MIF Working Group D. Migault
Internet-Draft Francetelecom - Orange
Intended status: Standards Track C. Williams
Expires: January 31, 2013 MCSR Labs
July 30, 2012

IPsec Multiple Interfaces Requirements
draft-mglt-mif-security-requirements-02.txt

Abstract

Multiple Interface Nodes (MIF Nodes) may use their Multiple Interfaces to perform Mobility, Multihoming. Then, these MIF Nodes may also manage traffic between these Multiple Interfaces. Because IPsec has not been designed for Multiple Interfaces, MIF Nodes have difficulties to benefit from MIF features with IPsec protected communications.

This document provides use cases where IPsec protected communications would take advantage of MIF features. From these uses cases, we identify the different IPsec features MIF Nodes would require. Then, we expose the limitations of the IPsec related protocols IKEv2 and MOBIKE regarding to these MIF features before listing the MIF IPsec Security Requirements that should be address by a extension of IKEv2 or MOBIKE.

Table of Contents

1. Requirements notation

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

2. Introduction

IPsec protocol suite [RFC4301],[RFC5996] is mainly used to:

- Extend a trusted domain over an untrusted network: This typically corresponds to the Virtual Private Network (VPN) use case. A Security Gateway is a trusted entry point to a trusted network. The end user is connected to an untrusted network and tunnels its traffic to the Security Gateway in a encrypted tunnel using the IPsec tunnel mode. The Security Gateway decapsulates the traffic and forwards it on the trusted network. Once the traffic is in the trusted network it is usually not encrypted anymore. In other words, the traffic is protected from the end user terminal to the Security Gateway, that it to say over the untrusted network.
- Provide end-to-end security: With end to end security, the traffic is protected from the source - or the end user in our case - to the destination. The traffic does not require to be tunneled, and any segments of the network between the end user and the destination is considered as untrusted. With end-to-end security, one does not require encapsulation, and the IPsec transport mode can be used.

IPsec [RFC4301], [RFC5996] and its tunnel mode Mobility and Multihoming extension MOBIKE [RFC4555] have not been designed for Multiple Interface environment. As such MIF Nodes cannot take full advantage of MIF features with IPsec protected communications. In order to may IPsec protected communications compatible with MIF features, IPsec / IKEv2 extensions MUST be designed so:

- Mobility, Multihoming and Multiple Interface features can be provided for both IPsec tunnel and transport mode.
- IPsec nodes can dynamically ADD an new Interface for all ongoing IPsec protected communications
- IPsec nodes dynamically REMOVE an old Interface for all ongoing IPsec protected communications
- IPsec nodes can perform soft and hard handover handover
- IPsec nodes can manage IPsec traffic over Multiple Interfaces by selecting the IPsec Security Association a Multiple Interface operation (ADD, REMOVE, Soft/Hard Handover, Multihoming) occurs. This includes selecting a subtraffic as well as performing a Multiple Interface operation over multiple Security Associations in a single IKEv2 exchange.

The following document is structured as follows: Section 4 provides the use cases that motivated this document. This use cases show how IPsec currently do not fit with MIF features. From Section 4, this document identify IPsec MIF features in Section 5. For each feature, this document points how IPsec is impacted. Follows Section 6 with describes the problem statement by showing the current limitation of IKEv2 and MOBIKE protocols over the IPsec MIF features. Finally Section 7 provides the MIF IPsec requirements that should be considered by an IPsec / IKEv2 extension so that IPsec communications can take full advantage of the MIF features.

3. Terminology

In this document, we use the following terminology:

- IPsec Node: designates a node that has one or more active Security Associations with another IPsec node.
- MIF Node: designates a node that has Multiple Interfaces.
- Mobile Node (MN): designates a Node that is likely to perform Mobility.
- Correspondent Node (CN): designates the node a MN has established communications with.
- Radio Access Network (RAN): designates the Cellular Access Network managed by ISPs
- Wireless Local Area Network (WLAN): designates the WiFi Access Network not necessarily managed by ISP.

Note that IPsec Node, MIF Node, Mobile Node and Correspondent Node are independent designations, and that a given Node can be designated with more than one designation.

4. Use Cases Scenarios

This section provides various use cases where MIF nodes would like to take advantage of MIF features for IPsec communications.

