

# CSTA Phase III

DESCRIPTION



## NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2019, Mitel Networks Corporation

All rights reserved

# 1

## INTRODUCTION

This document describes CSTA Phase III, which provides third-party call control of MX-ONE devices, primarily telephones. CSTA Phase III is an interface that external computer applications can use to remotely control a phone. Examples of operations that can be performed with CSTA Phase III are to dial a number (make a call), pick up a call, and terminate a call.

CSTA Phase III will be referred to as CSTA in the rest of the document.

**Note:** Support for CSTA3 with ECMA 285 ASN.1 has been withdrawn from MX-ONE 5.0 SP2 and onwards.

**Note:** CSTA Phase III with ECMA-348, i.e. SOAP/WSDL is still supported, but is not recommended to be used. It lacks certain functionality compared to XML and TR87.

### 1.1

## SCOPE

This document provides a high-level description of CSTA, the implementation in MX-ONE Service Node, which is a subset of the CSTA Phase III standard.

### 1.2

## TARGET GROUP

This document is intended for System Administrators.

### 1.3

## GLOSSARY

For a complete list of abbreviations and glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

## 2

## OVERVIEW

The Computer Supported Telecommunications Applications (CSTA) is an application protocol based on the ECMA-269 standard. This standard allows functional integration between a computing domain and a telephony domain.

ECMA-269 can be implemented in several ways, with different protocols, according to the ECMA-323 (XML) standard, the ECMA-348 (WSDL) or according to TR-87 (via SIP).

The ECMA-323 standard specifies an XML protocol for CSTA services.

The ECMA-348 standard specifies a SOAP/WSDL (XML based) protocol for CSTA services. (Limited functionality compared to the XML and TR87 protocols).

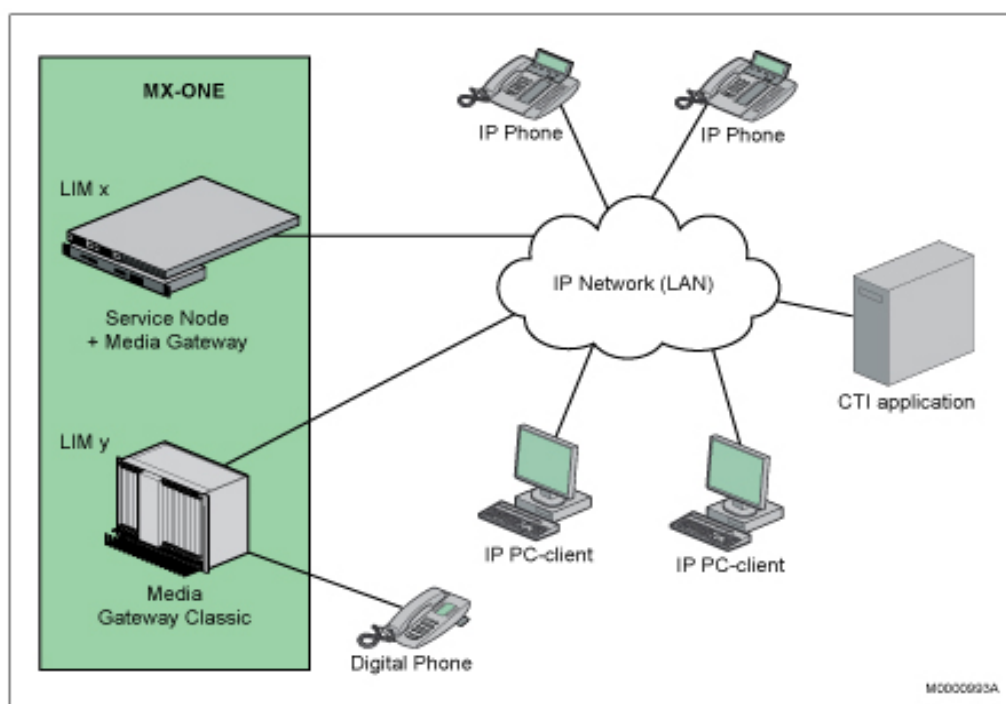
The ECMA-354 standard, Application Session Services (Authentication) is supported via the XML and TR87 protocols.

The TR-87 report (also called uaCSTA) specifies an XML-based protocol for CSTA services transported via SIP.

