LBNL-182358

Lawrence Berkeley National Laboratory

Design of an Open Smart Energy Gateway for Smart Meter Data Management

By: Janie Page, Chuck McParland, Mary Ann Piette and Stephen Czarnecki

Demand Response Research Center

Lawrence Berkeley National Laboratory, Berkeley, CA

March 2015

The work described in this report was coordinated by the Demand Response Research Center and funded by the California Energy Commission (Energy Commission), Public Interest Energy Research (PIER) Program, under Work for Others Contract No. 500-03- 026, and by the U.S. Department of Energy under Contract No. DE-AC02-05CH11231.

LBLN-182358

Energy Research and Development Division
FINAL PROJECT REPORT

DESIGN OF AN OPEN SMART ENERGY GATEWAY FOR SMART METER DATA MANAGEMENT

Prepared for: California Energy Commission
Prepared by: Lawrence Berkeley National Laboratory

MARCH 2015
CEC-500-2015-XXX

PREPARED BY:

Primary Author(s):
Janie Page
Chuck McParland
Mary Ann Piette
Steven Czarneck

Lawrence Berkeley National Laboratory
Demand Response Research Center
1 Cyclotron Road
Berkeley, CA 94720

Contract Number: 500-03-026

Prepared for:

California Energy Commission

David Hungerford
Contract Manager

Virginia Law
Office Manager
Energy XXXXXXXX Research Office

Laurie ten Hope
Deputy Director
ENERGY RESEARCH AND DEVELOPMENT DIVISION

Robert P. Oglesby
Executive Director

ACKNOWLEDGEMENTS

The work described in this report was coordinated by the Demand Response Research Center and funded by the California Energy Commission (Energy Commission), Public Interest Energy Research (PIER) Program, under Work for Others Contract No. 500-03- 026, and by the U.S. Department of Energy under Contract No. DE-AC02-05CH11231.

The authors would like to thank Roger Levy, Ron Hofmann, and former Lawrence Berkeley National Laboratory staff members David Watson for their contributions. The authors also acknowledge all others who assisted in review of this document, and the ongoing support of the California Energy Commission and PIER Program staff.

PREFACE

The California Energy Commission Energy Research and Development Division supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The Energy Research and Development Division conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The Energy Research and Development Division strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

Energy Research and Development Division funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

For more information about the Energy Research and Development Division, please visit the Energy Commission's website at www.energy.ca.gov/research/ or contact the Energy Commission at 916-327-1551.

LBNL DISCLAIMER

ABSTRACT

With the widespread deployment of electronic interval meters, commonly known as *smart meters,*came the promise of real-time data on electric energy consumption. Recognizing an opportunity to provide consumers access to their near real-time energy consumption data directly from their installed smart meter, we designed a mechanism for capturing those data for consumer use via an open smart energy gateway (OpenSEG). By design, OpenSEG provides a clearly defined boundary for equipment and data ownership.

OpenSEG is an open-source data management platform to enable better data management of smart meter data. Effectively, it is an information architecture designed to work with the ZigBee Smart Energy Profile 1.x (SEP 1.x). It was specifically designed to reduce cyber-security risks and provide secure information directly from smart meters to consumers in near real time, using display devices already owned by the consumers. OpenSEG stores 48 hours of recent consumption data in a circular cache using a format consistent with commonly available archived (not real-time) consumption data such as Green Button, which is based on the Energy Services Provider Interface (ESPI) data standard. It consists of a common XML format for energy usage information and a data exchange protocol to facilitate automated data transfer upon utility customer authorization.

Included in the design is an application program interface by which users can acquire data from OpenSEG for further post processing. A sample data display application is included in the initial software product. The data display application demonstrates that OpenSEG can help electricity use data to be retrieved from a smart meter and ported to a wide variety of user-owned devices such as cell phones or a user-selected database. This system can be used for homes, multi-family buildings, or small commercial buildings in California.

Keywords: Home Area Network, gateway, security, Zigbee, Smart Energy Profile, SEP 1.x.

