WT-369: User Services Platform

Version 1.0-DRAFT-03

**Table of Contents**

Main Specification

1. [Introduction](#introduction)
2. [Architecture](./architecture)
3. [Discovery and Advertisement](./discovery)
4. [Message Transfer Protocols](./mtp)
5. [Message Encoding](./encoding)
6. [End to End Message Exchange](./e2e-message-exchange)
7. [Messages](./messages)
8. [Security](./security)

Extensions

Annex A. [HTTP Bulk Data Transfer](./extensions/http-bulk-data-collection) Annex B. [Software Module Management](./extensions/software-module-management)

# Introduction

## Legal Notice

### Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Working Text is a draft, is subject to change, and has not been approved by members of the Forum. This Working Text is copyrighted by the Broadband Forum, and portions of this Working Text may be copyrighted by Broadband Forum members. This Working Text is for use by Broadband Forum members only. Advance written permission by the Broadband Forum is required for distribution of this Working Text in its entirety or in portions outside the Broadband Forum.

### Intellectual Property

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Working Text if it were to be adopted as a Technical Report, and to provide supporting documentation.

### Terms of Use

This Working Text (i) is made available to non-members for internal study purposes only, (ii) may be implemented by Broadband Forum members in a product or service made commercially available, and (iii) may only be copied and distributed internally for the purpose of exercising Broadband Forum membership rights and benefits.

### Confidentiality

All materials submitted for possible incorporation into Technical Reports or other work product shall be regarded as confidential until such time as the Technical Report or other work product in question is publicly released. In the event that any material, or portion of any material, is not included in the Technical Report or other work product in question, or if such Technical Report or other work product is never publicly released, such material shall remain confidential until such time, if ever, as the submitter makes the same publicly available, or it otherwise becomes publicly disclosed other than by a breach of a Member’s obligations under this Confidentiality Policy. Member representatives shall have access to confidential materials in such manner as may from time to time be provided in Broadband Forum’s procedural rules, and shall not copy or further distribute such materials, except internally, to the extent necessary to exercise their participation rights as Members.

THIS WORKING TEXT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS WORKING TEXT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS WORKING TEXT.

## Revision History

### Version 1.0-DRAFT-03

* Single document format

### Version 1.0-DRAFT-02

* Editorial updates
* Added requirement for OnBoardRequest retry mechanism

### Version 1.0-DRAFT-01

* Initial public draft

## Acknowledgements

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Company | Email | Role |
| Barbara Stark | AT&T | barbara.stark@att.com | Editor/USP Project Lead |
| Tim Spets | Green Wave Systems | tim.spets@greenwavesystems.com | Editor/USP Project Lead |
| Jason Walls | QA Cafe, LLC | jason@qacafe.com | Editor/Broadband User Services Work Area Director |
| John Blackford | Arris | john.blackford@arris.com | Editor/Broadband User Services Work Area Director |
| William Lupton | Broadband Forum | wlupton@broadband-forum.org | BBF Software Architect |
| Timothy Carey | Nokia | timothy.carey@nokia.com | Contributor |
| Steven Nicolai | Arris | Steven.Nicolai@arris.com | Contributor |
| Apostolos Papageorgiou | NEC | apostolos.Papageorgiou@neclab.eu | Contributor |
| Mark Tabry | Google | mtab@google.com | Contributor |
| Klaus Wich | Huawei | klaus.wich@huawei.com | Contributor |

## Executive Summary

This document describes the architecture, protocol, and data model that builds an intelligent User Services Platform. It is targeted towards application developers, application service providers, CPE vendors, consumer electronics manufacturers, and broadband and mobile network providers who want to expand the value of the end user’s network connection and their connected devices.

The term "connected device" is a broad one, applying to the vast array of network connected CPE, consumer electronics, and computing resources that today’s consumers are using at an increasing rate. With the advent of "smart" platforms (phones, tablets, and wearables) plus the emerging Internet of Things, the number of connected devices the average user or household contains is growing by several orders of magnitude.

