Recent Standardization and Other Activities in Ubiquitous Open Platform Forum

Takamasa Uchiyama, Yuka Kamizuru, Shin Miyakawa†, and Hiroyuki Ichikawa

Abstract

This article describes standardization activities related to technical specifications in the Ubiquitous Open Platform Forum (UOPF), past progress, and the future outlook. UOPF has established outcomes, such as technical specifications and reference guides, and it released all of them to the public in April 2007. Trials and experimental proofs have been done using these established specifications.

1. UOPF

The Ubiquitous Open Platform Forum (UOPF) [1] is a technical forum established by fourteen electric appliance manufacturers and Internet service providers (ISPs) in February 2004. The members have worked to promote Internet-accessible home electric/electronic appliances, as well as to widen the broadband market by standardizing network specifications. The purpose of UOPF is to establish an open common platform that will facilitate easy setup of electronic devices, safe online billing, and realtime data communications among home electronic devices. The UOPF member companies will also work closely with application and content providers in order to create common frameworks. UOPF has four Working Groups (WGs). Their directives are shown in **Fig. 1**.

2. Standardization in UOPF

The progress of standardization of technical specifications in UOPF is given in **Table 1**. UOPF released established outcomes in April 2007; these are listed in **Table 2**. The standardization policy is based on open specifications made by other standardization bodies such as the Internet Engineering Task Force (IETF), Digital Living Network Alliance (DLNA), and Public Key Cryptography Standards (PKCS). The main open specifications used in UOPF are:

- SIP (session initiation protocol, IETF)
- IPsec (security architecture for the Internet protocol, IETF)
- TLS (transport layer security, IETF).

After the initial release of standards, new goals were established at the last UOPF general meeting (April 19, 2007), as listed below.

- Distribution of the outcomes established by UOPF to companies so that they can promote the outcomes in the business phase.
- Release of the outcomes so that everyone can use them to work on the Ubiquitous Open Platform.
- Establishment of a new organization to support the above activities.

3. Usage trends of UOPF specifications

One example of a technical test using UOPF specifications is the “Universal Plug and Play (UPnP) interconnectivity test”, which was a theme of the “next generation home network demonstration test” [3] of the Ministry of Internal Affairs and Communications in March 2008. In that test, we evaluated the behavior of a variety of SOHO (small office home office) routers as UPnP Internet gateway devices

† Innovative IP Architecture Center, NTT Communications
Minato-ku, 108-8118 Japan

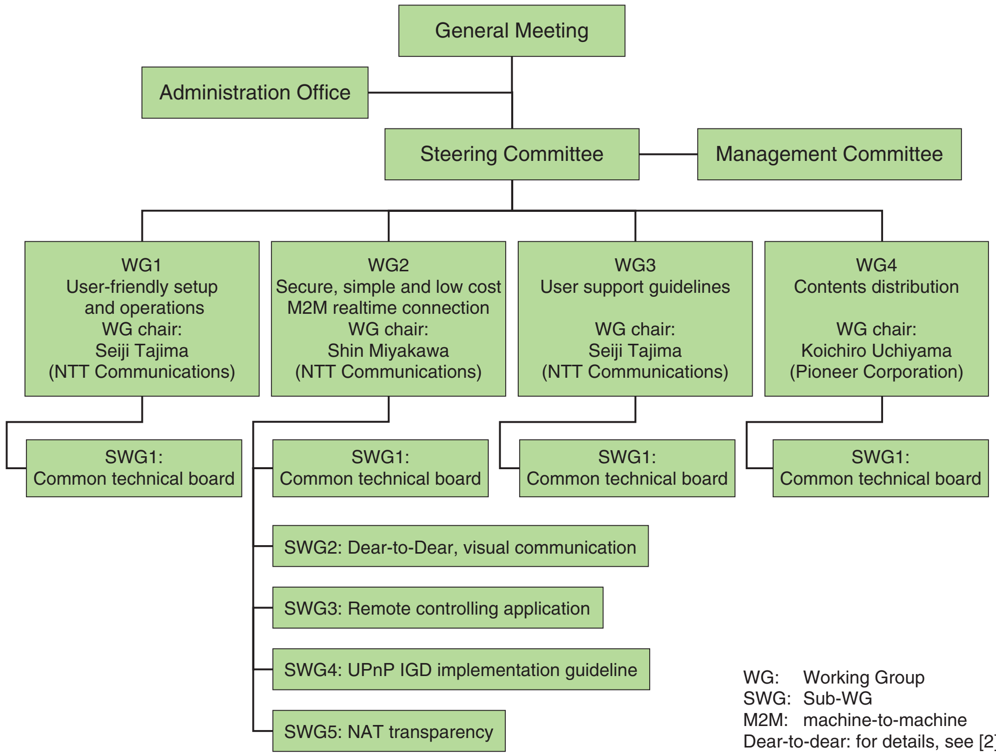

Fig. 1. Organization of UOPF.