4.1. Offload Use Cases

4.1.1. Differences between RAN and WLAN requires MIF and Security

Radio Access Network (RAN) are not expected to be able to support the demand for mobile data. As such, ISPs are looking to offload the communications currently supported by RAN to WLAN networks. RAN and WLAN have different characteristics, and the Mobile Node is expected to overcome these differences:

- WLAN does not handle with Mobility: RAN are managed by the ISP which is responsible for handling the Mobile Node Mobility with multiple handovers between the RAN cells. Handover is performed with the Radio Layer, making Mobility transparent to the IP layer. WLAN Access are not expected to communicate between each other. They eventually may belong to different ISPs or IP Networks and thus provide different IP addresses to their attached nodes. Therefore, when the Mobile Node moves from one WLAN Access Point to another one, its IP address may be changed. The Mobile has to deal with these changes of IP address. WLAN Mobility is handled by the Mobile node whereas RAN Mobility is handled by the Network.
- WLAN may be untrusted Networks: RAN is managed by the ISP which is responsible of each of the RAN Access Points, and the Mobile Node has a trusted relationship with the ISP it has subscribed to. As a result, ISP Network behind the RAN Access Point is considered as a trusted network, and only the attachment from the Mobile Node to the Access Point needs to be secured. Layer 2 or Radio Layer was sufficient to provide a secure attachment to a trusted network. On the other hand, WLAN Access Points may be provided by various third parties, that may not have trusted relations with the ISP. WLAN Access Point may be managed, for example, by an independent provider, an Hotel, an individual. As a result, no trusted relationship exists between the Mobile Node and the WLAN Access Point, and secure attachment to a trusted network requires upper layer security. This document considers securing the IP layer with IPsec [RFC4301].
- WLAN are unreliable Networks: In addition to a trusted relationship, the Mobile Node and its ISP have also availability constraints. Since WLAN Access Points may not be managed by the ISP, they may have no reliability or Quality of Service constraints toward the connected Mobile Nodes. For example, if a Mobile Node is attached to a DSL box, nothing prevents the owner of the DSL box to reboot its box or disconnect the attached Mobile Nodes. To overcome the Network unreliability, we consider, in this document two different mechanisms 1) Multihoming and 2) Simultaneous Use of Multiple Interfaces. Both mechanisms require the Mobile Node is able to to be attached to various WLAN Access Points and so, to have Multiple Interfaces. With Multihoming the Mobile Node runs a communication on a single Primary Interface, and provides its Correspondent Node Alternate IP addresses that may be used if the the Primary Interface is not reachable. With Simultaneous Use of Multiple Interfaces, the Mobile Node is able to spread its communications between the Interfaces which lower the probability a communication is interrupted. Furthermore, the Mobile Node may also use the different Interfaces for a given

communication also known as bandwidth aggregation. Multihoming and Simultaneous Use of Multiple Interfaces may also be combined. SCTP [RFC4960] and MPTCP [RFC6182] have especially been designed to implement these mechanisms.

4.1.2. Offloading Internet Access from RAN to WLAN

In this section, we consider that the ISP offload Internet Access by providing the Mobile Nodes a Security Gateway as a security entry point to the ISP trusted network. The Mobile Node builds an IPsec tunnel to the Security Gateway. This IPsec tunnel extends the trusted Network over the WLAN untrusted Network, and thus overcome the WLAN untrusted issue.

To overcome the Mobility issue, the Mobile Node is able to update the IP address provided by the WLAN Access Point. Note that in this section, because the communication is tunneled to the Security Gateway, Mobility is performed by updating the outer IP address. The outer IP address is defined by IPsec and so Mobility can be performed by updating the IPsec configuration. Updating the outer IP address of the tunnel results in Hard Handover Mobility and does not require Multiple Interfaces. On the other hand, Soft Handover Mobility requires Multiple Interfaces. Soft Handover Mobility may be performed before the new Interface is available, similarly to the Hard Handover. We note, in this document, UPDATE and SOFT_HAND_OVER the respective Hard Handover and Soft Handover Mobility. On the other hand, Soft Handover may also be performed once the Mobile Node has at least two active Interfaces. In fact, in most cases, the Mobile Node may not know which Interface is going to be used, so it may be wise to use Multiple Interfaces, and provide time to the connection manager to decide which Interfaces are to be used or removed.