In addition, users of the fixed and mobile broadband network are hungry for advanced broadband and intelligent cloud services. As this desire increases, users are turning towards over-the-top providers to consume the entertainment, productivity, and storage applications they want.

These realities have created an opportunity for CE vendors, application developers, and broadband and mobile network providers. These connected devices and services need to be managed, monitored, troubleshot, and controlled in an easy to develop and interoperable way. A unified framework for these is attractive if we want to enable providers, developers, and vendors to create value for the end user. The goal should be to create system for developing, deploying, and supporting these services for end users on the platform created by their connectivity and components, that is, to be able to treat the connected user herself as a platform for applications.

This is not the first time this problem has surfaced, however. When the Broadband Forum created the CPE WAN Management Protocol - commonly known by its document number, "TR-069" - this same need existed, focused on managing and deploying the end user’s gateway and other home networking equipment, adding value for the end user and reducing costs for providers. With the advent of CWMP, this created a new market for CPE management. As the protocol matured, it added the ability to extend the capabilities of user’s CPE through software modules, and the ability to manage and monitor any device in the home by its proxy mechanism. Coupled with robust and standardized data model covering a wide variety of domains, this flagship of the Broadband Forum has of the writing of this document reached over 350 million devices world-wide.

This new world of the connected user as a platform provides the perfect opportunity to leverage the expertise and experience gained with CWMP. This allows us to improve on, evolve, and expand the use cases of CWMP including:

* App-store capabilities enabling the connected user to select, purchase, and install applications that utilize their connectivity and devices, and learn of new services that can be made available with suggested hardware.
* The ability to quickly and easily activate and provision smart home, voice and video, security, gaming, and energy services.
* Allowing the user to interact with their devices and services using customer portals or control points on their own smart devices.
* Service provider delivered assured broadband services with dedicated bandwidth or QoS.
* The ability to have both the application and network service provider manage, troubleshoot, and control different aspects of the services they are responsible for, and enabling provider partnerships.
* Providing a consistent user experience from mobile to home.

This User Services Platform provides a scalable, interoperable, and efficient mechanism to meet the needs of the connected user and their application and network providers.

## Purpose and Scope

### Purpose

This document provides the normative requirements and operational description of the User Services Platform (USP). It is meant to be consumed by remote gateway, home network, and consumer electronics vendors; cloud and smart application developers and providers; and network service providers to help build and deploy USP Agents, Controllers, and the applications and devices which make use of them.

This document describes:

* The overall architecture of USP Agents, Controllers, and Service Elements
* The proxy mechanisms for addressing non-USP Service Elements
* Requirements for the transport protocol(s) used to handle USP messages, and defined bindings for specific protocols
* The various USP messages, their requirements, and expected behavior patterns, along with on-the-wire encoding of USP messages
* The protocol requirements for discovery, end-to-end security, authentication, and authorization
* An explanation of the data model and how it is used to enable USP, Service Elements, proxying, and Object defined operations

### Scope

While the original CWMP was targeted toward remote gateways, it expanded to manage software modules, VoIP devices, set top boxes, network attached storage, etc. In the new connected world enabled by the virtualization of network functions and the "Internet of things", USP has an opportunity to apply to "virtual agents" as well as push out to more device types.

USP is designed for consumer electronics/IoT, home network/gateways, smart Wifi systems, and virtual services (though could theoretically be used for any connected device in many different verticals). It is targeted towards developers, application providers, and network service providers looking to deploy those products.

For the proxy of Service Elements, this document defines the proxy mechanisms but refrains from detailing the specific procedures for proxy of a particular third-party protocol or technology.

Lastly, USP makes use of and expands the Device:2 Data Model for TR-069 Devices [1](https://github.com/BroadbandForum/usp/tree/master/data-model). While particular Objects and parameters necessary to the function of USP are mentioned here, their normative description can be found in that XML document.

## References and Terminology

### Conventions

In this specification, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in [RFC 2119](https://www.ietf.org/rfc/rfc2119.txt).

**MUST**

This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification.

