



Security And Interoperability in Next Generation PPDR
Communication Infrastructures



Project Number: 313296

Deliverable 6.3

Protocol and middleware components - Intermediate

Scope	Scheduled deliverable
Lead Beneficiary	Rohill
Dissemination level	Public
Document creation date	26/May/2014
Document release date	21/March/2015
Contractual Date of Delivery	28/Feb/2015
Version	1.0
Status	Final

Abstract: Deliverable 6.3 provides a detailed description of the protocol to support Private Mobile Radio (PMR) functionality on top of LTE. This intermediate version is focusing on existing PMR functionality as well as interworking with legacy PMR networks. The definition of the applicable PMR functionalities can be found in deliverable D6.2. The middleware components are managed by Rohill within a Version Control System, and are made available to other partners for integration purposes.

AUTHORS

Name	Organisation	Email
Jérôme Brouet	ALU	jerome.brouet@alcatel-lucent.com
Bert Bouwers	ROH	bert.bouwers@rohill.nl
Panagiotis Galiotos	UPAT	pgaliot@gmail.com
Daniel Zerbib	CAS	daniel.zerbib@airbus.com
Olayinka Adigun	KU	O.Adigun@kingston.ac.uk

QUALITY ASSURANCE TEAM

Name	Organisation	Email
Hugo Marques	IT	hugo.marques@av.it.pt
David Jelenc	UL	david.jelenc@fri.uni-lj.si
Jernej Kos	UL	jernej.kos@fri.uni-lj.si

EXECUTIVE SUMMARY

The development of PPDR functionality on top of LTE supports the preferred migration scenario as described in section 4.1 of SALUS deliverable D4.3 [1]. This preferred scenario for "early adopters" is based on deployment of standards-based public and private LTE networks as well as fast deployable LTE systems, whereby an open "Over The Top" (OTT) solution is proposed for delivering voice and data PPDR communication services. This open OTT approach will converge into a standard-based solution when end-users and industry agree on 3GPP standards for mission-critical voice and data.

The open SALUS solution for PPDR functionality on top of LTE closely follows the requirements and architecture of emerging technologies that have been developed by the System Architecture (SA) workgroup within the TETRA + Critical Communications Association (TCCA). This allows for a seamless migration scenario for "early adopters" of LTE for PPDR by developing a multi-mode core solution.

This deliverable defines the protocol for all voice, status, text and location services that are required for typical PPDR applications, as well as interworking with radios on existing TETRA and TETRAPOL networks. In the final version of this document, the protocol is extended with services for transfer of pictures and video alongside voice and data applications, as well as a detailed specification of middleware components.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
TABLE OF CONTENTS	4
TABLE OF FIGURES	8
TABLE OF TABLES	8
1 INTRODUCTION	9
2 CVDP SOLUTION ARCHITECTURE	10
2.1 Overall architecture	10
2.2 Properties	11
3 MESSAGE SEQUENCE CHARTS	12
3.1 Attachment	12
3.2 Provisioning	14
3.3 Group Call	15
3.4 Individual Call	17
3.5 Messaging	18
3.6 Remote execution	19
4 CVDP MESSAGE CONTENT	21
4.1 Primitives	21
4.1.1 Attach	21
4.1.2 Attached	21
4.1.3 Authenticate	22
4.1.4 Connect	22
4.1.5 Connected	23
4.1.6 Execute	23
4.1.7 Executed	23
4.1.8 Message	24
4.1.9 MessageAck	24
4.1.10 MessageAcked	24
4.1.11 Proceed	25
4.1.12 Proceeded	25
4.1.13 Provide	26
4.1.14 ProvideAck	26
4.1.15 Release	26
4.1.16 Released	27
4.1.17 Subscribe	27

4.1.18	Subscribed	27
4.1.19	Traffic	28
4.2	Elements	29
4.2.1	GroupAttach	29
4.2.2	Record	29
4.3	Attributes	30
4.3.1	Ambience	30
4.3.2	Broadcast	30
4.3.3	Calling	30
4.3.4	Called	30
4.3.5	Cause	30
4.3.6	Challenge	31
4.3.7	Class	31
4.3.8	Codec	31
4.3.9	Data	31
4.3.10	Device	31
4.3.11	Domain	32
4.3.12	Duplex	32
4.3.13	Granted	32
4.3.14	Group	32
4.3.15	Hook	32
4.3.16	Key	33
4.3.17	Method	33
4.3.18	Mode	33
4.3.19	Name	33
4.3.20	Parameter	33
4.3.21	Pid	34
4.3.22	Priority	34
4.3.23	Progress	34
4.3.24	Reference	34
4.3.25	Reply	34
4.3.26	Response	35
4.3.27	Result	35
4.3.28	ScanPriority	35
4.3.29	Sequence	35
4.3.30	Status	35

4.3.31	Step	36
4.3.32	Talking	36
4.3.33	Text.....	36
4.3.34	Time.....	36
4.3.35	Timeout.....	36
4.3.36	User	37
4.3.37	Value.....	37
5	COMPLIANCE ANALYSIS	38
5.1	Performance	38
5.1.1	Call setup performance	38
5.1.2	Speech transfer latency.....	39
5.1.3	Number of voice calls	40
5.1.4	Speech quality.....	40
5.2	Scalability	41
5.3	Availability	42
5.3.1	Equipment redundancy	42
5.3.2	Fallback operation.....	42
5.3.3	Link redundancy.....	42
5.3.4	Multiple wireless networks.....	42
5.4	Security	43
5.5	Functional requirements.....	43
5.5.1	Basic services	43
5.5.2	PMR supplementary services.....	43
5.5.3	Telephony supplementary services	44
5.5.4	Security services	44
5.6	Interoperability with IP networks.....	45
5.6.1	Support of IP multicast	45
5.6.2	Limited bandwidth	45
5.6.3	High delay links	46
5.6.4	Packet drops	47
5.6.5	Network roaming	47
5.7	Interworking with Legacy PMR networks	48
5.7.1	TETRA	48
5.7.2	TETRAPOL	49
6	CONCLUDING REMARKS.....	50
	APPENDIX A - TETRA LIP format.....	51

Bibliography	52
Acronyms	53

TABLE OF FIGURES

Figure 1 - Architecture CVDP solution	10
Figure 2 - Authenticated Device attachment.....	12
Figure 3 - Mutually authenticated Device attachment	13
Figure 4 - Provisioning method.....	14
Figure 5 - Group Call.....	15
Figure 6 - Individual Call.....	17
Figure 7 - Message to group of Devices	19
Figure 8 - Message to individual Device	19
Figure 9 - Remote execution method.....	20
Figure 10 - High delay link scenario.....	46

TABLE OF TABLES

Table 1 - Delay budget for Group Call setup.....	39
Table 2 - Delay budget for Speech Transfer	39
Table 3 - CVDP supported speech vocoder standards	41
Table 4 - Compliance of PMR basic services	43
Table 5 - Compliance of PMR supplementary services.....	44
Table 6 - Compliance of telephony supplementary services	44
Table 7 - Compliance of security services	44
Table 8 - IP bandwidth calculation.....	45
Table 9 - End-to-end delays for satellite link scenario.....	46
Table 10 - Capabilities of TETRA gateway	48
Table 11 - Capabilities of TETRAPOL gateway	49

1 INTRODUCTION

This document describes the protocol and middleware components that are developed within SALUS in order to support PPDR functionality on top of LTE. The document is structured as follows:

Section 2 describes the system architecture, interfaces and middleware components of the proposed Critical Voice and Data Protocol (CVDP) based solution that includes multiple LTE devices, dispatcher stations, voice-data logging and gateways to TETRA and TETRAPOL. Also the main properties of CVDP are described.

Section 3 explains the Message Sequence Charts (MSCs) that clarify the exchange and purpose of CVDP messages for all applicable services. Also the features and services that are implemented by means of application logic that falls outside of the CVDP scope are listed for each of the main CVDP applications.

Section 4 defines the content of CVDP messages, including the attributes that carry the information from one to another CVDP-capable endpoint.

Section 5 provides a detailed analysis of compliance against the requirements defined in deliverable D6.2. These compliance items include functional and non-functional requirements as well as IP network interoperability (integration) and legacy PMR network interworking requirements.

Finally, section 6 summarizes the status, open issues and next steps in order to create deliverable D6.6.

2 CVDP SOLUTION ARCHITECTURE

The design and implementation of PMR functionality on top of LTE is loosely based on existing concepts for PMR system interconnection developed by Rohill Technologies, referred to as On-Demand Intelligent Network Interface (ODINI). Similar to ODINI, CVDP is also based on unique IPR of Rohill Technologies for fast and robust operation of Push-To-Talk operations [11].

For operation of large number of mobile devices within a private or public LTE network, specific innovations have been development within the SALUS project that addresses issues including scalability, performance, reliability and ease of configuration. This has resulted in the Critical Voice and Data Protocol (CVDP).

Note that CVDP is an interim solution that fills the gap until standards for PMR functionality on top of LTE are completed within the ETSI and 3GPP standardisation bodies. It is expected that the CVDP system architecture can be reused for implementation of emerging standards, whereby customers can be offered a smooth migration path.

2.1 Overall architecture

The core solution consists of a single CVDP Relay. The CVDP Relay application connects dispatchers, gateways and storage solutions over fixed IP networks to user devices that operate in LTE and Wi-Fi networks.

As the name Relay implies, the application forwards signalling, voice and data packets from the transmitting device to one or more listening or recording devices. In addition, the CVDP Relay performs device authentication and provisioning, as well as the supporting typical PMR functionalities like priority handling, pre-emption and queuing.

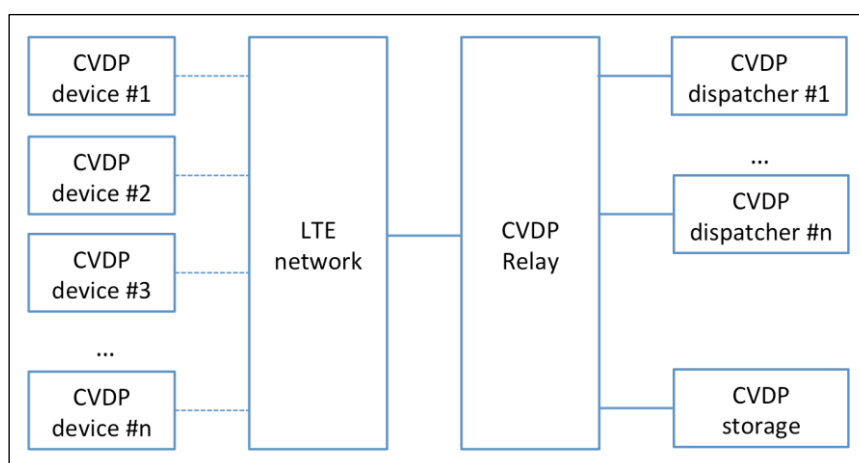


Figure 1 - CVDP solution Architecture

The simplicity and low overhead of CVDP allows very efficient distribution of signalling and voice packets to multiple devices. The typical performance of a server platform allows decoding of signalling and voice packets of hundreds of calls, and delivery of signalling and voice packets to thousands of devices. In addition, the solution is scalable and can be made resilient by adding additional CVDP relays for additional capacity and redundancy.