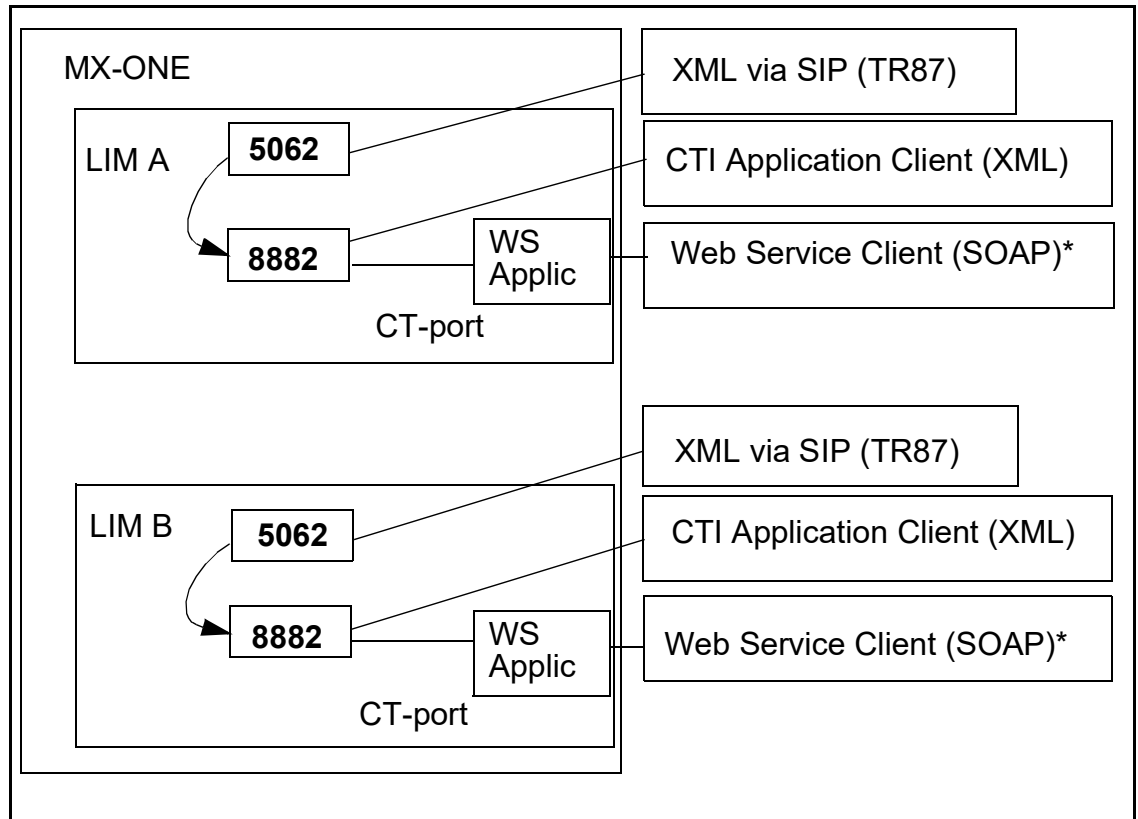
CSTA Phase III can either be implemented using .net or java (web-application). Earlier CSTA could only be implemented using .net.

CSTA makes applications and services available to domains, that normally do not support such applications without major enhancements or redesign. The purpose of this functionality is to support a Computer Telephony Integration (CTI) protocol, between a telephony domain (MX-ONE Service Node and the protocol converter) and a computing domain (host computer with CTI application) or a Web Server serving the Web Service Clients. The CSTA application in the MX-ONE Service Node functions as a server to support the CSTA clients.

The full CSTA functionality is valid for voice calls and voice handling devices, but call events are also sent for instant messaging, SMS and video calls. Some of the CSTA services are supported for non-voice calls and devices.



**Figure 1: General configuration, the CSTA Server is installed on the LIMs**



**Figure 2: Example, CSTA Server configuration (a rather unlikely one where both XML, Web Services/SOAP and XML via SIP (TR87) are used in the same system) CSTA Server configuration**

**Note:** CSTA Phase I and Application Link is still available. For more information on those, see the description for *COMPUTER SUPPORTED TELECOMMUNICATIONS APPLICATIONS (CSTA)*, *CS*.