**MUST NOT**

This phrase means that the definition is an absolute prohibition of the specification.

**SHOULD**

This word, or the term "RECOMMENDED", means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.

**SHOULD NOT**

This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.

**MAY**

This word, or the term "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

### References

The following references are of relevance to this Working Text. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Working Text are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at [www.broadband-forum.org](https://www.broadband-forum.org).

1. [Broadband Forum TR-181 Issue 2: *Device Data Model for TR-069 Endpoints and USP Agents*](https://github.com/BroadbandForum/usp/tree/master/data-model)
2. [Broadband Forum TR-069 Amendment 6: *CPE WAN Management Protocol*](https://www.broadband-forum.org/technical/download/TR-069.pdf)
3. [Broadband Forum TR-106 Amendment 8: *Data Model Template for TR-069 Enabled Devices*](https://www.broadband-forum.org/technical/download/TR-106_Amendment-8.pdf)
4. [IETF RFC 7228: *Terminology for Constrained-Node Networks*](https://tools.ietf.org/html/rfc7228)
5. [IETF RFC 2136: *Dynamic Updates in the Domain Name System*](https://tools.ietf.org/html/rfc2136)
6. [IETF RFC 3007: *Secure Domain Name System Dynamic Update*](https://tools.ietf.org/html/rfc3007)
7. [IETF RFC 6763: *DNS-Based Service Discovery*](https://tools.ietf.org/html/rfc6763)
8. [IETF RFC 6762: *Multicast DNS*](https://tools.ietf.org/html/rfc6762)
9. [IETF RFC 7252: *The Constrained Application Protocol (CoAP)*](https://tools.ietf.org/html/rfc7252)
10. [IETF RFC 7390: *Group Communication for the Constrained Application Protocol (CoAP)*](https://tools.ietf.org/html/rfc7390)
11. [IETF RFC 4033: *DNS Security Introduction and Requirements*](https://tools.ietf.org/html/rfc4033)
12. [*Protocol Buffers v3 Protocol Buffers Mechanism for Serializing Structured Data Version 3*](https://developers.google.com/protocol-buffers/docs/proto3)
13. [IEEE Registration Authority](https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries)
14. [IETF RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace](https://tools.ietf.org/html/rfc4122)
15. [IETF RFC 5290: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*](https://tools.ietf.org/html/rfc5280)
16. [IETF RFC 6818: *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*](https://tools.ietf.org/html/rfc6818)
17. [IETF RFC 2234 Augmented BNF for Syntax Specifications: ABNF](https://www.ietf.org/rfc/rfc2234.txt)
18. [IETF RFC 3986 Uniform Resource Identifier (URI): Generic Syntax](https://www.ietf.org/rfc/rfc3986.txt)
19. [IETF RFC 2141 URN Syntax](https://www.ietf.org/rfc/rfc2141.txt)

# Definitions

The following terminology is used throughout this specification.

**Agent**

An Agent is an Endpoint that exposes Service Elements to one or more Controllers.

**Binding**

A Binding is a means of sending Messages across an underlying Message Transfer Protocol.

**Command**

The term used to define and refer to an Object-specific Operation in the Agent’s Instantiated or Supported Data Model.

**Connection Capabilities**

Connection Capabilities are information related to an Endpoint that describe how to communicate with that Endpoint, and provide a very basic idea of what sort of function the Endpoint serves.

**User Services Platform**

The User Services Platform consists of a data model, architecture, and communications protocol to transform consumer broadband networks into a platform for the development, deployment, and support of broadband enabled applications and services.

**Controller**

A Controller is an Endpoint that manipulates Service Elements through one or more Agents.

**Device Type (DT) Definition**

A Device Type Definition (DT) is a description of the Service Elements an Agent is able to support, defining its Supported Data Model.

**Discovery**

Discovery is the process by which Controllers become aware of Agents and Agents become aware of Controllers.

**Endpoint**

An Endpoint is a termination point for a Message.

**Endpoint Identifier**

The Endpoint Identifier is a globally unique USP layer identifier of an Endpoint.

