF для передачи данных в реальном времени, таких как телефония, аудио и видео, определенных в RFC 3550. Безопасный протокол RTP (SRTP) является RTP-профилем для обеспечения конфиденциальности данных RTP и аутентификации для заголовка RTP и полезной нагрузки. SRTP - это стандарт IETF, определенный в RFC 3711 и разработанный в Рабочей группе по аудио/видео транспорта (AVT) IETF (https://github.com/cisco/libsrtp).

Стек libSRTP поддерживает стандартные криптографические функции для речевого шифрования SRTP для безопасной связи:
- Шифрование с использованием AES CM 128 бит;
- Аутентификация с помощью хеша HMAC-SHA1 80 бит и 32-разрядного хэша.

Шифрование DECT:

- Стандартный протокол шифрования DECT Standard Cipher (DSC) описан в стандарте ETSI EN 300 175-7; длина ключа шифрования 64 бит. Возможна отключение шифрования DECT через систему управления OMM для всей системы или для отдельных устройств.
- Стандартный алгоритм аутентификации DECT Standard Authentication Algorithm (DSAA) описан в стандарте ETSI EN 300 175-7; длина ключа 128 бит.