User Services Platform

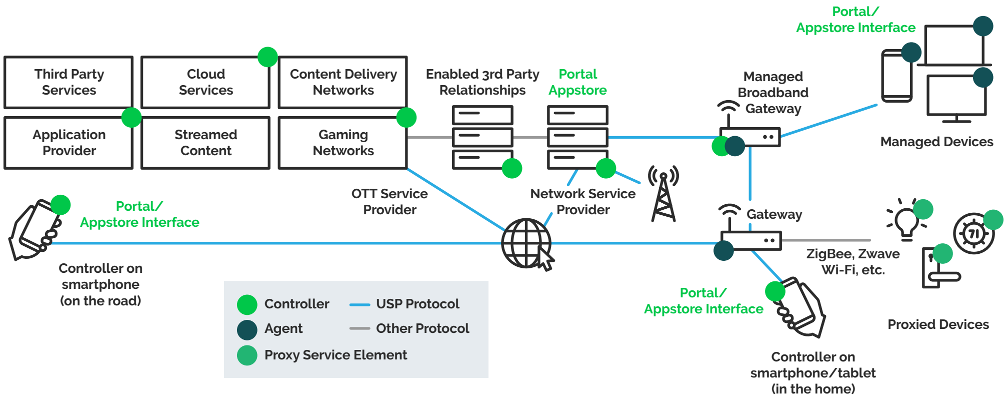
The journey to the connected home

User Services Platform (USP) is an integrated, standardized way to implement, deploy and manage all aspects of the connected home. USP is a network of Controllers and Agents that allow Applications to manipulate Service Elements. It consists of a data model, architecture, and standard communications protocol to transform consumer broadband networks into a platform for the development, deployment, and support of broadband enabled applications and services.

It enables a vast number of suppliers to integrate their products into provider service offerings and gives providers freedom to add customer services well beyond scope of TR-069. USP is an important step on the journey to an integrated, carrier-class connected home that will deliver an unprecedent quality of experience for users and control for providers.

USP builds on a massive foundation of nearly 1 billion TR-069 CPE WAN management protocol devices, developed in time to meet key new requirements

- Explosion of connected devices
- Leveraging and building on the knowledge gained
- Time for user services and improved access control
- Demand for improved support of pub-sub deployment models


Third Party Services
Cloud Services
Content Delivery Networks
Application Provider
Streamed Content
Gaming Networks
Enabled 3rd Party Relationships
Portal Appstore
Portal/ Appstore Interface
Managed Broadband Gateway
Managed Devices
OTT Service Provider
Network Service Provider
Portal/ Appstore Interface
Controller on smartphone (on the road)
Gateway
ZigBee, Zwave Wi-Fi, etc.
Proxied Devices
Portal/ Appstore Interface
Controller on smartphone/tablet (in the home)
Controller
Agent
Proxy Service Element
USP Protocol
Other Protocol

USP protocol allows providers, consumer electronics manufacturers, and end users to:

- Enable IoT and consumer electronics upgradability for critical security patches
- Bootstrap/configure new devices and virtual services
- Enable customer support to monitor and troubleshoot connected devices, services, and home network links
- Easily map the home network to control service quality and monitor threats
- Uses always-on communications for improved responsiveness
- Securely control IoT, connected home network functions locally or from the Cloud
- Enable multi-tenant/multi-stakeholder management
- Scale to meet an order of magnitude of increased demand and device types

Broadband Forum Demo at BBWF – October 2018

The demo uses a single protocol to control and manage an IoT system using multiple control points: the end-user's device and the service management system.

- One controls the IoT device
- The other can only see the state of the IoT device and is monitoring other network statistics to make sure the end user's experience seamless and valuable

USP enables more:

Multi-tenant management & control

- multiple operators manage & control the same devices at the same time

User management & control

- End users can manage & control their own devices (in conjunction with the operators)

Privacy

- Role-based Access Control = different roles assigned to different controlling endpoints

Robust, Secure communications

- provides RESTful operations tolerant to CPE variants
- Protocol-level encryption and application-level security

Fast adoption and coexistence

- Built on TR-181 for easy migration, can coexist with TR-069

Interoperability and compliance testing

As with TR-069, compliance to the USP specification and interoperability is a critical implementation requirement. The USP program to develop conformance test plans is in the planning phase and is targeted for completion in early 2019.

www.broadband-forum.org/usp | https://usp.technology

How does TR-369 (USP) compare with TR-069 (CWMP) and other approaches?

	TR-369 User Services Platform	TR-069 CPE WAN Management Protocol
Message Transfer Protocol	CoAP (LAN), WebSockets (Fixed-WAN), STOMP (WAN/Mobile)	HTTP
Data encoding	Google Protocol Buffers (binary wire format)	SOAP / XML (text wire format)
RPC structure	CRUD + Notify + Operate (general data model command execution mechanism)	CRUD + Notify (via Inform RPC, Events, and event specific RPCs) + several RPCs related to data model operations (schedule, upload, download, etc.)
Communications paradigm	Always-on/available direct communications channel established at device start-up allowing for free flow of messages and responsiveness	Short-lived sessions triggered by external events (timing, schedule, boot, wake-up, connection request, command queuing, sessions, XML, SOAP)
Management server	Multiple management servers are allowed at the same time without restriction of location (LAN, Fixed-WAN, Mobile)	A single management server at any given time with bootstrap logic/configuration
Security	DTLS/TLS message transport protocol security, controller trust establishment, access control list mechanism, end-to-end application level security/ encryption mechanism	TLS message transport protocol security, security through obscurity (CPE can only communicate with known ACS URL when it receives connection request)
Application to manage services	Network of controllers and Agents that allow Applications to manipulate Service Elements	

Comparison with other management solutions

	TR-369 User Services Platform	WebPA	Generic Cloud Solution (e.g. MQTT based)
Message Transfer Protocol	CoAP (LAN), WebSockets (Fixed-WAN), STOMP (WAN/Mobile)	WebSockets	Single message transport that - not ideal for all - cases
Data encoding	Google Protocol Buffers (binary wire format)	MsgPack (binary wire format)	Undefined
RPC structure	CRUD + Notify + Operate (general data model command execution mechanism)	RU-Only (static data model, no commands)	RESTful only – additional RPCs not standardized
Communications paradigm	Always-on/available direct communications channel established at device start-up allowing for free flow of messages and responsiveness	Always-on/available comms channel established at device start-up allowing for the free flow of messages	Always-on/always-available comms channel established at start-up allowing free flow of messages
Management server	Multiple management servers are allowed at the same time without restriction of location (LAN, Fixed-WAN, Mobile)	A single management server	Undefined – objects and messages are non-standard
Security	DTLS/TLS message transport protocol security, controller trust establishment, access control list mechanism, end-to-end application level security/ encryption mechanism	TLS message transport protocol security	TLS message transport protocol security if implemented, no standardized access control, communications through a proxy can be snooped