In order to take advantage of the Multiple Interfaces, when the Mobile Node detects a new Access Point and is assigned a new IP address, it may be able to select a communication and be able to ADD this Interface to it. Similarly, it also may be able to REMOVE this Interface from the communication.

Note that IPsec is using a ordered Security Policy Database (SPD). Unless the system has been designed with per Interface SPD, the Interface used by the outgoing tunnel is defined by the first SPD match. Outgoing packets with the same IP source and destination will always match a single Security Policy and use the same Interface. As a result, to take full advantage of Multiple Interfaces, SCTP or MPTCP should be used so to enable different source IP. More details are provided in Section 4.2.

In addition to the MPTCP / SCTP Multiple Interface features, the Mobile Node overcome WLAN unreliability with Multihoming and Traffic Selections. Multihoming makes possible the Mobile Node to inform its Correspond Node Alternate IP addresses. These IP addresses MUST be used if the currently used IP address is not reachable anymore. Traffic Selection makes possible connection managers to spread traffic among multiple Interfaces and to select the Access Network for each ongoing communications. SELECTORs are used to define the communication the UPDATE, ADD or REMOVE action is performed.

4.1.3. Offloading Services from RAN to WLAN

In this section we consider end-to-end security. With Offloading Internet Access, only the segment between the Mobile Node and the Security Gateway is secured with IPsec. With end-to-end security, the communication from the Mobile Node to the Correspondent Node is secured with IPsec. End-to-end security can be set both with the IPsec tunnel mode or with the IPsec transport mode. Using the IPsec transport mode ovoids the tunnel overhead, and makes the system more dynamic. This makes the IPsec transport mode preferred for applications with real time constraints. Compared to the Security Gateway architecture, end-to-end security avoids routing indirections, makes IPsec platforms deployed on a per services base which eases their load control and resource allocation.

When end-to-end Security is provided with the IPsec tunnel mode, one can refer to Section 4.1.2. In the remaining of this section, we consider the IPsec transport mode is used.

Unlike the Security Gateway architecture that uses the IPsec tunnel mode, the transport mode cannot perform Mobility. Mobility has to be performed by other protocols. SCTP and MPTCP are examples of protocols that may make Mobility possible with Multiple Interfaces. Other mechanisms like session resumption mechanisms can also be performed, for example, at the application layer. These upper layer mechanisms provide the ability to UPDATE, ADD or REMOVE an Interface to a given communication.

Thus, with the IPsec transport mode, IPsec Multiple Interface features should be seen as configuring the IPsec layer so these upper layer mechanisms can be applied on a IPsec protected communication. As a result, our Mobile Node is expected to be able to select an IPsec protected communication identified by its Security Association. For that selected communication, the Mobile Node MUST be able to UPDATE the IP addresses so that Hard Handover Mobility can be performed by upper layer mechanisms. The Mobile is also expected to ADD or REMOVE an Interface so that upper layer mechanisms can perform Mobility Soft Handover or perform traffic management between the various Interfaces.

4.2. Virtual Private Network (VPN)

Companies usually extends their private network by using IPsec VPN. The architecture used for VPN is very similar to the one described in Section 4.1.2. The architecture is the same, that is a Mobile Node tunnels is being assigned a private IP address by the Security Gateway, and the communication between the private destination or private proxy is tunneled in an IPsec tunnel between the untrusted WLAN Access Point to the Security Gateway.

The main difference with the case described in Section 4.1.2, is that WLAN is not considered as an alternative to the Radio Access Network, and the VPN is intentionally initiated by the Mobile Node. Thus, the main use case is an employee located outside its company that set up the VPN to access the company's internal resources from its PC. The Mobile Node as long been expected to be nomadic, rather than Mobile, and MOBIKE addressed this use case with Hard Handover Mobility. MOBIKE has been standardized in 2008, before iPhone has been available (2009), and now VPN end users do not only want to access their companies resources from a nomadic PC but also from Smartphones that have been widely available. Considering Smartphones rather than PCs considerably increases the Mobility Requirements of the today's VPN use case over the one in 2008. More specifically, Smartphones are always connected, and sessions are constantly exchanging packets. During a Hard Handover Mobility, packets may be lost. With an increasing number of sessions, and more and more exchanged data, the number of lost packets make reach the Replay Window counter. If the Security Gateway and the VPN client implements [RFC6311], the VPN client may renegotiate its IPsec counter. This adds an additional negotiation delay to the delay introduced by the lost packets. Without this mechanism the VPN is broken and MUST be re-established. Soft Handover Mobility would reduce the number of lost packets over a Hard Handover Mobility and avoids the client VPN to renegotiate the IPsec counters.