**Note:** Events are not sent for instant messages sessions established with MSRP.

**Note:** \* The SOAP protocol, which is planned to be phased out, has limited functionality compared to the XML and TR87 protocols. Functions added after MX-ONE 5.0 SP3 are not supported by SOAP, so this protocol is not recommended.

**Note:** If TLS security is used for XML, the port number 8883 is used instead of 8882.

## 2.1

### WEB SERVICES (WS)

The CSTA Application supports the Web Service clients through a Web Server on a port different from the one used for CTI clients.

The rest of the document will refer to the CSTA Application in MX-ONE as CSTA Server.

The main type of application for the CSTA implementation is call centers, where agents handling incoming calls can get synchronized screen updates with the telephone calls. When a call arrives at an agent position, a message is sent from the exchange to the computer, informing the computer of the event. The message will contain information about the call, for example:

- Which agent received the call
- Who is calling (A-number)

- What number was dialed

The computer will take this information and do a database search to update the computer screen of the agent with the caller's profile.

Normally, the agent would handle the telephony traffic from the computer terminal, causing CSTA requests to be sent from the computer to the exchange. It is possible for the agents to wear head-sets, and use the computer terminal as a telephone.

Other types of applications could be outbound call centers, like tele-marketing or debt collection.

The CSTA Server in the MX-ONE supports the CTI application or the Web Service clients via the following functions:

- Generating CSTA events for monitored objects, that is, the status of the object or the queue status of the object.
- Performing telephony functions that are requested from the CTI application, for example, to make calls.

A monitored object can be an analog extension, a CAS extension, a digital extension, an IP extension, an integrated DECT, or a remote extension.

**Note:** Multi-terminal extensions can be monitored but only a limited number of services are supported. For more information please see section Capacities and limitations.

### 2.1.1

## SYSTEM REQUIREMENTS

- Linux OS

### 2.1.2

## CONFIGURATION SCENARIOS

CSTA can be deployed on any LIM in the system. LIMs are assigned to the CSTA server with command *csta -i*. CSTA can be installed in Software or Turnkey mode. Software mode is usually used at the customer premises and Turnkey mode at the factory.

For more information regarding installation, see INSTALLING CSTA PHASE III Web Services Application.

## 3

## KEY FEATURES

**CSTA TR87 (XML through SIP)** and **CTI Application Client (XML)** have the following key features:

- Support a number of standard CSTA services (GetCSTAFeature/GetCSTAFeatureResponse lists supported features), and Authentication services (Application Session Services).
- Command for setup
- Command for authentication configuration
- Support for TLS 1.0 and TLS 1.2 (Transport Layer Security)

**CSTA Web Services/SOAP Application** has the following key features:

- Support of a number of services, that is, authentication services (proprietary) and standard CSTA services.
- Command for setup
- Support for TLS 1.0

## 3.1

## SUPPORTED SERVICES

## 3.1.1

## GENERAL

A number of services are supported by CSTA, and each service provides a number of operations. Some operations generate events (if the device is monitored).

All supported services except authentication services are standard CSTA services. A subset of the CSTA functionality as described in the ECMA-269 standard is supported.

All available operations for the Web Services protocol are formally described in the Web Services Description Language (WSDL) file.

The following services and operations are supported by CSTA Phase III, with both XML, TR87 and Web Services:

Service	Operation	Description
Capability Exchange Services	Get Logical Device Information	Is used to obtain the current set of characteristics or capabilities associated with the logical element of a given device.
	Get CSTA Features Information	Is used to obtain the current set of supported services and events in the system. (Only supported by XML and TR87 protocols).
System Services	Change System Status Filter	Is used by the computing function to change the filter options for a current system registration.
	Request System Status	Is used by the computing function or switching function to obtain (that is, query) the system status of its peer function.
Logical Device Features	Call Back	Allows a computing function to request that the switching function originates a call back call between two devices, that is, requests the called device to return the call when the called device returns to idle.

