MARKET UPDATE

Realizing the Promise of the Connected Home with User Services Platform (TR-369)

MU-461

Realizing the Promise of the Connected Home with User Services Platform (TR-369)

The IoT enhanced Connected Home presents service providers with unparalleled opportunities and challenges … With over 1 billion deployments globally, look to the evolution of TR-069 for a clear path forward

Introduction

Broadband service providers across the board have seen increased pressure for years to provide faster and better-quality broadband experiences for their customers. For service providers, this presents a great opportunity for differentiation and new revenue sources. However, in order to achieve success, they have to overcome two challenges:

1. They need to deliver a better experience, which is a combination of leveraging the right technologies, enabling the right broadband ecosystem, and delivering the services with an agility that meets or exceeds customer expectations.
2. They need to achieve the first objective as efficiently and cost effectively as possible.

Early on, service providers realized that managing across these objectives would require proactive management of the home network, starting with the residential gateway, set-top-boxes, and other devices and applications critical to the customer's experience. This gave birth to the CPE WAN Management Protocol, more commonly known as TR-069. With over 1 billion installations today, TR-069 laid the foundation for mass adoption of broadband globally, and the broadband experience of today.

> **An opportunity to rethink how the broadband experience is delivered and measured in the home and business, and opened the way for a new protocol to emerge.**

However, the advent of the Internet of Things (IoT), the concept of the smart home, new security challenges, new cloud-based business models, new competitors for control of the Connected Home, and changing consumer expectations and requirements has created an opportunity to rethink how the broadband experience is delivered and measured in the home and business, and opened the way for a new protocol to emerge.

This paper explores some of the current pain points that consumers and service providers are experiencing in the market today, and how the broadband ecosystem is adjusting in multiple ways. Despite a steady stream of technological and operational innovations, over half of today's broadband customers are dissatisfied with their service. To address this, the industry is seeing the following responses:

1. The consumer electronics industry is attempting to gain control of the broadband experience by creating vertically integrated solutions for customers of their products

2. Some traditional telecom and cable vendors are working with service providers to create "walled garden" ecosystems composed of one-off integrations that allow a defined set of products to work together in harmony
3. Savvy service providers and vendors are pursuing standardized solutions that that are scalable, flexible, secure, and built as an evolution of existing infrastructure.

The winning strategies for owning the Connected Home of tomorrow are playing out today. However, one strategy – Broadband Forum's User Services Platform (USP) – stands above the others in providing a comprehensive long-term solution that balances the needs of the customer and the service provider, and as the evolution of TR-069, leverages the investment service providers have made in the over 1 billion broadband installations that already exist.

Providers Need to Control the Connected Home Business Model

With the accelerating mass proliferation of broadband-ready IoT devices, service providers face new challenges when it comes to both providing services to and monetizing the Connected Home. The average consumer often finds smart home "things" difficult to set up, use, and manage. As a result, consumers are increasingly turning to their broadband service providers for customer support on device-related issues. Additionally, operators are being held responsible for poor device and application performance by their customers because they perceive the integration of devices, applications, and Internet service as part of their overall broadband experience.

This is most acutely felt with the performance of Wi-Fi connectivity. Consumers do not differentiate between "the Wi-Fi" and "the Internet", despite the reality that many consumers buy their Wi-Fi equipment independently of their service provider. Although Wi-Fi mesh technologies are supposed to provide consumers with better Wi-Fi performance in their homes, they are also introducing significantly more complexity. A truly managed Wi-Fi as a service solution, based on mass telemetry and data analytics that is either owned by the provider or enhanced by vetted third party solutions, is critical to monetizing broadband connections and the smart home. That said, this type of Wi-Fi as a service solution is only deployed in a small minority of broadband homes and businesses today.

The opportunity for service providers is that the Wi-Fi gateway is the preeminent source of relevant data for the Connected Home. Managing and controlling the gateway - and by extension, all parts of the Connected Home - enables new services and offers the best opportunity to secure the service provider's place as the experience enabler for the future of the home. Unfortunately, managing these services has proven challenging for service providers. Few service providers today are leveraging the Wi-Fi gateway to its full potential as a powerful broadband experience and new service enabler.