Now, the VPN use case considers taking advantage of Multiple Interfaces in order to perform bandwidth aggregation and Soft Handover Mobility. Similarly to the use case described in Section 4.1.2, when the Mobile Node detects a new Access Point and is assigned a new IP address, it MUST be able to ADD this Interface to the VPN. Similarly, it also MUST be able to REMOVE this Interface from the VPN, to perform a Soft Handover Mobility or a Hard Handover Mobility.

As mentioned in Section 4.1.2, to fully take advantage of the Multiple Interface features, like bandwidth aggregation or Soft

Handover Mobility, it is recommended to use protocols like MPTCP in combination with IPsec. However, regular VPN using TCP can still benefit from using Multiple Interfaces.

First, if a Mobile Node is using MPTCP detects a new Interface, it can ADD this new Interface to the MPTCP session. ADDing this Interface to the IPsec layer means that we consider two tunnels one that tunnels the packets from the old interface, and one that considers the packets from the new Interface. Which Interface will be used as the outer IP address will be defined by the Security Association. If the Mobile Node is using TCP, the new Interface cannot be added to the TCP session. Using the two Interfaces would mean that the IPsec Security Association would alternatively use one or the other Interface. This MAY be done by using Security Policy Databases per Interface in conjunction of a traffic load balancer that would balance the traffic between the two Interfaces. However, current system uses a centralized Security Database which is an order database. Security Associations are mainly indexed with IP addresses and ports. In the case of TCP these values does not change, and a single Security Association is chosen, thus making all traffic going to a single Interface. With TCP, ADDing an Interface would mean creating a Security Association that tunnels the TCP session to the new Interface. This Security Association SHOULD have a lower order than the Security Association tunneling the TCP session to the old Interface, which prevent the TCP session to be interrupted during the negotiation. Once set, the Mobile Node is sending the TCP session packet to the old Interface, but is likely to receive IPsec packets on both Interfaces. This is the property we use to perform Soft Handover Mobility by changing the order between the two Security Associations. This prevents packet lost.

4.3. IPsec as a distributed firewall

Some companies are using IPsec to secure their private network and prevent unauthorized hosts to be connected to the servers. The IPsec property used in that case is the authentication part rather than the confidentiality and encryption part. Similarly end-to-end security is usually using the IPsec transport mode. Resources MAY be accessed by PCs and Smartphones connected over WLAN Access Points.

When these devices are assigned new IP addresses, they currently cannot update their IPsec Security Association and need to re-negotiate a new IPsec Association. Negotiation and authentication interrupts or delay the ongoing session. Updating the IPsec configuration would avoid to perform the re-authentication. Multiple Interface properties would make possible Soft Handover. Currently none of this actions can be performed, and MOBIKE has only considered Mobility Hard Handover for the IPsec tunnel mode.

4.4. Cloud Computing distributing Security Domains

With Cloud computing, multiple security domains may be hosted on various pieces of hardware connected via IPsec. As a result these different pieces of hardware are exchanging information using multiple IPsec sessions - at least one per security domain. When a piece of hardware is changing its IP address, or when it acquires a additional Interface, it currently needs to renegotiate each IPsec connection separately. With the tunnel mode and MOBIKE, re-authentication can be avoided. MOBIKE makes possible Multihoming, Hard Handover Mobility. All other operations requires a per Security Association negotiation, which may include or not a re-authentication.

In this case, hosts want to be able to update Security Association in IPsec transport mode and in Tunnel mode. Then the hosts want to be able to announce Interface changes in a single announcement, avoiding the per Security Association announcement. On the other hand, load balancing the resources may also require mobility, to be performed only for a subtraffic. Soft Handover Mobility may also be used for traffic management, so the hosts need to be able to select some IPsec communications.

