Internet Research Task Force
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

J. Jeong, Ed.
Sungkyunkwan University
Y. Shen
Ajou University
Y. Ahn
Sungkyunkwan University
Y. Kim
Soongsil University
E. Duarte Jr.
Federal University of Parana
K. Yao
China Mobile

20 October 2025

A Framework for the Interface to In-Network Computing Functions (I2ICF)
draft-jeong-nmrg-i2icf-framework-00

Abstract

This document specifies a framework to define Interface to In-Network Computing Functions (I2ICF) for user services both on the network-level and application-level. In-Network Computing Functions (ICF) include In-Network Network Functions (INF), defined in the context of Network Functions Virtualization (NFV) and Software-Defined Networking (SDN). ICFs also include In-Network Application Functions (IAF) which appear in the context of Internet-of-Things (IoT) Devices, Software-Defined Vehicles (SDV), and Unmanned Aerial Vehicles (UAV). This document describes an I2ICF framework, which includes components and interfaces to configure and monitor the ICFs that implement applications and services.

Table of Contents

1. Introduction 2
2. Terminology 3
3. A Framework for the Interface to In-Network Computing Functions 5
4. Interfaces in the I2ICF Framework 11
5. IANA Considerations 13
6. Security Considerations 13
7. References 13
7.1. Normative References 14
7.2. Informative References 14
Acknowledgments 20
Contributors 20
Authors' Addresses 21

1. Introduction

Network softwarization has been widely adopted in multiple environments, such as in cloud and edge computing, as well as in the network infrastructure itself, facilitating the deployment of network services (e.g., 5G mobile networks [TS-23.501]). The multiple technologies behind network softwarization include Network Functions Virtualization (NFV) [ETSI-NFV][ETSI-NFV-Release-2] and Software-Defined Networking (SDN) [RFC7149]. Furthermore, there is also an integration with Intent-BasedNetworking (IBN)[RFC9315][Survey-IBN-CST-2023], which can be used to define and deploy intelligent network services as well as intelligent application services.

In the context of Computing in the Network (COIN) terminology [I-D.irtf-coinrg-coin-terminology], a Programmable Network Device (PND) in an In-Network Computing (INC) environment can have multiple kinds of features and capabilities. A PND can also interact with

other PNDs. PNDs from different product lines or vendors can provide different functionalities for INC functions. In order to compose a COIN system consisting of multiple PDNs that interact among themselves, it is necessary to define a standard interface for PNDs to be exposed so that they can learn about each other's capabilities and properly interact with each other.

A standard framework to define the interfaces of Application Functions (AFs) and Network Functions (NFs) is required to allow the configuration and monitoring of applications and network services consisting of those functions. There is currently no standard data model to describe the capabilities of AFs and NFs. Furthermore, there is no standard data model defining an interface to register the capabilities of AFs and NFs with a controller-like device that would process service requests for those functions. In addition, there are no standard interfaces to configure and monitor those AFs and NFs according to a user's intent. The Interface to Network Security Functions (I2NSF) was standardized for the control and management of Network Security Services with Network Security Functions (NSFs) [RFC8329] [I-D.ietf-i2nsf-applicability]. The present document is defined taking into account the I2NSF document, but the purpose is beyond the scope of Security Functions, defining a more general control and management framework for intelligent services consisting of AFs and NFs.

This document specifies a framework for the definition of the Interface to In-Network Computing Functions (I2ICF) for In-Network Computing Functions (ICFs), assuming arbitrary functionalities, features and capabilities. The ICFs consist of Network Functions (NFs) including PNDs and Application Functions (AFs) and are used to compose user services. First of all, ICFs include In-Network Network Functions (INF) which are NFs defined within the context of NFV and SDN [I-D.irtf-coinrg-use-cases]. Secondly, they also include In-Network Application Functions (IAF) which are AFs employed by Internet-of-Things (IoT) Devices, Software-Defined Vehicles (SDV) [AUTOSAR-SDV][Eclipse-SDV][COVESA], and Unmanned Aerial Vehicles (UAV). Finally, this document shows how Intent-Based Networking (IBN) can be realized with the proposed I2ICF framework and its interfaces for user services that consist of a combination of ICFs in a target network.

2. Terminology

This document uses the terminology described in [RFC9315], [RFC8329], [I-D.irtf-coinrg-coin-terminology], [I-D.irtf-coinrg-use-cases], [I-D.jeong-nmrg-security-management-automation], [I-D.jeong-nmrg-ibn-network-management-automation], and [SPT]. In addition, the following terms are defined below:

* Intent: the set of operational goals (that a network should meet) and outcomes (that a network is supposed to deliver) defined in a declarative manner without specifying how they are achieved or should be implemented [RFC9315].

* Intent-Based System (IBS): the system that enforces an intent from a user (or administrator) into a target system (e.g., SDV). An intent can be expressed in Natural Language (e.g., English) and can be translated into a policy (i.e., network policy and application policy) using Natural Language Processing (NLP) [Flan-T5][GPT-3] [USENIX-ATC-Lumi][BERT] [Deep-Learning]. In this document, the intent can be translated into a corresponding high-level policy by an intent translator [I-D.jeong-nmrg-security-management-automation]. The high-level policy can also be translated into the corresponding low-level policy by a Policy Translator (PT) [SPT]. The low-level policy is dispatched to appropriate Service Functions (SFs). Through the monitoring of the SFs, the activity and performance of the SFs is monitored and analyzed. If needed, the rules of the high-level or low-level network policy are augmented or new rules are generated and configured to appropriate SFs.