The following CVDP devices are envisaged:

- Smartphone app that implements the User Interface and Call Logic to operate as a voice & data capable PMR radio within a LTE network;
- Embedded PC running a dedicated application for voice & data capabilities, for example to serve as a communications hub within a train, tram or bus for a Public Transport application.

A range of CVDP applications can be connected directly by means of fixed IP links to the CVDP relay to provide other typical PMR system components:

- PC-based dispatcher application to allow the operator to communicate with users in the field by means of voice and data capabilities;
- Storage device to provide structured logging of all voice and data that is carried over the CVDP Relay;
- Gateways to legacy PMR networks, including TETRA and TETRAPOL radio networks.

CVDP is designed in such a way that all applications can "speak the same language", offering a simple but powerful ecosystem in order to provide PMR functionality on top of LTE as well as supporting interoperability with existing PMR networks.

2.2 Properties

The Critical Voice and Data Protocol (CVDP) defines the messages to transport voice and data traffic as well as the signalling needed to establish, maintain and terminate the calls. CVDP is an application layer protocol designed to be independent of the underlying transport layer. It is a text-based protocol based on the Extensible Markup Language (XML) [2], although the abstraction of XML allows encoding of CVDP into other structures for encoding, transmitting and decoding of protocol messages, element and attributes.

CVDP works in conjunction with several other application layer protocols that identify and carry the signalling, voice and data messages. CVDP typically employs the standard User Datagram Protocol over the Internet Protocol (UDP/IP) [3], and can be encrypted with Transport Layer Security (TLS) [4].

CVDP can be operated in IP unicast, multicast and broadcast modes. Mechanisms are included in CVDP to let applications attach to an IP multicast address or IP broadcast address.

Automatic Repeat Request (ARQ) mechanisms are applied for a number of message sequences in order to improve transport reliability in the event of packet drops. The standard stop-and-wait ARQ method is applied for the following message sequences:

- Provide > ProvideAck;
- Message > MessageAck;
- MessageAck > MessageAacked.

By default, the timeout for retransmission is 1 second and the maximum number of transmissions is set to 3. Each packet includes a unique reference and/or sequence number to allow for out-of-sequence acknowledgements.

3 MESSAGE SEQUENCE CHARTS

The services of CVDP are defined by messages that contain elements and attributes. These messages are transferred in a specific order and under certain conditions to implement the functionality as described for each service within deliverable D6.2 [5].

This section describes the so-called Message Sequence Charts (MSCs) for all PMR services. While many services are variations on other services (like "Priority Call" as variation on a "Group Call"), CVDP is designed to support these variations simply by adding additional attributes in the already defined messages.

3.1 Attachment

The attachment procedure in CVDP covers all functionality that is required to allow instant operation of the CVDP device or application on the CVDP relay, including secure authentication features to prevent unauthorised access. This covers the following services:

- Registration (Device attachment);
- Network roaming (Device attachment);
- De-registration (Device detachment);
- User assignment (User attachment);
- Device authentication;
- User authentication;
- Mutual authentication;
- Group attachment;
- User assignment;
- Dynamic regrouping.

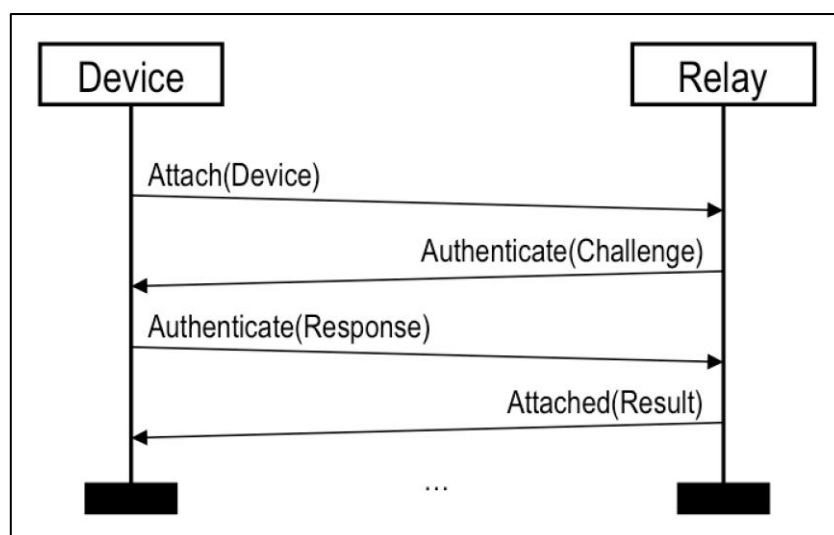


Figure 2 - Authenticated Device attachment

The MSC above describes the CVDP device procedure that covers both the registration and authentication services. The **Attach** request includes the *Device* name (configurable or retrieved from the hardware or operating system). The **Authenticate** request includes the *Challenge* to check if the key on the device is the same as the shared key on the Relay.

The **Authenticate** response includes the *Response* for the *Challenge*, and the final **Attached** response confirms the *Result* of the attachment and authentication, as well as further details on the Device (dial number, alias name).

The CVDP user attachment scenario is applicable to CVDP applications that require entry of a user identification and passphrase. This could be a Personnel number with a matching Personal Identification Number (PIN), or an email address with a matching password, etc. Depending on the use case, device attachment could already enable some or all services, whereby user attachment is optional or not used at all. As a third option, it is possible to skip CVDP device attachment, and immediately proceed with CVDP user attachment.

Mutual Authentication is an additional but important option to ensure that the CVDP Relay is not compromised (e.g. being substituted):

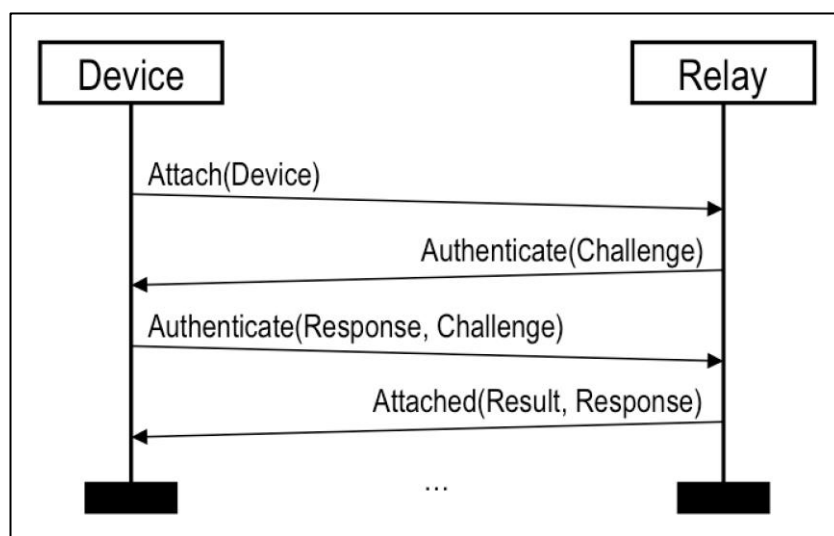


Figure 3 - Mutually authenticated Device attachment

The **Attach** request includes the *Device* name (configurable or retrieved from the hardware or operating system). The **Authenticate** request includes the *Challenge* to check if the key on the device is the same as the shared key on the Relay. The **Authenticate** response includes the *Response* for the *Challenge* and another *Challenge* for the Relay. The final **Attached** response confirms the *Result* of the attachment and authentication, the *Response* for the *Challenge* from the Device, as well as further details on the Device (dial number, alias name). The CVDP device itself can now conclude itself whether the Relay is genuine or not.

Mutual Authentication can also be applied to User attachments, or used instead of Device attachments with Mutual Authentication.

After initial registration and (mutual) authentication, Devices remain connected to the Relay by means of a simpler periodic Device **Attach** without authentication. This periodic **Attach** confirms reachability of the Relay by the Device and vice-versa, and allows the Device IP address to change due to roaming of Devices into another network. The default interval for periodic Device **Attach** is 5 seconds; overriding this interval is possible by assigning a different Lifetime value in either the **Attach** or **Attached** message. A Device is assumed detached (de-registered) if no periodic **Attach** is received by the Relay for Lifetime x 3,5 seconds, allowing for a maximum of two lost **Attach** messages.

3.2 Provisioning

Provisioning is included in CVDP to allow for efficient deployment of Devices. After registration, the applicable configuration, phonebook and group lists can be downloaded and synchronised on demand. Provisioning covers the following services:

- Configuration download;
- Group list download;
- User list download;
- Group list synchronisation;
- User list synchronisation.

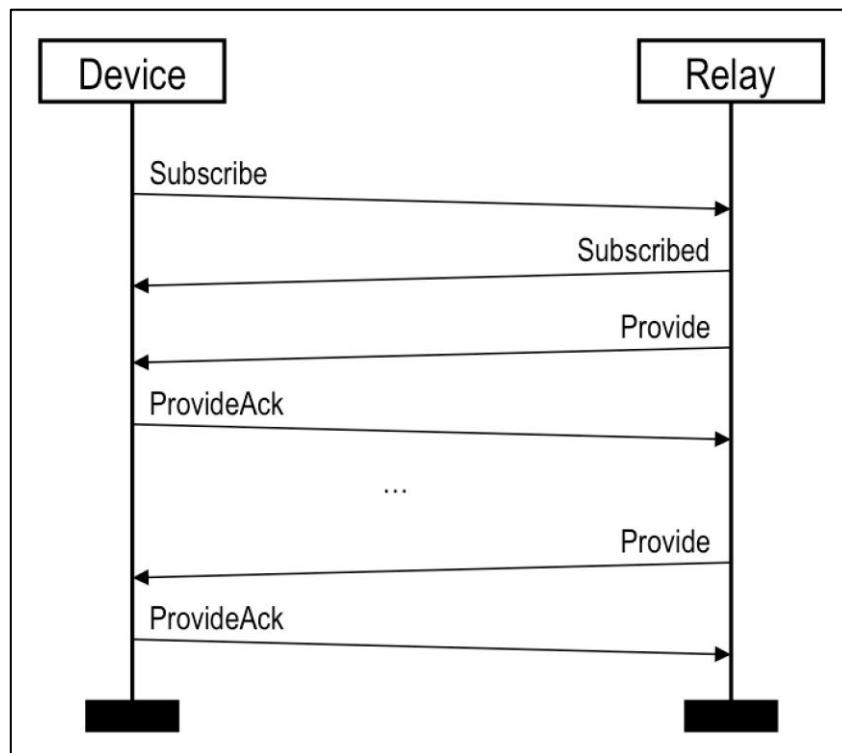


Figure 4 - Provisioning method

Subscribe includes the Class and optional Domain attributes. Valid Class values include Configuration, Users and Groups. The optional Domain attribute allows downloading of a subset of records, for example a fleet or agency. The **Subscribe** request is confirmed by the **Subscribed** response.

