Internet Engineering Task Force (IETF)
Request for Comments: 7843
Updates: 6887
Category: Standards Track
ISSN: 2070-1721

A. Ripke
R. Winter
T. Dietz
J. Quittek
NEC
R. da Silva
Telefonica I+D

May 2016

Port Control Protocol (PCP) Third-Party ID Option

Abstract

This document describes a new Port Control Protocol (PCP) option called the THIRD_PARTY_ID option. It is designed to be used together with the THIRD_PARTY option specified in RFC 6887.

The THIRD_PARTY_ID option serves to identify a third party in situations where a third party's IP address contained in the THIRD_PARTY option does not provide sufficient information to create requested mappings in a PCP-controlled device.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7843.

Table of Contents

1. Introduction

The IETF has specified the Port Control Protocol (PCP) [RFC6887] to control how packets are translated and/or forwarded by a PCP-controlled device such as a Network Address Translator (NAT) or a firewall.

This document focuses on scenarios where the PCP client sends requests that concern internal addresses other than the address of the PCP client itself.

There is already an option defined for this purpose in [RFC6887] called the THIRD_PARTY option. The THIRD_PARTY option carries the IP address of a host for which a PCP client requests an action at the PCP server. For example, the THIRD_PARTY option can be used if port mapping requests for a Carrier-Grade NAT (CGN) are not sent from PCP clients at subscriber terminals but instead from a PCP Interworking Function (IWF), which requests port mappings.

In some cases, the THIRD_PARTY option alone is not sufficient and further means are needed for identifying the third party. Such cases are addressed by the THIRD_PARTY_ID option, which is specified in this document.

The primary issue addressed by the THIRD_PARTY_ID option is that there are CGN deployments that do not distinguish internal hosts by their IP address alone, but use further identifiers (IDs) for unique subscriber identification. For example, this is the case if a CGN supports overlapping private or shared IP address spaces [RFC1918] [RFC6598] for internal hosts of different subscribers. In such cases, different internal hosts are identified and mapped at the CGN by their IP address and/or another ID, for example, the ID of a tunnel between the CGN and the subscriber. In these scenarios (and similar ones), the internal IP address contained in the THIRD_PARTY option is not sufficient to demultiplex connections from internal hosts. An additional identifier needs to be present in the PCP message in order to uniquely identify an internal host. The THIRD_PARTY_ID option is used to carry this ID.

This applies to some of the PCP deployment scenarios that are listed in Section 2.1 of [RFC6887], in particular to a L2-aware NAT, which is described in more detail in Section 3, as well as in other scenarios where overlapping address spaces occur like in [RFC6674] or [RFC6619].

The THIRD_PARTY_ID option is defined for the PCP opcodes MAP and PEER to be used together with the THIRD_PARTY option, which is specified in [RFC6887].

2. Terminology

The terminology defined in the specification of PCP [RFC6887] applies.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Target Scenarios

This section describes two scenarios that illustrate the use of the THIRD_PARTY_ID option:

1. A UPnP IGD-PCP IWF (Universal Plug and Play Internet Gateway Device - Port Control Protocol Interworking Function [RFC6970]).

2. A carrier web portal for port mapping.

These are just two examples that illustrate the use and applicability of the THIRD_PARTY_ID option. While these are just two examples, there might be other conceivable use cases. However, the use of the THIRD_PARTY_ID option as specified in this document is restricted to scenarios where the option is needed for the purpose of uniquely identifying an internal host in addition to the information found in the THIRD_PARTY option.

Both scenarios elaborated in this document are refinements of the same basic scenario shown in Figure 1 that is considered as a PCP deployment scenario employing L2-aware NATs as listed in Section 2.1 of [RFC6887]. It has a carrier operating a CGN and a Port Control Protocol Interworking Function (PCP IWF) [RFC6970] for subscribers to request port mappings at the CGN. The PCP IWF communicates with the CGN using PCP. For this purpose, the PCP IWF contains a PCP client serving multiple subscribers and the CGN is co-located with a PCP server. The way subscribers interact with the PCP IWF for requesting port mappings for their internal hosts is not specified in this basic scenario, but it is elaborated on more in the specific scenarios in Sections 3.1 and 3.2.