* Mobile Object (MO): the object that is capable of moving with its own power source and wireless communication capability, e.g., in the context of 5G Vehicle-to-Everything (e.g., 5G V2X). An MO can be an Internet-of-Things (IoT) device, Software-Defined Vehicle (SDV) [AUTOSAR-SDV][Eclipse-SDV][COVESA], and Unmanned Aerial Vehicle (UAV). An MO is a Programmable Network Device (PND) [I-D.irtf-coinrg-coin-terminology] that can be reconfigured for different network requirements inside the MO.

* In-Network Network Functions (INF): the service functions that work for computing in the network infrastructure. They are a group of COIN programs [I-D.irtf-coinrg-coin-terminology] to provide required computing tasks and functions.

* In-Network Application Functions (IAF): the service functions that work for applications in Mobile Objects. They are a group of COIN programs [I-D.irtf-coinrg-coin-terminology] to provide the required application tasks and functions.

* In-Network Computing Functions (ICF): the service functions that include In-Network Network Functions (INF) and In-Network Application Functions (IAF).

* Interface to In-Network Computing Functions (I2ICF): the interfaces that are used between a pair of ICFs for the interaction, configuration and monitoring.

* A Framework for the Interface to In-Network Computing Functions (I2ICF): the framework that consists of components and interfaces to configure and monitor ICFs that can be employed by applications and services in the network infrastructure and MOs.

3. A Framework for the Interface to In-Network Computing Functions

This section specifies a framework for defining the Interface to In-Network Computing Functions (I2ICF), including its components and the interfaces among those components. Figure 1 shows Wireless and Wired Networks of a Central Cloud. The I2ICF framework includes network entities and Mobile Objects (MO). Figure 2 shows a VNF-Consensus Architecture that allows the I2ICF framework to synchronize flow table information of all the replicated SDN Controllers in the same Edge Cloud [NFV-COIN].

