Workgroup: I2NSF Working Group
Internet-Draft:
draft-kim-i2nsf-security-controller-interface-
dm-01
Published: 28 March 2023
Intended Status: Standards Track
Expires: 29 September 2023
Authors: J. Kim
Sungkyunkwan University
P. Lingga
Sungkyunkwan University
R. Marin-Lopez
University of Murcia
J. Jeong, Ed.
Sungkyunkwan University
S. Hares
Huawei

I2NSF Security Controller-Facing Interface YANG Data Model for Cross-Domain IPsec Flow Protection

Abstract

This document defines an information model and a YANG data model for the Security Controller-Facing Interface between two security controllers in an Interface to Network Security Functions (I2NSF) framework located in different Domains. This interface is used for the exchange of IPsec flow protection to protect the IP Communication between two Network Security Functions (NSFs) in cross-domain environments. The YANG data model in this document is built on the basis of the YANG data model for IPsec flow protection based on Software-Defined Networking (SDN).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 September 2023.

Table of Contents

1. Introduction

Interface to Network Security Functions (I2NSF) defines a framework and its interfaces for the security management and monitoring of Network Security Functions (NSFs) for security services. [RFC8329].

To support multiple security services for a traffic flow with multiple NSFs, a Service Function Chaining (SFC) [RFC7665] can be used. In SFC, the integrity and confidentiality of security services between the NSFs must be guaranteed. [RFC9061] protects the flow between NSFs under the control of the same I2NSF security controller. The security controller is in charge of generating, managing and distributing the IPsec Security Associations. This document describes the flow protection and key management process (i.e., IKE case and IKE-less case) between two NSFs within the

coverage of I2NSF managed by one security controller, i.e., within one I2NSF domain (e.g., an autonomous system (AS)).

However, recently, as described in [I-D.ietf-bess-bgp-sdwan-usage], multiple Software-Defined WANs (SD-WANs) scenarios demand a centralized way of flow protection using IPsec between SD-WAN peers(NSFs). In the scenarios, some SD-WAN peers that are located in different spaces (virtual or physical) are connected only by untrusted public networks.

Therefore, to ensure secure communication between NSFs located in different SD-WANs over untrusted public networks, flow protection is required. Additionally, an interface for exchanging information (e.g., security policies and IPsec parameters) between different SD-WANs is necessary.

In response to these requirements, I2NSF needs to extend by using [RFC9061]. The I2NSF security controller needs to extend to centrally manage multiple I2NSFs that are located in different domains, and needs to extend to exchange information between two I2NSFs located in two different domains.

To extend I2NSF, a centralized point that can manage multiple I2NSF domains is needed. It is necessary to introduce a new interface for centralized management and exchanging information between NSFs located in different I2NSF domains, i.e., a cross-domain environment with multiple ASes.

Therefore, this document proposes an information model and a YANG data model for a Security Controller-Facing Interface (SFI) for exchanging information (e.g., security policies and IPsec parameters) between security controllers. This interface performs the exchange of a security policy and provides flow protection among NSFs located in cross-domain environments. This document suggests two scenarios of configuration between peer-to-peer security controller cases (see Section 5.1.) and configuration in hierarchical security controller cases (see Section 5.2.).

2. Terminology

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

I2NSF Domain: An area that an I2NSF security controller can manage.

Security Contorller-Facing Interface (SFI): An interface for the exchange of information between two security controllers located in two different I2NSF domains.