The **Provide** message contains one or more database records of the requested subscription. The Device should confirm every **Provide** by means of a **ProvideAck**. An unsolicited **Provide** is distributed by the Relay to all subscribed Devices when database records are added, deleted or modified.

3.3 Group Call

CVDP offers very efficient, fast and robust operation of group calls by adopting an innovative method to handle speech items. A single speech item covers the activity of a radio user from pressing the PTT until releasing the PTT, thus including speech transfer from the talking user to all users that are listening to the group.

A single CVDP message flow for Group Call supports the following basic and supplementary services:

- Group Call;
- Broadcast Call;
- Late Entry;
- Priority Call;
- Pre-emptive Priority Call;
- Emergency Call;
- Talking Party Identification;
- Speech Item Pre-emption.

The following sub-features and supplementary services are supported by the application logic on the CVDP relay and endpoints:

- Hang timer;
- Maximum call duration;
- Speech item contention;
- User disconnect;
- Queuing mechanisms;
- Resource pre-emption;
- Subscriber pre-emption;
- Discreet Listening.

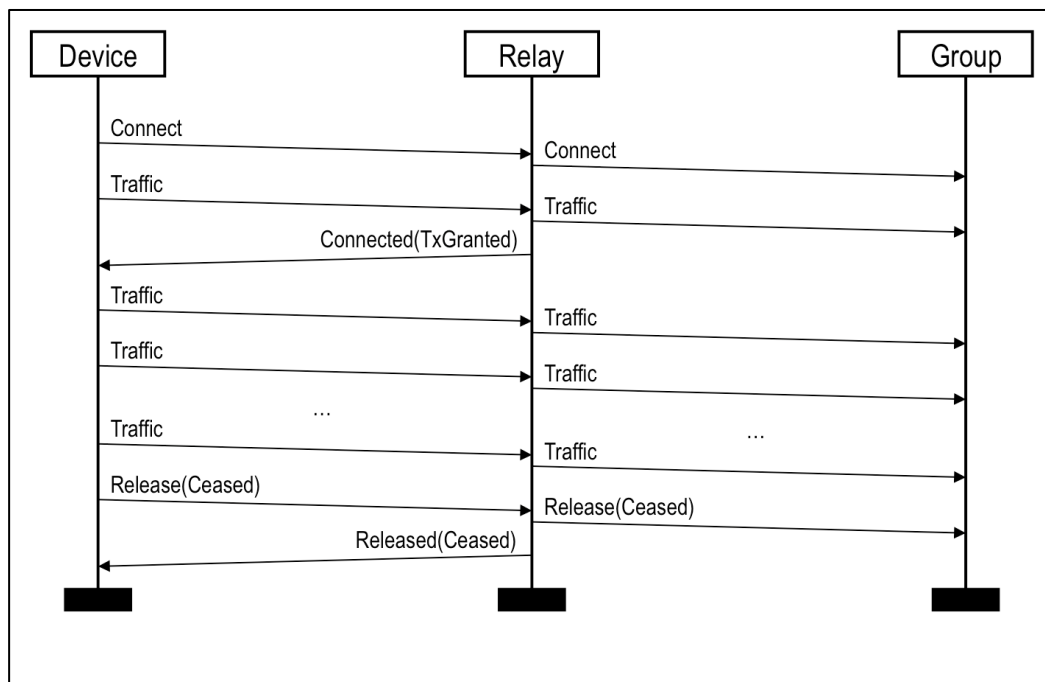


Figure 5 - Group Call

The **Connect** message indicates a new speech item to the Relay. This message shall include the Called user or group. The Calling user is optional to allow the Relay to distinguish between several User identities on which the Device is attached to the Relay. The Reference is assigned by the Relay after receiving the initial Connect message from the Device. The Priority field and Time stamp are optional.

The optional **Connected** message is returned by the Relay to inform the Device whether transmission can continue, delayed until further notice, or rejected. This message includes the speech item Reference to correlate this message with previous and future messages. Note that the transmitting node should not delay transmission of speech until this message is received.

The **Traffic** message carries a single speech packet. This message includes the Codec type, the Data block with the data of a single speech packet, an optional Sequence number for detection of missing speech packets, and a speech item Reference to correlate the speech packet with the correct Connect message.

The **Release** message indicates the end of a speech item to the Relay. This message includes the speech item Reference to correlate this message with the correct Connect message.

It is permitted for the CVDP device to start voice traffic transmission already before the **Connected** message is received. The Connected message will then instruct the CVDP device whether to continue or stop transmission. The following variants on the above MSC scenario should be considered:

- User is permitted to continue talking: Connected with granted status Transmit returned immediately (as shown in MSC above);
- User is not permitted to establish this call: Connected with granted status Reject returned immediately, talking user should be informed about rejected call;
- User is not permitted to talk (other user already speaks): Connected with granted status Queue returned immediately, talking user should be alerted, no more Traffic packets may be sent until further notice;
- User is permitted to talk after other user stops talking while PTT is still pressed: Connected with granted status Transmit is returned as soon as other user stops talking, allowing transmission of Traffic packets to be resumed;
- User is interrupted during talking due to a higher priority speech item (Speech Item Pre-emption): Connected with granted status Rejected attribute is returned as soon as other higher priority user starts talking, talking user should be alerted, no more Traffic packets may be sent.

Other notes:

- The Release message is sent after releasing the PTT button in any of the described scenarios;
- The CVDP Relay sends late entries as repetitive Connect messages with the same content as the initial Connect message;
- Traffic packets are sent by the transmitting device or application and retransmitted by the CVDP Relay with a fixed interval, unlike the timing shown in the MSC whereby the stream is interrupted by the Connect packet.

3.4 Individual Call

The CVDP message flow for Individual Call covers the following basic and supplementary services:

- Individual Call;
- Telephony Call;
- Call Identification;
- Include Call;
- Call transfer;
- Call Authorised by Dispatcher;
- Ambience Listening.

The following sub-features and supplementary services are supported by the application logic on the CVDP relay and endpoints:

- Direct connect;
- Hook signalling;
- Simplex / duplex operation;
- Speech item contention;
- Hang timer;
- Maximum call duration;
- User disconnection;
- Queuing mechanisms;
- Resource pre-emption;
- Subscriber pre-emption;
- Direct Dial In;
- Discreet Listening.

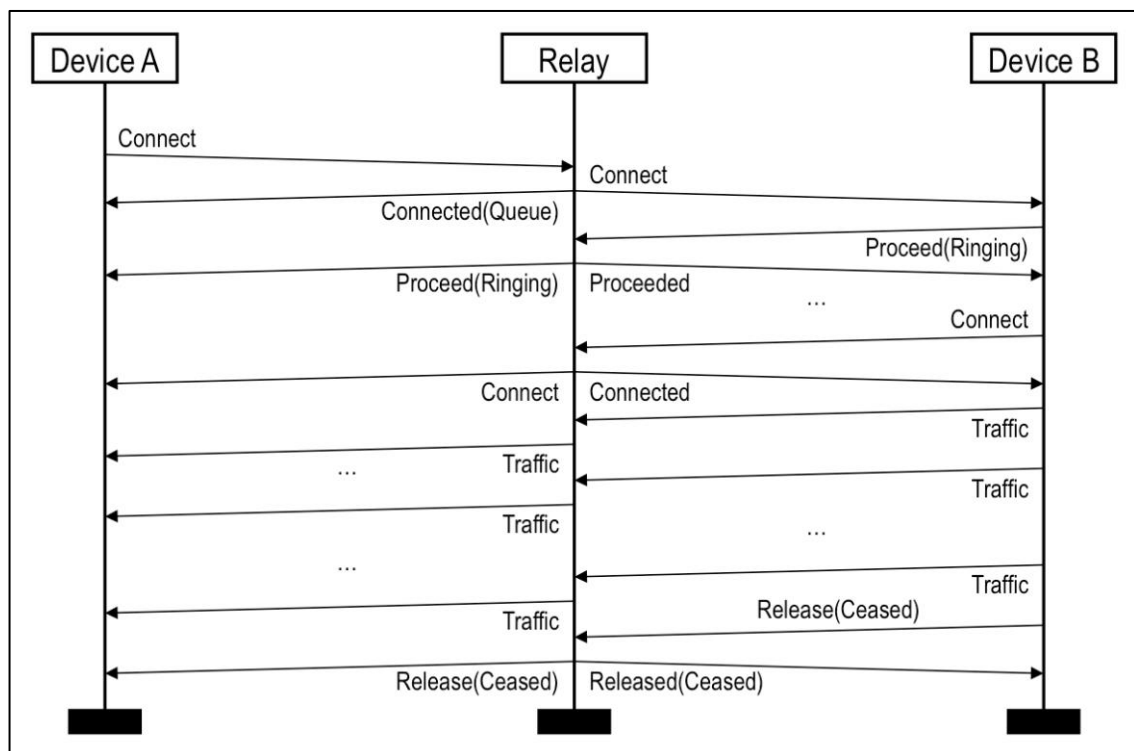


Figure 6 - Individual Call

The **Connect** message indicates a new individual call with speech item to the Relay. This message shall include the Called user. The Calling user is optional to allow the Relay to distinguish between several User identities on which the Device is attached to the Relay. The Reference is assigned by the Relay after receiving the initial **Connect** message from the Device. The Priority field and Time stamp are optional.

The **Connected** message is returned by the Relay to confirm the Granted status; when the called device is provisioned in the Relay to accept the call manually (referred to as "Hook signalling"), the Grant status Queue is returned. No further **Traffic** packets may be sent then, and an audible and visible indication must be presented to the user to indicate the queuing status.

After receiving the **Connect** message, the called Device returns a **Proceed** message with step Ringing to indicate that the Device has started ringing. The Relay forwards this message to the calling Device, and returns a **Proceeded** message to the called Device, both with a timeout on accepting the call.

When the user accepts the call, the called Device confirms this with a **Connect**. Again the Relay forwards this message to the calling Device, and returns a **Connected** message to the called Device, now with an inactivity timeout.

The **Traffic** message carries a single speech packet. This message includes the Codec type, the Data block with the data of a single speech packet, an optional Sequence number for detection of missing speech packets, and a speech item Reference to correlate the speech packet with the correct **Connect** message.

The **Release** message indicates the end of a speech item to the Relay. This message includes the speech item Reference to correlate this message with the correct **Connect** message. The Relay forwards this message to the other Device, and returns a **Released** message to the previously transmitting Device. Note that the call is still active on the Relay and Devices while waiting for follow-up speech items or a request to end the call by one of the users.

Variations:

- Include call: any authorised party can initiate an include call by means of a Connect with the same Reference as the on-going call.

3.5 Messaging

The CVDP message flow for Messaging covers the following basic and supplementary services for individual and group addressed messaging:

- Status Messaging;
- Text Messaging;
- Binary Messaging;
- Key delivery for End-to-End-Encryption;
- Location messages;
- Call Identification;
- Flash Message.

The following sub-features and supplementary services are supported by the application logic on the CVDP relay and endpoints:

- Transport Layer (TL) protocol;
- Location Services;
- Transport of Sensor Data;
- Discreet Listening.

