4th NG112 Emergency Services Plugtests; Remote event; 22nd February to 5th March 2021

Keywords
Testing, Interoperability, NG112

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

1 Executive Summary

ETSI, in partnership with EENA (the European Emergency Number Association) and NENA (The 9-1-1 Association), has organized the fourth Next Generation (NG112) Emergency Services Plugtests™ event. This event was run remotely by ETSI and IIT, 22nd February to 5th March 2021.

The aim of the event was to trial independently and jointly all components of the 112 communication chain based on Next Generation networks. Different topics were addressed, including TLS communication, Location Based Emergency Call Routing, Policy Based Emergency Call Routing, Next Generation Media Types.

10 organizations from around the world, including Asia, Europe, and North America, had the opportunity to connect their equipment to the test infrastructure and validate the interoperability and conformity of their market solutions using different scenarios and test cases, operating remotely from their own labs.

The scope of the event included TLS communications and content-rich emergency calling, such as video calling and TOTAL conversation. Participants put their products to the test, gaining valuable insights from experiencing a variety of scenarios. Tested technologies included Advanced Mobile Location (AML), TLS secured communication, Lightweight Messaging Protocol for Emergency Service Accessibility (LMPE).

The event was used to validate the standard ETSI TS 103 479 [i.1]: “Core elements for network independent access to emergency services”. This standard is published in 2019 and now is open for update. Test descriptions are available in the ETSI TS 103 480 [i.5] :”Interoperability testing of core elements for network independent access to emergency services”, available as draft. Additionally, in this 4th event, conformance tests were performed and can provide a basis for future certifications.

The results of the tests show that the NG112 technology is mature and that a large number of vendors provide the various elements of the NG112 equiment chain and that those elements interoperate with each other. Thus providing a large choice of innovative products to build next generation emergency communication solutions. With the upcoming publication of ETSI TS 103 479 [i.1] and its accompanying standards, the conditions for procurement and deployement are reached.

2 References

The following base specifications were validated in the Plugtest.

[i.1] ETSI TS 103 479: “Emergency Communications (EMTEL); Core elements for network independent access to emergency services”;

[i.2] ETSI TS 103 625: “Emergency Communications (EMTEL); Advanced Mobile Location (AML) for Emergency Calls”;

[i.3] ETSI TS 103 698: “Emergency Communications (EMTEL); Lightweight Messaging Protocol for Emergency Service Accessibility (LMPE)”;

[i.4] ETSI TS 101 470: “Emergency Communications (EMTEL); Total Conversation Access to Emergency Services”;

[i.5] ETSI TS 103 480 (Draft): “Emergency Communications (EMTEL); Interoperability testing of core elements for network independent access to emergency services”;

[i.6] ETSI TS 103 659: “Emergency Communications (EMTEL); Conformance test specifications for NG112”;

[i.7] ETSI TR 103 201: “Emergency Communications (EMTEL); Total Conversation for Emergency Communications, Implementation Guidelines”;

[i.8] 3GPP. TS 22.173: IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and Supplementary Services; Stage 1, Version 9.4.0, December 2009.

[i.9] 3GPP. TS 23.167: IP Multimedia Subsystem (IMS) Emergency Sessions, Version 9.3.0, December 2009.

[i.10] 3GPP. TS 24.229: IP Multimedia Call Control Protocol Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), Stage 3, Release 11, Version 11.4.0, June 2012

[i.11] Summary of all test resources at https://forge.etsi.org/rep/emergency-communications/NG112

3 Abbreviations

AML	Advanced Mobile Location
BCF	Border Control Function
ECRF	Emegency Call Routing Function
ESRP	Emergency Service Routing Proxy
GW	Gateway
HELD	HTTP-Enabled Location Delivery
IBCF	Interconnection Border Control Function
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IUT	Implementation Under Test
LIS	Location Information Server
LoST	LoST: A Location-to-Service Translation Protocol
LMPE	Lightweight Messaging Protocol for Emergency Service Accessibility
LRF	Location Retrieval Function
LTE	Long Term Evolution
MNO	Mobile Network Operator
PBX	Private Branch Exchange
PSAP	Public Safety Answering Point
SDP	Session Description Language
SIP	Session Initiation Protocol
SIP UA	SIPl User Agent
VoIP	Voice over IP
VoLTE	Voice over LTE
VSP	VoIP Service Provider
WS	Web Sockeet

4 Participants

The teams which executed tests during the ETSI Plugtest are listed below.

- Atos Public Safety
- Beta 80 S.p.A.
- DEC112 | Verein zur Förderung der Weiterentwicklung von standardisierten und barrierefreien Notrufen
- Frequentis AG

- GridGears GmbH
- Hellenic Mediterranean University
- HUAWEI TECHNOLOGIES Co. Ltd.
- Intersys AG
- MicroAutomation
- Oracle
- T-Mobile USA
- INdigital

5 Scope of the event

5.1 Objectives

Main objectives of this event were to:

- validate the interoperability of different solutions on the market on end to end emergency services communications untilizing NG112 core services;
- provide an opportunity for developers from different companies to get together to test their implementations and ensure interoperability between products;
- test the interoperability between European und US emergency communication standards;
- to evaluate the level of conformance of several implementations to interface specification (RFCs, TS, …).

5.2 Description

In this event three groups of tests considering different scenarios and test cases (examples: location based call routing, accessibility, different types of originating networks) were performed:

- NG112 core service conformance and interoperability tests;
- TLS communication interoperability tests with or without mutual authentication;
- Cross-Atlatic interoperability tests.

5.3 NG112 Conformance Tests

5.3.1 General

Conformance tests for the LIS, ECRF, PSAP and ESRP NG112 elements were performed. Test components were deployed 2 weeks before the event using ETSI HIVE infrastructure for organisations willing to participate in conformance tests. Test cases were defined in the ETSI TS 103 659 [i.6].

Note The NG112 Conformance tests was an optional ETSI service.

5.3.2 Location Information Service

Location is fundamental to the operation of the emergency services, and the generic functional entity that provides location is a Location Information Server (LIS). The Figure 1 lists scenarios considered for conformance testing.