Please use the following citation for this report:

Page, Janie, McParland, Chuck, Pietttе, Mary Ann, Czarnecki, Stephen
Lawrence Berkeley National Laboratory. 2015. ***Design of an Open Smart Energy Gateway for Smart Meter Data Management,*** California Energy Commission. Publication number: CEC-500-YYYY-XXX.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: Introduction and Context for the Open Smart Energy Gateway

Historically, digital near-real-time energy consumption data have not been widely available for electric energy users. Access to pulse output ports that are available on some meters requires specialized knowledge and interface equipment to access the data. More recently, however, digital smart meters, known as the advanced meter infrastructure (AMI), have been installed in California to provide two distinct mechanisms for transmitting energy consumption data. One is secured to a communication network directly to the utility for billing purposes. The other mechanism transmits the same energy data to a home area network (HAN) device using the ZigBee Smart Energy Profile (SEP) (ZigBee Alliance, 2011). Note that AMI is distinct from automated meter reading (AMR) devices that were deployed earlier. The AMR devices provide a data collection mechanism by which aggregated kilowatt-hour (kWh) usage—and in some cases, peak monthly demand data—can be acquired remotely by a utility using drive-by or walk-by based technology. In contrast, AMI devices can provide a more substantial payload of real-time, meter-based data to both the utility and the consumer (Roche, 2008]. The term "smart meter" typically refers to AMI meters.

Approximately 50 million smart meters have been installed in the United States (Cooper, 2012). Another 80 million smart meters are planned for installation in Europe from 2014 on. California's investor-owned utility (IOU) installations are nearly at planned levels, currently representing about 23 percent of the U.S. total, with over 11 million smart meters in homes and small commercial facilities with under 200 kilowatts (kW) in peak power service requirements. The next largest deployment is in Texas, where 7 million smart meters were installed between 2009 and 2013 (Smart Meter Texas, 2013). Figure 1 graphically displays how the AMI and SEP systems are related.

Figure 1. Relationship between utility, meter, and home with AMI and SEP

Smart meters measure electricity consumption at regular intervals and store the information in an internal memory chip until it can be transmitted. Measurements are typically made on a sub-second scale, then compiled in storage to various user-selectable time intervals, some as small as

every four seconds. Smart meters allow two-way communication to the meter to enable a utility to retrieve meter readings remotely and upload meter firmware updates and other application instructions to the meter. Smart meters also provide an integrated Home Area Network (HAN) gateway, enhanced meter data management capability, and a meter communication network capable of supporting expanded signals into the premises, capability to take appliance-specific data out of the premises, and enhanced capability to manage the operation of devices within the premises. To do this in California, smart meters use two distinct radios to transmit consumption data: one radio is dedicated to sending information to the utility back office at least daily for monitoring and billing purposes via the Advanced Metering Infrastructure (AMI), while a second radio is designed to send home area network (HAN) information via the ZigBee Smart Energy Profile 1.x (SEP 1.x) to connected devices within the consumer's premises.

A smart meter with an integrated HAN was designed for a variety of uses, such as enhanced customer education, demand response (DR), dynamic pricing, and system operations. Additional system operation improvements that were expected with smart meter installations include outage detection, remote connect or disconnect, demand limiting, and enhanced customer HAN device monitoring and control. These expectations improved the conventional regulatory business case used to justify systemwide deployment of smart meters and the supporting Advanced Metering Infrastructure (AMI) required to get billing information back to the utility billing office. On the other side of the meter, in order to be useful to customers, metered electricity usage data needs to be conveyed to them in a timely manner, so that it can influence behavior choices that impact energy use, utility bills, participation in demand response, and other factors important to the consumer and the utility.

Recognizing an opportunity to provide consumers access to their near-real-time energy consumption data directly from their installed smart meter, we designed a mechanism for securely capturing those data for consumer use via an open smart energy gateway (OpenSEG). OpenSEG is an information architecture designed to work with ZigBee Smart Energy Profile 1.x (SEP 1.x). It was specifically designed to reduce cyber-security risks and provide secure information directly from smart meters to consumers in near real time, using display devices already owned by the consumers. Direct access to smart meter data could help consumers better measure their efforts to manage consumption and offer new opportunities for authorized third-party vendors to develop more effective means for local control of energy consumption.

This report describes the design of OpenSEG and compares the utility meter data acquisition systems on the market today. It begins with an overview of the home area network context in which OpenSEG was developed. With this as background, the concept of OpenSEG is introduced. We begin with an overview of how OpenSEG fits into the current market via a set of use cases. From there, a more technical explanation of the OpenSEG follows. Finally, we

describe testing and demonstrations of OpenSEG completed to date. This report is intended for utility regulators, energy planners, smart meter software development companies, engineering firms, utilities, and demand response aggregators.