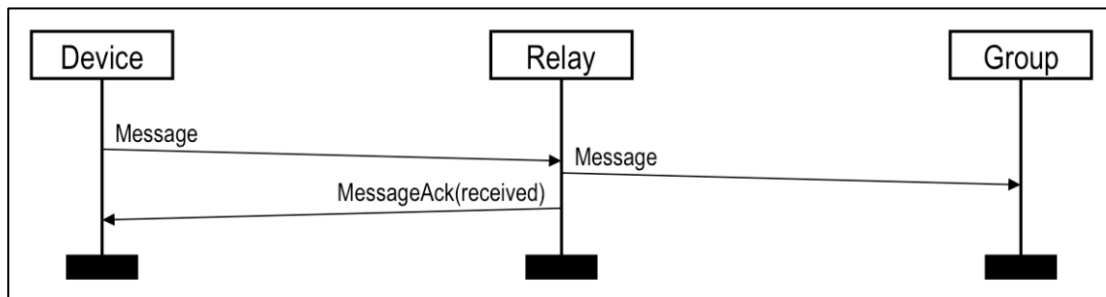


Figure 7 - Message to group of Devices

Messaging starts with a **Message** that is sent from one Device to either a group or an individual Device. The Message can carry text, status or a binary data. Well-defined variants include location messages and key delivery messages; these are both binary messages with a specific Pid (Protocol ID). For transfer of a message to a group of devices, the sender will receive a **MessageAck** with a received indication, while no confirmation of delivery is received from the group members.

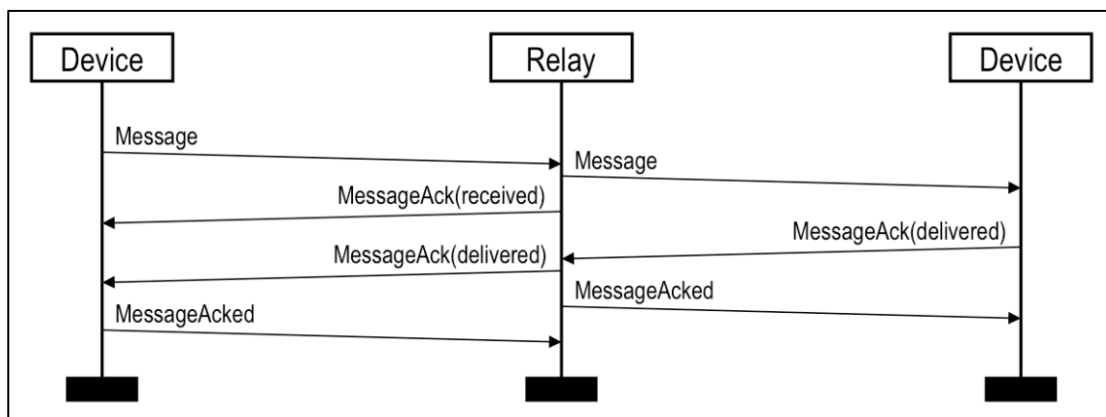


Figure 8 - Message to individual Device

For transfer of a message to specific devices, the sender will receive first a **MessageAck** with a *Received* indication, followed by a **MessageAck** with a *Delivered* indication as soon as the called Device confirms message reception. A **MessageAcked** should confirm this **MessageAck** in order to ensure end-to-end delivery.

3.6 Remote execution

Remote execution functionality allows triggering certain functionality on a CVDP application by the CVDP relay or another CVDP application. The following supplementary services are implemented by means of Remote execution over CVDP:

- Disable and Enable;
- Permanent Disable;
- DTMF over dial.

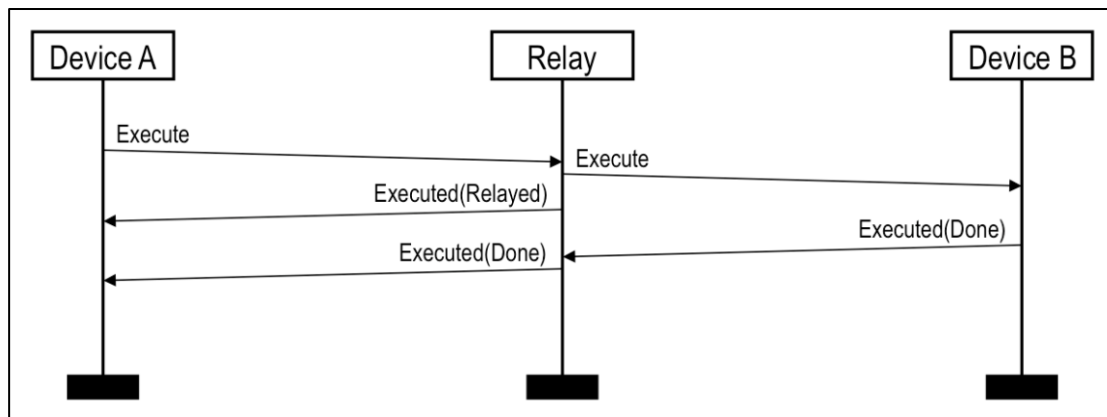


Figure 9 - Remote execution method

Remote execution is triggered with an **Execute** message that is sent from one Device to another Device through the Relay. The **Execute** message includes the method, optional parameter and a sequence number. Relaying and execution of the remote procedure is confirmed by an **Executed** message with respectively a **Relayed** and **Done** response.

4 CVDP MESSAGE CONTENT

The following sections provide an overview of messages defined for the Critical Voice and Data Protocol (CVDP).

4.1 Primitives

4.1.1 Attach

Primitive	Attach		
Description	Attach device, user or group		
Applicable MSCs	Attachment		
Response to	-		
Response expected	Attached, Authenticate		
Attribute	Type	C/O/M	Remark
Device	Cdata	O	Device to attach
User	Cdata	O	User to attach
GroupAttach	Element	O	Group(s) to attach
Reference	Integer	O	Message reference
Examples XML			
<Attach Device="AP1284"/>			
<Attach Reference "1279"> <GroupAttach Group="9001" Mode="Selected"/> </Attach>			

4.1.2 Attached

Primitive	Attached		
Description	Confirmation that device, user or group is attached		
Applicable MSCs	Attachment		
Response to	Attach, Authenticate		
Response expected	-		
Attribute	Type	C/O/M	Remark
Device	Cdata	O	Attached device
User	Cdata	O	Attached user
GroupAttach	Cdata	O	Attached group(s)
Result	Enum	M	Result of attachment
Reference	Integer	M	Message reference
Examples XML			
<Attached Device="AP1284" Reference="1276" Result="Accept"/>			

4.1.3 Authenticate

Primitive	Authenticate		
Description	Authenticate device or user		
Applicable MSCs	Attachment		
Response to	Attach / Authenticate		
Response expected	Authenticate / Attached		
Attribute	Type	C/O/M	Remark
Device	Cdata	O	Device to authenticate
User	Cdata	O	User to authenticate
Challenge	Cdata	O	Challenge data
Response	Cdata	O	Response data
Reference	Integer	M	Call reference number
Example XML			
<Authenticate Device="AP1284" Challenge="6F5Ed7aG" Reference "1277"/>			

4.1.4 Connect

Primitive	Connect		
Description	Connect with group or individual user		
Applicable MSCs	Group Call, Individual Call		
Response to	-		
Response expected	- / Connected / Proceed		
Attribute	Type	C/O/M	Remark
Called	Cdata	M	Called group or user
Calling	Cdata	O	Calling / talking user
Name	Cdata	O	Name alias of calling / talking user
Time	Integer	O	Timestamp
Priority	Integer	O	Call priority
Broadcast	Integer	O	Broadcast flag
Hook	Integer	O	Hook signalling
Duplex	Integer	O	Duplex flag
Ambience	Integer	O	Ambience listening flag
Timeout	Integer	O	Timeout for inactivity
Reference	Integer	O	Message reference
Example XML			
<Connect Called="Interop" Calling="2405" Time="48886032" Priority="0" Reference "3844"/>			

4.1.5 Connected

Primitive	Connected		
Description	Confirms connect status		
Applicable MSCs	Group Call, Individual Call		
Response to	Connect		
Response expected	-		
Attribute	Type	C/O/M	Remark
Granted	Enum	M	Granted status
Timeout	Attribute	O	Timeout for inactivity
Reference	Integer	M	Message reference
Example XML			
<Connected Granted="Transmit" Timeout="7" Reference "3844"/>			

4.1.6 Execute

Primitive	Execute		
Description	Remote procedure execution		
Applicable MSCs	Remote execution		
Response to	-		
Response expected	Executed		
Attribute	Type	C/O/M	Remark
Called	Cdata	M	Addressed device
Method	Enum	M	Method to execute
Parameter	Cdata	O	Parameter value
Reference	Integer	O	Message reference
Example XML			
<Execute Called="3506" Method="Disable" Reference "4198"/>			

4.1.7 Executed

Primitive	Executed		
Description	Confirm remote procedure execution		
Applicable MSCs	Remote execution		
Response to	Execute		
Response expected	- / MessageAcked		
Attribute	Type	C/O/M	Remark
Reply	Enum	M	Reply on remote execution
Reference	Integer	M	Message reference
Example XML			
<MessageAck Progress="Received" Reference "4198"/>			

4.1.8 Message

Primitive	Message		
Description	Status, text or binary message		
Applicable MSCs	Messaging		
Response to	-		
Response expected	MessageAck		
Attribute	Type	C/O/M	Remark
Called	Cdata	M	Called device, user or group
Pid	Cdata	O	Protocol Identifier
Status	Integer	O	Status number
Text	Cdata	O	Text message content
Data	Cdata	O	Binary message content
Reference	Integer	O	Message reference
Example XML			
<Message Text="Hello, world" Reference "4193"/>			
<Message Pid="LIP" Binary="0dEH1x9rW5kPQ"/>			

4.1.9 MessageAck

Primitive	MessageAck		
Description	Message acknowledge		
Applicable MSCs	Messaging		
Response to	Message		
Response expected	- / MessageAked		
Attribute	Type	C/O/M	Remark
Progress	Cdata	M	Progress indication
Reference	Integer	M	Message reference
Example XML			
<MessageAck Progress="Relayed" Reference "4193"/>			

4.1.10 MessageAked

Primitive	MessageAked		
Description	Message acknowledged		
Applicable MSCs	Messaging		
Response to	MessageAck		
Response expected	-		
Attribute	Type	C/O/M	Remark
Reference	Integer	M	Call and speech item reference
Example XML			
<MessageAked Reference "4193"/>			

4.1.11 Proceed

Primitive	Proceed		
Description	Proceeds the call		
Applicable MSCs	Individual Call		
Response to	Connect / -		
Response expected	Proceeded / -		
Attribute	Type	C/O/M	Remark
Step	Enum	M	Proceed step
Timeout	Integer	O	Timeout for inactivity
Reference	Integer	M	Message reference
Example XML			
<Proceed Step="Ringing" Reference "3910"/>			