Service	Operation	Description
	Cancel Call Back	Allows the computing function to cancel a previous (or all) Call Back feature at a device. Note that this service cancels call backs that were created with either call related or non-call related Call Back features.
	Get Do Not Disturb	Provides the do not disturb feature status at a specified device. The do not disturb feature is used to prevent incoming calls at a device.
	Get Forwarding	Provides the forwarding feature status at a specified device. The status returned may consist of one or more forwarding types that are active at the specified device based on user defined conditions. The forwarding feature is used to redirect calls that arrive at a specified device to an alternate destination.
	Set Do Not Disturb	Allows the computing function to control the do not disturb feature at a specified device. The do not disturb feature is typically used to prevent a specified device from being alerted.
	Set Forwarding	Allows the computing function to control the forwarding feature at a specified device based on user defined conditions. The forwarding feature is used to redirect calls that arrive at a specified device to an alternate destination. This service allows only one user-specified setting (forwarding type/forward-destination combination) to be changed per service invocation.
Physical Device Features	Button Press (Fixed and programmable keys)	Allows a computing function to simulate the activation of a specified button at a specified device.
	Get Message Waiting Indicator	Provides the message waiting feature status at a specified device. The message waiting feature is typically used to notify a user (typically via a dedicated lamp on a phone device) when messages are available.
	Set Message Waiting Indicator	Allows a computing function to control the status of the message waiting feature at a specified device. The message waiting feature is typically used to notify a user (typically via a dedicated lamp on a phone device) when messages are available.
	Set Display	Allows the computing function to set text on the display associated with a device.
Vendor Specific Extensions Services	Escape Message Diversion String EricDigestResponse	Is used by an implementation to send a non-standardized (implementation specific) feature using the CSTA protocol. This service shall not be used for features that can be invoked with standardized services. The Escape service allows an implementation to escape from standard operations in order to exploit some special feature of an implementation. This mechanism also allows manufacturers to experiment with new features that may, at a later date, become standardized.
Snapshot Services	Snapshot Call	Provides information about the devices participating in a specified call. The information provided includes device identifiers, their connections in the call, and local connection states of the devices in the call as well as call related information.
	Snapshot Device	Provides information about calls associated with a given device. The information provided identifies each call the device is participating in and the local connection state of the device in that call.
Monitoring Services	Change Monitor Filter	Is used to modify the set of event reports that are filtered out (not sent) over an existing monitor. The new set of filtered out event reports may be listed in the service acknowledgement.



Service	Operation	Description
	Monitor Start	Initiates event reports (otherwise known as events) for a call, device, or for one or more calls involving a device. The server starts a monitor, allocates a Monitor Cross Reference Identifier that uniquely identifies the monitor, and then positively acknowledges the request. All activities satisfying the filter provided trigger events which are delivered as a stream of event reports to the server. Each event contains the Monitor Cross Reference Identifier that correlates the event back to the Monitor Start service that established the monitor.
	Monitor Stop	The Monitor Stop service is used to cancel a previously initiated Monitor Start service. The Monitor Stop service can be issued by a function to terminate or signal the termination of a corresponding Monitor Start service. A positive acknowledgement to the service request indicates that the Cross Reference ID used by the Monitor Start service has become invalid.
Call Associated Features	Associate Data	Associates computing function information (such as correlated data, account code, authorization code, call qualifying data, call characteristics, subject of call, language preferences, and so on) with a specified call. This service does not affect the state or progress of a call.
	Generate Digits	Causes a series of digits to be sent on behalf of a connection in a call. The digits may be sent in the form of DTMF tones or pulse code signaling from rotary dialing phones. This service also supports optional parameters to control digit generation. This service is used for generating end-to-end information that is to be sent to a device in a call (that is, not to address or select a device). This service does not affect the state or progress of a call.
Call Control Features	Accept Call	The Accept Call service causes an offered call to transmit from the offered mode to the Ringing or Entering Distribution mode of the alerting state,
	Alternate Call	Places an existing active call on hold and then retrieves a previously held call. This service is also used to place an active call on hold and then connect to an alerting or queued call at the same device (that is, to answer a call-waiting call).
	Answer Call	Connects an alerting or queued call. This service is typically associated with devices that have attached speakerphone units and headset telephones to connect to a call via hands-free operation. For example, when the call is answered, one of the following actions may occur: If the specified device has a speaker and a microphone, the speaker and microphone are turned on. If the specified device only has a speaker, the speaker is turned on. The handset must be picked up in order to have a two way conversation. If there is no speaker, then the handset must be picked up in order to have a two-way conversation. If the specified device has a headset, the headset is turned on.
	Camp On Call	Allows the computing function to queue a call for a device, which is typically busy, until the device becomes available, for example after finishing a current call or any previously queued calls.
	Clear Call	Releases all devices from an existing call. In the case of a conference call, all devices in the conference call are released from the call.