CHAPTER 2: Smart Meters and the Home Area Network

In 2006, Southern California Edison planned to deploy approximately five million smart meters that would collectively support "1,000 megawatts (MW) of new peak demand response" by 2015, while supporting "0.5% annual energy conservation efforts across all customers" (Gunther, 2007). A key driver for the smart meter installations, as cited by Southern California Edison, is that "the new meters will help customers more effectively manage their electricity use, helping them to save energy, money, and the environment" (Edison SmartConnect, 2008).

Figure 2 displays the associated costs and benefits identified by Southern California Edison in support for their deployment of SmartConnect, their branded smart meter project (Montoya, 2006). Operating benefits would accrue largely from the AMI side of the meter, whereas benefits from load control or price response would accrue for the homeowner on the HAN side of the meter.

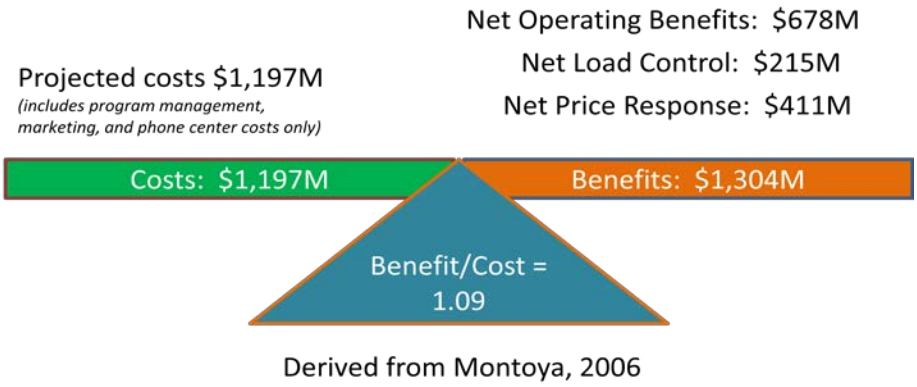


Figure 2. Southern California Edison proposed cost-benefit analysis for smart meter implementations

The use of the HAN side of meter communications has been slow across most utility service areas, including California (see Table 1). Although implementation of smart meters began around 2008, HAN activations at the beginning of 2013 were estimated to represent less than 0.1 percent of the available meter population (Cooper, 2012). A recent report on HAN implementations in Texas actually shows a decline in the number of connected devices between 2013 and 2014 (Lewin et al., 2014). Of the reported seven million smart meters installed in Texas, less than 1 percent of the associated customers logged into the Smart Meter Texas portal and

less than 0.2 percent of the devices received a request for connection from an external device. Technical and cyber security issues have been cited as a key reason for delayed activation of HAN applications (Cleveland, 2009).

Table 1. HAN activations in California

Investor-Owned Utility	HAN Activation Requests *As of October 2013*	Devices Validated
Pacific Gas and Electric	364	5
San Diego Gas & Electric	230	14 (9 available)
Southern California Edison	128 customer, 922 pilot	9

Source: California Public Utilities Commission. California Smart Grid, 2014

HAN Architecture

One early goal of the smart meter-embedded HAN radio was to provide a signal to SEP-capable consumer-owned devices so that they could change their demand for electricity use according to preplanned methods when electric consumption or prices achieved preset levels. The original HAN architecture (Gunther, 2007) depicted in Figure 3 uses the meter itself as the gateway that communicates directly with enabled consumer-owned devices, such as display devices, appliances, and programmable thermostats. Devices using the HAN radio could either simply receive usage data or could establish a two-way communication as needed (e.g., to provide information on appliance operations or to confirm device identification).

The original architecture promoted by California utilities envisioned a number of household devices directly participating in a ZigBee-based network controlled by and administered through the smart meter itself. At that time, the ZigBee family of protocols were solely layered on the IEEE 802.15.4 MAC layer standard. Some research, targeted solely at the 802.15.4 MAC layer, identified security concerns (see Sokullu, 2008; O'Flynn, 2011). Exploitation of these security issues could bring the link to the network down but would not provide access to application layer packet contents. While the additional security layers provided by the ZigBee protocols addressed these concerns, design and implementation discussions of the proposed (802.15.4 plus ZigBee and SEP) system took place in closed and proprietary settings that did not allow substantive external input. As a result, any concerns—real or perceived—about the performance or security of the proposed system were often left unaddressed. The true risks and benefits associated with embedding and integrating a HAN into new smart meters became difficult to weigh—even by many within the utilities themselves. And, lacking access to the larger, open engineering and academic community, authoritative evaluation of perceived and actual risks was severely limited and compromised.