Service providers who embrace a Wi-Fi gateway model can deploy, optimize and manage Wi-Fi and smart home devices, thereby establishing the foundation for connected services offered in the home. In contrast, today's operators are often missing the capability to collect key performance indicators from the Wi-Fi gateways with sufficient frequency and resolution. For them, installing new software on the gateway is a tedious and risky operation. Multiple data models, access technologies, vendors and chipsets complicate any analysis of data. Supporting legacy devices and OSS / BSS systems, as well as new ones within budget-constraints, without risking vendor lock-in, is a difficult task.

However, today's service providers are in a unique position to offer a unified smart home service due to several opportunities:

1. The home router is standard equipment for any subscriber. It serves as a central point for connectivity and network security in the home and can act as a central service point.
2. Service providers can act as a centralized service center that manages other services, with a single point for billing and customer support, simplifying a complex environment for the end-user.
3. Service providers possess the technical expertise for installation and troubleshooting, often more than the consumer electronics manufacturers themselves, as they have a direct touch point to the consumer's home network problems.
4. Service providers are responsible for the WAN connectivity required for third-party cloud services to function.

Though challenging, Wi-Fi connectivity and the promise of the smart home presents a great opportunity for providers to offer premium services that are self-branded or facilitated by a third-party service.

Top Challenges When Becoming a Connected Home Provider

Service providers face a number of challenges when trying to take ownership of the Connected Home.

Stunted Ecosystem

There is a heated race to capture ownership of the Connected Home going on in the consumer electronics community. As a result, many CE manufacturers are building their own proprietary solutions, or even "pre-standard" versions of standardized solutions. This is understandable given the massive pressure generated by the promise of monetizing the Connected Home.

Unfortunately, picking solutions like these has the potential to result in a stunted ecosystem, whereby a provider becomes dependent on a very limited ecosystem of vendors, or even a completely vertical solution developed by a single vendor. This creates an environment of reduced competition (which leads to higher risk), less innovation (which leads to less differentiation), and a potential for higher solution costs (due to limited options). Many of these stunted ecosystem and/or single vendor solutions exist now in the market – as they are in most technology markets in the early stages of development – and some service providers are taking advantage of them in order to meet their immediate needs. Other providers are also building their own solutions to these problems, pressuring vendors to comply with internal requirements - which can have the same effect in the long term, as vendors are forced to divert resources developing bespoke solutions.

Even solutions by vendors that are allegedly "open-source" can suffer from a stunted ecosystem. If an "open-source" solution has not been developed and standardized in a transparent way with input from many different stakeholders, critical design choices made early on by the vendor may be "locked-in" and dependent on the vendor to maintain it. In the worst-case scenario, these solutions masquerading as "open-source" may be dependent on their other software solutions in order for their solutions to interoperate.

Security

A challenge that comes from both consumer and regulatory demand is the security of Connected Home devices, privacy of the end user, and the assurance of privacy. Due to either ignorance or poor design, many smart devices, home gateways, and Wi-Fi products on the market have serious security flaws that are being specifically targeted by malicious attackers - effectively leaving service providers exposed. Although security issues by their very nature are a moving target that is constantly evolving and leaving the Connected Home potentially vulnerable, they can be mitigated by having robust and easy to execute upgrade paths for connected devices that can remain agile as security challenges change, as well as hardened and vetted software and protocols enabling these systems to provide a solid, secure service foundation.

Closely associated with security challenges are the issues of privacy and privacy assurance. When connected devices are transmitting very sensitive and private consumer information, it's imperative that this information is not only secured from malicious entities, but also has its access limited to those parties who are specifically authorized to access it and only for the use cases and time period necessary.

Maintaining Legacy Systems

Service providers have made significant investments not only in their installed base of customer premises equipment (CPE) (the vast majority of which are using TR-069, and its standardized data model, for management), but also in the Operations Support Systems (OSS) and Business Support Systems (BSS) that manage the infrastructure and operation of their network and subscribers. Any attempt to capture the Connected Home market will need to be able to seamlessly migrate - or evolve - these systems as transitions are made.

Staying Future Proof

The technologies behind Wi-Fi and whole-home connectivity, plus the smart home and IoT, are constantly evolving, providing new challenges and new opportunities in monetizing the connected consumer. It's important when seeking solutions that service providers think ahead and choose solutions that meet the criteria for being future proof. For example, service providers should:

1. Choose a solution that can be easily expanded and revised over time
2. Find vendors and organizations that can listen to and adapt to their needs
3. Choose a solution that has a definite upgrade path and methods for upgrading existing equipment
4. Choose a solution that can co-exist with legacy deployments
5. As mentioned above, avoid a stunted ecosystem if possible, to ensure long-term stability

An Overview of TR-369 (User Services Platform - USP)

To tackle these problems head-on, service providers and managed device manufacturers have come together to develop the User Services Platform (USP), specified by the Broadband Forum standard TR-369. TR-369 (USP) represents the natural evolution of TR-069 (CWMP), designed to be flexible, secure, scalable, and standardized to meet the demands of the Connected Home both now and in the future.