3. I2NSF Cross Domain IPsec Management Description

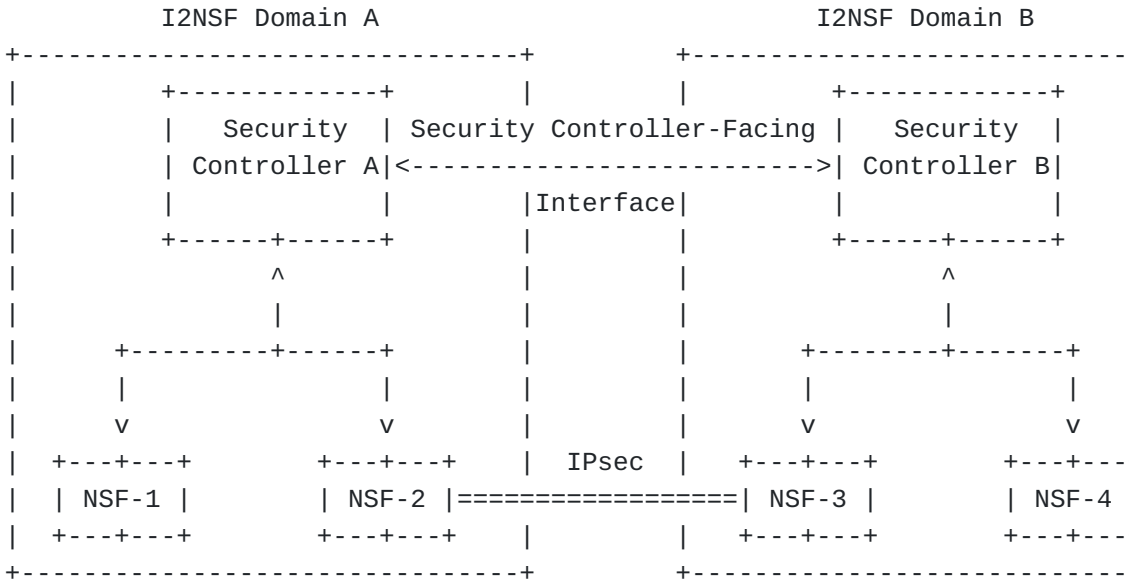

Figure 1: I2NSF Framework for Cross-Domain IPsec Flow Protection

Figure 1 show the conceptual architecture of I2NSF framework for Cross-Domain IPsec flow protection. As shown in Figure 1, the two I2NSF security controllers located in different I2NSF domains, i.e., I2NSF Domains A and B. In one domain, the security controller only can manage NSFs registered by the Developer's Management System (DMS). Therefore, the security controller is not aware of the existence of NSFs in other domains. To enable communication between NSFs located in different I2NSF domains, each with its own security controller, a security controller can be used as an intermediary. The two security controllers in different domains MUST have a secure and trusted connection; the setup of this connection is out of the scope of this document. Through this secure connection, the security controllers can exchange the IPsec parameters using SFI and configure the NSFs located in different I2NSF domains so that they can establish IPsec SAs to protect data traffic between them.

4. Information Model for Security Controller-Facing Interface

In [RFC9061], the I2NSF security controller enables the key management for flow protection between NSFs in the I2NSF domain that it manages. Therefore, this section introduces the information model for exchanging information in different domains using Security

Controller-Facing Interface (called SFI) between I2NSF Security Controllers to provide flow protection between NSFs existing in different I2NSF domains.

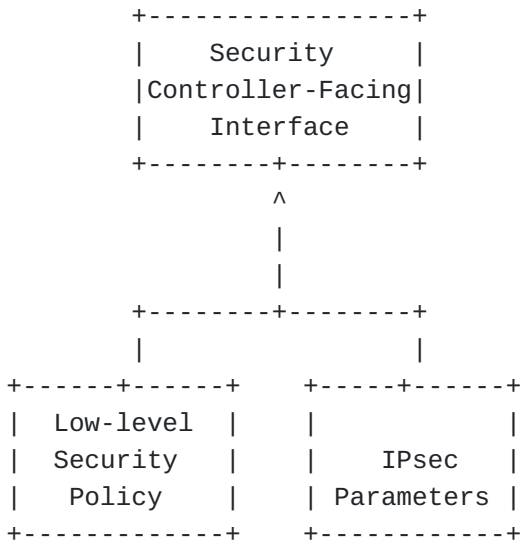

Figure 2: Diagram for Security Controller-Facing Interface

Figure 2 shows the high-level concept of SFI to deliver cross-domain flow protection for IPsec. Information that can be delivered through SFI is as follows:

* Low-level Security Policy : A low-level security policy to configure NSFs located in a cross-domain environment. The low-level security policy means the translated security policy that the security administrator wants to configure, such as blocking the SNS website, and flow protection between NSFs A and B. The security controller can deliver the low-level security policy to the security controllers other I2NSF domains through SFI. After receiving the security policy, the security controller can deliver the security policy to the target NSFs via the NSF-Facing Interface [I-D.ietf-i2nsf-nsf-facing-interface-dm].

* IPsec Parameters: Parameters required to establish IPsec Security Associations (SAs) [RFC9061]. To establish IPsec SAs with NSFs located in a different domain, the security controller MUST be able to securely exchange the necessary parameters for those SAs.