**Error**

An Error is a Message that contains failure information associated with a Request.

**Event**

An Event is a set of conditions that, when met, triggers the sending of a Notification.

**Expression**

See also Search Expression

**Expression Component**

An Expression Component is the part of a Search Expression that gives the matching Parameter criteria for the search. It is comprised of an Expression Parameter followed by an Expression Operator followed by an Expression Constant.

**Expression Constant**

The Expression Constant is the value used to compare against the Expression Component to determine if a search matches a given Object.

**Expression Operator**

The Expression Operator is the operator used to determine how the Expression Component will be evaluated against the Expression Constant, i.e., equals (==), not equals (!=), less than (<), greater than (>), less than or equal (<=), and greater than or equal (>=).

**Expression Parameter**

The Expression Parameter is a Parameter relative to the path where an Expression Variable occurs that will be used with the Expression Constant to evaluate the Expression Component.

**Expression Variable**

The Expression Variable is an identifier used to allow relative addressing when building an Expression Component.

**Supported Data Model**

The Supported Data Model of an Agent represents the complete set of Service Elements it is capable of exposing to a Controller. It is defined by the union of all of the Device Type Definitions the Agent exposes to the Controller.

**Instantiated Data Model**

The Instantiated Data Model of an Agent represents the current set of Service Elements (and their state) that are exposed to one or more Controllers.

**Instance Identifier**

A term used to identify to an Instance of a Multi-Instance Object (also called a Row of a Table). While all Multi-Instance Objects have an Instance Number that can be used as an Instance Identifier, an Object Instance can also be referenced using that Object’s Unique Key.

**Instance Number**

An Instance Number is a numeric Instance Identifier assigned by the Agent to instances of Multi-Instance Objects in an Agent’s Instantiated Data Model.

**Instance Path**

An Instance Path is a Path Name that addresses an Instance of a Multi-Instance Object (also called a Row of a Table). It includes the Object Path followed by an Instance Identifier.

**Message**

A Message refers to the contents of a USP layer communication including exactly one Message Header and at most one Message Body.

**Message Body**

The Message Body is the portion of a Message that contains one of the following: Request, Response, or Error.

**Message Header**

The portion of a Message that contains elements that provide information about the message, including the Endpoint Identifier of the sender and receiver, message type, and Message ID elements.

**Message ID**

A Message ID is an identifier used to associate a Response or Error with a Request.

**Message Transfer Protocol**

A Message Transfer Protocol (MTP) is the protocol at a layer below USP that carries a Message, i.e., CoAP.

**Multi-Instance Object**

A Multi-Instance Object refers to an Object that can be created or deleted in the Agent’s Instantiated Data Model. Also called a Table.

**Notification**

A Notification is a Request from an Agent that conveys information about an Event to a Controller that has a Subscription to that event.

**Object**

An Object refers to a defined type that an Agent represents and exposes. A Service Element may be comprised of one or more Objects and Sub-Objects.

**Object Instance**

An Object Instance refers to a single instance Object of a type defined by a Multi-Instance Object in the Agent’s Instantiated Data Model. Also called a Row of a Table.

**Object Path**

An Object Path is a Path Name that addresses an Object. In the case of Multi-Instance Objects, an Object Path addresses the Object type itself rather than instances of that Object, which are addressed by Instance Paths

**Operation**

A method defined for a particular Service Element that can be invoked with the Operate message.

**Parameter**

A Parameter is a variable or attribute of an Object. Parameters have both type and value.

**Parameter Path**

A Parameter Path is a Path Name that addresses a Parameter of an Object or Object Instance.

**Path Name**

A Path Name is a fully qualified reference to an Object, Object Instance, or Parameter in an Agent’s instantiated or Supported Data Model.

**Path Reference**

A Path Reference is a Parameter data type that contains a Path Name to an Object or Parameter that may be automatically followed by using certain Path Name syntax.

**Relative Path**

A Relative Path is the remaining path information necessary to form a Path Name given a parent Object Path. It is used for message efficiency when addressing Path Names.