USP is built on the powerful legacy of TR-069. In addition to a design built on the experience of deploying managed services through complex network environments, USP allows access to hundreds of "service elements" – a term referring to the collection of objects, parameters, events, and operations that represent a certain interface or function, like Wi-Fi, performance statistics, smart home objects, and more. Specified in a data model (Device:2, also known as TR-181 Issue 2), these standardized elements have been vetted, expanded, and improved upon with diverse industry input for more than 10 years.

Major Features

USP consists of a network of Controllers and Agents that allow applications to manipulate service elements. An Agent exposes service elements to one or more Controllers. It can represent service elements on a device directly, or by proxy (USP has a robust proxy mechanism to represent virtual elements or elements that may be on other systems).

An application can use a controller, interacting with one or more agents, to manage a customer's network and other systems, much like today's TR-069 Auto-Configuration Servers (ACS), but with the additional benefit of allowing third-party applications to manage specific aspects of the customer's services. An application can also use a controller as a user-facing application in the cloud, on a gateway or smart hub, or on a customer's smartphone. With a network of controllers and agents, it can also act as part of an automated smart home or intelligent building system.

Using USP, connected devices can be deployed and onboarded without the need for on-site support. Long support cycles can be enabled through managed firmware upgrades that ensure a seamless end-user experience. Multiple parties, including the customer, can be given access to control, diagnostics, and even smart application data in a secure and privacy conscious manner.

Robust Service Set

While TR-369 defines the architecture and protocol for USP operation, its true power comes from the robust set of services defined in the Device:2 Data Model for CWMP Endpoints and USP Agents, also known as TR-181 Issue 2. This standard defines the objects and their properties that are used to manage and control a wide array of network elements and customer services.

Services enabled by TR-369/TR-181 include:

- **Management and monitoring of network interfaces -** Device:2 contains elements for managing and gathering statistics from a device's entire network stack. This includes physical interfaces (Ethernet, Wi-Fi, Cellular, ZigBee, etc.), SSIDs and MAC layer information, IPv4 and IPv6 interfaces, DHCP, tunneling, and more. These components are connected and read via an Interface Stack object that describes a device's active connections.
- **Management and monitoring network services and clients -** Device:2 exposes elements for managing access to network and security services, including firewall, DNS, network time (NTP), QoS, routing policies, connected hosts, and user access, plus application layer connection interfaces such as MQTT, XMPP, STOMP, etc.
- **Performance measurement and diagnostics -** Device:2 allows a controller to initiate download and upload performance measurements, measurements and network mapping using LMAP and TWMAP, plus diagnostics using ping, packet capture, and more.
- **Management of containers and applications -** USP allows users to install, monitor, and manage the lifecycle of software modules and execution containers on a system represented by a USP Agent, using objects, parameters, and operations built into the Device:2 data model.

New features and elements are added to the Device:2 data model through collaboration and iterative work by the industry, through Broadband Forum. New releases of the data model are produced every 6-9 months. In addition, TR-181 allows manufacturers to define their own elements using a standard syntax for vendor defined objects, parameters, commands, and events.

Deployment Flexibility

USP is designed to be flexible in its use cases and features. It is expandable to support future uses and new technologies. Many management or IoT solutions – even those that are open-source – are tied to very specific technologies that limit the universality of the solution to a single use case.

Compatibility with Legacy Deployments

USP was specifically designed to co-exist with existing deployments, like those enabled by TR-069. Because USP makes use of the Device:2 data model, legacy deployments can migrate from TR-069 to USP or make use of TR-069 for existing use cases while enabling new services with USP.

Multi-controller Architecture

Perhaps the most powerful aspect of USP is the agent's ability to be accessed by multiple control points from a number of different stakeholders. USP includes mechanisms for discovery, trust establishment, secure end-to-end communication, and access control mechanisms to limit the permissions of controllers to only those services they are permitted to see or manipulate.