5. Use Cases for the Security Controller-Facing Interface in Cross-Domain Environments

5.1. Peer-to-Peer Use Case for the Security Controller-Facing Interface in Cross-Domain Environments

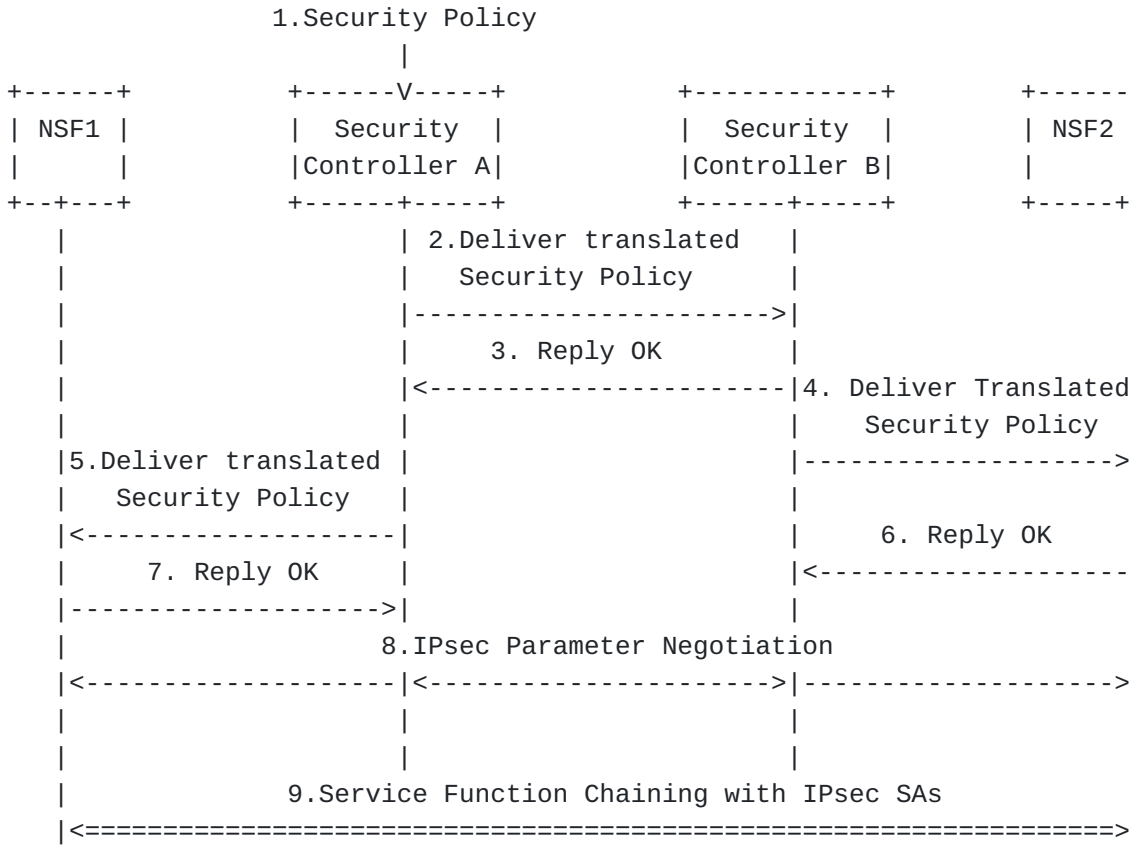

Figure 3: Use Case of the Peer-to-Peer Security Controllers

Figure 3 shows the peer-to-peer security controller use case's message sequence between entities in multiple domains. In this use case, an I2NSF A's administrator requests a security service that cannot address by only the NSFs located in their own I2NSF domain. The security controller A can request to cooperate with a trusted peer security controller B in a different I2NSF domain for the required security service. In this scenario, it is assumed that the secure connection between the two security controllers is already set up. The detailed sequence is as follows:

1. I2NSF A's administrator requests a security service that cannot be addressed by only the NSFs located in their own I2NSF domain.

2. Security Controller A delivers the security policy for NSF2 through SFI to Security Controller B in a cross-domain environment.

3. If Security Controller B can handle the received security policy, reply OK message to Security Controller A.

4. Security Controller B delivers the security policy to NSF2 for checking that NSF2 can be configured by the sent policy.

5. Security Controller A deliver the translated security policy for NSF1.

6. If NSF2 can handle the received security policy, it replies OK message to Security Controller B.

7. If NSF1 can handle the received security policy, it replies OK message to Security Controller A.

8. NSF1 and NSF2 negotiate IPsec parameters through Security Controller A and Security Controller B.

9. NSF1 and NSF2 establish IPsec SAs using the received IPsec parameters and provide the requested security service to the user through SFC.