Service	Operation	Description
	Clear Connection	Releases a specific device from a call. In the case of a two-party call, this may result in the call being torn down. In the case of a conference call, this results in the specific party being removed from the conference. This service can also be used to inactivate a bridged appearance.
	Conference Call	Provides a conference option for a held call and another active call on a conference device. The two calls are merged into a single call and the two connections on the conference device are resolved into a single connection. The connection IDs formerly associated with the conference connections are released and a new connection ID for the resulting connection is created.
	Consultation Call	Places an existing active call at a device on hold and initiates a new call from the same device. The existing active call may include two or more devices. Note that Consultation Call relies on the possibility to tell the device (UA) to hold the ongoing call, and make a new call. This is often not supported by soft-clients, nor by certain third party phones.
	Deflect Call	Allows the computing function to divert a call to another destination that may be inside or outside the switching sub-domain.
	Directed Pickup Call	Moves a specified call and connects it at a new specified destination. This results in the connection being diverted to a new destination inside the switching sub-domain.
	Group Pickup Call	Moves a call that is a member of a specified or default pickup group to a new specified destination. This results in a connection in a pickup group to be connected to a new specified destination inside the switching sub-domain. Note that the difference between this service and the Directed Pickup Call service is that Directed Pickup Call service specifies the actual connection to be picked up while the Group Pickup Call service does not.
	Hold Call	Places a connected connection on hold at the same device. This service interrupts communication for an existing call at a device.
	Intrude Call	Adds the calling device to a call at a busy called device. Depending upon the switching function, the result will be that the calling device is either actively or silently participating in the called device's existing call or consulting with the called device with a new call.

Service	Operation	Description
	Make Call	<p>Allows the computing function to set up a call between a calling device and a called device.</p> <p>The service creates a new call and establishes an initiated or connected connection with the calling device. The Make Call service assigns a ConnectionID to the calling device and returns it in the positive acknowledgement.</p> <p>In the process of establishing the connection with the calling device, the calling device may be prompted to go off-hook (if necessary) and when that device does so, a call to the called device is originated or the calling device is still in the process of dialing the called device.</p> <p>The function differs a bit for different extension types, so a more detailed description of the function follows:</p> <p><b>Calling party is IPeX</b> Supported for all types of SIP terminals, but only for proprietary H.323 terminals. A line or line key in idle or register state is required. If the request is not for a supported type of IP terminal, or in the supported states, the request will be ignored.</p> <p><b>Calling party is CXN or RXN</b> The requesting extension must be in idle or register state. If not, the request will be ignored. If the service is requested in idle state, a call set up ("recall seizure and ringing") will be made towards the extension. When answered, the call setup proceeds towards the number addressed in the Make Call request.</p> <p><b>Calling party is DTS (ODN or ADN)</b> A call setup attempt will be made if the line is in register state or idle. If not, the request will be ignored.</p> <p><b>Calling party is analog extension</b> The requested extension must be in idle or register state. If not, the request is ignored. If the service is requested when the requested extension is in idle state, a call setup (recall seizure and ringing) is made towards the extension. When answered, the call setup proceeds towards the number addressed in the Make Call request.</p> <p><b>Calling party is CAS extension</b> A call setup is made if the extension is in register state and the handset is off-hook. If not, the request is ignored.</p>
	Reconnect Call	Clears a specified connection at the reconnecting device and retrieves a specified held connection at the same device.
	Retrieve Call	Connects a specified held connection.
	Single Step Transfer Call	<p>Transfers an existing connection at a device to another device. This transfer is performed in a single-step, that is the device doing the transfer does not have to place the existing call on hold before issuing the Single Step Transfer Call service.</p> <p>The transferring connection may be in the Alerting, Connected, Failed, Held, or Queued state.</p>
	Transfer Call	<p>Transfers a call held at a device to an active call at the same device. The held and active calls at the transferring device shall be merged into a new call. Also, the Connections of the held and active calls at the transferring device shall become Null and their Connection IDs shall be released (that is, the transferring device is no longer involved with the call).</p>

Service	Operation	Description
Data Collection Services	Start Data Collection	Is used to collect information such as DTMF digits or pulse code signaling from rotary dialing phones and telephony tones from a connection at a specified device. Data Collection may be started on either an existing connection or on the first connection that appears at a device after the service request has been acknowledged.