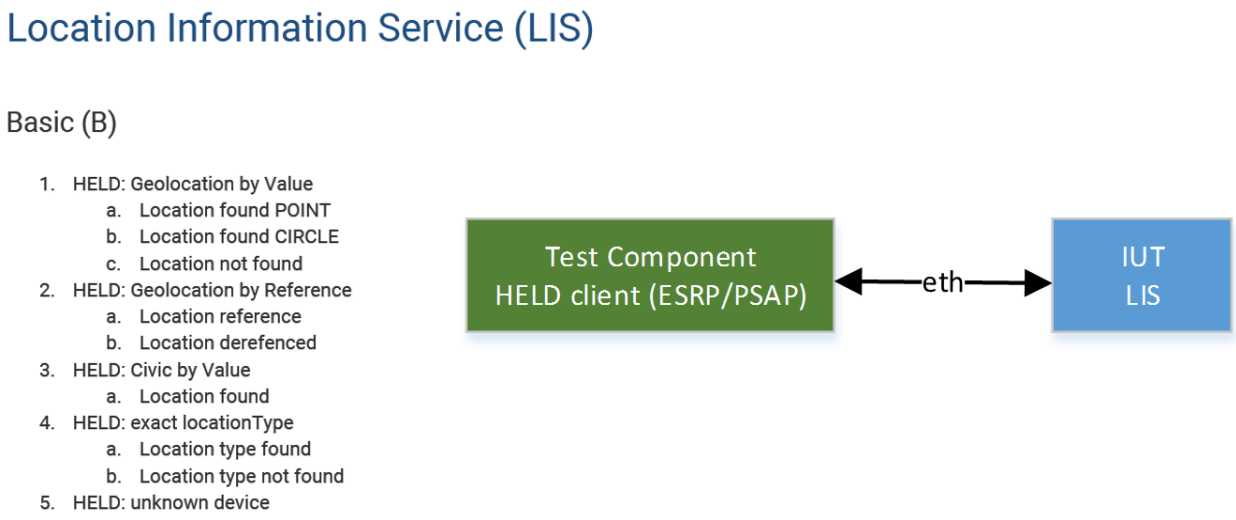

Figure 1: Scope of LIS tests

5.3.3 Emergency Call Routing Function

The functional element responsible for providing routing information to the various querying entities is the Emergency Call Routing Function (ECRF). The Figure 2 lists scenarios considered for conformance testing.

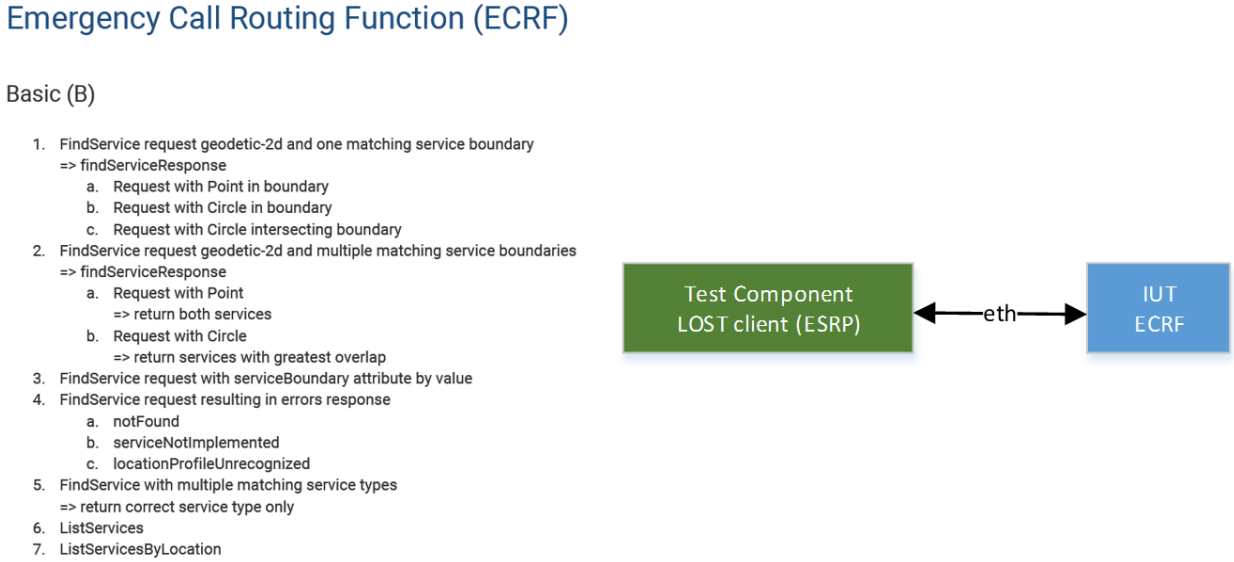

Figure 2: Scope of ECRF tests

5.3.4 Public Safety Answering Point

The PSAP deploys the SIP call interface including the multimedia capability, and the non-human-initiated call (emergency event) capability. The Figure 3 lists scenarios considered for conformance testing.

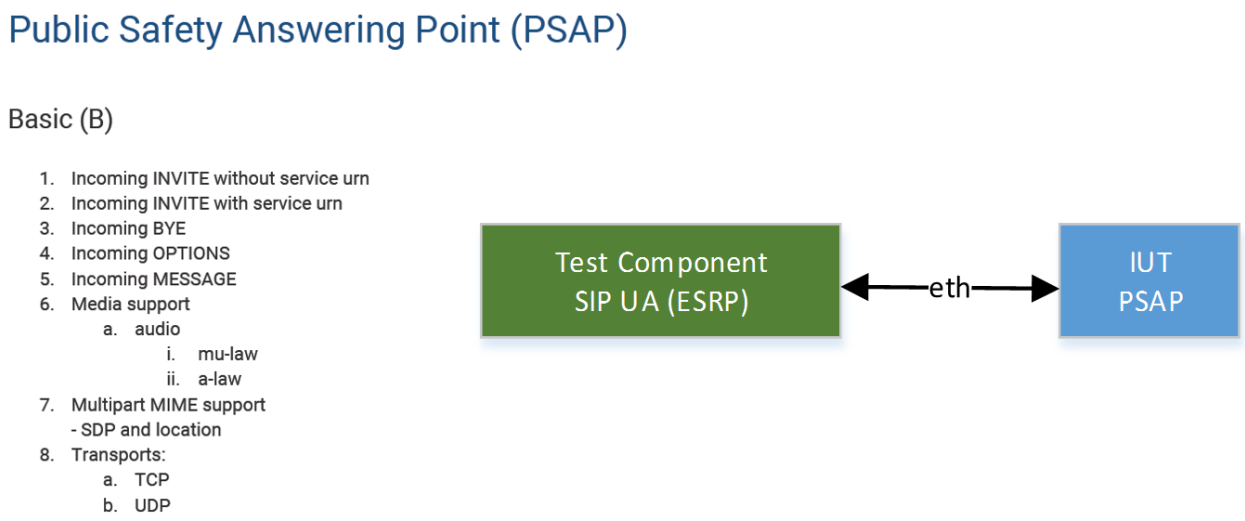

Figure 3: Scope of PSAP tests

5.3.5 Emergency Service Routing Proxy

The Emergency Service Routing Proxy (ESRP) is the base routing function for emergency calls. It shares interfaces with an LIS, ECRF, PSAP and BCF. The Figure 4 lists scenarios considered for conformance testing.