5.2. Hierarchical Use Cases for the Security Controller-Facing Interface in Cross-Domain Environments

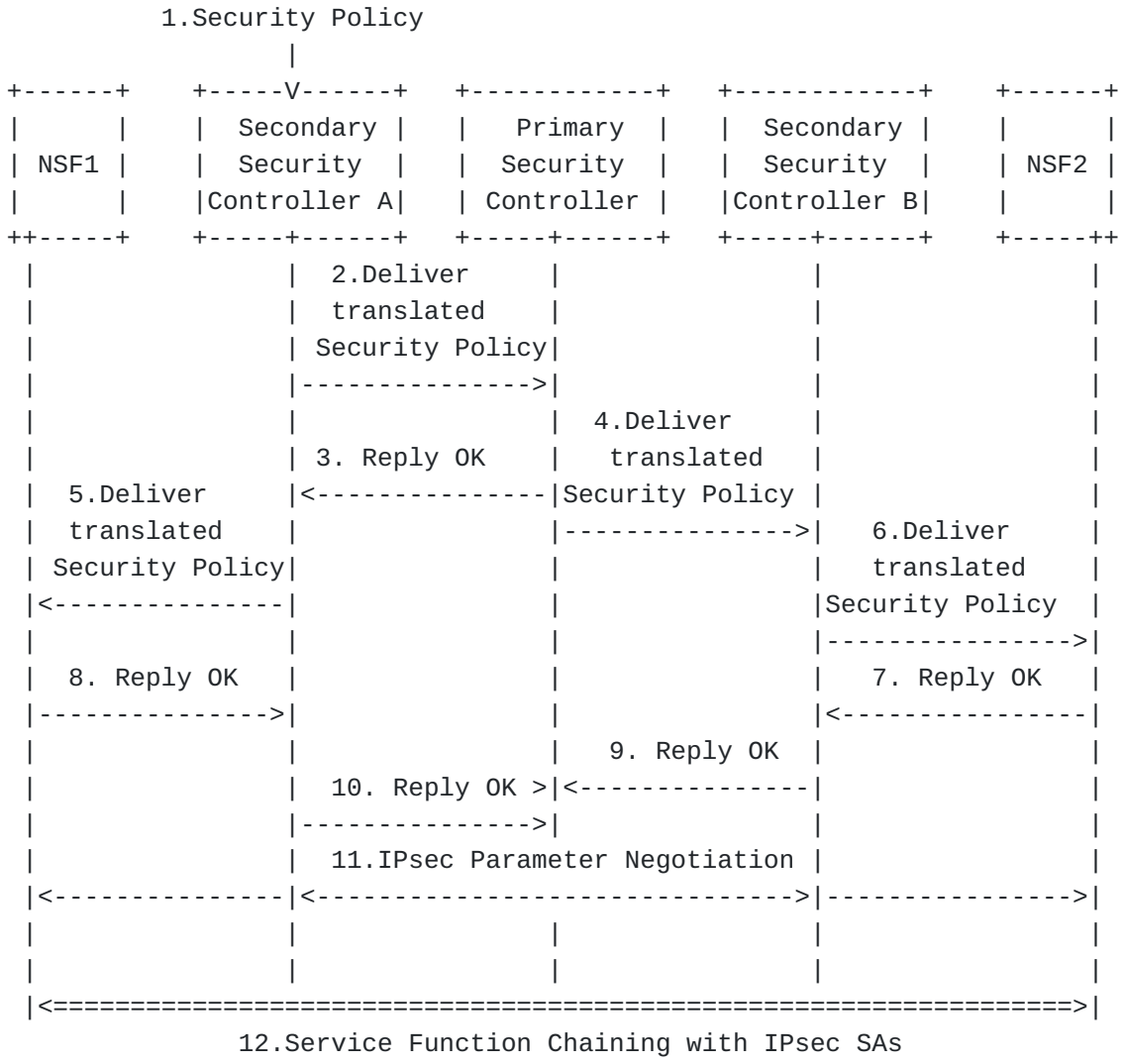

Figure 4: Use Case of the Hierarchical Distribution Security Controllers

Figure 4 shows a message sequence between entities in multiple domains with a primary Security Controller. The primary Security Controller can act as a centralized controller. The primary Security Controller between secondary Security Controllers has a secure connection in advance. How to establish this secure connection is out of the scope of this document. Using this secure connection, the primary Security Controller collects all of the secondary Security Controller's information via SFI. In this usecase, when the administrator of an I2NSF A requests a security service that is not available in its own I2NSF domain, then the secondary Security Controller A, with the help of the primary Security Controller, can

collaborate with a trusted peer Security Controller B from a different I2NSF domain to obtain the required security service. The detailed sequence is as follows:

1. I2NSF A's administrator requests a security service that cannot be addressed only by the NSFs located in its own I2NSF domain.