Table 1. Standardization progress in UOPF.

February 2004	UOPF was established.
March 2004	WGs 1–3 were set up.
September 2004	WG4 was set up.
May 2005	Interconnect testing of visual communication
December 2006	Submission of all established technical specifications and other outcomes
March 2007	Interconnect testing of UPnP-IGD
April 2007	Release of established technical specifications and other outcomes (UOPF1-33)

(UPnP-IGDs), using UOPF18-compliance testing tools. Meanwhile, NTT Communications is providing a free connectivity trial of a UOPF5rev.1-compliant server on the Internet [4]. The purpose of the trial is to promote the development of new applications and services. It is particularly aimed at m2m-x (machine-to-machine for anything) communication [5].

4. Standardization policy of UOPF WG2

This section explains the established policies of UOPF WG2. Its standardization policies focus on security, simplicity, and low cost.

People using home appliances are usually not familiar with the latest network technology, so security and simplicity are important policies for UOPF WG2 discussions. Established specifications suggest the enhancement of security and simplicity by providing functions for authentication, encryption, easy setup, etc, which are provided from the UOPF WG2 compliance server.

Because the client/server (C/S) communication model is more expensive because it requires servers to be set up, UOPF WG2 used a peer-to-peer (P2P) communication model that makes media connections between two devices without a relay server. This resulted in a large reduction in relay server cost.

Table 2. Lists of established outcomes.

No.	WG in charge	Title of deliverables
UOPF 1 (G)	WG3 SWG1	Network Connection Information Display Guidelines
UOPF 2 (G)	WG3 SWG1	Network Connection Information Terms Guidelines
UOPF 3 (G) rev.1	WG2 SWG1	UOPF Guideline for the Establishment of a Work Group for M2M Real-Time Communications (Revised)
UOPF 4 (G)	WG2 SWG1	Specifications Development Guideline for M2M Real-Time Communications
UOPF 5 (S) rev.1	WG2 SWG1	UOPF M2M Real-Time Communications Signaling Specifications (Revised)
UOPF 6 (S) rev.1	WG2 SWG2	Media Channel Specifications for Visual Communications (Revised)
UOPF 7 (S) rev.1	WG2 SWG2	Presence Specifications for Visual Communications (Revised)
Obsolete: UOPF 8 (S)	WG2 SWG2	Policy Control Specifications for Visual Communications
UOPF 9 (S) rev.1	WG2 SWG3	Framework Specifications for Remote Controlling Home Appliances (Revised)
UOPF10 (S) rev.1	WG2 SWG3	Presence Specifications for Remote Controlling Home Appliances (Revised)
UOPF11 (G)	WG1 SWG1	Requirement Specifications for Realizing Easy Setup and Easy Operation Version 1.0
Obsolete: UOPF12 (S)	WG1 SWG1	Specifications for Authentication and Setup Interface Version 1.0
UOPF13 (G) rev.1	WG2 SWG4	IGD Implementation Guidelines (Revised)
Obsolete: UOPF14 (S)	WG1 SWG1	Specifications for Authentication Result Notification Interface
UOPF15 (S)	WG4 SWG1	Contents Distribution System Interface Specifications (Revised) Version 1.20
UOPF16 (G)	WG2 SWG1	IPv6 Firewall Traversal
UOPF17 (S)	WG2 SWG1	Specifications for Authentication and Setup Interface Version 2.0
UOPF18 (G)	WG2 SWG1	UPnP-IGD Implementation Guidelines Conformance Test
UOPF19 (S)	WG2 SWG1, SWG2	Presence Request Specifications for M2M Real-Time communications
UOPF20 (S)	WG2 SWG1, SWG2	UOPF M2M Real-Time Communications Presence Common Specifications
UOPF21 (S)	WG2 SWG1, SWG2	Group Management Specifications Using Presence
UOPF22 (S)	WG2 SWG1, SWG2	UOPF M2M Real-Time Communications Signaling IPv4/IPv6 Dual-stack Extended Specifications
UOPF23 (S)	WG2 SWG1, SWG2	UOPF M2M Real-Time Communications Setting Interface Framework
UOPF24 (S)	WG2 SWG1, SWG2	UOPF M2M Real-Time Communications CC-PS Setting Interface Specifications
UOPF25 (S)	WG2 SWG1, SWG2	UOPF M2M Real-Time Communications CC-CM Setting Interface Specifications
UOPF26 (S)	WG2 SWG1, SWG2	UOPF M2M Real-Time Communications Terminal Setting Framework
UOPF27 (S)	WG2 SWG1, SWG2	Implementation Guidelines for Visual Communication Terminal
UOPF28 (S)	WG3 SWG3	UOPF-Supporting Implementation Guidelines for UPnP Devices
UOPF29 (S)	WG2 SWG5	UOPF M2M Real-Time Communications REGISTER Extended Framework
UOPF30 (S)	WG2 SWG5	UOPF M2M Real-Time Communications Signaling Channel NAT Transparency Specifications
UOPF31 (S)	WG2 SWG5	UOPF M2M Real-Time Communications TCP Media NAT Transparency Specifications
UOPF32 (S)	WG2 SWG5	UOPF M2M Real-Time Communications Relay Specifications for NAT Transparency
UOPF33 (S)	WG2 SWG5	UOPF M2M Real-Time Communications Media NAT Transparency Specifications