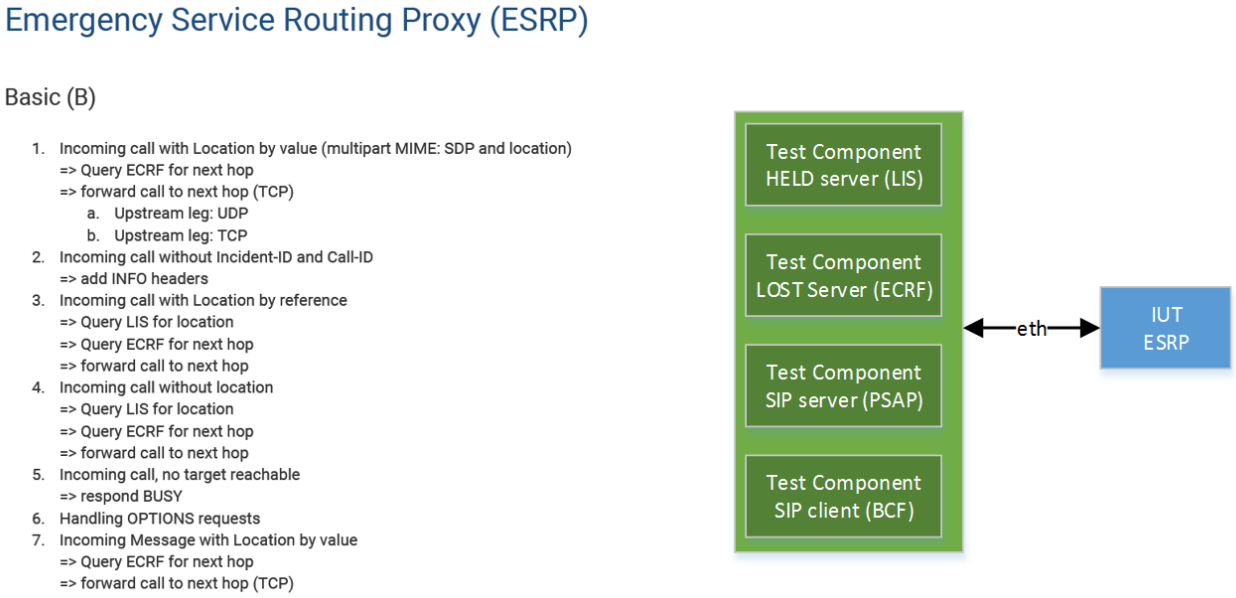

Figure 4: Scope of ESRP tests

5.4 NG112 Interoperability Tests

5.4.1 General

As in the previous editions of the NG112 Communications Plugtests event, the NG112 components and their interfaces, as shown in Figure 5, of different vendors were tested working together. Scenarios and vendors combinations were planned and tests were executed.

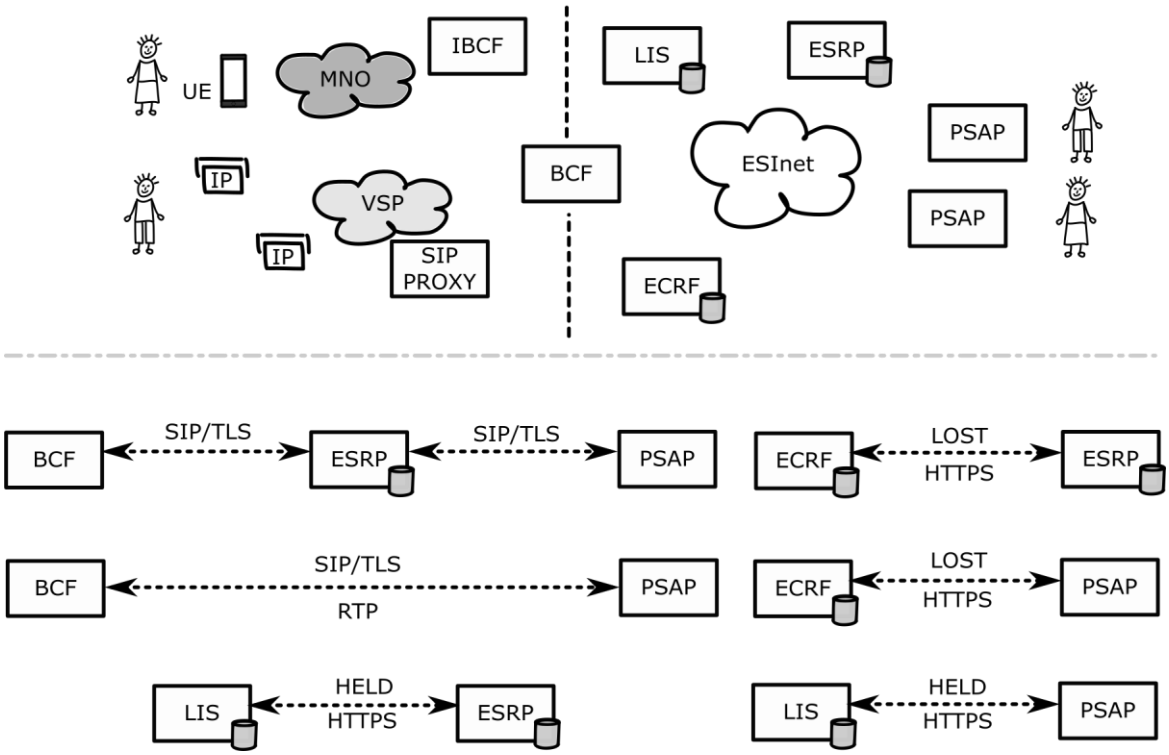

Figure 5: Functional elements and interfaces

The objectives of the tests were:

- **Connectivity**: Tests covered basic connectivity between functional elements at both, network and application layer
- **Routing**: Tests covered variants of location based emergency call routing. These included different methods how user location is assessed and how this information is delivered
- **Media**: Tests covered different media types in order to contact emergency services
- **Location**: Tests covered variants of location configuration and conveyance methods such as advanced mobile location (AML)
- **Security**: Tests covered the use of certificates for TLS client and server authentication (HTTPS and SIP/TLS)
- **ESInet**: Tests covered peering scenarios of different networks

5.4.2 Test Data

Testing several scenarios required to defince simple polygons that define PSAP areas (or service boundaries) surrounding the ETSI building. Figure 6 and Figure 7 show twelve polygons (rectangles) and predefined locations, three per each PSAP service boundary (2x point, 1x circle). ECRFs were configured with PSAP areas and SIP uris that represent a PSAP vendor's call processing equipment. LISs were preconfigured with locations (pin icons in Figure 6), for instance, sip:alice-01@plugtets.net, sip:bob-01@plugtets.net, sip:carol-01@plugtets.net (refert to Figure 7) resolve to a location within the top-left PSAP area shown in Figure 6, and, therefore, calls originated by ***alice-01*** shall route the the PSAP configured for that region (***PSAP01***).