As a result, several major utilities delayed activation of ZigBee/SEP features in deployed smart meters. Although the potential risk of damaging smart meter security breaches was arguably small, a number of utilities perceived the security built into SEP 1.x as being insufficient to prevent network attacks or the introduction of malicious code from a connected device (see, for example, Centerpoint, 2009 or Lee and Chason, 2011). These concerns led to the development of various processes by which devices must be approved before joining the network. Essentially, most utilities chose to limit the devices that could attach to the HAN radio to those that passed well-defined screening processes at the utility level.

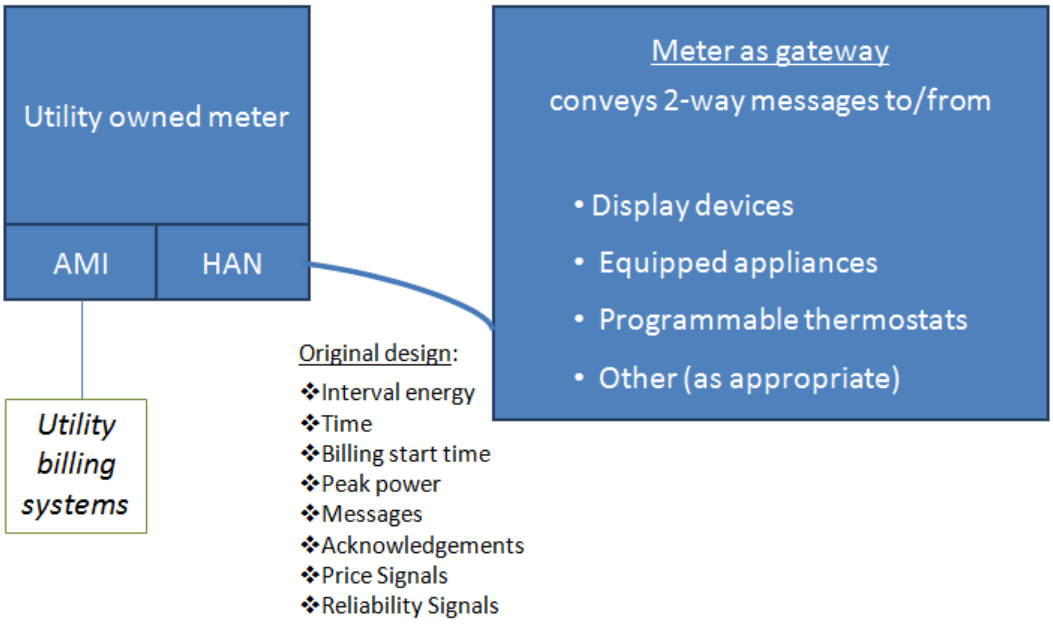


Figure 3. The Original HAN architecture with the Smart Meter as gateway

In addition to cybersecurity concerns, there are an additional three areas where the traditional ZigBee SEP 1.x communications-based home area network architectures fail to meet consumer expectations:

1. **ACCESSIBILITY:** HAN accessibility is limited by inadequate coverage from low-power ZigBee 802.14 radio to less than 75 feet from the meter. That signal can be further diminished by some building materials or interference from other wireless devices typically owned by consumers.
2. **RELIABILITY:** If a HAN device connection with the meter is inconsistent, it jeopardizes the ability of the consumer to receive and act on received data.
3. **PORTABILITY:** Connections between devices and home area networks should be consistent from one location to another, but (1) different advanced metering and ZigBee SEP customization options can create networks with proprietary meter-HAN interfaces

unique to each utility; and (2) close component integration of meter and HAN create meter-related firmware upgrade dependencies that raise significant legal, technical, cost, operational, and competitiveness issues

OpenSEG Architecture in context of Smart Meter HAN

In response to concerns identified with implementing smart meter HAN systems, we began developing the Open Smart Energy Gateway. The original intention was to enhance both real and perceived smart meter security issues through straightforward architectural constraints, thus enabling secure collection of near-real-time smart meter data that could be conveyed to other equipment within the consumer's premises. These architectural constraints consisted of limiting, through utility policy, the number of SEP 1.x devices binding to a smart meter to one, and by requiring that single device to implement a well-understood data access algorithm. Further, the data access algorithm was limited to only allow simple "read-only" transactions with the smart meter. The "smart energy" in the name of the Open Smart Energy Gateway acknowledges the use of the Smart Energy Profile from the ZigBee Alliance (ZigBee, 2011).

