LIAISON STATEMENT

Title:	Liaison Statement to IETF on HOST ID standardization
Date:	
From (source):	ETSI E2NA
Contact(s):	Luca Pesando (luca.pesendo@telecomitalia.it)
	Sonia Compans (e2naSupport@etsi.org)
To:	IETF OPS Area
	Joel Jaeggli (joelja@bogus.com)
	IETF APS Activity
	Dirk von Hugo (Dirk.von-Hugo@telekom.de)
	Behcet Sarikaya (sarikaya@ieee.org)
Copy to:	ETSI M/493
Response to: (if applicable)	
Attachments: (if applicable)	EC Mandate M/493: www.etsi.org/images/files/ECMandates/m493.pdf

1. Overall description:

ETSI E2NA with collaboration of a number of other ETSI Technical Bodies is developing an architectural framework in response to the European Commission Mandate M/493 about delivery and transport of the emergency caller's location.

The EC Mandate requires that, the emergency caller's location information be provided by the Voice Service Providers (VSPs) in signaling messages they send towards PSAPs (Public Safety Answering Points) via an Emergency Service Routing Proxy (ESRP). This information is used to reveal the caller's location to the selected PSAP and to select the correct PSAP to be involved for an emergency call.

This requires the VSP call server receiving an emergency call request to identify the relevant fixed access network and to query a Location Information Server (LIS) in this network using a suitable look-up key. In the simplest case, the source IP address of the IP packet carrying the call request is used both for identifying the fixed access network (thanks to a reverse DNS query) and as a look-up key to query the LIS. However, relying on the source IP address is not always sufficient to locate the initiator of an emergency call, especially in the following cases:

1) If there is a NAT between the user and the VSP, or
2) If the emergency call established over a VPN tunnel (e.g., an employee remotely connected to a company VoIP server through a tunnel wishes to make an emergency call).

In such cases, the source IP address received by the VSP call server will identity the NAT or the address assigned to the caller equipment by the VSP (i.e., the address inside the tunnel) and cannot be used by the call server to query the LIS.

ETSI E2NA has received contributions from its members on two potential solutions to this issue, one of which is based on injecting a HOST ID (as per draft-ietf-intarea-nat-reveal-analysis-10) in all packets forwarded by the NAT or the tunnel endpoint. As this solution was considered promising, the latest draft of the architectural framework specification (ES 203 178) includes a high-level description of a HOST ID-based solution.

ETSI E2NA would be interested in receiving confirmation from the IETF OPS area that the HOST ID approach is suitable for the M/493 use case.

ETSI E2NA would be interested in receiving information from the IETF OPS area on their work plan and milestones for further developing the HOST ID solution. Our goal is to approve the architectural framework document by the end of this year and a follow-up protocol specification by the end of next year.

2. Actions:

IETF OPS area to confirm that the HOST ID approach is suitable for the M/493 use case.

IETF OPS area to provide information on their work plan and milestones for further developing the HOST ID solution.

3. Date of next meetings of the originator:

22-25 October 2013

16-20 December 2013