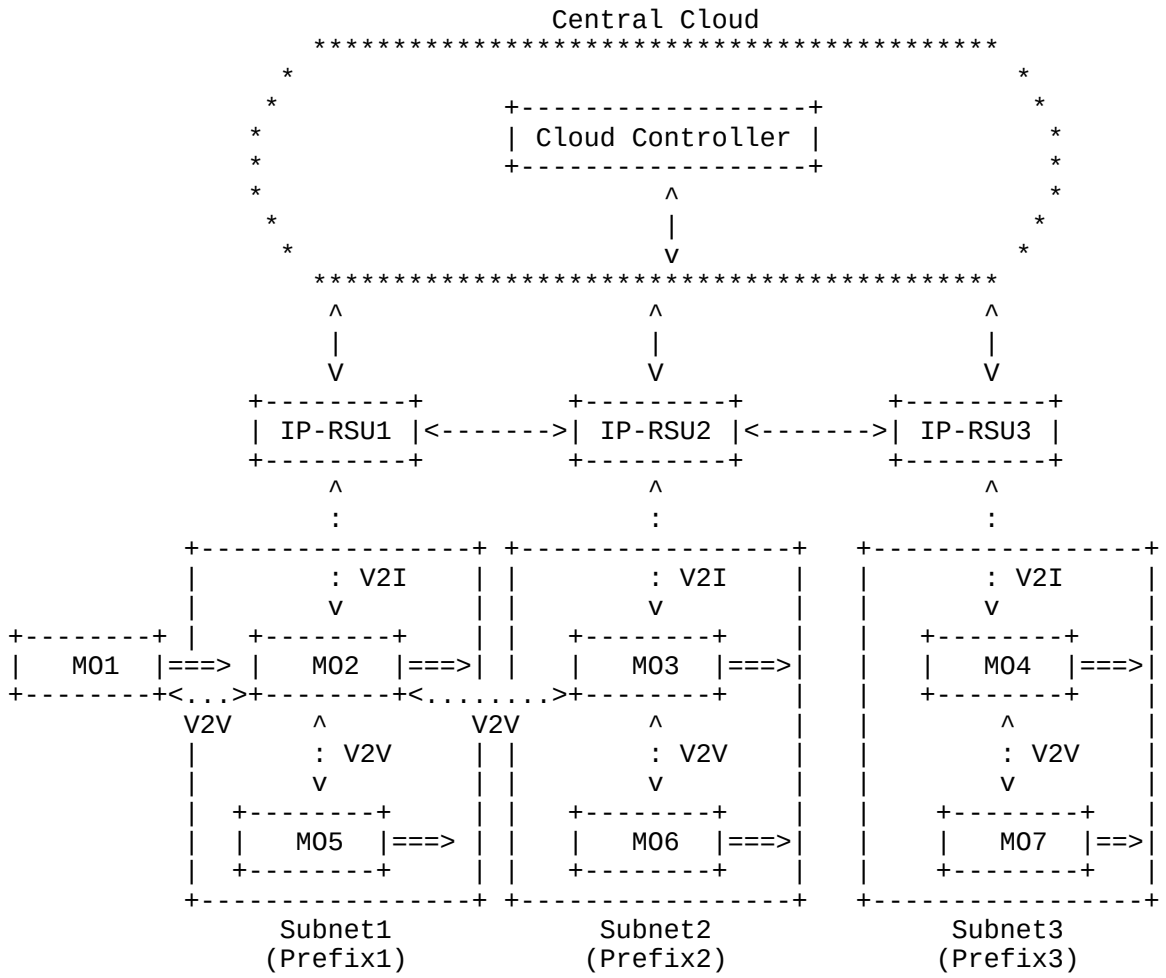

Figure 1: I2ICF Framework: Wireless and Wired Networks in a Central Cloud

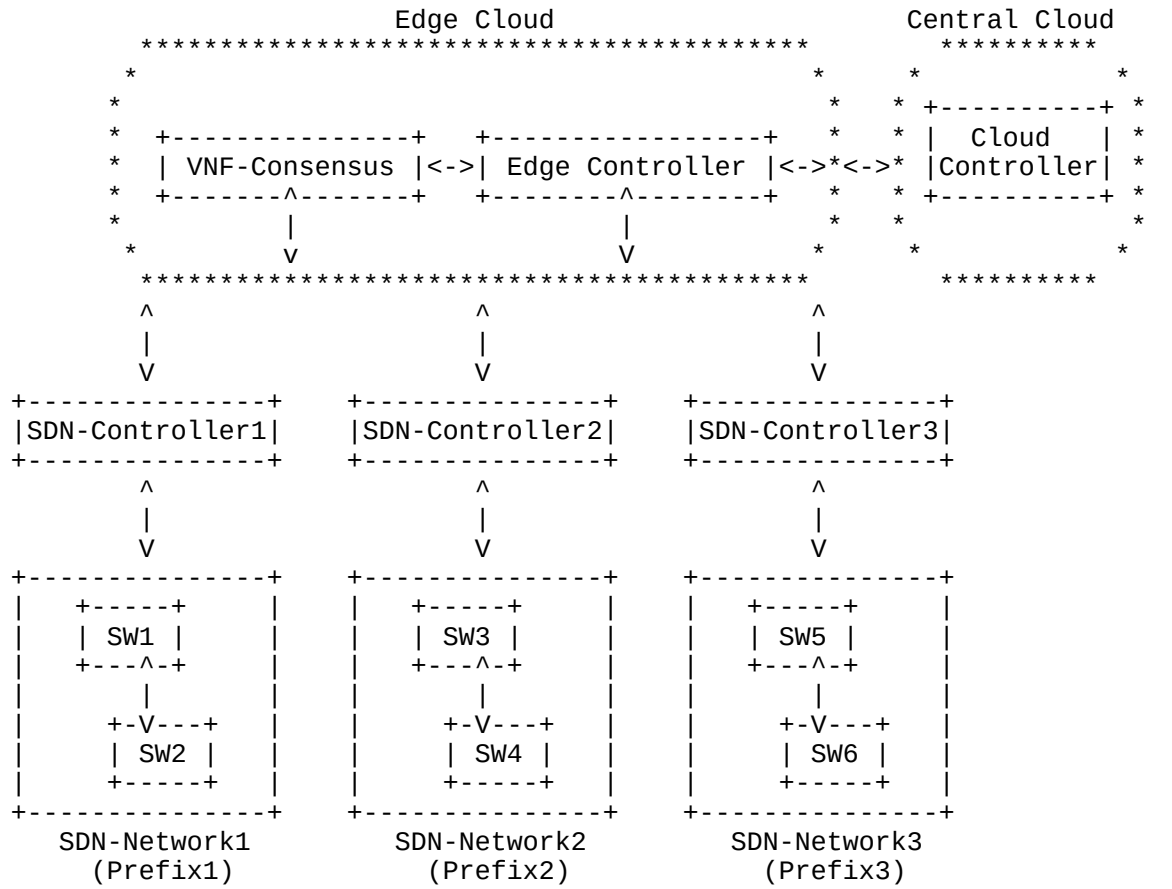

Figure 2: I2ICF Framework: VNF-Consensus Architecture in an Edge Cloud

An intent-based management strategy is required between the central cloud and MOs to allow the automatic configuration of MOs [I-D.jeong-nmrg-ibn-network-management-automation]. Figure 3 shows an instance of the I2ICF framework as an IBS for an MO. The framework in this case includes a Central Cloud and an MO. Figure 4 shows an I2ICF framework as an IBS for an Edge Cloud. The framework in this case consists of a Central Cloud and an Edge Cloud.