5. IPsec MIF features

From the different use cases detailed in Section 4, we identify the following IPsec MIF features.

5.1. Multihoming

Multihoming is the ability to provision Interfaces in case the running Interface is not reachable anymore. For an IPsec secure communication, the EU wants to provide one or a range of Alternate IP addresses that MUST be used in case the Primary Interface is not reachable. The difference with ADDing an interface to an given communication is that with Multihoming the Alternate MUST be used only if the Primary Interface is not reachable.

On an IPsec point of view, it means that IPsec MUST be configured to DISCARD any packets of the communication unless the Primary Interface is not reachable. When the Primary Interface is not reachable, then IPsec MUST be configured to PROTECT or BYPASS the traffic for the given communication.

5.2. Hard Handover Mobility

Hard handover Mobility is the ability for a host to update an Interface with another.

On an IPsec point of view, Mobility Hard Handover consists in modifying an existing Security Association. More specifically, the IP addresses used as the selectors of the Security Association MUST be modified when the transport mode is used. When the tunnel mode is used, the tunnel IP addresses MUST be modified.

5.3. Soft Handover Mobility

Soft Handover Mobility is the ability for a host to smoothly move traffic from one Interface to the other. Soft Handover requires that the host is able to handle two Interfaces.

On an IPsec point of view, Soft Handover Mobility consists in ADDing an new Security Association that is derived from an existing established Security Association and then REMOVing the existing Security Association.

When the IPsec transport mode is used, Soft Handover MUST be performed in conjunction with upper layer mechanisms like those provided by SCTP, MPTCP or session resumption.

5.4. Dynamic addition of an Interface

Dynamic addition of an Interface is the ability for a host to send traffic of an ongoing communication to a additional and newly added Interface

On an IPsec point of view, dynamic addition of an Interface requires to create a new Security Association derived from an existing Security Association.

5.5. Dynamic removal of an Interface

Dynamic removal of an Interface is the ability for a host to configure all its sessions so that traffic is not sent or received from an still existing or not anymore existing Interface.

On an IPsec point of view, this consists of removing all or a subset of Security Association that concerns a given Interface and discarding the traffic sent to or received on this Interface.

5.6. Traffic Selection

Traffic Selection consists in selecting a single, a set or all communications in order to perform an action.

On an IPsec point of view, Traffic Selection consist in selecting a the single, a set or all Security Association associated between two hosts. This makes possible to apply a IPsec action on a given subtraffic as well as to configure multiple Security Associations in a single exchange.

6. Problem Statement

6.1. MOBIKE limitations

MOBIKE [RFC4555] is the IKEv2 extension that has been designed to handle Mobility and Multihoming. However, it presents the following limitations:

- MOBIKE does not consider the transport mode: MOBIKE has only been designed for the Tunnel mode.
- MOBIKE has not been designed for Multiple Interfaces: MOBIKE has only been designed for a single Interface.
- MOBIKE does not consider Soft Handover Mobility: MOBIKE has only been designed for Hard Handover Mobility. In fact a Soft Handover Mobility would require the simultaneous use of two Interfaces. Since MOBIKE has only been designed for nodes with a single Interface, Soft Handover Mobility is out of scope of MOBIKE.
- MOBIKE does not consider Mobility or Multihoming for a specific communication: In fact MOBIKE has been designed for nodes with a single Interface, thus Mobility or Multihoming operations affect all tunneled IPsec ongoing communications, as well as the IKEv2 signaling channel.

6.2. IKEv2 limitations

IKEv2 [RFC5996] has been designed to negotiate Security Associations. It has neither been designed to handle Mobility nor Multihoming. Multiple Interface operations like ADD REMOVE and therefore SOFT_HAND_OVER can be considered as a IKEv2 or combinations of IKEv2 operations.