(G) Guideline
(S) Specification

5. Basic mechanism in UOPF WG2

This section explains the basic mechanism of UOPF5rev.1 (**Fig. 2**) which was established as a main technical specification of UOPF WG2. In UOPF5rev.1, a general "SIP server" is called the "Communication Manager (CM)", and a "User Agent (UA)" is called the "Communication Client (CC)".

First, the CC on the network registers its identification (ID) on CM in advance, using a SIP REGISTER message, as shown by (a) in Fig. 2. In this registration sequence, an encrypted communication channel is established between the CM and CC using IPsec or TLS. In the CM registration procedure, a registered user is authenticated using a pre-shared key (PSK) or electronic certification.

Second, when starting the actual end-to-end communication, the CC starts the session by designating its ID of the other CC in an INVITE message, as shown by (b). This INVITE message is transmitted to the CM. Through the exchange of these INVITE messages, CCs share various kinds of information such as

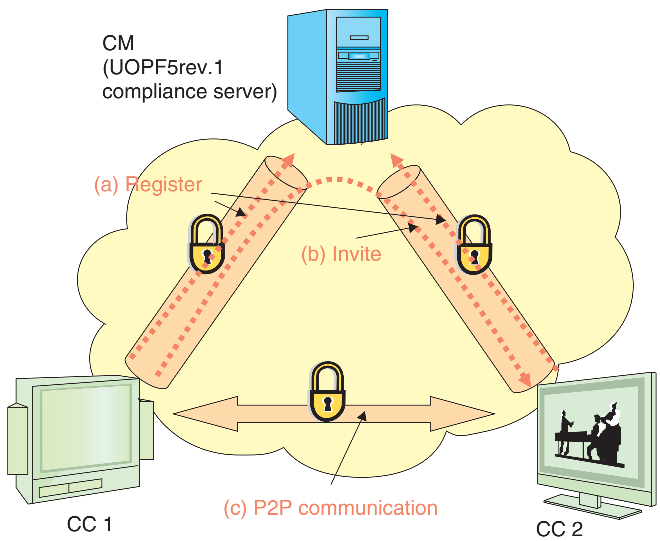

Fig. 2. Basic mechanism of UOPF5rev.1.