In USP, discovery is accomplished through pre-configuration, DHCP options, or the use of mDNS when inside a user's network. Trust establishment, and role assignment are performed using certificate-based identity management. A USP agent can be pre-configured for a relationship with a particular controller, containing the necessary certificates and role associations for the controller to successfully communicate with it. A trusted controller can have permission to enable additional controllers and set up initial trust relationships. A user who wants their system to communicate with a new controller (such as on their smart device) can also use challenge-based negotiation to manually establish a trust relationship.

Multiple Transport Types

In USP, the lines between protocol and transport (which we call message transfer protocols, or MTPs) are very clearly defined. This not only allows for future expansion, but ensures that the protocol will operate the same way regardless of the transport used. Different transports are built for different use cases.

- **WebSockets -** In USP, WebSockets were included as a transport for point-to-point legacy devices - an improvement over HTTP for a protocol that communicates frequently.
- **STOMP -** The STOMP protocol is a message broker style transport built for cloud controllers supporting LAN side devices and devices that may move from one network to another. STOMP was chosen originally over MQTT, though MQTT support will be included in version 1.1 of the specification due to provider demand (notably, the type of feedback a standards-based solution can respond to).
- **CoAP -** The Constrained Application Protocol is built for LAN communication between LAN side controllers (i.e., in a smartphone or control hub), consumer electronics with fewer available resources, and a need for real time communication. This means USP solutions that are built for customer interaction are not dependent on the cloud.

In addition to these transports, USP defines an out-of-band mechanism for collecting large amounts of bulk data in JSON or CSV format over HTTP. Specified for both TR-069 and TR-369, this is known as the “HTTP bulk data collection mechanism” and is included in an annex of both specifications.

What About Interoperability?

The three scenarios outlined above are distinct use cases. Controllers that are operating in a particular use case only need to support the transports that fit that use case. In addition, the “MTP Proxy” that has been contributed to the TR-369 project allows, for example, a LAN-based USP Agent that only communicates via CoAP to have its messages proxied over STOMP/MQTT to a controller in the cloud.

Proxying non-USP Devices

In USP, an agent is not bound to representing elements that are contained within the same platform as itself. Systems that communicate via a protocol other than USP (for example, ZigBee or Z-Wave), or via some other system bus, can be represented by the USP data model’s robust proxy mechanism. This “ProxiedDevice” table populates with elements that may be hosted on other devices - such as IoT components - and allows a controller to use USP to manage, monitor, and control them.

Combined with its rich messages, notifications, and more, the device proxy feature of USP builds an interoperable ecosystem for connected devices.

Standardized Development

The complete USP system described by standards like TR-369, TR-181, etc. are developed in an open and collaborative environment through Broadband Forum, with IPR policies that respect the rights and products of providers and manufacturers. Though many solutions bill themselves as "open-sourced", there is a significant difference between open-source work that has been developed in accordance with a standard, among multiple parties, rather than those solutions that have been released by one particular company.

Standards-based solutions have a number of benefits:

- **Rigorous design:** Through an iterative process involving engineers from consumer electronics, device management providers, and network service providers, USP has seen a level of detail and rigor that is often missed in solutions that race to open-source or are developed by a single company. The lessons of decades of protocol design and deployment make for better solutions that are robust and future proof.
- **Industry responsiveness:** Standards organizations like Broadband Forum are a consortium of influencers that span entire industries. As a result, standards like USP are responsive to service provider and vendor input. New feature requests are processed in an efficient, open, and collaborative way to make sure that standards evolve while remaining rigorous.
- **Testing and certification:** Broadband Forum helps to ensure that solutions based on USP will work, and work well, in production. One of the ways it does this is through its Plugfest series, which are live, group test events that allow direct cooperation between implementers. This both improves the design of products for deployment and gives valuable feedback back into protocol design. The USP Plugfest series is on-going and sees between 2-3 events per year per technology.

In addition, Broadband Forum develops comprehensive conformance and interoperability test plans to serve as the industry benchmark for certification of USP implementations. Look for a full-scale certification program with self-test capability for USP Agents coming in the second half of 2019.

An Open-Source and Standardized USP Agent

Broadband Forum has started an open-source project for a USP Agent, called Open Broadband USP Agent (OB-USP-Agent). You can find details on this project on GitHub at: https://github.com/BroadbandForum/obuspa

Using TR-369 (USP) to Realize the Wi-Fi Connected Home

USP Use Cases for Managed Wi-Fi

Managed Wi-Fi has emerged as a critical part of enabling the Connected Home, since the vast majority of IoT devices connect to their broadband service via Wi-Fi. USP offers several approaches for optimizing and managing Wi-Fi. Here we will present three methods USP offers for Wi-Fi management. These methods showcase the flexibility USP offers, as every Operator has different needs and technological maturity.