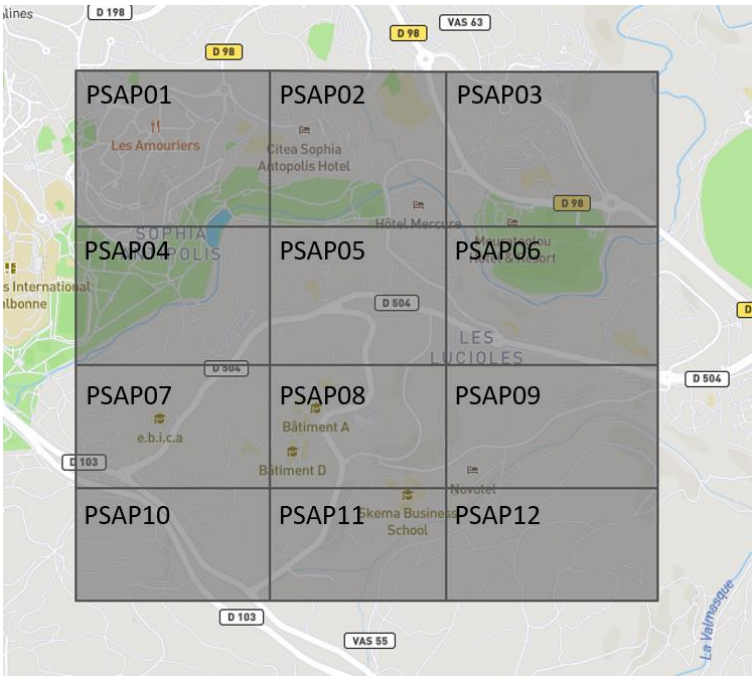

Figure 6: PSAP service boundaries (map source: geojson.io)

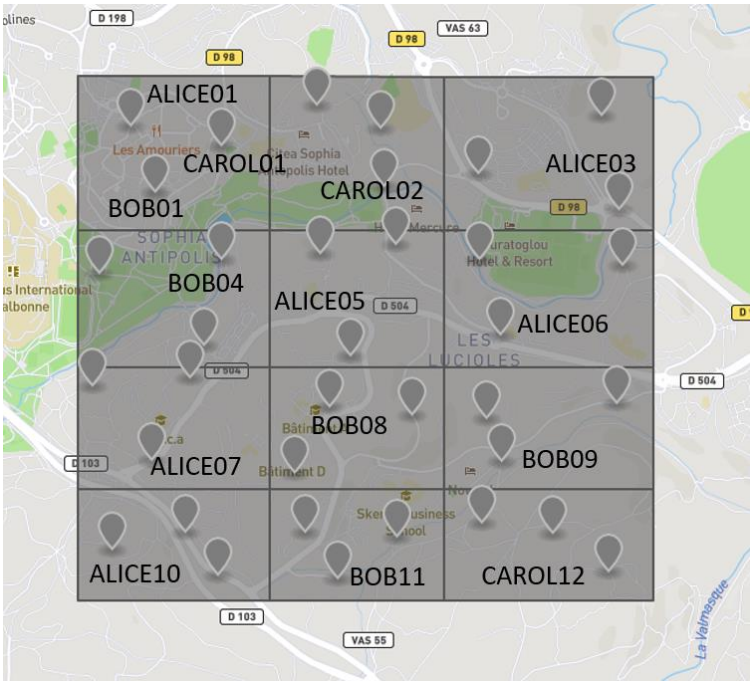

Figure 7: Service regions and manually configured locations (map source: geojson.io)

5.4.3 Configuration

Differnet test configurations were used to test interoperability among different service instances from different vendors. The basic configurion, as briefly shown in Figure 8 below, supports Next Generation Core Service (NGCS) testing scenarios, including scenarios with different service urns (URN), multimedia communication (audio, video and text) and location delivery using identities (sip and tel URIs). Most test calls were placed from local user equipment (UE) configured to register one of the predefined identities with a SIP proxy (emulated VSP scenario). Depending on the emergency numbers dialled, the SIP proxy forwarded calls to the border control function (BCF) inserting corresponding service urns, listed as follows:

- 112 (urn:service:sos), or 911 (urn:service:sos)

- 15 (urn:service:sos.ambulance)
- 17 (urn:service:sos.police)
- 18 (urn:service:sos.fire)

BCFs used static routing or a preloaded route to forward calls to the ESRP used in specific scenarios or combinations. A pre-loaded route supports the automatic selection of an ESRP, i.e. a possibility to define the combination of individual core services already in the source network and thus helps to simplify the test process. To route to the correct PSAP based on the location received or requested at the LIS via HELD, the ESRP was requesting routing information at the configured ECRF, and finally forwarding the emergency call to the PSAP serving the location at which the caller is located.

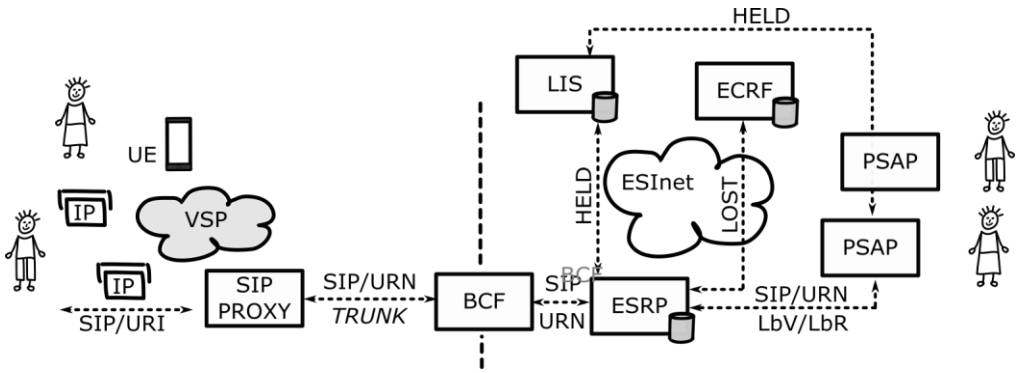

Figure 8: General NGCS Configuration

Minor changes to the basic configuration were needed to support location by reference (LbR) testing. In that scenario, the *public* (VSP) SIP proxy requested location information at the LIS using the identity (tel or sip uri) received with the emergency call. The reponse in a LbR scenario is an URL to be inserted in the SIP request as Geolocation header value. The next downstream element that requires location information uses the URL to dereference location information via HTTPS.