Additions in MX-ONE, XML/TR87 protocols only:

Service	Operation	Description
Authentication (XML/TR87)	Start Application Session	Is used by the CSTA Client to initiate (log on) a session via the CSTA3 interface (with the XML or TR87 protocol), if authentication is OK. The authentication uses an application identity, version information and password as mandatory parts, but can also optionally use duration time.
	Stop Application Session	Is used by the CSTA Client to stop (log off) a session via the CSTA3 interface (with the XML or TR87 protocol). The same criteria as for Start Application Session are valid.
	Reset Application Session Timer	Is used by the CSTA Client to reset the application session timer optionally running in the PBX/server side. The requesting application is authenticated. (Only supported by XML and TR87 protocols).
	Application Session Terminated	Is used by the PBX system to inform the CSTA Client that an application session has terminated, for example due to time-out.
Query Switching Function Devices (XML/TR87)	Get Switching Function Devices	Is used by the CSTA Client to query which devices exist in the PBX/server side for a particular directory number, since there can be several devices registered (forked) to one directory number. The device identities are sent in the response. This service does not affect the state or progress of a call.

Additions in MX-ONE, Web Service protocol only:

Service	Operation	Description
Authentication (WS)	CSTA Login	Is used by the CSTA Client to log on to the CSTA Server. Login is required before any other request can be sent. When the session expires, the client will receive an error message and must redo the login. <b>Proprietary, for Web Services only.</b>
	CSTA Logoff	Is used by the CSTA Client to log off from the CSTA Server and end the session. <b>Proprietary, for Web Services only.</b>

The following events can be generated (all protocols, but WS lacks some events and some data in other events):

Service	Event	Description
Call Associated Features	Digits Generated	Indicates that DTMF digits or pulse code signaling from rotary dialing phones have been generated at a device.

Service	Event	Description
Device Maintenance	Back In Service	Indicates that the device has been returned to service and is operating normally.
	Out Of Service	Indicates that the device has entered a maintenance state (that is, has been taken out of service) and can no longer accept calls and some categories of CSTA service requests (for example, Call Control services).
	Partially Back In Service	Indicates that the device has returned to service, but is not fully operational. (For groups, for example when calls can be queued, but there may be no member available to take the call).
Call Control Features	Call Cleared	Indicates that all devices have been removed from an existing call.
	Conferenced	Indicates that the conferencing device has conferenced itself or another device with an existing call.
	Connection Cleared	Indicates that a device in a call has disconnected or dropped out from a call.
	Delivered	Indicates that a call is being presented to a device in either the Ringing or Entering Distribution modes of the alerting state.
	Diverted	Indicates that a call has been diverted from a device.
	Established	Indicates that a device has answered or has been connected to a call.
	Failed	Indicates that a call cannot be completed and/or a connection has entered the Fail state.
	Held	Indicates that an existing call has been put on hold.
	Network Reached	Indicates that a call has been connected to an external network using a Network Interface Device, for example, trunk, CO Line).
	Offered	Indicates that a call is in a pre-delivery state at a device (for example, prior to ringing indication or delivering ringback).
	Originated	Indicates that a call is being attempted from a device.
	Queued	Indicates that a call has been queued.
	Retrieved	Indicates that a previously held call has been retrieved.
	Service Initiated	Indicates that a device has gone off-hook for service or is being prompted to go off-hook.
	Transferred	Indicates that an existing call has been transferred to another device and that the device transferring the call has been dropped from the call.
Logical Device Features	Do Not Disturb	Indicates that the do not disturb status has changed.
	Forwarding	Indicates that the forwarding status has changed.
Vendor Specific Services	Private Event	Provides a mechanism to send implementation-specific extended information event. - Media encryption keys of the IP end-points (H.323 or SIP) to the VoIP recording application. - Sends personal number list whether it is active or not. When personal number list is active, it sends active list number.

For more information about standard CSTA services and events, see  
<http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-269.pdf>.

### 3.1.2 TR87 AND CTI APPLICATION CLIENT (XML) VERSUS WEB SERVICES, DIFFERENCES

TR87 and CTI Application Client (XML) support basically the same services and events in ECMA-323 and ECMA TR87 respectively.