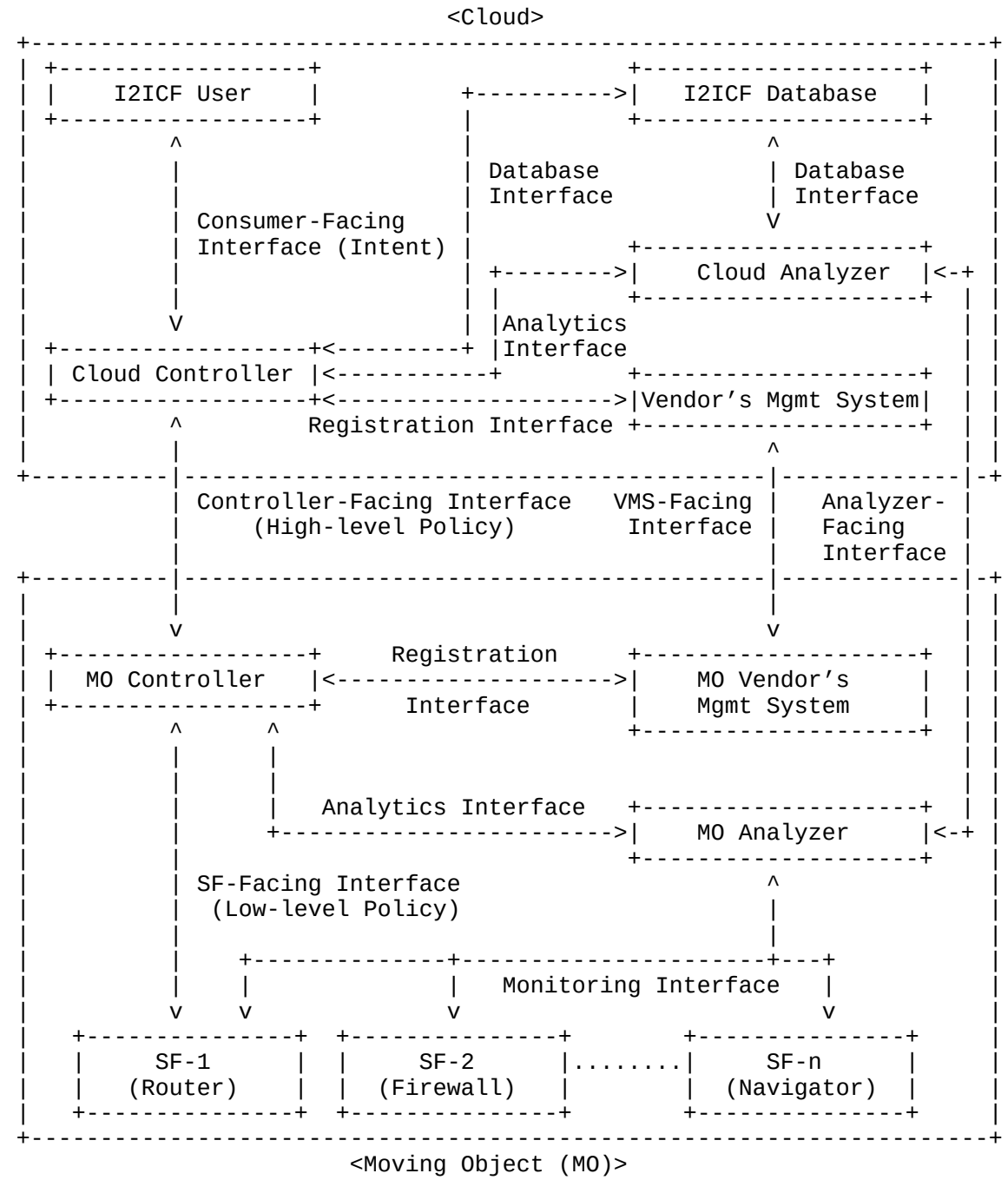

Figure 3: I2ICF Framework for a Moving Object

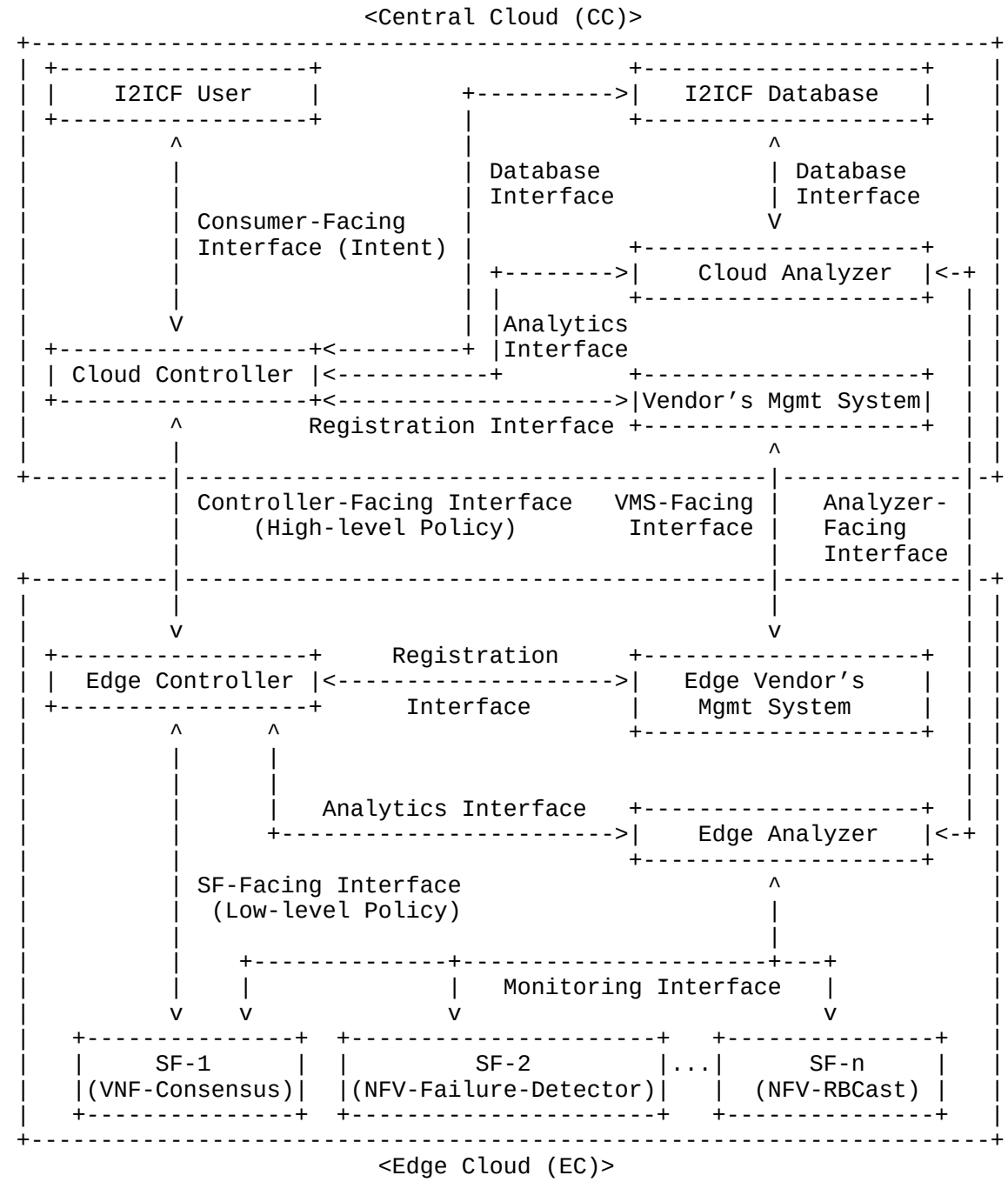

Figure 4: I2ICF Framework for an Edge Cloud

A Central Cloud (CC) consists of an I2ICF User (as network administrator), a Cloud Controller (which acts as an orchestrator for the central cloud), an I2ICF Database (which is the main repository for ICF management and monitoring information), and a Cloud Analyzer (as a monitoring data analyzer for MOs and ECs) such as Network Data Analytics Function (NWDAF) in 5G networks [TS-23.288][TS-29.520]. These and other components are defined next:

* I2ICF User: the software (e.g., web-browser-based user interface) that is used by I2ICF administrators to deliver network intents to MO controllers and edge controllers. In the 3GPP intent-driven management service document, it is assumed that a network intent is configured by an intent data model [TS-28.312] [TR-28.812].

* Cloud Controller: the main component that is responsible for the management and control of other system components of the central cloud, including security. From a security point of view, a security service policy can be transmitted to the service function (SF) by converting the I2ICF User’s security service intent into the corresponding security service policy and selecting an SF that provides an appropriate security service.

* Cloud Vendor’s Management System: the component that provides images of virtualized SFs for cloud services and registers the SFs and access information with the Cloud Controller.

* Cloud Analyzer: the component that gathers and evaluates monitoring data from MO Analyzers and Edge Analyzers to ensure the functionality and performance of SFs, e.g., the network data analytics function (NWDAF) in 5G networks.