2. The secondary Security Controller A delivers the translated security policy through SFI to the primary Security Controller.

3. If the primary Security Controller knows which secondary Security Controller can handle the delivered security policy, the primary Security Controller sends an OK message to Security Controller A.

4. The primary Security Controller delivers the received security policy to the secondary Security Controller that can provide the requested security services, i.e., the secondary Security Controller B.

5. The secondary Security Controller A delivers the translated security policy to NSF1 via NFI.

6. The secondary Security Controller B delivers the received security policy to NSF2 via NFI.

7. If NSF2 can handle the received security policy, it replies OK message to the secondary Security Controller B.

8. If NSF1 can handle the received security policy, it replies OK message to the secondary Security Controller A.

9. The secondary Security Controller B delivers NSF2's reply OK message to the primary Security Controller.

10. The secondary Security Controller A delivers NSF1's reply OK message to the primary Security Controller.

11. Security Controller A and Security Controller B negotiate IPsec parameters through the primary Security Controller.

12. NSF1 and NSF2 establish IPsec SAs using the received IPsec parameters and provide the requested security service to the user through SFC.

6. YANG Data Model for Security Controller-Facing Interface

TBD

7. IANA Considerations

This document does not require any IANA actions.

8. Security Considerations

The same security considerations for the I2NSF framework [RFC8329] are applicable to this document.

9. References

9.1. Normative References

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

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8329] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, DOI 10.17487/RFC8329, February 2018, <https://www.rfc-editor.org/info/rfc8329>.

[RFC9061] Marin-Lopez, R., Lopez-Millan, G., and F. Pereniguez-Garcia, "A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)", RFC 9061, DOI 10.17487/RFC9061, July 2021, <https://www.rfc-editor.org/info/rfc9061>.

9.2. Informative References

[I-D.ietf-i2nsf-nsf-facing-interface-dm] Kim, J. T., Jeong, J. P., Jung-Soo, J., Hares, S., and Q. Lin, "I2NSF Network Security Function-Facing Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-nsf-facing-interface-dm-29, 1 June 2022, <https://

datatracker.ietf.org/doc/html/draft-ietf-i2nsf-nsf-facing-interface-dm-29>.

[I-D.ietf-idr-sdwan-edge-discovery]
Dunbar, L., Hares, S., Raszuk, R., Majumdar, K., and G. S. Mishra, "BGP UPDATE for SDWAN Edge Discovery", Work in Progress, Internet-Draft, draft-ietf-idr-sdwan-edge-discovery-07, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-sdwan-edge-discovery-07>.

[I-D.ietf-bess-bgp-sdwan-usage]
Dunbar, L., Guichard, J., Sajassi, A., Drake, J., Najem, B., and D. Carrel, "BGP Usage for SDWAN Overlay Networks", Work in Progress, Internet-Draft, draft-ietf-bess-bgp-sdwan-usage-08, 26 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-bess-bgp-sdwan-usage-08>.

Appendix A. Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government, Ministry of Science and ICT (MSIT) (No. 2023R1A2C2002990).

This work was supported in part by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT)(No. 2022-0-01015, Development of Candidate Element Technology for Intelligent 6G Mobile Core Network).

Appendix B. Contributors

The following are coauthors of this document:

Jung-Soo Park
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu
Daejeon
34129
Republic of Korea

Email: pjs@etri.re.kr

Yunchul Choi
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu
Daejeon
34129
Republic of Korea

Email: cyc79@etri.re.kr

Gabriel Lopez-Millan
University of Murcia
Faculty of Computer Science
Campus de Espinardo S/N
30100 Murcia
Spain

Email: gabilm@um.es

Fernando Pereniguez-Garcia
University Defense Center
Spanish Air Force Academy
San Javier Murcia
30720 Murcia
Spain

Email: fernando.pereniguez@cud.upct.es

Appendix C. Changes from draft-kim-i2nsf-security-controller-interface-dm-00

The following changes are made from draft-kim-i2nsf-security-controller-interface-dm-00:

*This version has been revised with Rafa Marin-Lopez's comments.

Authors' Addresses

Jeonghyeon Joshua Kim
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4957
Email: jeonghyeon12@skku.edu

Jaehoon Paul Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Patrick Lingga
Department of Electrical and Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4957
Email: patricklink@skku.edu

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
United States of America

Phone: +1-734-604-0332
Email: shares@ndzh.com

Rafa Marin-Lopez
University of Murcia
Faculty of Computer Science
Campus de Espinardo S/N
30100 Murcia
Spain

Phone: +34 868 88 85 01
Email: rafa@um.es