The CGN operates as a L2-aware NAT. Unlike a standard NAT, it includes a subscriber identifier in addition to the source IP address in entries of the NAT mapping table.

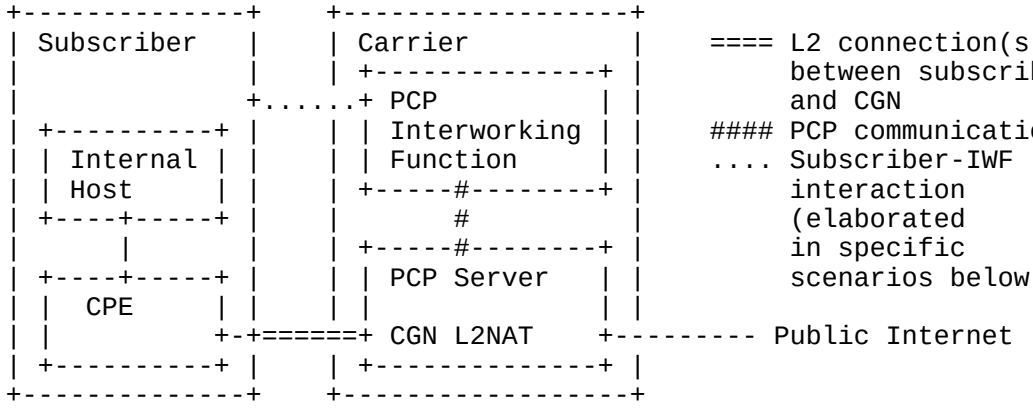


Figure 1: Carrier Hosted PCP IWF for Port Mapping Requests

Internal hosts in the subscriber's network use private IP addresses [RFC1918]. There is no NAT between the internal host and the CGN, and there is an overlap of addresses used by internal hosts of different subscribers. That is why the CGN needs more than just the internal host's IP address to distinguish internal hosts of different subscribers. A commonly deployed method for solving this issue is using an additional identifier for this purpose. A natural candidate for this additional identifier at the CGN is the ID of the tunnel that connects the CGN to the subscriber's network. The subscriber's Customer Premises Equipment (CPE) operates as a Layer 2 bridge.

Requests for port mappings from the PCP IWF to the CGN need to uniquely identify the internal host for which a port mapping is to be established or modified. Already existing for this purpose is the THIRD_PARTY option that can be used to specify the internal host's IP address. The THIRD_PARTY_ID option is introduced for carrying the additional third-party information needed to identify the internal host in this scenario.

The additional identifier for internal hosts needs to be included in MAP requests from the PCP IWF in order to uniquely identify the internal host that should have its address mapped. This is the purpose that the new THIRD_PARTY_ID option serves in this scenario. It carries the additional identifier, that is the tunnel ID, that serves for identifying an internal host in combination with the internal host's (private) IP address. The IP address of the internal host is included in the PCP IWF's mapping requests by using the THIRD_PARTY option.

The information carried by the THIRD_PARTY_ID option is not just needed to identify an internal host in a PCP request. The CGN needs this information in its internal mapping tables for translating packet addresses and for forwarding packets to subscriber-specific tunnels.

How the carrier PCP IWF is managing port mappings, such as, for example, automatically extending the lifetime of a mapping, is beyond the scope of this document.

3.1. Carrier-Hosted UPnP IGD-PCP IWF

This scenario further elaborates the basic one above by choosing UPnP-IGD as the communication protocol between the subscriber and the carrier's PCP IWF. Then obviously, the PCP IWF is realized as a UPnP IGD-PCP IWF as specified in [RFC6970].

As shown in Figure 2, it is assumed here that the UPnP IGD-PCP IWF is not embedded in the subscriber premises router, but offered as a service to the subscriber. Further, it is assumed that the UPnP IGD-PCP IWF is not providing NAT functionality.