* I2ICF Database: the database that manages the information of MOs and ECs, including network and security configuration and status of MOs and ECs. For example, for MOs it maintains the current locations and navigation paths (e.g., SDVs). For ECs, it maintains network configuration information, including for instance the status of AFs and NFs within the edge cloud.

An IBS in an MO (or EC) is composed of an MO Controller (or Edge Controller) which acts as a manager for the MO (or EC), an MO Analyzer (or Edge Analyzer) which acts as a monitoring data analyzer for an MO (or EC))
[I-D.jeong-nmrg-ibn-network-management-automation], it can also include a Vendor’s Management System (as a vendor system to provide cloud-native containers) [RFC8329], and Service Functions (SFs). SFs for the MO require NFs such as routers, DNS servers, and firewalls [I-D.jeong-nmrg-ibn-network-management-automation]), and AFs include safe driver devices and navigators. SFs for the EC include NFs such

as VNF-Consensus, NFV-Failure-Detector, and NFV-RBCast (i.e., NFV Reliable-Ordered Broadcast) [NFV-COIN]). Those components are further described next:

* MO Controller: the component that controls and manages other components of the MO framework (or the EC framework). It translates the high-level policies received from the Cloud Controller into a low-level policies that the SF can understand. Any SF can be selected to execute any low-level service. Yet another task is the transmission of the policy to the SF.

* MO Vendor Management System (or Edge Vendor Management System): the component that provides an image of a virtualized SF for MO services (or EC services) to the MO framework (or the EC framework). Also responsible for registering functions and SF access control information on MO Controller (or the Edge Controller).