When a new interface is detected by the end user, it may add it to the current communication by negotiating a new Security Association, independent from the Security Associations that already exist. A complete IKEv2 exchange that includes the authentication can be initiated. However, this includes a 4 message exchange, with an authentication that may delay of a few seconds the Security Association negotiation. To avoid re-authentication, the CREATE_CHILD exchange can be used for that purpose. However, the CREATE_CHILD exchange presents the following limitations:

- CREATE_CHILD is not mandatory for IKEv2: This means that all IKEv2 implementations do not provide the ability to renegotiate the IPsec Traffic Selectors of a given Security Association.
- CREATE_CHILD support is not advertised to the peers: Whether an IPsec node implements or not the CREATE_CHILD exchange is not advertised. This MAY result in breaking a communication. For example, a IPsec Mobile Node may initiate a CREATE_CHILD exchange for a Mobility Hard Handover that is rejected by the Correspondent Node.
- CREATE_CHILD is a 2 packet exchange: In the case of Soft Handover two exchanges are required, which makes soft Handover as a 4 packet exchange. Mobility operations are sensitive operations and should be as straight forward as possible, with a single exchange.
- CREATE_CHILD is a per SA negotiation: In the case a Mobile Node has Multiple IPsec Security Associations with its Correspondent Node, Multiple CREATE_CHILD exchanges are required. Mobility operations are sensitive operation and should be as straight forward as possible. One exchange is expected. For a Mobile Node sharing n IPsec Security Associations with its Correspondent Node, a Soft Handover with CREATE_CHILD would require 2 * n CREATE_CHILD exchanges. We expect this number of exchanges to be reduced to 1.
- CREATE_CHILD is complex: The CREATE_CHILD exchange has been designed to completely renegotiate a Security Association. As a result, all parameters of the Security Association Database can be mentioned. This results in quite complex exchange, which is the reason lightweight IKEv2 implementations are not required to implement this exchange. The Multihoming, Mobility operations in this document do not interact with other parameters than the IP addresses associated to the Security Association. We expect a much appropriate an simpler syntax.

To REMOVE an Interface, IKEv2 provides the DELETE Notify Payload. This exchange is quite straight forward but:

- DELETE is a per SA exchange: (see CREATE_CHILD item)

SOFT_HAND_OVER can be considered as a combination of ADD and REMOVE actions. However neither IKEV2 does not provide the ability to perform them with a single message exchange. For performance issues, we want that Soft Handover Mobility can be performed with a single message exchange (SOFT_HAND_OVER).

IKEV2 does not provide the ability to select a set or all Security

Associations associated to an Interface. Traffic Selectors are negotiated to define the traffic selectors associated to an Security Association. As a result IKEv2 only provides the granularity for a single Security Association or for all Security Association associated to an IKEv2 channel or IKEv2 session. This granularity does not ease traffic management based on Interfaces.

7. IPsec MIF Requirements

Finally, MIF requires IPsec /IKEv2 / MOBIKE to be extended so:
- Mobility, Multihoming and Multiple Interface features can be provided for both IPsec tunnel and transport mode.
- IPsec nodes can dynamically ADD an new Interface for all ongoing IPsec protected communications
- IPsec nodes dynamically REMOVE an old Interface for all ongoing IPsec protected communications
- IPsec nodes can perform soft and hard handover handover
- IPsec nodes can manage IPsec traffic over Multiple Interfaces by selecting the IPsec Security Association a Multiple Interface operation (ADD, REMOVE, Soft/Hard Handover, Multihoming) occurs.
  This includes selecting a subtraffic as well as performing a Multiple Interface operation over multiple Security Associations in a single IKEv2 exchange.

8. Security Considerations

The whole document sets MIF requirements for a security protocol.

9. IANA Considerations

There is no IANA consideration here.

10. Acknowledgment

We would like to thank Daniel Palomares, Pierrick Seite, Brian Carpenter, Hui Deng, Jong-Hyouk Lee, Juan Carlos Zuniga and Konstantinos Pentikousis for their useful comments.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6311] Singh, R., Kalyani, G., Nir, Y., Sheffer, Y., and D. Zhang, "Protocol Support for High Availability of IKEv2/IPsec", RFC 6311, July 2011.

11.2. Informational References

[RFC6182] Ford, A., Raiciu, C., Handley, M., Barre, S., and J. Iyengar, "Architectural Guidelines for Multipath TCP Development", RFC 6182, March 2011.

Authors' Addresses

Daniel Migault
Francetelecom - Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: mglt.ietf@gmail.com

Carl Williams
MCSR Labs
Philadelphia, PA 19103
USA

Phone: 650-279-5903
Email: carlw@mcsr-labs.org