4.1.12 Proceeded

Primitive	Proceeded		
Description	Call is proceeding		
Applicable MSCs	Individual Call		
Response to	Proceed		
Response expected	-		
Attribute	Type	C/O/M	Remark
Step	Enum	M	Proceed step
Timeout	Integer	O	Timeout for inactivity
Reference	Integer	M	Message reference
Example XML			
<Proceeded Step="Ringing" Timeout="20" Reference "3910"/>			

4.1.13 Provide

Primitive	Provide		
Description	Provide records		
Applicable MSCs	Provisioning		
Response to	- / ProvideAck		
Response expected	ProvideAck		
Attribute	Type	C/O/M	Remark
Reference	Integer	M	Message reference
Sequence	Integer	O	Sequence number
Class	Enum	M	Class of subscription
Record	Element	O	Record(s) to transfer
Example XML			
<pre><Provide Reference "3844" Sequence="2" Class="Groups"> <Record Key="9001" Value="Group 9001"/> <Record Index="9002" Value="Group 9002"/> </Provide></pre>			

4.1.14 ProvideAck

Primitive	ProvideAck		
Description	Confirm records		
Applicable MSCs	Provisioning		
Response to	Provide		
Response expected	- / Provide		
Attribute	Type	C/O/M	Remark
Reference	Integer	M	Message reference
Sequence	Integer	O	Sequence number
Example XML			
<pre><ProvideAck Reference "3844" Sequence="2"/></pre>			

4.1.15 Release

Primitive	Release		
Description	Indicates end of speech item or call		
Applicable MSCs	Group Call, Individual Call		
Response to	-		
Response expected	- / Released		
Attribute	Type	C/O/M	Remark
Cause	Enum	M	Cause of release
Timeout	Integer	O	Timeout for extending call
Reference	Integer	M	Message reference
Example XML			
<pre><Release Cause="Ceased" Reference "3844"/></pre>			

4.1.16 Released

Primitive	Released		
Description	Confirms end of speech item or call		
Applicable MSCs	Group Call, Individual Call		
Response to	Release		
Response expected	-		
Attribute	Type	C/O/M	Remark
Cause	Enum	M	Cause of release
Timeout	Integer	O	Timeout for extending call
Reference	Integer	M	Message reference
Example XML			
<Released Cause="Ceased" Reference "3844"/>			

4.1.17 Subscribe

Primitive	Subscribe		
Description	Subscribe to database		
Applicable MSCs	Provisioning		
Response to	-		
Response expected	Subscribed		
Attribute	Type	C/O/M	Remark
Calling	Cdata	O	User or device requesting for subscription
Class	Enum	M	Class of subscription
Domain	Cdata	O	Information domain
Example XML			
<Subscribe Class="Groups"/>			

4.1.18 Subscribed

Primitive	Subscribed		
Description	Confirm subscription		
Applicable MSCs	Provisioning		
Response to	Subscribe		
Response expected	-		
Attribute	Type	C/O/M	Remark
Calling	Cdata	O	User requesting for subscription
Class	Enum	M	Class of subscription
Domain	Cdata	O	Information domain
Example XML			
<Subscribed Class="Groups"/>			

4.1.19 Traffic

Primitive	Traffic		
Description	Single speech packet		
Applicable MSCs	Group Call, Individual Call		
Response to	-		
Response expected	-		
Attribute	Type	C/O/M	Remark
Codec	Enum	M	Codec type
Data	Cdata	M	Speech packet data
Sequence	Integer	O	Speech packet sequence number
Reference	Integer	M	Message reference
Example XML			
<Traffic Codec="ACELP" Data="1neX7sAAA)d9mBz7cgOf9kAA" Reference "3844"/>			

4.2 Elements

4.2.1 GroupAttach

Element	GroupAttach		
Description	Group attachment request or response		
Used in	Attach, Attached		
Attribute	Type	C/O/M	Remark
Group	Cdata	M	Group identity
Mode	Enum	O	Attachment mode
ScanPriority	Integer	O	Scan priority
Address	Cdata	O	Multicast IP address
Port	Cdata	O	Port number
Example XML			
<pre><GroupAttach Group="9001" Mode="Selected" ScanPriority="0" Address="230.155.67.109" Port="32566"/></pre>			

4.2.2 Record

Element	Record		
Description	Database record		
Used in	Provide		
Attribute	Type	C/O/M	Remark
Key	Cdata	M	Group, user or configuration key
Value	Cdata	M	Value to assign
Example XML			
<pre><Record Key="9001" Value="Group 9001"/></pre>			

4.3 Attributes

4.3.1 Ambience

Attribute	Ambience		
Description	Ambience listening flag		
Used in	Connect		
Type	Value	Description	Remark
Integer	0	Normal voice call	Default
	1	Ambience listening call	

4.3.2 Broadcast

Attribute	Broadcast		
Description	Broadcast flag		
Used in	Connect		
Type	Value	Description	Remark
Integer	0	No broadcast	Possible to talk back (default)
	1	Broadcast	Not possible to talk back

4.3.3 Calling

Attribute	Calling		
Description	Calling user		
Used in	Connect, Subscribe, Subscribed		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.4 Called

Attribute	Called		
Description	Called user, group or device		
Used in	Connect, Execute, Message		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.5 Cause

Attribute	Cause		
Description	Cause of release		
Used in	Release, Released		
Attribute	Value	Description	Remark
Enum	Ceased	Ceased PTT button	
	Inactivity	Expiry of inactivity timeout	
	Timeout	Expiry of call timeout	
	User	User ended call	

4.3.6 Challenge

Attribute	Challenge		
Description	Challenge data		
Used in	Authenticate		
Type	Value	Units	Remark
Cdata	String	n/a	Encoded in Base64 [10]

4.3.7 Class

Attribute	Class		
Description	Class of subscription		
Used in	Provide, ProvideAck, Subscribe, Subscribed		
Attribute	Value	Description	Remark
Enum	Configuration	Configuration database	
	Users	User database	
	Groups	Group database	

4.3.8 Codec

Attribute	Codec		
Description	Specifies codec type		
Used in	Traffic		
Attribute	Value	Description	Remark
Enum	ACELP	TETRA ACELP vocoder	
	AMR	AMR 12 kbps vocoder	
	ADPCM	ADPCM 32 kbps codec	
	PCM	PCM 64 kbps codec	

4.3.9 Data

Attribute	Data		
Description	Speech or binary data		
Used in	Traffic, Message		
Type	Value	Units	Remark
Cdata	String	n/a	Encoded in Base64 [10]

4.3.10 Device

Attribute	Device		
Description	Device identity		
Used in	Attach, Attached, Authenticate		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.11 Domain

Attribute	Domain		
Description	Information domain		
Used in	Subscribe, Subscribed		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.12 Duplex

Attribute	Duplex		
Description	Duplex flag		
Used in	Connect		
Type	Value	Description	Remark
Integer	0	Simplex / semi-duplex	User must press PTT to talk
	1	Full duplex	User can talk and listen simult.

4.3.13 Granted

Attribute	Granted		
Description	Granted status		
Used in	Connected		
Attribute	Value	Description	Remark
Enum	Transmit	Granted to transmit	
	Reject	Not granted	
	Queue	Wait for later granting	

4.3.14 Group

Attribute	Group		
Description	Group identity		
Used in	GroupAttach		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.15 Hook

Attribute	Hook		
Description	Hook signalling		
Used in	Connect		
Type	Value	Description	Remark
Integer	0	Direct connect	No request to accept call
	1	Hook signalling	Request to accept call (default)

4.3.16 Key

Attribute	Key		
Description	Group, user or configuration key		
Used in	Record		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.17 Method

Attribute	Method		
Description	Method to execute		
Used in	Execute		
Attribute	Value	Description	Remark
Enum	Disable	Remote disable	
	Enable	Remote enable	
	PermanentDisable	Remote permanent disable	

4.3.18 Mode

Attribute	Mode		
Description	Group attachment mode		
Used in	GroupAttach		
Attribute	Value	Description	Remark
Enum	Selected	Group selected	
	Selectable	Group selectable	
	NotSelectable	Group not selectable	

4.3.19 Name

Attribute	Name		
Description	Name alias		
Used in	Connect		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.20 Parameter

Attribute	Parameter		
Description	Parameter value		
Used in	Execute		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.21 Pid

Attribute	Pid		
Description	Protocol Identifier		
Used in	Message		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.22 Priority

Attribute	Priority		
Description	Priority level		
Used in	Connect		
Type	Value	Units	Remark
Integer	0 ~ 15	n/a	

4.3.23 Progress

Attribute	Progress		
Description	Progress indication		
Used in	MessageAck		
Attribute	Value	Description	Remark
Enum	Delivered	Message delivered	
	Read	Message read by user	
	Relayed	Message relayed	

4.3.24 Reference

Attribute	Reference		
Description	Message reference		
Used in	Attach, Attached, Authenticate, Connect, Connected, Execute, Executed, Message, MessageAck, MessageAcked, Proceed, Proceeded, Provide, ProvideAck, Release, Released, Traffic		
Type	Value	Units	Remark
Unsigned Integer	0 ~ 2 ³² -1	n/a	

4.3.25 Reply

Attribute	Reply		
Description	Reply on remote execution		
Used in	Executed		
Attribute	Value	Description	Remark
Enum	Done	Execution done	
	Relayed	Execution relayed	
	Rejected	Execution rejected	

4.3.26 Response

Attribute	Response		
Description	Response on challenge		
Used in	Authenticate		
Type	Value	Units	Remark
Cdata	String	n/a	Encoded in Base64 [10]

4.3.27 Result

Attribute	Result		
Description	Result of attachment and authentication		
Used in	Attached		
Attribute	Value	Description	Remark
Enum	Accept	Accepted	
	AuthenticationFailure	Authentication Failure	
	DeviceNotFound	Device not in database	
	GroupNotFound	Group not in database	
	UserNotFound	User not in database	

4.3.28 ScanPriority

Attribute	ScanPriority		
Description	Scan priority		
Used in	Attach, Attached		
Type	Value	Units	Remark
Integer	0 ~ 15	n/a	

4.3.29 Sequence

Attribute	Sequence		
Description	Sequence number		
Used in	Traffic, Provide, ProvideAck		
Type	Value	Units	Remark
Unsigned Integer	0 ~ $2^{32}-1$	n/a	

4.3.30 Status

Attribute	Status		
Description	Status number		
Used in	Message		
Type	Value	Units	Remark
Integer	0 ~ 65535	n/a	

4.3.31 Step

Attribute	Step		
Description	Proceed step		
Used in	Proceed, Proceeded		
Attribute	Value	Description	Remark
Enum	Accept	Call accepted by user	
	Reject	Call rejected by user	
	Ringing	Device is ringing	

4.3.32 Talking

Attribute	Talking		
Description	Talking party number		
Used in	Connected		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.33 Text

Attribute	Text		
Description	Text message content		
Used in	Message		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.34 Time

Attribute	Time		
Description	Timestamp		
Used in	Connect		
Type	Value	Units	Remark
Integer	0 ~ 86399999	ms	Time in ms since 0:00

4.3.35 Timeout

Attribute	Timeout		
Description	Timeout for follow-up signalling		
Used in	Connect, Connected, Proceed, Proceeded, Release, Released		
Type	Value	Units	Remark
Integer	0 ~ 3600000	ms	Maximum 1 hour

4.3.36 User

Attribute	User		
Description	User identity		
Used in	Attach, Attached, Authenticate		
Type	Value	Units	Remark
Cdata	String	n/a	

4.3.37 Value

Attribute	Value		
Description	Value to assign		
Used in	Record		
Type	Value	Units	Remark
Cdata	String	n/a	

5 COMPLIANCE ANALYSIS

This section describes the properties of CVDP that ensure compliance with the requirements as defined in deliverable D6.2.