* Service Function (SF): the component that can be either a virtual network function (VNF), cloud-native network function (CNF), or physical network function (PNF) of a specific service. In the context of security, SFs provide security services such as firewalls, web filters, DDoS attack mitigators, and anti-viruses. In addition, networks and application services can also operate as SFs.

* MO Analyzer (or Edge Analyzer): the component that collects monitoring data from SFs of MOs (or ECs) and analyzes the collected data to monitor the activity and performance of SFs. The MO Analyzer (or Edge Analyzer) acts as NWDAF of a 5G network. If there are problems (e.g., security attacks, traffic congestion, QoS degradation) in the MO network (or EC network), the MO Analyzer (or Edge Analyzer) requests either policy reconfigurations or feedback information to MO Controller (or Edge Controller) to restore security or troubleshoot the network.

4. Interfaces in the I2ICF Framework

Together with the I2ICF framework, interfaces are also defined between pairs of system components in the central cloud and MO (or EC), respectively. These interfaces are shown in Figure 3 and Figure 4 and include the following:

* Consumer-Facing Interface: the interface between I2ICF User Internet and the Cloud Controller. This interface is used for communicating intents.

* Controller-Facing Interface: the interface between the Cloud Controller and the MO Controller (or Edge Controller) for the transmission of high-level policies corresponding to translated intents.

* SF-Facing Interface: the interface between the MO Controller (or Edge Controller) and SF for the transmission of translated lower-level policies.

* Registration Interface: the interface used to transfer information about SF capabilities and access control for the registration of the SF with either the Cloud Controller or MO Controller (or Edge Controller). This interface is also used to deliver SF queries issued for searching for a requested SF. For an MO, this can be the interface between the Cloud Controller and the Cloud Vendor Management System (Cloud VMS), or between MO Controller and MO Vendor Management System (MO VMS). Also, for an EC, this can be the interface between the Cloud Controller and the Cloud Vendor Management System (Cloud VMS), or between Edge Controller and Edge Vendor Management System (Edge VMS).

* Monitoring Interface: the interface between the SF and the MO Analyzer (or Edge Analyzer) used to collect the SF monitoring data and is employed to identify security, system, and network issues related to the SF.

* Analytics Interface: the interface for the transmission of policy reconfigurations or feedback produced as a result of analyzing the SF monitoring data. For an MO, this is an interface between the MO Analyzer and MO Controller, or between the Cloud Analyzer and Cloud Controller. Also, for an EC, this is an interface between the Edge Analyzer and the Edge Controller, or between the Cloud Analyzer and the Cloud Controller.

* Analyzer-Facing Interface: the interface between the MO Analyzer (or Edge Analyzer) and the Cloud Analyzer for the exchange of security, network, and system-related analysis of SFs.

* VMS-Facing Interface: the interface between the Cloud VMS and the MO VMS (or Edge VMS) used to exchange SF feature information, such as SF container images.

* Database Interface: the interface for exchanging data of an I2ICF Database. This is an interface between the I2INC Database and the Cloud Controller, or between the I2ICF Database and the Cloud Analyzer.

The intents, high-level policies, and low-level policies can be either XML documents [RFC6020][RFC7950] or YAML documents [YAML]. They can be delivered to the destination components using NETCONF [RFC6241], RESTCONF [RFC8040], or REST API [REST].

As shown in Figure 3 and Figure 4, the I2ICF Framework receives an intent from the I2ICF User, entered by a user (who can be an administrator) into a target system such as an MO (e.g., SDV) or an Edge Cloud. The intent from the I2ICF User can be translated into the corresponding high-level policy by an intent translator [I-D.gu-nmrg-intent-translator] in the Cloud Controller of the Central Cloud. The high-level policy can also be translated into the corresponding low-level policy by a policy translator in the MO Controller of the MO or the Edge Controller of the Edge Cloud [I-D.jeong-nmrg-security-management-automation][SPT]. For the MO, as shown in Figure 3, the low-level policy is dispatched from the MO Controller to the appropriate Service Functions (SFs) in the MO, examples of which include a Router or a Firewall. Also, in the context of the EC, as shown in Figure 4, the low-level policy is dispatched from the Edge Controller to appropriate Service Functions (SFs) in the EC, such as VNF-Consensus, NFV-Failure-Detector, and NFV-RBCast. Through the monitoring of the SFs, the activity and performance of the SFs in the MO (or EC) is monitored and analyzed by the MO Analyzer (or Edge Analyzer) in the MO (or EC). If needed, the rules of the high-level or low-level network policy can be augmented by the MO Analyzer (or Edge Analyzer). Also, new rules can be automatically generated and configured to appropriate SFs by the MO Analyzer (or Edge Analyzer).

In conclusion, this document proposed an I2ICF framework as an IBS for both MOs and ECs. Through this IBS, the SFs (i.e., NFs and AFs) in the MOs and ECs can be configured and managed. Based on the proposed framework, both virtualized NFs and AFs can be efficiently orchestrated, also allowing agile resource reconfigurations and flexible updates.

5. IANA Considerations

This document does not require any IANA actions.

6. Security Considerations

The same security considerations for the Interface to Network Security Functions (I2NSF) Framework [RFC8329] are applicable to the Intent-Based System this document.