SEP 1.x includes six application clusters. Three of these applications provide one-way communication of data into the premise:

(1) *Simple Metering* provides access to near-real-time meter data.

(2) *Price* provides rate and energy price information.

(3) *One way, application-level messaging* (as opposed to bidirectional communications at lower protocol layers) provides text capability to notify customers of DR, price, or other events.

SEP 1.x also includes three two-way applications, including Prepayment, Complex Metering, and Demand Response, all of which have the capability to pull information from inside the premises for transmission to utility backend systems.

As shown in figures 4 and 5, OpenSEG reduces concerns about cybersecurity by eliminating communication from the consumer's premises back through the meter (Searle and McParland, 2013). Security is vastly improved for a smart grid network containing SEP1.x-based radios if the meter only uses the HAN for one-way, information-only applications to the consumer premises. Restricting or limiting HAN applications can be accomplished by disabling the SEP software for specific SEP application clusters. Specifically, for SEP 1.x, one-way applications are limited to simple metering, pricing, and messaging. Although pricing and billing information do not pose a risk per se, they are not included in OpenSEG data by design. To maintain security on the network, utilities or third-party vendors may provide all other HAN

functionality, including pricing, using alternate, more secure communication such as wires or wireless internet gateways. If the HAN application functionality is moved out of the meter to an in-premises, customer-owned gateway, the gateway can then provide consumers with control over HAN operation, data privacy, and third-party relationships. The gateway outside of the meter also provides a degree of insulation between the utility and customer systems.

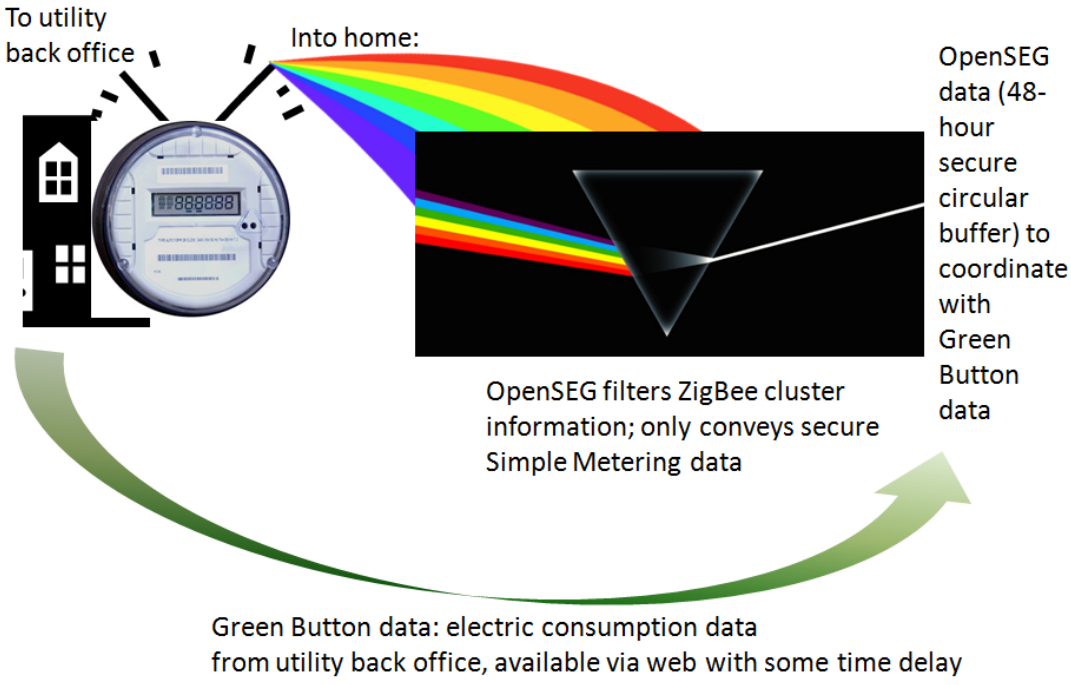


Figure 4. OpenSEG filters ZigBee clusters to convey usage data securely into premises