The supported set of services and events are the same as for Web Services, with the exception of Authentication, which has different implementations, and with the addition of some services and events (group functions, multiple terminal functions, and certain query functions), which are not supported by Web Services.

The TR87 and CTI Application XML client can request a complete list of the supported CSTA services and events, using the GetCSTAFeatures request.

## 3.2 CSTA SERVICES WITH MULTIPLE TERMINALS (XML/TR87 ONLY)

### 3.2.1 GENERAL

For extension users with multiple terminals, forked on the same directory number, there are some special considerations:

When a user with multiple terminals is monitored by CSTA3, the MX-ONE system reports up to 4 device identities that are available. The device identity will be sent in the response to the *Get Switching Function Devices* request and in the CSTA events. The CSTA application may start monitoring and request CSTA services for any of the reported terminals.

**Note:** Certain applications, soft-clients and third party devices do not support the device identity, and may either have a default behavior of selecting the first reported terminal, or not support the CSTA services at all for multiple terminal users. The SOAP/WS protocol does not support device identity. Both user (number) and terminals must be monitored to get the events.

### 3.2.2 SUPPORTED SERVICES AND EVENTS WHEN DEVICE IDENTITY IS SUPPORTED

All CSTA3 service requests and event reporting available for a (monitored) single extension are also supported for an extension with multiple terminal service, if the Switching Function Representation method (see CSTA standard ECMA-269) of specifying the device ID is used. This allows the CSTA application to identify a specific terminal by a device/terminal identity.

### 3.2.3 SUPPORTED SERVICES AND EVENTS WHEN DEVICE IDENTITY IS NOT SUPPORTED

If the Switching Function Representation method is **not** used, and only the device directory number is used, the following CSTA services are supported:

- CSTA Monitor Start/Stop Device
- Snapshot Device
- Get/Set Forwarding
- Get/Set Do-Not-Disturb

- Get/Set Message Waiting Indicator
- Set Display
- Set Feature.

All CSTA Event reporting is supported.

### 3.2.4

## DEVICE IDENTITY PRINCIPLES

The MX-ONE can provide a list of all available (forked) devices on a specific directory number (the terminal/device identity of all logged on devices) to the CSTA application, used by the end user. The devices in the list are stored in lexical order, so the most significant parts of the data will determine this order.

Most significant is the type of device, in the order SIP, H.323, Mobile extension and TDM DECT.

CSTA will, if it finds for example a newly logged in Mitel SIP desk-phone, rearrange the list of device identities sent to the application, and put the SIP phone in the first position, as SIP has priority over any other phone type.

It is thereafter up to the CSTA application to include the device identity to be used when executing CSTA Call Control services (e.g. answering a call or setting up a new call). For users with multiple devices the CSTA application must deliver the device identity of the device to be controlled/used. If the device identity is not provided, the MX-ONE will neglect/discard the CSTA request.

**Note:** Different CSTA applications have different levels of support for the Device Identity. Some may not support it at all, others fully, and yet other partly.

## 4

# INTERFACES AND PROTOCOLS

The following interfaces and protocols are available for CSTA Phase III:

- XML (ECMA-323, and ECMA-354).
- XML via SIP (TR87).
- SOAP/WSDL (ECMA-348), limited functionality (no further development).

For more information about SOAP, see the interface description *CSTA Phase III Web Services*.

## 5

# OPERATION AND MAINTENANCE

### 5.1

## COMMANDS

The CSTA Server process in the MX-ONE Service Node is configured and controlled by using unix style commands, called *csta*. The commands can initialize, print current status, and remove the CSTA Server.

The initiation command defines LIM number, TCP port number, and protocol parameter (which indicate the client/application communication protocol type, e.g. XML or TR87). It also defines if TLS encryption shall be used or not.

For the XML/TR87 protocols, the *csta\_authentication* commands configure or print the settings for the CSTA application session authentication function.

For more information about the commands, see the *Technical Reference Guide, unix commands, the csta and csta\_authentication commands*.

## 5.2 SECURITY

### 5.2.1 WEB SERVICE APPLICATIONS

HTTPS and Authentication are valid for the Web Service application (i.e. for SOAP/WSDL, ECMA-348).

#### 5.2.1.1 HTTPS

In CSTA (XML and TR87) both HTTP and HTTPS are supported.

TLS, Transport Layer Security, can be used to communicate between CSTA application (the client) and MX-ONE (the CSTA server).