7. References

7.1. Normative References

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <https://www.rfc-editor.org/info/rfc7149>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[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>.

[RFC9315] Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", RFC 9315, DOI 10.17487/RFC9315, October 2022, <https://www.rfc-editor.org/info/rfc9315>.

[RFC9365] Jeong, J., Ed., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", RFC 9365, DOI 10.17487/RFC9365, March 2023, <https://www.rfc-editor.org/info/rfc9365>.

7.2. Informative References

[I-D.ietf-i2nsf-applicability]
Jeong, J. P., Hyun, S., Ahn, T., Hares, S., and D. Lopez, "Applicability of Interfaces to Network Security Functions to Network-Based Security Services", Work in Progress, Internet-Draft, draft-ietf-i2nsf-applicability-19, 3 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-applicability-19>.

[I-D.irtf-coinrg-coin-terminology]
Hong, J., Kunze, I., Wehrle, K., Trossen, D., Montpetit, M., de Foy, X., Griffin, D., and M. Rio, "Terminology for Computing in the Network", Work in Progress, Internet-Draft, draft-irtf-coinrg-coin-terminology-01, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-coin-terminology-01>.

[I-D.irtf-coinrg-use-cases]
Kunze, I., Wehrle, K., Trossen, D., Montpetit, M., de Foy, X., Griffin, D., and M. Rio, "Use Cases for In-Network Computing", Work in Progress, Internet-Draft, draft-irtf-coinrg-use-cases-07, 4 December 2024, <https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-use-cases-07>.

[I-D.ietf-i2nsf-capability-data-model]
Hares, S., Jeong, J. P., Kim, J. T., Moskowitz, R., and Q. Lin, "I2NSF Capability YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-capability-data-model-32, 23 May 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-capability-data-model-32>.

[I-D.ietf-i2nsf-registration-interface-dm]
Hyun, S., Jeong, J. P., Roh, T., Wi, S., and J. Jung-Soo, "I2NSF Registration Interface YANG Data Model for NSF Capability Registration", Work in Progress, Internet-Draft, draft-ietf-i2nsf-registration-interface-dm-26, 10 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-registration-interface-dm-26>.

[I-D.ietf-i2nsf-consumer-facing-interface-dm]
Jeong, J. P., Chung, C., Ahn, T., Kumar, R., and S. Hares, "I2NSF Consumer-Facing Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-consumer-facing-interface-dm-31, 15 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-consumer-facing-interface-dm-31>.

[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-i2nsf-nsf-monitoring-data-model]
Jeong, J. P., Lingga, P., Hares, S., Xia, L., and H. Birkholz, "I2NSF NSF Monitoring Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-nsf-monitoring-data-model-20, 1 June 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-nsf-monitoring-data-model-20>.

[I-D.lingga-nmrg-analytics-interface-dm]
Lingga, P., Jeong, J. P., and Y. Choi, "A YANG Data Model for Interface to Network Security Functions (I2NSF) Analytics Interface", Work in Progress, Internet-Draft, draft-lingga-nmrg-analytics-interface-dm-00, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-lingga-nmrg-analytics-interface-dm-00>.

[I-D.gu-nmrg-intent-translator]
Gu, M., Jeong, J. P., and Y. Ahn, "An Intent Translation Framework for IoT Networks", Work in Progress, Internet-Draft, draft-gu-nmrg-intent-translator-01, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-gu-nmrg-intent-translator-01>.

[I-D.jeong-nmrg-security-management-automation]
Jeong, J. P., Lingga, P., Park, J., Lopez, D. R., and S. Hares, "An I2NSF Framework for Security Management Automation in Cloud-Based Security Systems", Work in Progress, Internet-Draft, draft-jeong-nmrg-security-management-automation-00, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-jeong-nmrg-security-management-automation-00>.

[I-D.jeong-nmrg-ibn-network-management-automation]
Jeong, J. P., Ahn, Y., Gu, M., Kim, Y., and J. Jung-Soo, "Intent-Based Network Management Automation in 5G Networks", Work in Progress, Internet-Draft, draft-jeong-nmrg-ibn-network-management-automation-06, 9 June 2025, <https://datatracker.ietf.org/doc/html/draft-jeong-nmrg-ibn-network-management-automation-06>.

[SPT] Lingga, P., Jeong, J., Yang, J., and J. Kim, "SPT: Security Policy Translator for Network Security Functions in Cloud-Based Security Services", IEEE Transactions on Dependable and Secure Computing, Volume 21, Issue 6, DOI https://doi.org/10.1109/TDSC.2024.3371788, November 2024, <https://doi.org/https://doi.org/10.1109/TDSC.2024.3371788>.

[YAML] Ingerson, B., Evans, C., and O. Ben-Kiki, "Yet Another Markup Language (YAML) 1.0", Available: https://yaml.org/spec/history/2001-05-26.html, October 2023.

[TS-23.501] "System Architecture for the 5G System (5GS)", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144, September 2023.

[TS-28.312] "Intent Driven Management Services for Mobile Networks", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554, September 2023.

[TR-28.812] "Study on Scenarios for Intent Driven Management Services for Mobile Networks", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3553, December 2020.