Registering and linking OpenSEG as a solo device that communicates with the smart meter simplifies general device certification and verification because those devices are now customer owned and link to the meter data, but not the meter itself. The OpenSEG architecture (Figure 5) incorporates the recommendations outlined above via a simple but effective change to the assumed HAN architecture. Instead of allowing any number of approved devices to bind directly with the ZigBee radio associated with the smart meter HAN, OpenSEG acts as an single, secure point of ZigBee connection to acquire real-time electric energy consumption data that can be viewed directly or used by other applications. As part of the security protocol, the gateway filters the ZigBee signal for only the Simple Metering cluster of data, which it stores as data pairs (time, usage) in the 48-hour data circular data cache that provides context for the most recently acquired information.

SEP 1.x also supports read-only access to pricing information. In addition to accessing meter power and energy consumption data, the OpenSEG platform is capable of reading, caching, and serving this pricing information to various HAN devices. While the OpenSEG application can be expanded to include such functionality, our present research goals focused solely on conveying household consumption data to end users and, as a result, this feature is not presently included in OpenSEG. Furthermore, some confusion and controversy surrounds the ability of current AMI back office systems to provide energy pricing information through the meter with sufficient fidelity to satisfy consumers. Pricing/consumption tiers, as well as end-of-month energy cost surcharges, limit the accuracy of real-time price information distributed through utility AMI systems. As more systematic mechanisms are developed to create more meaningful real-time energy cost estimates, we will revisit the inclusion of price in the set of read-only measurements made available by the OpenSEG gateway.