To test location as a value, the *public* (VSP) SIP proxy forwarded calls either already with a service urn and location information or by inserting a service urn, in which case the ESRP requested location information at the LIS using the identity (tel or sip uri) received with the emergency call. In addition, the ESRP inserts location information as a value (PIDF-LO) into the SIP message as part of a multipart MIME body. The next downstream element that requires location information (e.g., PSAP) uses the location received as a value in the message.

Testing AML required to interface with a mobile network operator (4G) using a location independent phone number, VoIP gateway (GW) services of a public VoIP service provider and a termination point within the lab (SIP PBX/PROXY), refer to Figure 9 below.

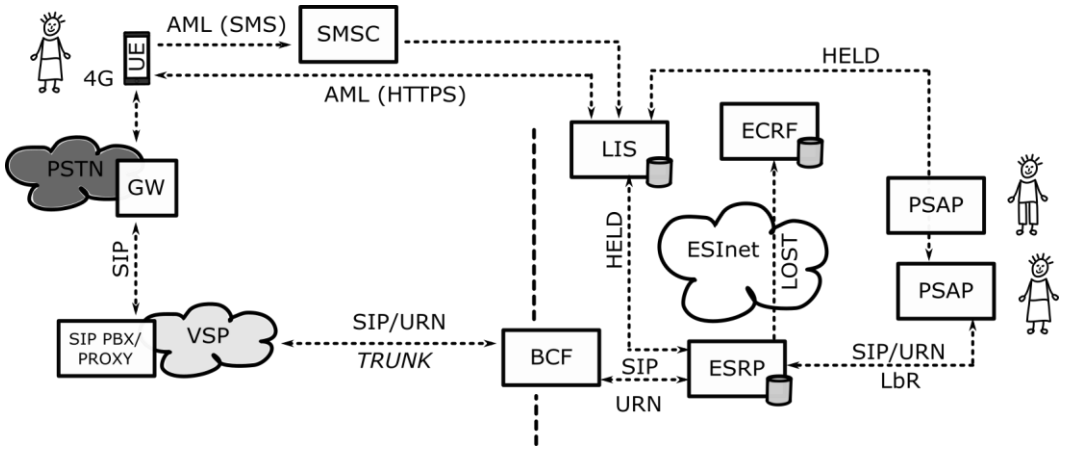

Figure 9: AML Test Configuration

To perform the test, an AML test endpoint for the location independent phone number (pseudo emergency number) was configured using a special application on the UE. Each call was routed to the ESInet and an AML trigger was started in parallel. Subsequently, the current location was queried at the LIS by means of the caller's number.

Testing with an MNO required to interface with IMS functional elements supporting VoLTE emergency calling. Simplified, these are the LRF and IBCF as shown in Figure 10. Emergency calls originating in the MNO network contained LbR and LbV in addition to the service urn. Thus, scenarios with both variants of location transmission could be tested.

NOTE: Since no European MNO participated, these tests were performed in the course of transatlantic testing.

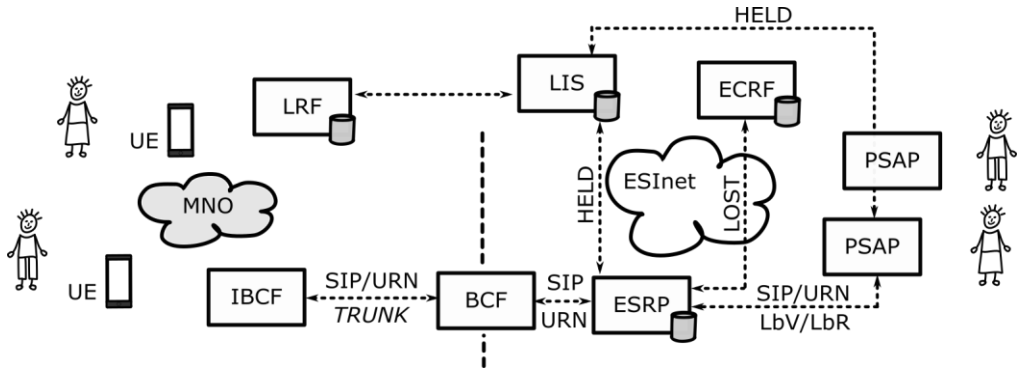

Figure 10: MNO Test Configuration

LMPE was tested including LMPE capable endpoints. In this case a test application registered as both origin and destination at the respective endpoint (SIP PROXY and PSAP) illustrated in Figure 11. In contrast to other scenarios, signaling information was also transmitted via WebSocket (WS) in these tests and, according to the LMPE specification, no additional media channel was required. Since LMPE includes location information as value (LbV), a LIS was not required for testing.

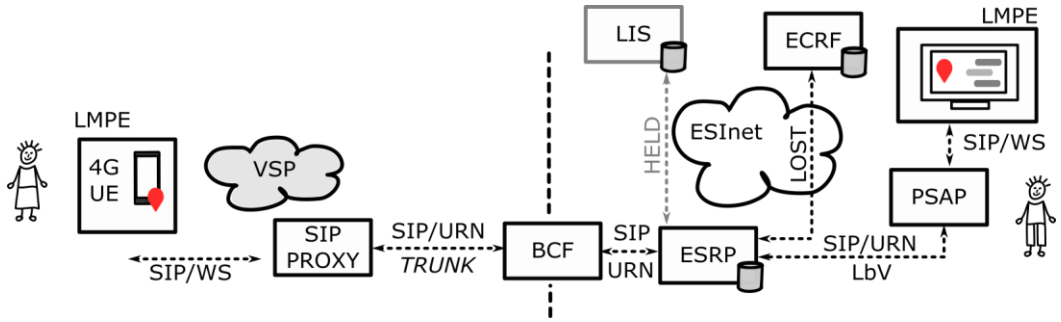

Figure 11: LMPE Test Configuration

Basic steps to test calls in each of the configurations were: registering an UE using a specific identity (to get a location), dialing an emergency number, and setting up audio, or multimedia calls.