[TS-23.288] "Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579, September 2023.

[TS-29.520] "Network Data Analytics Services", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3355, September 2023.

[ETSI-NFV] "Network Functions Virtualisation (NFV); Architectural Framework", Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf, December 2014.

[ETSI-NFV-Release-2] "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Architectural Framework Specification", Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/006/02.01.01_60/gs_nfv006v020101p.pdf, January 2021.

[NFV-COIN] Venancio, G., Turchetti, R., and E. Duarte Jr., "NFV-COIN: Unleashing The Power of In-Network Computing with Virtualization Technologies", SBC Journal of Internet Services and Applications, Available: https://journals-sol.sbc.org.br/index.php/jisa/article/view/2342, December 2022.

[REST] Fielding, R. and R. Taylor, "Principled Design of the Modern Web Architecture", ACM Transactions on Internet Technology, Vol. 2, Issue 2,, Available: https://dl.acm.org/doi/10.1145/514183.514185, May 2002.

[Flan-T5] Chung, H., "Scaling Instruction-Finetuned Language Models", arXiv arXiv:2210.11416, Available: https://arxiv.org/abs/2210.11416, October 2022.

[GPT-3] Brown, T., "Language Models are Few-Shot Learners", arXiv arXiv:2005.14165, Available: https://arxiv.org/abs/2005.14165, May 2020.

[USENIX-ATC-Lumi] Jacobs, A., Pfitscher, R., Ribeiro, R., Ferreira, R., Granville, L., Willinger, W., and S. Rao, "Hey, Lumi! Using Natural Language for Intent-Based Network Management", USENIX Annual Technical Conference, Available: https://www.usenix.org/conference/atc21/presentation/jacobs, July 2021.

[BERT] Devlin, J., Chang, M., Lee, K., and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding", NAACL-HLT Conference, Available: https://aclanthology.org/N19-1423.pdf, June 2019.

[Deep-Learning] Goodfellow, I., Bengio, Y., and A. Courville, "Deep Learning", Publisher: The MIT Press, Available: https://www.deeplearningbook.org/, November 2016.

[AUTOSAR-SDV] "AUTOSAR Adaptive Platform", Available: https://www.autosar.org/standards/adaptive-platform, March 2024.

[Eclipse-SDV] "Eclipse Software Defined Vehicle Working Group Charter", Available: https://www.eclipse.org/org/workinggroups/sdv-charter.php, March 2024.

[COVESA] "Connected Vehicle Systems Alliance", Available: https://covesa.global/, March 2024.

[Kubernetes] "Kubernetes: Cloud Native Computing Platform", Available: https://kubernetes.io/, March 2024.

[Survey-IBN-CST-2023] Leivadeas, A. and M. Falkner, "A Survey on Intent-Based Networking", Available: https://ieeexplore.ieee.org/document/9925251, March 2023.

[ClickINC-Sigcomm-2023] Xu, W., Zhang, Z., Feng, Y., Song, H., Chen, Z., Wu, W., Liu, G., Zhang, Y., Liu, S., Tian, Z., and B. Liu, "ClickINC: In-network Computing as a Service in Heterogeneous Programmable Data-center Networks", Publisher: ACM SIGCOMM, Available: https://dl.acm.org/doi/10.1145/3603269.3604835, September 2023.

Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. RS-2024-00398199 and RS-2022-II221015).

Contributors

This document is made by the group effort of OPWAWG, greatly benefiting from inputs and texts by Linda Dunbar (Futurewei), Yong-Geun Hong (Daejeon University), and Joo-Sang Youn (Dong-Eui University). The authors sincerely appreciate their contributions.

The following are coauthors of this document:

Mose Gu
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: rna0415@skku.edu
URI: http://iotlab.skku.edu/people-Moses-Gu.php

Juwon Hong
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: hongju2024@skku.edu
URI: http://iotlab.skku.edu/people-Joo-Won-Hong.php

Jiwon Suh
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: sjw6136@skku.edu
URI: http://iotlab.skku.edu/people-Jiwon-Suh.php

Jisuk Chae
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: sue030124
URI: http://iotlab.skku.edu/people-Jisuk-Chae.php

Giovanni Venancio
Department of Informatics
Federal University of Parana
Brazil
Email: giovanni@inf.ufpr.br

Authors' Addresses

Jaehoon Paul Jeong (editor)
Department of Computer Science & 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

Yiwen Shen
Department of Software
Ajou University
206 Worldcup-Ro, Yeongtong-Gu
Suwon
Gyeonggi-Do
16499
Republic of Korea
Email: chrisshen@ajou.ac.kr
URI: https://chrisshen.github.io

Yoseop Ahn
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: ahnjs124@skku.edu
URI: http://iotlab.skku.edu/people-Ahn-Yoseop.php

Younghan Kim
School of Electronic Engineering
Soongsil University
369, Sangdo-ro, Dongjak-gu
Seoul
06978
Republic of Korea
Email: younghak@ssu.ac.kr

Elias P. Duarte Jr.
Department of Informatics
Federal University of Parana
Brazil
Email: elias@inf.ufpr.br

Kehan Yao
China Mobile
Beijing
100053
China
Email: yaokehan@chinamobile.com