This requires that the subscriber can connect to the UPnP IGD-PCP IWF to request port mappings at the CGN using UPnP-IGD as specified in [RFC6970]. In this scenario, the connection is provided via (one of the) tunnel(s) connecting the subscriber's network to the Broadband Remote Access Server (BRAS) and an extension of this tunnel from the BRAS to the UPnP IGD-PCP IWF. Note that there are other alternatives that can be used for providing the connection to the UPnP IGD-PCP IWF. The tunnel extension used in this scenario can, for example, be realized by a forwarding function for UPnP messages at the BRAS that forwards such messages through per-subscriber tunnels to the UPnP IGD-PCP IWF. Depending on an actual implementation, the UPnP IGD-PCP IWF can then either use the ID of the tunnel in which the UPnP message arrived directly as the THIRD_PARTY_ID option for PCP requests to the CGN, or it uses the ID of the tunnel to retrieve the THIRD_PARTY_ID option from the Authentication, Authorization, and Accounting (AAA) server.

To support the latter option, the BRAS needs to register the subscriber's tunnel IDs at the AAA server at the time it contacts the AAA server for authentication and/or authorization of the subscriber. The tunnel IDs to be registered per subscriber at the AAA server may include the tunnel between CPE and BRAS, between BRAS and UPnP IGD-PCP IWF, and between BRAS and CGN. The UPnP IGD-PCP IWF queries the AAA server for the ID of the tunnel between BRAS and CGN, because this is the identifier to be used as the THIRD_PARTY_ID option in the subsequent port mapping request.

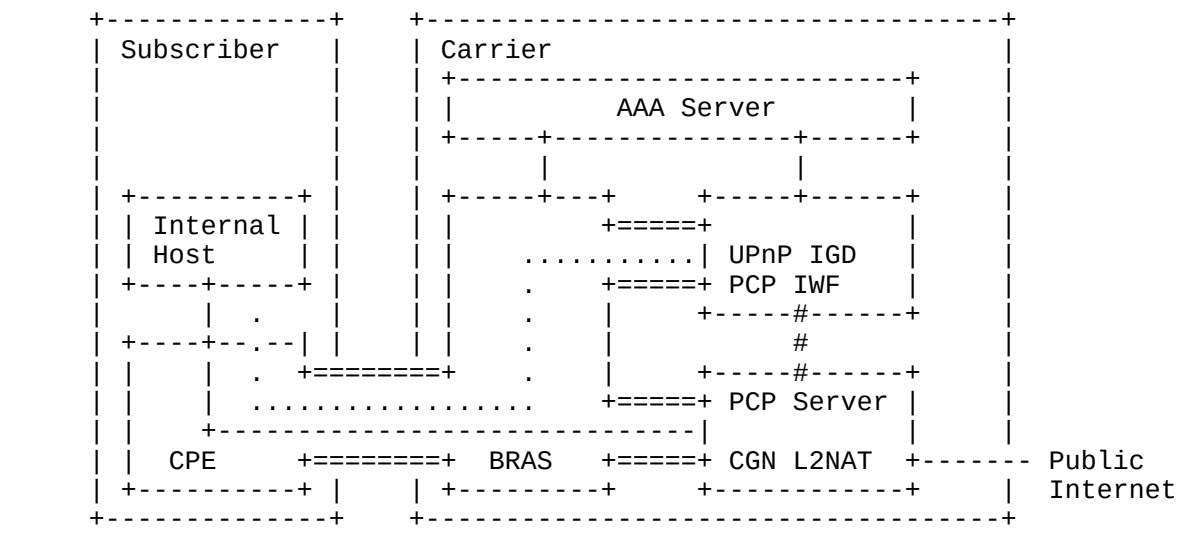


Figure 2: UPnP IGD-PCP IWF

A potential extension to [RFC6970] regarding an additional state variable for the THIRD_PARTY_ID option and regarding an additional error code for a mismatched THIRD_PARTY_ID option and its processing might be a logical next step. However, this is not in the scope of this document.