5.5 Transatlantic Interoperability Tests

5.5.1 General

In this plugtests event a peering of two independent ESInet deployments was tested for the first time. Not only implementations based on NG112/9-1-1 standards of different SDOs were tested but also secure transmission using certificates. These certificates were issued by NENA PCA for US participants and by ETSI for EU participants (for testing purposes only). Mutual trust was enabled by passing on the corresponding root CAs.

In the course of test preparation, two peering variants were considered - via BGB/GRE tunnel (ETSI VPN) or via the public Internet (refer to A and B in Figure 12). Both options are representing a valid peering scenario, whereas the variant via public Internet is somewhat more complex in connection with VoIP due to NAT.

Since variant B requires additional elements on both sides, it was not possible to implement a symmetrical configuration with this variant in the course of the tests due to a lack of suitable components, so most of the tests were carried out via variant A.

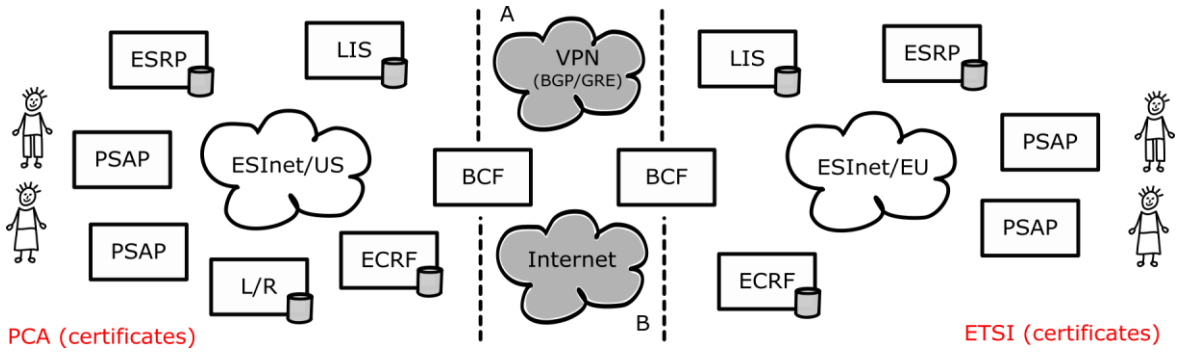

Figure 12: Transatlantic Testing

5.5.2 Test Data

The test data (refer to 5.4.2) was supplemented with US test locations and mappings to service regions (US PSAPs).

5.4.3 Configuration

To emulate a roaming scenario, a location in the source network (VSP) assigned to the other ESInet was used in the test. As an example, in the case of a VoIP UE with US VSP, European location data was selected (see elements drawn in blue in Figure 13). During the test, emergency calls were always delivered locally and subsequently forwarded from the local core services (ESRP, ECRF, FG) to the remote ESInet (see green arrows in Figure 13). Depending on the peering variant, a BCF was used in the remote ESInet or forwarded directly to the remote ESRP. In the remote ESInet, the responsible PSAP was determined based on the defined mapping.

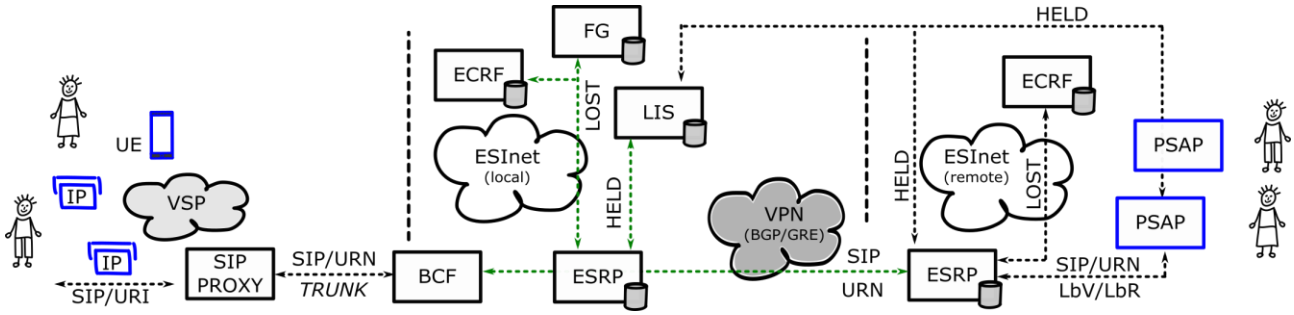

Figure 13: VSP Transatlantic Test Configuration

For MNO tests, another variant was chosen to emulate a roaming scenario. In this case, an emergency call was forwarded to a geographically non-responsible ESInet by means of a static route in the BCF (see green arrows in Figure 14). Using ESRP, ECRF and FG, the destination ESInet was determined and forwarded accordingly. For example, an emergency call originating in US was first routed to the European ESInet and correctly routed based on the actual location. This made it possible to receive emergency calls from an MNO in both ESInets, for example, by means of policy routing.

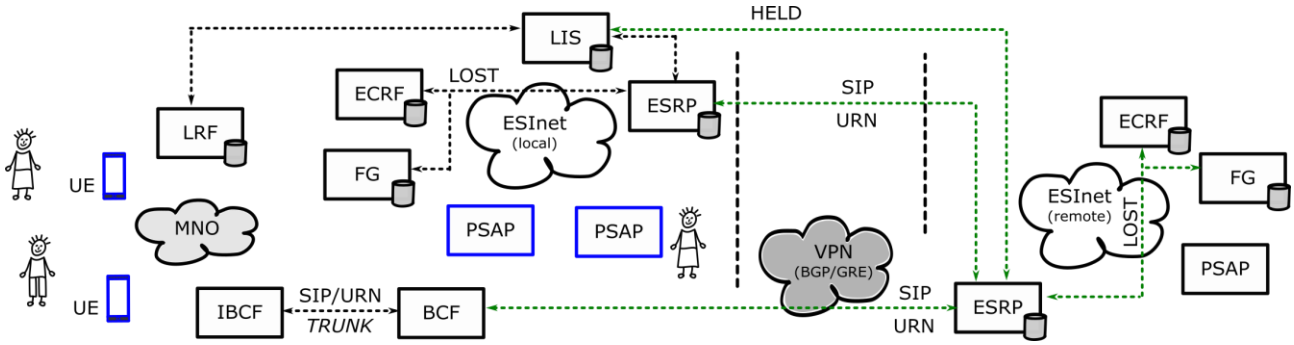

Figure 14: MNO Transatlantic Test Configuration

In each test, certificates were used for secure transmission (HTTPS and SIP/TLS) and for client and server authentication. Strictly speaking, these were certificates issued by different credentialing agencies.