Key to all of these methods for Wi-Fi management is the Device:2 Data Model for USP. This model has been used for Wi-Fi network setup and monitoring for more than 10 years and is regularly updated and maintained. Having a data model that can be used on legacy CPE, as well as being future proof for new devices, will simplify implementing a unified Wi-Fi management system without any compromise.

On-demand Troubleshooting

Understanding Wi-Fi quality is a highly complex analytical challenge given the existence of unlicensed radio spectrums and unmanaged environments. No other Internet access technology is as volatile, as Wi-Fi connectivity and performance changes multiple times per second. Quality and frequency of data collection is key to success, but as the data volume increases, so does the cost. Processing costs need to be under control to maintain a strong business case. Hence, modern and effective protocols for data collection are needed. USP supports this by being a lightweight, flexible method of gathering Wi-Fi statistics, deliverable over modern transport protocols built for different use cases, including the STOMP messaging protocol and MQTT (coming in version 1.1 of USP).

Wi-Fi configuration and telemetry have been standardized in the Device:2 data model for almost a decade, receiving updates and improvements frequently through Broadband Forum, including the addition of Wi-Fi mesh network telemetry (coming in Q2 of 2019) based on the Wi-Fi Alliance Data Elements standard. Using this standardized telemetry paired with these modern, scalable and relatively low-cost messaging protocols USP supports dynamic sampling of Wi-Fi KPIs and remote configuration. This will allow for optimization and troubleshooting in the cloud.

Enabling Machine Learning and Optimization Algorithms through Real-time Telemetry

Every Wi-Fi system supports hundreds of configurations from simple channel changes to tuning the number of packages to aggregate. Many of these configurations are tradeoffs between coverage, latency and throughput. Historically, Wi-Fi management systems have tended to deploy the same standard configuration across the entire population, leaving most of the Wi-Fi networks with sub-optimal performance.

Machine Learning offers a new opportunity with the potential of automating management and optimization of home networks (including Wi-Fi). Machine Learning methodologies can find the optimal configuration for every single device. To enable this, vast amounts of data need to be aggregated and gathered in a cloud solution. In order to have a business case for optimizing Wi-Fi with Machine Learning (or any other big data approach), the data collection needs to be done in an extremely cost-efficient manner.

USP bulk data collection allows for aggregation and sending data to a cloud endpoint in a scheduled manner. Through the USP management channel, users are given full control over which data points should be gathered and sent to which cloud resource, and at what regular frequency. The bulk data collection mechanism has minuscule cost, as the agent can simply publish the data to an end-point. As with most Machine Learning use-cases, the more data, the better the performance of the algorithms. Low-cost data acquisition is the key enabler.

Advanced Network Functions through Software Module Management

Optimizing and troubleshooting Wi-Fi on the in-home network is a major step to enabling the Connected Home, but it is not complete. By having software on a smart gateway, it's possible to do much more - from active steering of end-user devices on bands to more advanced features like classifying traffic, fingerprinting end-user devices, prioritization and optimizing Wi-Fi for specific use cases.

Issues regarding adding new software to edge devices is slowing down the development of advanced network functions. Legal responsibilities, privacy issues and severe consequences on fault make it difficult for Operators and 3rd parties to implement additional software on top of the firmware. In a world where Internet giants and startups alike publish software daily, slow release cycle and time-consuming quality assurance processes make it hard for service providers to compete.

USP software module management allows for a containerized approach to software development on these devices. Software module management gives the operator control to manage access and resources, upgrade, uninstall and handle faults and errors from the software module, removing almost all the risk that today is associated with such software deployments. In addition, USP's multi-controller architecture allows for valuable third-party relationships to be built while still maintaining provider ownership.

Take the example of Wi-Fi management middleware being installed on a device. That software can be triggered to be installed using USP's software module management commands, upgraded when necessary, and removed when it's no longer needed. As part of the installation, the software may create new objects or parameters in the agent's supported data model that are intended to be managed specifically by the third-party, due to an arrangement between the service and application providers. The application provider's controller will have access to the data fields it needs to function, while remaining isolated from other aspects of a user's services that are managed by USP.