3.2. Carrier Web Portal

This scenario shown in Figure 3 is different from the previous one concerning the protocol used between the subscriber and the IWF. Here, HTTP(S) is the protocol that the subscriber uses for port mapping requests. The subscriber may make requests manually using a web browser or automatically -- as in the previous scenario -- with applications in the subscriber's network issuing port mapping requests on demand. The web portal queries the AAA server for the subscriber's ID of the tunnel (BRAS to CGN) that was reported by the BRAS. The returned ID of the tunnel (BRAS to CGN) is used as the THIRD_PARTY_ID option in the subsequent port mapping request.

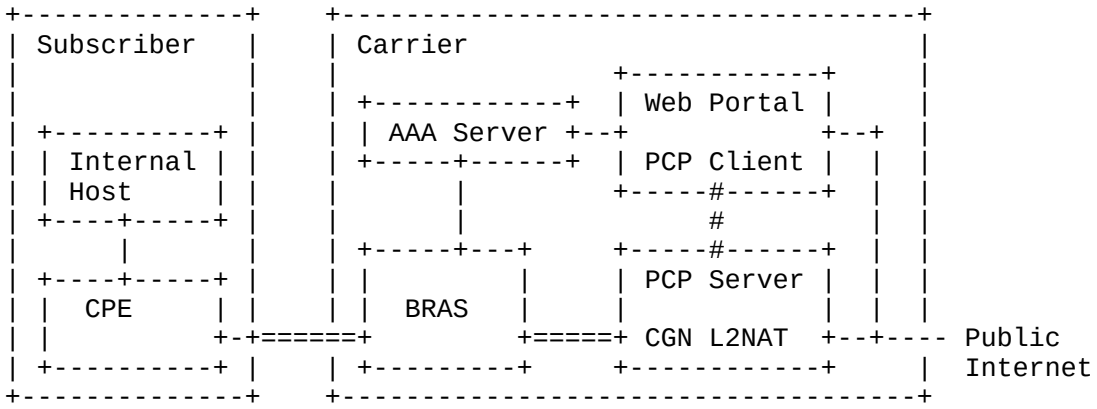
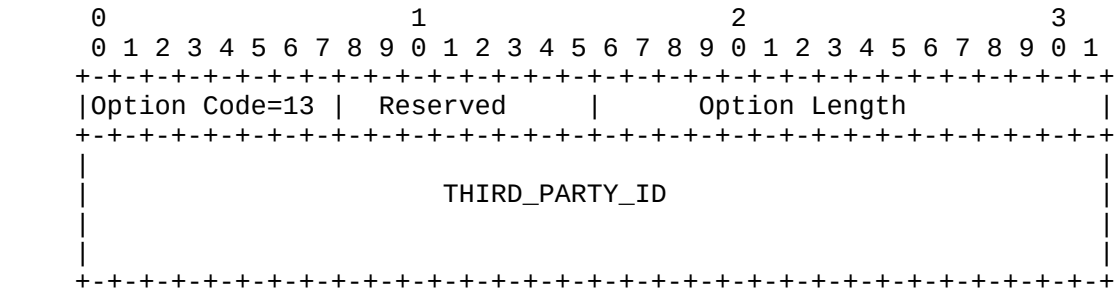


Figure 3: Carrier Web Portal

The PCP IWF is realized as a combination of a web server and a PCP client.

4. Format

The THIRD_PARTY_ID option as shown in Figure 4 uses the format of PCP options as specified in [RFC6887]:



Option Name: THIRD_PARTY_ID
Option Code: 13
Purpose: Together with the THIRD_PARTY option, the THIRD_PARTY_ID option identifies a third party for which a request for an external IP address and port is made.
Valid for Opcodes: MAP, PEER
Length: Variable; maximum 1016 octets.
May appear in: Request. May appear in response only if it appeared in the associated request.
Maximum occurrences: 1

Figure 4: THIRD_PARTY_ID Option

The "Reserved" field and the "Option length" field are to be set as specified in Section 7.3 of [RFC6887].