5.1 Performance

5.1.1 Call setup performance

Call setup performance is measured as the period time between initiating the call on the calling device until the reception of the call by the called device. The call setup performance depends on various aspects, including call setup procedure (group call, individual call), signalling protocol and delay aspects caused by the system architecture. It should be noted that group calls is the primary mode of PMR operation, which requires fast call setup in order to speak immediately, especially during emergency situations.

For reference, traditional telephone calls over GSM and 3G are established in between a period of 3 to 11 seconds [6] due to the traditional circuit-switched system architecture. Voice-over-LTE (VoLTE) improves the call setup performance of telephony calls to the order of 2 to 4 seconds [7]; the protocol and system architecture of VoLTE using the IP Multimedia Subsystem (IMS) still adds significant complexity [8] and thus increased overhead for processing of signalling messages. This is also true for standards-based PTT-over-Cellular (PoC) [9] over LTE, which is known to offer a call setup period in the order of 0,5 to 1 second for group calls.

Note that IMS based functionality is the de-facto method for 3G and VoLTE based 4G telephony and therefore useful for making standard telephone calls by PPDR users in public networks.

For comparison, the proposed CVDP signalling messages and system architecture is much simplified for faster operation to allow for sub 300 ms group call setup performance over LTE, without compromising reliability. In fact, the typical group call setup delay can be reduced to less than 150 ms for typical performance of current UEs (smartphones, embedded PC-based devices) and the CVDP Relay application that runs on a standard COTS server platform. This is possible thanks to the streamlined operation of group calls, for which the signalling and voice stream is send forward while waiting for confirmation to continue talking [11]. This is illustrated by Table 1, in which the end-to-end call setup performance is measured and shown as a series of delays, assuming a 30 ms transit delay of the LTE network when using HARQ (see section 5.6.4).

The total end-to-end call setup performance is thus 60 ms (calling UE) plus 55 ms (called UE) = 115 ms when using the proper QCI (assume QCI 5)..

The fast call setup performance provides ample headroom for parallel transmission of large number of downlink Connects to the called UEs when IP unicast is available only for multi-party calls. The parallel transmission of large number of packets through the LTE network is primary limited by the downlink capacity of a single LTE base station, whereby a typical capacity of reaching 10 different UEs per milli-seconds is assumed.

Entity	Delay aspect	Uplink calling Device	Downlink calling Device	Downlink called Device
Calling Device	Recognise PTT	20 ms		
Calling Device	Call processing	5 ms		
LTE network	Transfer initiating Connect	30 ms		
CVDP Relay	Call processing	5 ms		
LTE network	Transfer returned Connected		30 ms	
Calling Device	Call processing		5 ms	
Calling Device	Visual feedback		20 ms	
LTE network	Transfer forwarded Connect			30 ms
Called Device	Call processing			5 ms
Called Device	Visual feedback			20 ms
TOTAL delay		60 ms	55 ms	55 ms

Table 1 - Delay budget for Group Call setup

Considering the scenario of calling 300 users in a single cell, one Connect message can thus be forwarded per 0,1 ms for transmission over a single LTE cell, resulting in approximate $300 \times 0,1 \text{ ms} = 30 \text{ ms}$ for the latest called UE to be reached. The worst-case end-to-end call setup performance of $115 + 30 = 145 \text{ ms}$ is thus still lower than 300 ms. It is to be noted that the call-set up delay will also be influence by the cell load; specific QCI will have to be used to ensure that the Connect messages will get the required quality of service criteria indicator (QCI) and priority level over the LTE system (for instance QCI 5 which is provided high priority non guaranteed bit rate bearer).

5.1.2 Speech transfer latency

Transfer of speech can be executed in parallel with the group call setup; this means that the microphone path can already be opened when pressing the PTT button in order to minimise speech transfer latency. For speech encoding the TETRA ACELP vocoder [12] with a speech frame size of 60 ms is chosen.

Entity	Delay aspect	Downlink calling Device	Downlink called Device
Calling Device	Buffer and encoding of speech	80 ms	
LTE network	Transfer Traffic packet from source UE	30 ms	
CVDP Relay	Traffic packet relay	5 ms	
LTE network	Transfer Traffic packet to destination UE		30 ms
Called Device	Decoding and playout of speech packet		70 ms
TOTAL delay		115 ms	100 ms

Table 2 - Delay budget for Speech Transfer

The total end-to-end speech transfer latency is thus 115 ms (calling UE) plus 100 ms (called UE) = 215 ms. Again considering the scenario of reaching 300 users in a single cell, the latest listening UE will receive the ACELP encoded Traffic packet after $300 \times 0,1 \text{ ms} = 30 \text{ ms}$, resulting in a worst-case end-to-end speech delay of $215 + 30 = 245 \text{ ms}$.

It is to be noted that the speech transfer delay will also be influenced by the cell load; specific QCI will have to be used to ensure that the Connect messages will get the required quality of service criteria indicator (QCI) and priority level over the LTE system (for instance QCI 1 that is providing guaranteed bit rate with low delay budget and high priority).

5.1.3 Number of voice calls

The following three aspects are related to the supported number of voice calls:

- The number of voice calls that can be established per second;
- The maximum number of simultaneous voice calls;
- The maximum number of simultaneous voice streams to all devices.

The supported number of voice calls is mostly limited by the capabilities and performance of wireless IP networks and base stations. With limited or no support of IP multicast or broadcast, a separate call and voice stream has to be established to each Device within an active group call. This results in very high number of signalling and voice packets to a large number of Devices.

As an example, 300 Devices that are attached to a single group on a single base station require delivery of $300 \times (1.000 / 60) = 5.000$ voice packets per second (on basis of ACELP coded voice packets with 60 ms duration consisting of two concatenated 30 ms frames) if no IP multicast or broadcast is supported, whereby the base station must allow 300 simultaneous active data connections.

The maximum number of simultaneous voice streams to all devices is also the expected bottleneck for performance of the CVDP solution, while the number of voice packets exceeds by far the number of signalling packets that are required for establishing and maintaining voice calls. For comparison, a group call to the same 300 devices during a 5 second period and 2 second late entry interval requires $300 \times (1 + 2) = 900$ signalling packets and $5.000 \times 5 = 25.000$ voice packets.

CVDP addresses this challenge by offering a high degree of scalability due to the low amount of processing required for CVDP support of the Relay. The most critical aspect of distributing voice packets to a large number of Devices is addressed by using the same IP packet content for each addressed Device, eliminating the need to encode each IP packet separately.

Regarding the requirements in deliverable D6.2 that are aligned with the limits of the TETRA standard, it is expected that the 900 simultaneous voice streams (3 calls with 300 members each, 15 calls with 60 members each) is easy to achieve. Also the requirement of 15 calls per second, using IP unicast, multicast or broadcast, should be no problem for the CVDP solution. Obviously, support of multiple base stations require transmission of a multitude of number of packets, although for multi-site solutions the expected load for the total number of Devices will be more spread over the network.

5.1.4 Speech quality

The speech quality is determined by the vocoder technology used for compression of speech. CVDP supports a number of modern and legacy vocoder standards in order to balance speech quality and bitrate, as well as lossless transfer of speech by supporting the legacy vocoder standards.

The following table specifies the supported vocoder standards with the Mean Opinion Score (MOS), packet duration, packet size and resulting bitrate:

Vocoder standard	Application	Mean Opinion Score (MOS)	Frame duration	Frame length	Bits per second
PCM [13]	Telephony	4,45	20 ms	1.280 bits	64.000 bps
ADPCM [14]	Telephony	4,30	20 ms	640 bits	32.000 bps
AMR [15]	3G / LTE	4,14	20 ms	244 bits	12.200 bps
OPUS [16]	Internet	3,80	20 ms	160 bits	8.000 bps
TETRA ACELP [12]	TETRA	3,40	30 ms	137 bits	4.566 bps

Table 3 - CVDP supported speech vocoder standards

The best compromise on voice quality and bitrate is delivered by the Adaptive Multi-Rate (AMR) vocoder. AMR narrowband quality exceeds the MOS value of 4, enabling toll quality voice for a reasonable bitrate, also in PPDR environments [27]. For interworking with TETRA, obviously the TETRA ACELP vocoder should be chosen to avoid transcoding, causing further voice quality degradation (impact of MOS) and additional speech delay. CVDP allows real-time switching between speech vocoder standards in order to support interworking scenarios.

5.2 Scalability

A high degree of scalability is provided by the low amount of CPU performance required for operation of the CVDP Relay. Relevant aspects for this low amount of processing include:

- Most CVDP messages can be forwarded without modification by the Relay - re-encoding of messages is thus not necessary;
- The call setup and voice packets for multiple listeners in a group call are identical, allowing the same message to be used for transmission to all applicable IP addresses when IP unicast is available only;
- Only a few states and timers need to be maintained per call and Device, allowing look-up tables to be allocated in memory instead of requiring database access;
- CVDP transactions are simple by design, allowing implementation in a single protocol layer on application level.

The typical performance of a server platform allows decoding of signalling and voice packets of hundreds of simultaneous calls, and delivery of signalling and voice packets to thousands of devices. Scalability beyond a single server is enabled by partitioning of Relays, for example by using a Relay per agency or part of an agency. Methods for call routing between relays and cascading of Relays is outside the scope of the present specification document, but can be made more or less invisible to Devices.

The simple solution architecture and low processing overhead of CVDP is particular advantageous for small deployments, like stand-alone operation within fast deployable LTE networks. The 3GPP-based IP Multimedia Subsystem (IMS) framework is often proposed for PTT operations over LTE network, but the heavy architecture of IMS [8] requires far more processing and communication between components, and therefore suitable only for public LTE networks that require roaming and handover of standard telephony voice calls between different GSM, UMTS and LTE networks.

5.3 Availability

The following aspects should be considered in order to improve availability:

- Support of equipment redundancy;
- Support of fallback configurations;
- Support of link redundancy;
- Support of multiple wireless networks.

5.3.1 Equipment redundancy

Equipment redundancy protects against hardware and software failures. High availability requires fast detection and recovery from a failing component. Within a CVDP-based solution the requirement for equipment redundancy can be fulfilled by means of redundant Relays, whereby the a specific IP address can be claimed by the active Relay only, or by two or more Relays with separate IP addresses that can be active simultaneously.

To support both scenarios, each Device should be configured for at least two IP addresses in order to connect automatically to the active Relay. Selection of the next IP address in the list can be triggered when not receiving a response to the Device Attach message.