USP Use Cases for a Managed Smart Home

USP was built with a broad and expandable scope of possible use cases, limited only by the imagination of developers building USP enabled systems. These new applications give providers the edge they need to compete against over the top services, but also enable partnerships with other stakeholders in the ever-growing world of the smart home.

OTT and Customer Enabled Controls

USP's unique multi-controller architecture with robust access control allows for a number of new and different opportunities for providers looking to form relationships with application developers to deliver new services. Beyond Wi-Fi management mentioned above, network security and parental control services, home security, home automation, and a host of other services can all be enabled with a system of USP agents and controllers.

USP's unique multi-controller architecture with robust access control allows for a number of new and different opportunities for providers.

Service providers can provide a better customer experience with the development of smartphone apps that act as USP controllers. Users can take steps to troubleshoot their own networks (dramatically reducing support calls), or provide a secondary channel for data collection that is activated temporarily to preserve privacy and security.

Additionally, very real, standardized smart home applications can be developed and deployed with USP. Application providers or emergency service providers can be given temporary access to specific components, isolating them from any data not reserved for the user or the service provider. Customers with controllers on their smartphone can freely roam to other networks while still securely controlling and monitoring their smart home and network.

Standardized Interfaces and IoT Functions

One of the fundamental problems in developing for the Connected Home are the myriad of devices with different ways of describing what they are and what they can do. It's so widespread that many different organizations are attempting to unify them - resulting in an equally diverse set of solutions. Additionally, with the convergence of the consumer electronics and networking worlds catalyzed by IoT, manufacturers not experienced with networking must look towards industry to provide them with standardized models for building interfaces and networking stacks. This empowers service providers to be able to effectively onboard, troubleshoot, upgrade, and monitor IoT devices - perhaps as a premium service.

Fortunately, the data model used by USP, Device:2, has developed these standardized interfaces, and has deployed and refined them for more than ten years. This includes physical and MAC interfaces for Ethernet, Wi-Fi, etc.; IPv4, IPv6, and all related protocols; plus IoT interfaces like ZigBee and MQTT. Standardized commands exist for diagnostic tests, firmware management and upgrades, and more.

USP Agents can report in great detail the specific functions they support, as well as standardized commands, events, and triggers, giving an application a clear picture of its capabilities. Troubleshooting can be done by monitoring network interfaces and performing diagnostics.

A robust and flexible IoT controls and sensors data model, built through industry collaboration, will be added to the Device:2 data model, targeted for the second half of 2019.

Device Proxy

The reality is that no matter how much standardization happens, different types of connectivity and configuration schemes will demand that any IoT solution that seeks to unify the Connected Home must actively recognize these differences. Different standards like ZigBee, Zwave, etc. are prevalent, and not all Wi-Fi enabled smart devices will be able to speak a singular protocol like USP.

Fortunately, USP provides an incredibly robust proxy mechanism that allows for discovery, onboarding, and lifecycle management of IoT devices, plus the ability to manipulate standardized IoT functions. Using a USP agent's "ProxiedDevice" table, applications can learn device types, software and firmware information, statistics, and capabilities. With the proper integration, IoT commands can be translated from USP to other smart home protocols while still presenting a seamless, quality user experience to the end user - a critical value-add for service providers to offer.

Conclusions

Realizing the Promise of the Connected Home

No matter the threat faced by service providers - reducing costs, improving customer support, or differentiating themselves to consumers - the User Services Platform (USP) was designed and developed specifically to meet these difficult challenges.

USP provides a platform for success in mastering the Connected Home via:

- **Flexibility -** its design looks forward to the future, ready to adapt to new services made possible by the fully Connected Home.
- **Security -** it enables third-party application relationships and new provider options while still respecting end-user security and privacy.
- **Standardization -** it represents the input of industry leaders in broadband, consumer electronics, and management solutions, built on the knowledge gained and lessons learned in fifteen years of TR-069 deployments, and backwards compatible with systems that have already been enabled by CWMP.

Although other options exist right now for meeting the short-term needs of service provider, no other solution provides a more robust solution for realizing the promise of the Connected Home of tomorrow. With USP, service providers are armed with a standardized solution that reduces risk and provides peace-of-mind that they will be able to address the challenges of the future head-on.

Service providers or developers looking to take advantage of this powerful solution can find information at https://usp.technology/.

Broadband Forum's Connected Home Council would like to recognize the following for their valued contributions to this document:

Jason Walls – QA Cafe

Tim Spets – Greenwave Systems

Magnus Olden – Domos

Geoff Burke – Broadband Forum