**Request**

A Request is a type of Message that either requests the Agent perform some action (create, update, delete, operate, etc.), requests information about an Agent or one or more Service Elements, or acts as a means to deliver Notifications from the Agent to the Controller. A Request usually requires a Response.

**Response**

A Response is a type of Message that provides return information about the successful processing of a Request.

**Row**

The term Row refers to an Instance of a Multi-Instance Object in the Agent’s Instantiated Data Model.

**Search Expression**

A Search Expression is used in a Search Path to apply specified search criteria to address a set of Multi-Instance Objects and/or their Parameters.

**Search Path**

A Search Path is a Path Name that contains search criteria for addressing a set of Multi-Instance Objects and/or their Parameters. A Search Path may contain a Search Expression or Wildcard.

**Service Element**

A Service Element represents a piece of service functionality that is exposed by an Agent, usually represented by one or more Objects.

**Source Endpoint**

An Endpoint that was the sender of a message. **Subscription**

A Subscription is a set of logic that tells an Agent which Notifications to send to a particular Controller.

**Table**

The term Table refers to a Multi-Instance Object in an Agent’s Instantiated or Supported Data Model.

**Target Endpoint**

An Endpoint that was the intended receiver of a message.

**Unique Key**

The Unique Key of a Multi-Instance Object is a set of Parameters that uniquely identify the instance of an Object in the Agent’s Instantiated Data Model and can be used as an Instance Identifier.

**USP Record Message**

The USP Record message is defined as the transport layer payload, encapsulating a sequence of datagrams that comprise the USP Message as well as providing additional metadata needed for secure and reliable delivery of fragmented USP Messages.

**Wildcard**

A Wildcard is used in a Search Path to address all Object Instances of a Multi-Instance Object.

## Abbreviations

This specification uses the following abbreviations:

|  |  |
| --- | --- |
| abbreviation | term |
| ABNF | Augmented Backus-Naur Form |
| CoAP | Constrained Application Protocol |
| USP | User Services Platform |
| CWMP | CPE WAN Management Protocol |
| DNS | Domain Name Service |
| DNS-SD | Domain Name Service - Service Definition |
| DT | Device Type Definition |
| E2E | End to End (Message Exchange) |
| HMAC | Hash Message Authentication Code |
| HTTP | Hypertext Transport Protocol |
| mDNS | Multicast Domain Name Service |
| IPv4/v6 | Internet Protocol (version 4 or version 6) |
| LAN | Local Area Network |
| MAC | Message Authentication Code |
| MTP | Message Transfer Protocol |
| OUI | Organizationally Unique Identifier |
| PSS | Probabilistic Signature Scheme |
| SAR | Segmentation And Reassembly |
| SMM | Software Module Management |
| TLS | Tranport Layer Security |
| TR | Technical Report |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UUID | Universally Unique Identifier |
| WAN | Wide Area Network |

# Specification Impact

## Energy efficiency

The User Services Platform reaches into more and newer connected devices, and expands on the management of physical hardware, including power management. In addition, USP directly enables smart home, smart building, and other smart energy applications.

## Security

Any solution that provides a mechanism to manage, monitor, diagnose, and control a connected user’s network, devices, and applications must prioritize security to protect user data and prevent malicious use of the system. This is especially important with certain high-risk smart applications like medicine or emergency services.

However reliable the security of communications protocols, in a platform that enables interoperable components that may or may not be connected with protocols outside the scope of the specification, security must be considered from end-to-end. To realize this, USP contains its own security mechanisms.

## Privacy

**Privacy** is the right of an individual or group to control or influence what information related to them may be collected, processed, and stored and by whom, and to whom that information may be disclosed.

**Assurance of privacy** depends on whether stakeholders expect, or are legally required, to have information protected or controlled from certain uses. As with security, the ability for users to control who has access to their data is of primary importance in the world of the connected user, made clear by users as well as regulators.

USP contains rigorous access control and authorization mechanisms to ensure that data is only used by those that have been enabled by the user.

[Architecture -->](/specification/architecture/)