The "THIRD_PARTY_ID" field contains a deployment-specific identifier that identifies a realm of a NAT map entry. Together with a THIRD_PARTY option it can be used to identify a subscriber’s session on a PCP-controlled device. It has no other semantics.

The "THIRD_PARTY_ID" is not bound to any specific identifier. It can contain any deployment-specific value that the PCP client and the PCP server agree on. How this agreement is reached if both PCP server and client are not administered by the same entity is beyond the scope of this document. Also, the client does not need to have an understanding of how the ID is being used at the PCP server.

If an identifier is used that is based on an existing standard, then the encoding rules of that standard must be followed. As an example, in case a session ID of the Layer 2 Tunneling Protocol version 3

(L2TPv3) [RFC3931] is being used, then that identifier has to be encoded the same way it would be encoded in the L2TPv3 session header. This allows for a simple octet-by-octet comparison at the PCP-controlled device.

[RFC6887] expects option data to always come in multiples of an octet. An ID, however, might not fulfill this criterion. As an example, an MPLS label is 20 bits wide. In these cases, padding is done by appending 0 bits until the byte boundary is reached. After that, the padding rules of [RFC6887] apply.

The option number is in the mandatory-to-process range (0-127), meaning that a request with a THIRD_PARTY_ID option is processed by the PCP server if and only if the THIRD_PARTY_ID option is supported by the PCP server. Therefore, it should not be included unless the PCP client is certain that a mapping without the THIRD_PARTY_ID is impossible.

4.1. Result Codes

The following PCP Result Codes are new:

24: THIRD_PARTY_ID_UNKNOWN: The provided identifier in a THIRD_PARTY_ID option is unknown/unavailable to the PCP server. This is a long lifetime error.

25: THIRD_PARTY_MISSING_OPTION: This error occurs if both THIRD_PARTY and THIRD_PARTY_ID options are expected in a request but one option is missing. This is a long lifetime error.

26: UNSUPP_THIRD_PARTY_ID_LENGTH: The received option length is not supported. This is a long lifetime error.

5. Behavior

The following sections describe the operations of a PCP client and a PCP server when generating the request and processing the request and response.

5.1. Generating a Request

In addition to generating a PCP request that is described in [RFC6887], the following has to be applied. The THIRD_PARTY_ID option MAY be included either in a PCP MAP or PEER opcode. It MUST be used in combination with the THIRD_PARTY option, which provides an IP address. The THIRD_PARTY_ID option holds an identifier to allow the PCP-controlled device to uniquely identify the internal host

(specified in the THIRD_PARTY option) for which the port mapping is to be established or modified. The padding rules described in Section 4 apply.

5.2. Processing a Request

The THIRD_PARTY_ID option is in the mandatory-to-process range; if the PCP server does not support this option, it MUST return an UNSUPP_OPTION response. If the provided identifier in a THIRD_PARTY_ID option is unknown/unavailable, the PCP server MUST return a THIRD_PARTY_ID_UNKNOWN response. If the PCP server receives a request with an unsupported THIRD_PARTY_ID option length, it MUST return an UNSUPP_THIRD_PARTY_ID_LENGTH response. If the PCP server receives a THIRD_PARTY_ID option without a THIRD_PARTY option, it MUST return a THIRD_PARTY_MISSING_OPTION response.

Upon receiving a valid request with a legal THIRD_PARTY_ID option identifier, the message is processed as specified in [RFC6887], except that the identifier contained in the THIRD_PARTY_ID is used in addition when accessing a mapping table. Instead of just using the value contained in the THIRD_PARTY option when accessing the internal Internet address of a mapping table, now the combination of the two values contained in the THIRD_PARTY option and in the THIRD_PARTY_ID option is used to access the combination of the internal Internet address and the internal realm of a NAT map entry.

If two or more different tunnel technologies are being used, precautions need to be taken to handle potential overlap of the ID spaces of these technologies. For example, different PCP client/PCP server pairs can be used per tunnel technology.

5.3. Processing a Response

In addition to the response processing described in [RFC6887], if the PCP client receives a THIRD_PARTY_ID_UNKNOWN or a UNSUPP_THIRD_PARTY_ID_LENGTH or a THIRD_PARTY_MISSING_OPTION response back for its previous request, it SHOULD report an error. Where to report an error is based on policy.