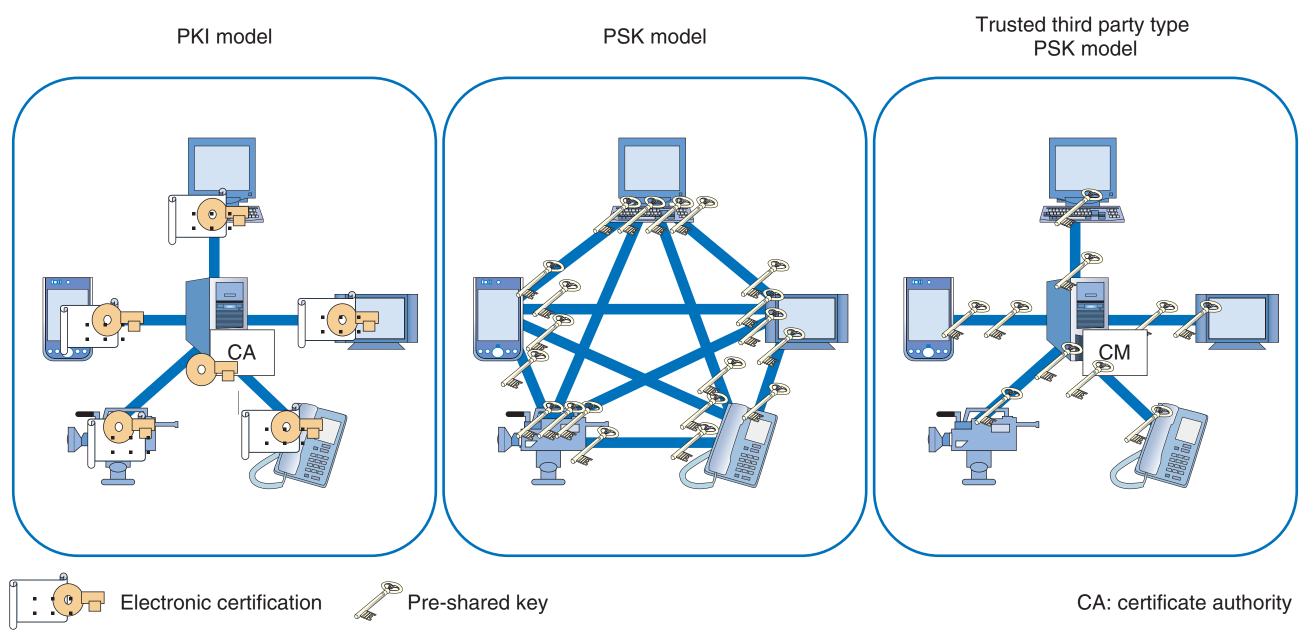

Fig. 3. Comparison of key storing types.

IP addresses, ports, and key data for encryption, and they then reach agreement on the protocol to be used for end-to-end connections. After that, end-to-end direct communication will be available without the CM. This is called P2P communication, as shown by (c).

It is difficult to enhance this mechanism's scalability when the PSK model is used because the model expects CCs to manage many keys that are used to connect the other individual CCs. In the public key infrastructure (PKI), the CC only has to manage one key, so it is easier to obtain scalability than in PSK. However, certification management is complicated for ordinary users, so the ease of use may be lower. Hence, UOPF WG2 recommends the use of a trusted third party (TTP) type PSK model, in which each CC manages only one key for communicating with CM, with the CCs trusting the CM (**Fig. 3**).

6. Future outlook

The technology has been developed through trials and discussions about the specifications among various manufacturers and ISPs, making this technology ready for commercialization. New applications besides those for home electronic appliances have been developed. Some parts of the UOPF outcomes have been proposed to the Broadband Forum and to IETF in order to promote those technologies. From now on, we will try to create a new market by strengthening partnerships and accelerating service development.

References

[1] http://www.uopf.org/en/
[2] Dear-to-dear: https://www.ipv6style.jp/en/netapplnc/20050523/index.shtml
[3] http://www.soumu.go.jp/s-news/2008/pdf/080212_2.pdf (in Japanese).
[4] http://www.m2m-x.net/ (in Japanese).
[5] http://www.v6.ntt.net/data/e_m2m-x_3.html

Takamasa Uchiyama
Research Engineer, Innovative IP Architecture Center, NTT Communication.
He received the B.E. and M.E. degrees in electronics and communication engineering from Waseda University, Tokyo, in 2000 and 2002, respectively. Since joining NTT Communications in 2002, he has been engaged in R&D of SIP and its expansion "m2m-x". He has been a technical member of UOPF since 2004.

Yuka Kamizuru
Manager, Innovative IP Architecture Center, NTT Communications.
She received the B.S. and M.E. degrees in computer science from the University of Electro-Communications, Tokyo, in 1991 and 1993, respectively. After joining NTT in 1993, she researched advanced Internet technologies. Since joining NTT Communications in 1999, she has been engaged in R&D of IPv6 and "m2m-x".

Shin Miyakawa
Director, Core Network Technology Team, Network Systems and Technologies Laboratory, Innovative IP Architecture Center, NTT Communications and, concurrently, member of the Corporate Planning Department.
He received the B.S., M.S., and Ph.D. degrees in computer science from Tokyo Institute of Technology in 1990, 1992, and 1995, respectively. After joining NTT Laboratories in 1995, he researched advanced Internet technologies. In 1997, he moved to NTT Multimedia Communication Laboratories in Silicon Valley, Palo Alto, California, and led NTT's IPv6 technology development and business incubation. He returned to NTT Communications in Tokyo in 2002. He has written several requests for comments (RFCs) related to IPv6 and is now also working on carrier-grade network address translation.

Hiroyuki Ichikawa
Executive Manager, Director of the Network Systems and Technologies Laboratory and the Service Management Systems Laboratory, Innovative IP Architecture Center, NTT Communications.
He received the B.E. and M.E. degrees in instrumentation engineering from Keio University, Kanagawa, in 1980 and 1982, respectively. After joining NTT Laboratories in 1982, he engaged in R&D of distributed packet switching systems, ATM switching systems, IP-VPN systems, and several other advanced Internet technologies. During 1993–1994, he worked as a visiting research scientist at the Center for Telecommunications Research at Columbia University, New York, USA. Since moving to NTT Communications in 2004, he has been leading R&D projects on SIP-VoIP communication service, MPLS-based transport systems, digital TV transport systems, and "m2m-x" overlay network systems.