With the default 5-second interval the recovery takes in average 8 seconds (first 0 to 5 seconds to recognise the failure, and an addition 5 seconds to recover from the failure). This is acceptable for PPDR applications that typically require 99,98% availability, while the 8 second recovery period allows for more than 780 of these switch-overs per year whereby a worst-case equipment MTBF of 80.000 hours results in just one switch-over per 9 years.

5.3.2 Fallback operation

Fallback operation is most appropriate for fast deployable networks, which do not guarantee interconnection to the regional or countrywide network. A fallback configuration consists of a stand-alone Relay for support of all local CVDP operations, allowing forwarding or expansion of calls when the called device(s) are not or not all available in the local network.

5.3.3 Link redundancy

Link redundancy can be either solved within the backhaul IP network (e.g. by means of IP/MPLS) [17] or by interconnecting components using two separate IP links or -networks. This requires two Ethernet ports per device, of which each port has its own IP address configuration. CVDP supports these two IP configurations by the same mechanism as used for equipment redundancy.

5.3.4 Multiple wireless networks

The fourth scenario for improving availability is the use of multiple wireless networks in order to improve coverage. Examples include roaming between multiple public LTE networks and indoor coverage by Wi-Fi networks in addition to outdoor coverage by LTE.

Proper routing of IP packets through a private IP network or the public Internet should allow the use of a single Relay for both networks. The mechanism to roam between different networks is further explained in section 3.1.

5.4 Security

Confidentiality, integrity, authentication, access control and non-repudiation of the overall CVDP-over-LTE solution is enabled by the following standard and optional security measures:

- The 3GPP based LTE standard supports commercial grade (mutual) authentication and encryption [18] in order to prevent eavesdropping and replay of IP packets over unicast and multicast bearers;
- Devices can be connected over an IPSec [19] tunnel to the CVDP Relay, adding additional protection for integrity, confidentiality and authentication;
- CVDP packets may be protected further by applying Transport Layer Security (TLS) [4], also adding additional protection for integrity, confidentiality and authentication;
- The current iteration of CVDP offers protection by means of public safety grade authentication and access control;
- The current iteration of CVDP offers protection against unauthorised access when Devices are lost or stolen by means of Remote Disable and Permanent Disable.
- The next iteration of CVDP will define End-to-End Encryption mechanisms [20] for support of public safety grade encryption algorithms based on the TETRA standard, adding additional protection for confidentiality, integrity and non-repudiation. This End-to-End Encryption can be applied to voice, data and signalling information.

Although IPSec and TLS are both standards based options that will further enhance the security of the CVDP solution with minimum specification and implementation effort, the required CPU performance for maintaining sessions and encrypting packets severely limits the capacity of the CVDP relay. In addition, IPSec and TLS both do not support simultaneous delivery of voice packets to multiple Devices by means of IP multicast and broadcast, required for more efficient group calls.

5.5 Functional requirements

5.5.1 Basic services

The PMR basic services are covered by the following CVDP messages and attributes:

Service	Message flow	Applicable attributes
Group call	Connect > Connected	Called
Individual Call	Connect > Connected	Called
Telephony Call	Connect > Connected	Called
Broadcast Call	Connect	Broadcast
Status messaging	Message	Status Text
Text messaging	Message	Text
Binary messaging	Message	Pid Data
(De-) Registration	Attach > Attached	Device
Group attachments	Attach > Attached	GroupAttach

Table 4 - Compliance of PMR basic services

5.5.2 PMR supplementary services

The PMR supplementary services are covered by the following CVDP messages and attributes:

Service	Message flow	Applicable attributes
Late Entry	Connect	Called
Priority	Connect	Priority
Pre-emptive Priority Call	Connect	Priority
Talking Party Identification	Connect	Calling
Call Identification	Connect	Calling
Speech Item Priority	Connect	t.b.d.
Dynamic Regrouping	Attach > Attached	GroupAttach
Ambience Listening	Connect	Ambience
Discreet Listening	Connect	n/a
Location Reporting	Message	Pid Data

Table 5 - Compliance of PMR supplementary services

5.5.3 Telephony supplementary services

The telephony supplementary services are covered by the following CVDP messages and attributes:

Service	Message flow	Applicable attributes
Barring of Incoming Calls	Connect	Called
Barring of Outgoing Calls	Connect	Calling
Call Authorised by Dispatcher	Connect	Priority
Call Forwarding on Busy	Connect	t.b.d.
Call Forwarding on No Reply	Connect	t.b.d.
Call Forwarding on Not Reachable	Connect	t.b.d.
Call Forwarding Unconditional	Connect	t.b.d.
Call Hold	Proceed	Step
Include Call	Connect	Called
Call Transfer	Connect	Called

Table 6 - Compliance of telephony supplementary services

5.5.4 Security services

The security services are covered by the following CVDP messages and attributes:

Service	Message flow	Applicable attributes
Authentication	Authenticate > Attached	Challenge Response Result
Mutual authentication	Authenticate > Attached	Challenge Response Result
Enable - disable	Execute > Executed	Method
Permanent disable	Execute > Executed	Method
End to End Encryption	Connect	t.b.d.

Table 7 - Compliance of security services

5.6 Interoperability with IP networks

5.6.1 Support of IP multicast

CVDP supports IP multicast [21] [25] by informing all devices on the specific multicast IP address and port number for each monitoring group, thus both the selected group used for talking and scanning group used for listening only.

This IP multicast configuration is transferred by means of the Address and Port attributes within the GroupAttach element, and is thus known beforehand when the Device is registered on the Relay.

Note that a specific multicast IP address and port number can also be reused for multiple groups, while the Called attribute still allows for additional filtering of group call setup and speech packets of monitoring groups. This is useful for scenarios where the allocated bandwidth for a multicast stream exceeds by far the required bandwidth for a single CVDP voice stream, or when concatenating messages is beneficial to limit the number of packets.

It should also be noted that likely other methods will be developed within 3GPP according the Group Communications System Enablers (GCSE) requirements that can also be used by the CVDP solution on application level. These may require different mechanisms for group attachments that are incompatible with the standard IP multicast methods.

5.6.2 Limited bandwidth

IP bandwidth requirements can be kept small by choosing speech codecs that offer high compression. For example, the TETRA ACELP speech codec [12] generates 137 bits per sub-frame of 30 ms, resulting in 274 bits for each 60 ms period. The total required bandwidth for CVDP speech transfer is calculated in the following table:

Component	Number of bytes
ACELP speech packet of 274 bits encoded in Base64 [10]	$274 / 6 = 46$ bytes (rounded up)
Overhead for XML encoding ¹	49 bytes
Overhead for UDP/IP header ²	28 bytes
TOTAL IP packet size	$46 + 49 + 28 = 123$ bytes
IP bandwidth required for one voice stream	$1000 / 60 \times 123 \times 8 = \mathbf{16,4\text{ kbps}}$ ³

Table 8 - IP bandwidth calculation

Notes:

1. The Real-Time Protocol (RTP) is not applied to voice packets to avoid extra overhead and enabling easier references between signalling and voice packets.
2. IPv6 will be considered in deliverable D6.6.
3. The IP bandwidth can be dramatically decreased by compression of XML and UDP/IP headers. This enables reduction of IP packet size to approximately $1000 / 60 \times 60$ bytes = 8 kbps.

5.6.3 High delay links

High delay links are well supported by CVDP while a call setup does not require a confirmation from the relay and receiving device before speech packets are sent. Especially with high delay links this results in significant improvement of the call setup period, as illustrated in the next figure:

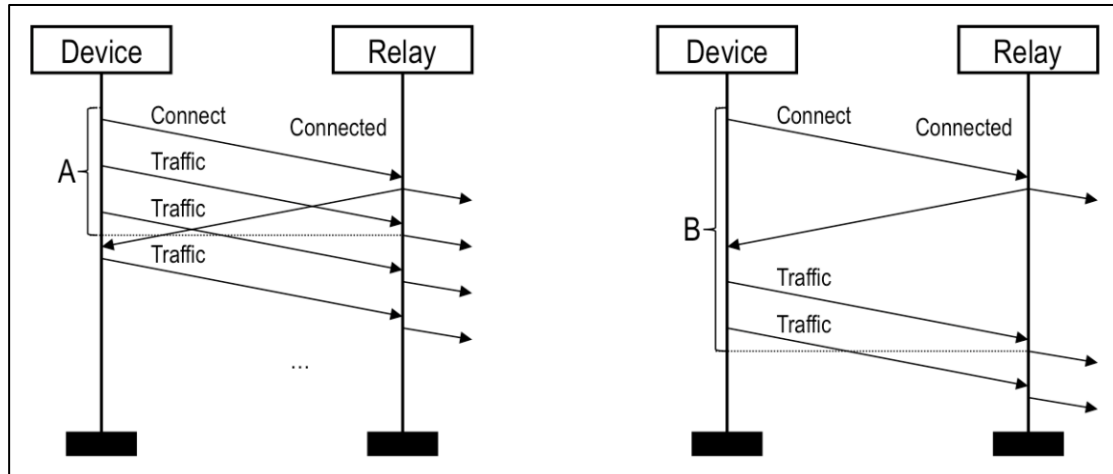


Figure 10 - High delay link scenario

The following table compares the call setup period including first speech packet transfer based on a 400 ms satellite link for interconnection of Device A, whereby a generic 20 ms processing delay and 60 ms codec speech delay is assumed, and a negligible link delay is assumed for interconnection of Device B.

Component	Delay A	Delay B
Processing delay Device A	20 ms	20 ms
Encoding delay speech Device A	60 ms	60 ms
Satellite link delay for Connect	400 ms	400 ms
Processing delay of Relay	20 ms	20 ms
Processing delay Device B	-	20 ms
Processing delay of Relay	-	20 ms
Satellite link delay for Connected	-	400 ms
Processing delay Device A	-	20 ms
Satellite link delay for Traffic	-	400 ms
Processing delay Device B	20	20 ms
Decoding delay speech Device B	60	60 ms
TOTAL end-to-end delay	580 ms	1.440 ms

Table 9 - End-to-end delays for satellite link scenario

5.6.4 Packet drops

Packet drops frequently occur in wireless communication systems due to an inadequate signal-to-noise ratio or disturbance caused by interference and signal reflections.

LTE supports IP packet retransmissions in the link layer in order to reduce the chance of packet drops. The Hybrid Automatic Repeat Request (HARQ) method implemented in LTE uses Forward Error Correcting (FEC) mechanisms in combination with selective acknowledgements and retransmissions, allowing transmission errors on the air interface to be corrected typically within a period from 8 to 24 ms if a maximum of 3 retransmissions is assumed [24].

The HARQ method to decrease the number of packet drops is significantly superior to e.g. the application of TCP/IP for correcting packet drops, while TCP/IP does not allow real-time delivery of speech packets and is not suitable for broadcast and multicast IP packet delivery. Instead, CVDP relies on UDP/IP, which is perfectly suitable for delivery of speech packets, and with some specific measures can be made suitable for signalling and data transfer as well.