6. IANA Considerations

The following PCP Option Code has been allocated in the mandatory-to-process range:

- 13: THIRD_PARTY_ID

The following PCP Result Codes have been allocated:

- 24: THIRD_PARTY_ID_UNKNOWN
- 25: THIRD_PARTY_MISSING_OPTION
- 26: UNSUPP_THIRD_PARTY_ID_LENGTH

7. Security Considerations

This option is to be used in combination with the THIRD_PARTY option. Consequently, all corresponding security considerations in Section 18.1.1 of [RFC6887] apply. In particular, the network on which the PCP messages are sent must be sufficiently protected. Further, it is RECOMMENDED to use PCP authentication [RFC7652] unless the network already has appropriate authentication means in place.

The THIRD_PARTY_ID option carries a context identifier whose type and length is deployment and implementation dependent. This identifier might carry privacy sensitive information. It is therefore RECOMMENDED to utilize identifiers that do not have such privacy concerns. Means to protect unauthorized access to this information MUST be put in place. In the scenarios described in this document, for example, access to the web portal or UPnP IGD-PCP IWF MUST be authenticated. Generally speaking, the identifier itself MUST only be accessible by the network operator and MUST only be handled on operator equipment. For example, creation of a PCP message on the web portal or the UPnP IGD PCP IWF is triggered by the subscriber, but the actual option filling is done by an operator-controlled entity.

8. References

8.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <http://www.rfc-editor.org/info/rfc1918>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6598] Weil, J., Kuarsingh, V., Donley, C., Liljenstolpe, C., and M. Azinger, "IANA-Reserved IPv4 Prefix for Shared Address Space", BCP 153, RFC 6598, DOI 10.17487/RFC6598, April 2012, <http://www.rfc-editor.org/info/rfc6598>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, DOI 10.17487/RFC6887, April 2013, <http://www.rfc-editor.org/info/rfc6887>.

8.2. Informative References

[RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed., "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, DOI 10.17487/RFC3931, March 2005, <http://www.rfc-editor.org/info/rfc3931>.

[RFC6619] Arkko, J., Eggert, L., and M. Townsley, "Scalable Operation of Address Translators with Per-Interface Bindings", RFC 6619, DOI 10.17487/RFC6619, June 2012, <http://www.rfc-editor.org/info/rfc6619>.

[RFC6674] Brockners, F., Gundavelli, S., Speicher, S., and D. Ward, "Gateway-Initiated Dual-Stack Lite Deployment", RFC 6674, DOI 10.17487/RFC6674, July 2012, <http://www.rfc-editor.org/info/rfc6674>.

[RFC6970] Boucadair, M., Penno, R., and D. Wing, "Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF)", RFC 6970, DOI 10.17487/RFC6970, July 2013, <http://www.rfc-editor.org/info/rfc6970>.

[RFC7652] Cullen, M., Hartman, S., Zhang, D., and T. Reddy, "Port Control Protocol (PCP) Authentication Mechanism", RFC 7652, DOI 10.17487/RFC7652, September 2015, <http://www.rfc-editor.org/info/rfc7652>.

Acknowledgments

Thanks to Mohamed Boucadair for many valuable suggestions, in particular for suggesting a variable length for the THIRD_PARTY_ID option. Thanks to Dave Thaler, Tom Taylor, and Dan Wing for their comments and review.

Authors' Addresses

Andreas Ripke
NEC
Heidelberg
Germany

Email: ripke@neclab.eu

Rolf Winter
NEC
Heidelberg
Germany

Email: winter@neclab.eu

Thomas Dietz
NEC
Heidelberg
Germany

Email: dietz@neclab.eu

Juergen Quittek
NEC
Heidelberg
Germany

Email: quittek@neclab.eu

Rafael Lopez da Silva
Telefonica I+D
Madrid
Spain

Email: rafaelalejandro.lopezdasilva@telefonica.com