MX-ONE must have a certificate for TLS installed. To verify installed certificate or create/import a certificate, use the installation command *mxone\_certificate*.

The minimum version of TLS is defined in the *ip\_telephony.conf* file. Default minimum version is TLS 1.2. Altering the version can be done with the installation command *mxone\_maintenance*.

The CSTA server shall be configured to turn on security. For more information about the command *csta*, see Technical Reference Guide, unix commands.

In CSTA both HTTP and HTTPS are supported. For higher security, it is recommended to use a commercial digital certificate issued by a commercial Certification Authority.

#### 5.2.1.2 Authentication (WS)

When a login attempt is made, the client application validates the User ID towards a database. The user accounts (Linux accounts) are created by the administrator.

These user accounts shall have a low authority level and a password. The password can and should preferably be changed (i.e., for security reasons, do not use default admin level or default password).

### 5.2.2 TR87 AND CTI APPLICATION CLIENT (XML)

#### 5.2.2.1 HTTPS

In CSTA (XML and TR87) both HTTP and HTTPS are supported.

**Note:** TLS is not supported for TR87.

The user can use TLS and Transport Layer Security to communicate between CSTA application (the client) and MX-ONE (the CSTA server).



MX-ONE must have a certificate for TLS installed. To verify installed certificate or create/import a certificate, use the installation command *mxone\_certificate*.

The minimum version of TLS is defined in the *ip\_telephony.conf* file. It is recommended to use TLS version 1.2. The user can alter the version with the installation command *mxone\_maintenance*.

The CSTA server is configured to turn on security. For more information about the command *csta*, see *Technical Reference Guide, Unix commands*.

#### 5.2.2.2

#### *Authentication (XML)*

Authentication of CSTA applications is supported via the services of ECMA-354, Application Session Services, but only for the XML and TR87 protocols. The authentication can be turned off (for old applications that do not support it).

The services are:

- Start application session
- Stop application session
- Reset application session timer
- Application session terminated

The criteria for the application authentication can be configured via the command *csta\_authentication*, see *Technical Reference Guide, Unix commands*. If authentication is active, the parameters Application Identity, version and password are mandatory, while duration time is optional.

## 6

## CAPACITIES AND LIMITATIONS

- Directory Numbers in the CSTA interface can consist of up to 20 digits, but for many services the maximum length is 10 digits.
- Customer Identity can consist of up to 20 digits.
- All extensions (that support CSTA monitoring) and all ACD/CTI groups can be monitored.
- ISDN S0 extensions, Paging equipment and trunks cannot be monitored via CSTA.
- Call Identity, which is generated by the ASP 113, has the length 20 digits.
- The text in the Set Display service can be up to 240 characters.
- A maximum of 10 CSTA Servers (and 10 different Applications) are allowed to monitor the same device. Note that this does not limit the number of allowed external CTI clients, since multiple clients can connect to the same CSTA Server.
- For extensions with Multiple Terminal Service Forking, CSTA Monitoring (event reporting) and CSTA call control services are supported, if the terminal supports the Terminal Identity information. The SOAP/Web Services protocol does not support this functionality.
- The *Get Switching Function Devices* and the *Application Session Services* are only supported via the XML and TR87 protocols. The SOAP/Web Services protocol does not support this functionality.
- CSTA phase I (AppLink) and CSTA phase III (Xlink) can be used in the same system without restrictions, if they are handling different users. They may not both exercise call control for the same user. They may monitor the same user, but that will cause additional load due to duplicated event reporting.
- The Application Session Services do not support any white-listing or black-listing of the application's IP addresses.
- For extension users with multiple terminals, up to 4 terminals (4 different devices) can be handled (for SIP terminals). Other extension types allow only 1 terminal.
- The SOAP/Web Services protocol does not support TLS 1.2, only TLS 1.0.

**Note:** The ASN.1 protocol is **not** supported.

**Note:** The SOAP protocol has limited functionality compared to the XML and TR87 protocols, so SOAP is not recommended. Functions added after MX-ONE 5.0 SP3 are not supported by SOAP.

**Note:** Multi-terminal extensions can be monitored but which services are supported depends on the used application, and its support for Device Identity, see section 3.2 CSTA Services with multiple terminals (XML/TR87 only) on page 14. Call control events will be received for all logged on terminals.