Three mechanisms are included in CVDP to protect against remaining packet drops:

- The Connect message is sent periodically by the transmitting Device in order to ensure that the call is received by the receiving Device(s) even when the first message(s) are missed. This method is known as "Late Entry", and also allows Devices to join a call later when selecting the appropriate group or roaming to another wireless network.
- Certain messages are repeated until acknowledged by the Relay and receiving Device. In CVDP a simple ARQ scheme is proposed, which is applicable for provisioning, message transfer and remote execution of methods on a Device.
- Timeouts are defined to ensure that calls and attachments do not "hang" in the Device or Relay when follow-up messages are lost.

These mechanisms improve the CVDP call setup and speech transfer reliability much beyond the typical performance of other Voice-over-IP protocols like SIP.

5.6.5 Network roaming

Network roaming between different wireless networks is supported in CVDP by means of periodic Device Attachments. These Attachments confirm the availability and IP address of the Device to the Relay, and are executed every (say) 5 seconds to ensure sufficient fast recovery from lost connections. Wireless networks can include public LTE networks, private LTE networks as well as Wi-Fi networks. Note that roaming in between cells within a single LTE network are executed much faster due to the support of (almost) seamless roaming and handover of data connections by LTE.

Recovery of voice calls after network roaming is supported by the "Late Entry" mechanism in CVDP. This means that the voice call will be restored after execution of a Device Attachment in the new network. To enable faster recovery of voice calls it is possible to trigger an immediate Device Attachment when unexpected packet drops occur. This mechanism needs to be defined still.

5.7 Interworking with Legacy PMR networks

5.7.1 TETRA

CVDP is much inspired by the TETRA standard [25]; hence interworking with TETRA networks can be implemented relatively easily. The interworking is implemented by means of CVDP gateways, either by line or radio connected interfaces to the TETRA network. The support and level of interworking is listed for each functionality in the table below.

Functionality (SALUS naming)	Mobile gateway	Line gateway
Group Call	Yes	Yes
Group Attachment	No	Limited
Broadcast Call	Yes	Yes
Individual Call	Yes	Yes
Talking Party Identification	Yes	Yes
Call Identification	Yes	Yes
Late Entry	-	-
Priority Call	Yes	Yes
Pre-emptive Priority Call	Yes	Yes
Emergency Call	Yes	Yes
Speech Item Priority	Yes	Yes
Tactical Patch	-	-
Dynamic Regrouping	No	Limited
Telephony Call	Limited	Yes
Barring of Incoming Calls	-	-
Barring of Outgoing Calls	-	-
Call Authorised by Dispatcher	-	-
Include Call	-	-
Call Forwarding	Limited	Yes
Call Transfer	Limited	Yes
Ambient Listening	No	Yes
Discreet Listening	-	-
Status Messaging	Yes	Yes
Text Messaging	Yes	Yes
Binary Messaging	Limited	Yes
Location Reporting	Limited	Yes
Authentication	-	-
Mutual authentication	-	-
End to End Encryption	Limited	Yes
Enable disable	No	Yes
Permanent disable	No	Yes

Table 10 - Capabilities of TETRA gateway

5.7.2 TETRAPOL

Interworking with TETRAPOL networks is implemented by means of CVDP gateways, either by line or radio connected interfaces to the TETRAPOL network. The support and level of interworking is listed for each functionality in the table below.

Functionality (SALUS naming)	Mobile gateway	Line gateway
Group Call	Yes	Yes
Group Attachment	No	Limited
Broadcast Call	-	-
Individual Call	No	Yes
Talking Party Identification	Yes	Yes
Call Identification	Yes	Yes
Late Entry	-	-
Priority Call	Yes	Yes
Pre-emptive Priority Call	Yes	Yes
Emergency Call	Yes	Yes
Speech Item Priority	-	-
Tactical Patch	-	-
Dynamic Regrouping	No	Limited
Telephony Call	-	-
Barring of Incoming Calls	-	-
Barring of Outgoing Calls	-	-
Call Authorised by Dispatcher	-	-
Include Call	-	-
Call Forwarding	-	-
Call Transfer	-	-
Ambient Listening	-	-
Discreet Listening	-	-
Status Messaging	No	Yes
Text Messaging	No	Yes
Binary Messaging	-	-
Location Reporting	-	-
Authentication	-	-
Mutual authentication	-	-
End to End Encryption	Limited	Yes
Enable disable	-	-
Permanent disable	-	-

Table 11 - Capabilities of TETRAPOL gateway

6 CONCLUDING REMARKS

The Critical Voice and Data Protocol (CVDP) specification has evolved during the first half of the SALUS project duration into this specification document and a proof-of-concept implementation that has proven the scalability, robustness and performance of the protocol and solution.

Additional features will be specified and implemented until March 2015, enhancing and adding new capabilities for voice, status, text, location, picture and video transfer. It is also expected that some of the existing messages will be refined further to enable more robust exception handling.

The following work for specification of prototyping remains to be done for the final SALUS deliverable D6.6:

- Completion of CVDP support for Call Diversion, Include Call, Transfer Call, Call Hold, Call Authorised by Dispatcher and Speech Item Priority;
- Detailed description of algorithms used for Authentication (note: TETRA Authentication algorithms are used in the meantime, but these cannot be published);
- Methods for fast recovery of voice calls after roaming to another wireless network;
- CVDP support of Instant Messaging including Availability Status;
- CVDP support of standard TETRA End-to-End Encryption (E2EE) mechanisms and algorithms;
- New CVDP methods and protocol support to trigger and maintain standards-based picture and video streaming;
- Methods to compress XML coding and UDP/IP headers;
- Detailed specification of middleware components.

APPENDIX A - TETRA LIP format

The TETRA LIP format is used in CVDP for transferring location information. TETRA LIP [26] is widely used for PPDR applications using the TETRA standard, but also adopted within the Digital Mobile Radio (DMR) standard.

The TETRA LIP short format has a fixed packet length of 76 bits, and is transferred as a binary message with Pid = and 13 characters in Base64 [10] format within the Data attribute.

Information element	Length	C/O/M	Remark
PDU type	2	M	Value 0 = Short location report
Time elapsed	2	M	0 = less than 5 s, 1 = less than 5 min, 2 = less than 30 min, 3 = unknown
Longitude	25	M	Steps of $360/2^{25}$ degrees in range of -180 ~ +180 degrees
Latitude	24	M	Steps of $360/2^{24}$ degrees in range of -90 ~ +90 degrees
Position error	3	M	0 = less than 2 m, 1 = less than 20 m, 2 = less than 200 m, 3 = less than 2 km, 4 = less than 20 km, 5 = less than 200 km, 6 = more than 200 km, 7 = unknown
Horizontal velocity	7	M	Value 0 - 28 = speed in km/h; Value more than 28 = +3,8% for each step; Value 127 = speed unknown
Direction of travel	4	M	Steps of 22,5 degrees, whereby 0 = North (N); Value 15 = 33,7 degrees or unknown
Type of additional data	1	M	Not used
Reason for sending	8	O	Not used
User defined data	8	O	Not used

Bibliography

- [1] SALUS Deliverable 4.3 "Business Analysis – Intermediate", March 2015
- [2] W3C "Extensible Markup Language (XML) 1.0 (Fifth Edition)", November 2008
- [3] IETF RFC-768 "User Datagram Protocol", August 1980
- [4] IETF RFC 5246 "The Transport Layer Security (TLS) Protocol", version 1.2, August 2008
- [5] SALUS Deliverable D6.2 "PMR-over-LTE services definition - Intermediate", version 1.1, January 2015
- [6] Anacom report "Quality of Service Assessment", November 2011
- [7] Signals Research Group report "VoLTE Performance Analysis", November 2014
- [8] 3GPP TS 23.228 v13.1.0 "Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 13)"
- [9] Open Mobile Alliance OMA-AD-PoC-V2.1 "Push to talk Over Cellular (PoC) Architecture", August 2011
- [10] IETF RFC 3548 "The Base16, Base32, and Base64 Data Encodings", S. Josefsson, October 2006
- [11] Rohill patent EP2160050B1 "Fast inter system push to talk operation"
- [12] ETSI ETS 300 395-2 "Terrestrial Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 2: TETRA codec", February 1998
- [13] ITU-T Recommendation G.711 "Pulse Code Modulation (PCM) of Voice Frequencies"
- [14] ITU-T Recommendation G.726 "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)"
- [15] 3GPP TS 26.090 "Adaptive Multi-Rate (AMR) speech codec; Transcoding functions (Release 12)", version 12.0.0, September 2014
- [16] IETF RFC 6716 "Definition of the Opus Audio Codec", September 2012
- [17] IETF RFC 3469 "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery"
- [18] 3GPP TS 33.401 "3GPP System Architecture Evolution (SAE); Security architecture", version 12.13.0, December 2014
- [19] IETF RFC 4301 "Security Architecture for the Internet Protocol", December 2005
- [20] TETRA MoU SFPG Recommendation 02 "End-to-End Encryption", July 2001
- [21] IETF RFC 1112 "Host Extensions for IP Multicasting", August 1989
- [22] IETF RFC 3376 "Internet Group Management Protocol, Version 3", October 2002
- [23] IETF RFC 4604 "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", August 2006
- [24] 3GPP TS 36.213 "Evolved universal terrestrial radio access (E-UTRA); Physical layer procedures", version 12.4.0, January 2015
- [25] ETSI Technical Report ETR-300 1 "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Designers' guide; Part 1: Overview, technical description and radio aspects", May 1997
- [26] ETSI Technical Standard TS 100 392-18-1 "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D) and Direct Mode Operation (DMO); Part 18: Air interface optimized applications; Sub-part 1: Location Information Protocol (LIP)", version 1.3.1, April 2007
- [27] NTIA Report 13-493 "Intelligibility of the Adaptive Multi-Rate Speech Coder in Emergency-Response Environments", December 2012

Acronyms

3GPP	3rd Generation Partnership Project
ACELP	Algebraic Code-Excited Linear Prediction
ADPCM	Adaptive Differential Pulse Code Modulation
AMR	Adaptive Multi-Rate
ARQ	Automatic Repeat Request
CVDP	Critical Voice and Data Protocol
DMO	Direct Mode of Operations
DMR	Digital Mobile Radio
DTMF	Dual Tone Multi Frequency
E2EE	End to End Encryption
ETSI	European Telecommunications Standards Institute
EUTRAN	Evolved Universal Terrestrial Radio Access Network
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HARQ	Hybrid Automatic Repeat reQuest
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LIP	Location Information Protocol
LTE	Long Term Evolution
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
MSC	Message Sequence Chart
ODINI	On-Demand Intelligent Network Interface
OMA	Open Mobile Alliance
OTT	Over The Top
PCM	Pulse Code Modulation
PMR	Private Mobile Radio
PoC	PTT over Cellular
PPDR	Public Protection and Disaster Relief
PTT	Push To Talk
QCI	Quality of service Class Indicator
QoS	Quality of Service
RTP	Real-Time Protocol
TCCA	TETRA + Critical Communications Association
TCP	Transmission Control Protocol
TETRA	Terrestrial Trunked Radio Access
TLS	Transport Layer Security
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
VoLTE	Voice over LTE

Wi-Fi	Wireless Fidelity
XML	Extensible Markup Language