5.6 Services and network infrastructure

The remote test infrastructure was based on the connection of all the Equipment Under Test from all the participating companies to the Hub for Interoperability and Validation at ETSI (HIVE) via IPSec GRE VPN tunnels. In this setup, ETSI acted as a VPN HUB and enabled the interaction among any possible equipment combination over a secure transport network. Consequently, connecting the equipment under test to HIVE was a mandatory step to being able to participating to the remote pre-testing phase of the Plugtest.

In order to facilitate the integration of remote companies the following initiatives were put in place:

- A VPN request application accessible from the WIKI allowing participants to fill-in all their technical details, and get technical parameters provided by IT Plugtests team.
- VPN configurations based on various networking manufacturer products were provided, to facilitate VPN integration, as well as an HowTo Linux procedure.

The VPN request application also allowed participants and organisers to monitor the status and progress of the VPN creations.

The ETSI Plugtests network infrastructure also includes the connection with the parallel network infrastructure deployed on the North-American side in IIT, in order to execute Trans-Atlantic tests.

2 distinct DNS servers were provided to get DNS resolution for internal tests (via VPN tunnels), or for tests via internet (to get closer to the real world).

The network infrastructure is shown on the Figure 15.

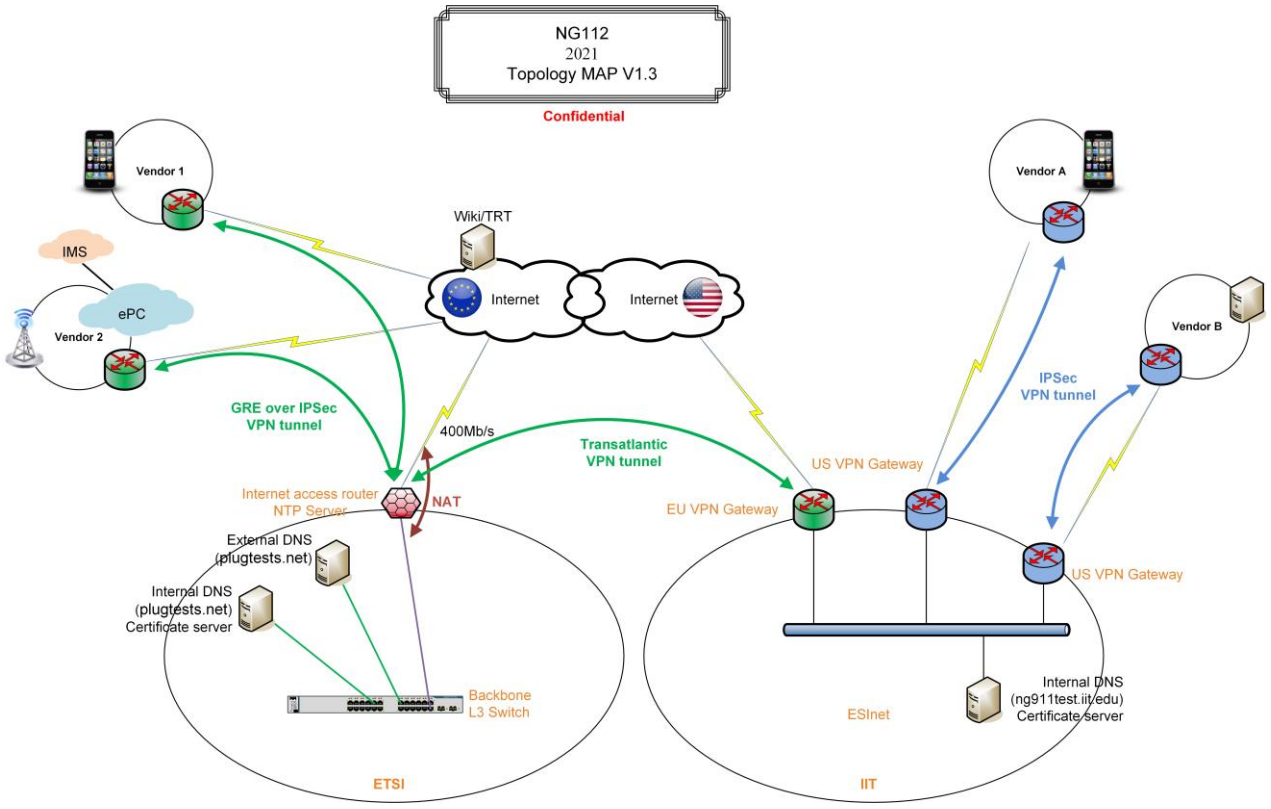

Figure 15: Network Infrastructure

6 Achieved Results

6.1 NG112 Conformance Testing Results

6.1.1 General Observations

- Conformance test successfully used
- LIS and ECRF conformance tests validated against multiple vendor implementations
- Issues identified on vendor implementations
- Quick verification of vendor fixes

In preparation of a future NG112 event, the NG112 conformance tests procedure shall be improved as following:

- the current test suites need to be updated with the latest version of the standards;
- due to the complexity of the configuration for Emergency Service Routing Proxy (ESRP) testing, it needs to validated specifically;
- US and Asiatic companies interested for the conformance tests of LIS, ECRF, PSAP and ESRP NG112 protocols should also have an access to the test suite.

6.2 NG112 Interoperability Testing Results

6.2.1 General Observations

- PSAPs and ESRPs can handle “Location by Reference” and “Location by Value” including audio, video calls
- BCFs performed successful interoperability with all originating and terminating networks, including audio, video calls
- All location boundaries were respected by the ECRFs and routed correctly by the ESRPs to the appropriate PSAPs
- Location provided by the LIS or by the end devices (as value) was used successfully
    - Calls via a public operator using AML were successful (HTTPS)
- Location dereferencing at LIS via both GET and POST requestsEmergency calls were successfully originated from Public VoIP network.
- Signaling and media interoperability with ESInet functional elements achieved
- Service urns sos, sos.fire, sos.ambulance, sos.police successfully tested
    - Routing to different PSAP areas and agencies according to the service urns
- Still lack of vendor support of real-time text (RTT)
- Certificates issued by ETSI for the purpose of testing were successfully used for secure transport and client/server mutual authentication
- A LoST hierarchy including a FG was successfully tested using recursion and iteration

6.2.2 Statistics

Overall results considering scenarios as introduced in 5.4.2

Table 1: Overall Results

Interoperability		Not Executed		Totals	
OK	**NO**	**N/A**	**OT**	**Run**	**Results**
240 (86.6%)	**37 (13.1%)**	**128 (31.6%)**	**(0.0%)**	**277 (68.4%)**	**405**

Group results considering individual scenarios as introduced in 5.4.2, with NGCS representing emergency call routing based on location considering all core service interfaces (UE, BCF, LIS, ECRF, ESRP and PSAP).

Table 2: Group Results

		Interoperability		Not Executed		Totals	
		OK	**NO**	**N/A**	**OT**	**Run**	**Results**
No TLS	**VoIP**	42 (75.0%)	14 (25.0%)	34 (37.8%)	0 (0.0%)	56 (62.2%)	90
	AML	4 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (100.0%)	4
	LMPE	4 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (100.0%)	4
	Trans-Atlantic EU to US	14 (100.0%)	0 (0.0%)	7(33.3%)	0 (0.0%)	14 (66.7%)	21

	Roaming						
	Trans-Atlantic EU to US Roaming (not executed)	0 (0.0%)	0 (0.0%)	21(100.0%)	0 (0.0%)	0 (0.0%)	21
TLS	**VoIP**	114 (91.3%)	11 (8.7%)	60 (31.9%)	0 (0.0%)	128 (68.1%)	188
	LMPE	24 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	24 (100.0%)	24
	Trans-Atlantic TLS	38(80.9%)	9(19.1%)	6(11.3%)	0 (0.0%)	47(88.6%)	53

Test results considering individual scenarios as introduced in 5.4.2, with MM/VID representing audio and video emergency calls, MM/RTT representing audio, video and real-time text ermegency calls, and location by value (RT/LBV) as well as location by reference (RT/LBR) call routing.

Table 3: Test Results

	Interoperability		**Not Executed**		**Totals**	
	OK	**NO**	**NA**	**OT**	**Run**	**Results**
LOC_LBV_01	7 (70.0%)	3 (30.0%)	29 (74.4%)	0 (0.0%)	10 (25.6%)	39
LOC_LBR_01	31 (91.2%)	3 (8.8%)	5 (12.8%)	0 (0.0%)	34 (87.2%)	39
LOC_AML_01	4 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (100.0%)	4
MME_AUD_01	27 (81.8%)	6 (18.2%)	6 (15.4%)	0 (0.0%)	33 (84.6%)	39
MSG_LMP_01	4 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (100.0%)	4
POL_TAD_01	0 (0.0%)	2 (100.0%)	37 (94.9%)	0 (0.0%)	2 (5.1%)	39
POL_SIP_01	32 (94.1%)	2 (5.9%)	5 (12.8%)	0 (0.0%)	34 (87.2%)	39
SEC_SIP_TLS_01	18 (100.0%)	0 (0.0%)	2 (10.0%)	0 (0.0%)	18 (90.0%)	20
SEC_SIP_AUTH_01	12 (75.0%)	4 (25.0%)	4 (20.0%)	0 (0.0%)	16 (80.0%)	20
SEC_SIP_TLS_02	16 (100.0%)	0 (0.0%)	2 (11.1%)	0 (0.0%)	16 (88.9%)	18
SEC_SIP_AUTH_02	12 (80.0%)	3 (20.0%)	4 (21.1%)	0 (0.0%)	15 (78.9%)	19
SEC_SIP_TLS_03	0 (0.0%)	0 (0.0%)	3 (100.0%)	0 (0.0%)	0 (0.0%)	3
SEC_SIP_AUTH_03	0 (0.0%)	0 (0.0%)	3 (100.0%)	0 (0.0%)	0 (0.0%)	3
SEC_HTTPS_TLS_01	14 (100.0%)	0 (0.0%)	2 (12.5%)	0 (0.0%)	14 (87.5%)	16
SEC_HTTPS_AUTH_01	6 (54.5%)	5 (45.5%)	5 (31.3%)	0 (0.0%)	11 (68.8%)	16
SEC_HTTPS_TLS_02	12 (100.0%)	0 (0.0%)	2 (14.3%)	0 (0.0%)	12 (85.7%)	14
SEC_HTTPS_AUTH_02	5 (55.6%)	4 (44.4%)	4 (30.8%)	0 (0.0%)	9 (69.2%)	13
SEC_HTTPS_TLS_03	18 (100.0%)	0 (0.0%)	2 (10.0%)	0 (0.0%)	18 (90.0%)	20
SEC_HTTPS_AUTH_03	10 (66.7%)	5 (33.3%)	5 (25.0%)	0 (0.0%)	15 (75.0%)	20

SEC_HTTPS_TLS_04	3 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (100.0%)	3
SEC_HTTPS_AUTH_04	3 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (100.0%)	3
SEC_HTTPS_TLS_05	3 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (100.0%)	3
SEC_HTTPS_AUTH_05	3 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (100.0%)	3
SEC_HTTPS_TLS_06	3 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (100.0%)	3
SEC_HTTPS_AUTH_06	3 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (100.0%)	3
MME_VID_01	1 (100.0%)	0 (0.0%)	5 (83.3%)	0 (0.0%)	1 (16.7%)	6
MME_RTT_01	1 (100.0%)	0 (0.0%)	5 (83.3%)	0 (0.0%)	1 (16.7%)	6

6.3 The standardization and industry impact

The results of the 4th edition of the NG112 Emergency Communications Plugtest event validate the interoperability of different solutions on the market related to end-to-end emergency services communications based on NG112 core services. They show that the technology is mature and available for implementation.

The tests concluded that European and US emergency communications standards are interoperable and therefore products developed on both sides of the Atlantic are compatible. This opens the market to companies that would be interested in commercialising their solutions in both European and US markets.

The standardisation process will benefit from the feedback and lessons learnt through the Plugtests. They will enhance currently published standards and will support the finalisation of the TS 103 480 “Interoperability testing of core elements for network independent access to emergency services”.

It is recommended to revise or add the following topics in the course of the NG112 standardization by ETSI EMTEL

- Behavior of NGCS (especially ESRP) when receiving multiple location information (civic and geodetic).
- Consideration of HELD dereferencing via POST request using time attributes ("emergencyRouting" or "emergencyDispatch") - in particular the effect on accuracy and response time for location queries.
- Support of different service URN namespaces in ESRP and ECRF
- More detailed description of the application of TLS mutual authentication mechanisms
- Technical options for ESInet peering

In addition, general topics such as international peering of national ESinet deployments and the use and operation of a forest guide (FG) should be discussed in various committees. Another important topic is PKI (e.g., credentialing agency) in the context of public safety.

History

Document history		
V0.1	30.03.2021	First draft
V0.2	14.04.2021	Stable draft
V0.3	19.04.2021	Publication
V0.4	28.05.2021	Corrigendum