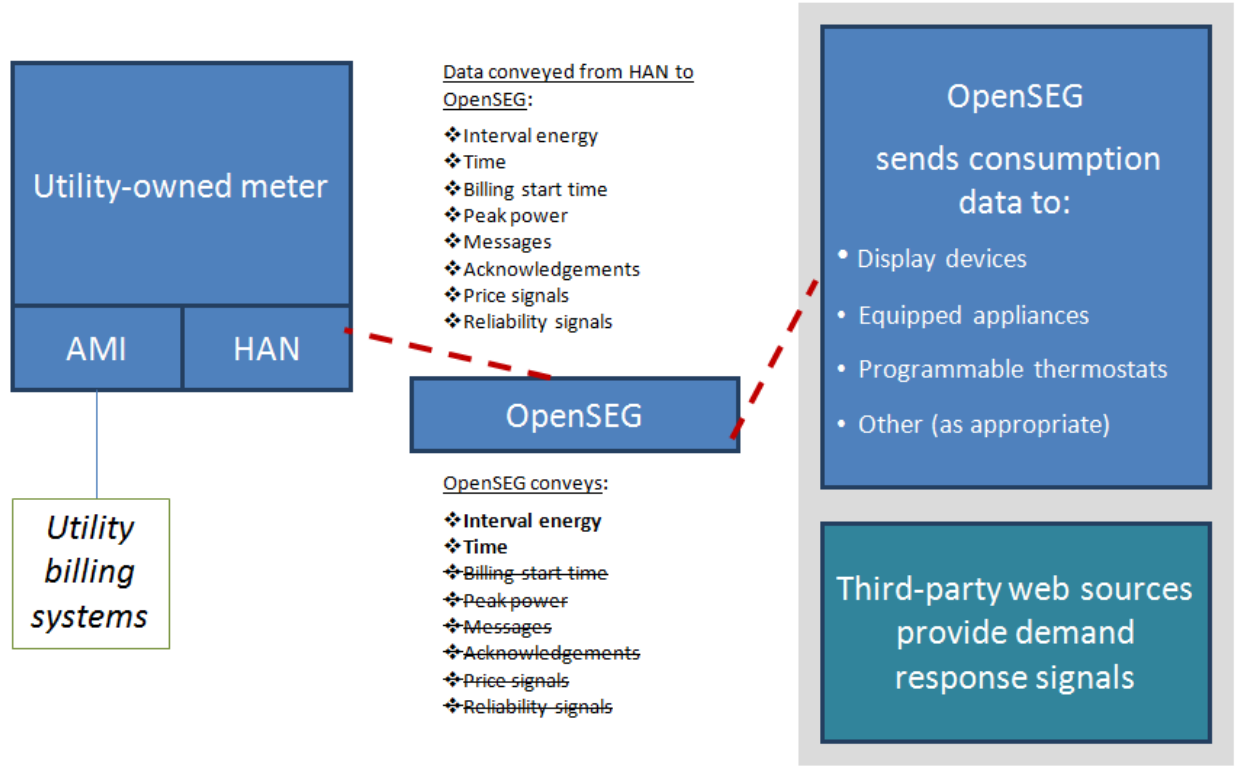


Figure 5. OpenSEG conveys electric consumption data

Rather than attempting to individually communicate with a residence's smart meter, appropriately equipped in-home devices requiring information about energy consumption can request those data from the OpenSEG gateway using common, widely implemented network protocols such as TCP/IP. In addition, users can view real-time energy consumption directly via code developed to meet the OpenSEG application programming interface (API). A simple

program is provided with OpenSEG to graph the data on consumer-owned devices such as laptops, tablets, and smart phones.

Market Potential

OpenSEG fundamentally alters the HAN architecture to simultaneously provide secure and immediate access to electric consumption data to consumers for the most recent 48 hours of consumption data. These data can be synchronized with historical records of usage such as Green Button data. The real-time consumption data provided are reliable because they stem from the same meter that provides utility billing data. Furthermore, OpenSEG's secure interface clearly marks the distinction between utility responsibility and homeowner responsibility. As such, it restores the value originally intended within the smart meter deployments for consumers and utilities.

Use Cases

OpenSEG is intended to enable new markets for data management for residential and small commercial facilities that use the smart meter data in near-real time or use the high-frequency data beyond what is stored in the utility Green Button archive. We describe five examples of the new service capabilities that OpenSEG enables.

1. **Energy Use Monitoring**

   OpenSEG provides a mechanism for consumers to collect near-real-time energy consumption data without the delays or latencies associated with it being transported to the utility data center and back to the consumer's application. This is useful in homes and small businesses, and OpenSEG can be extended to support electric vehicle charging programs by providing a mechanism for users to determine directly the amount of energy acquired, and when and where it was acquired.

2. **HAN Architecture Enhancement**

   OpenSEG provides a single point of access from the meter to the home, with all other home-based devices accessing meter data via OpenSEG. As such it provides a clear distinction between utility-controlled assets and those controlled by consumers, while establishing a reliable secure communication path between the two. In-home appliances can use the standard data formats provided by OpenSEG to obtain real-time consumption data that can be coordinated with other signals about grid reliability provided via the internet to supply timely demand response services when needed.

3. **Verification of Aggregate Load Changes**

Signaling DR events was originally proposed via meter communications (e.g. ZigBee SEP 1.x) into a home. However, the OpenSEG architecture assumes that IP is a more reliable and secure method for conveying DR signals than is ZigBee SEP 1.x. OpenSEG provides time-stamped energy consumption data that can provide (a) a commonly agreed upon clock against which responses can be scheduled, and (b) confirmation of aggregate response to a demand response event. Response can be confirmed directly only if individual participants are willing to share load data, but derivative data indicating changes in load shape as a function of time can also provide useful indications of changes in response to DR event signals. Because the rate at which energy data are acquired is configurable, OpenSEG can support confirmation of response in both traditional DR programs and those requiring a verifiable faster response (to 4- to-10-second intervals).

4. **HAN Network Performance Monitoring**
   Through a continuous comparison of time-integrated power measurements with periodically reported energy measurements, OpenSEG provides a means by which the state of the HAN network can be directly monitored locally. Data dropouts can be seen via a lack of continuity in the comparison. This non-intrusive technique can report out regularly on the difference between the two measures, with non-zero entries pointing to the time of disconnect without compromising the privacy of consumer data.

5. **Aggregating Electric Metering for Ancillary Services and Fast DR Programs**
   OpenSEG collects 10-second data that could be used to evaluate changes in electric load shapes for advanced demand response programs such as those in ancillary services programs. These data may be compliant with requirements by the California Independent System Operator for high-resolution electric load shape monitoring. Many buildings with these smart meters use over 100 kW, and the aggregation of a dozen or more small commercial buildings may provide a significant DR resource. An OpenSEG system could greatly reduce the cost for telemetry for these advanced DR programs.

OpenSEG was designed to provide a significant change to the HAN architecture, to enhance overall system security. It addresses network security concerns by segregating communication issues into those that must be provided by the meter itself, such as providing real-time consumption data, with those that can be handled directly via an alternate path. OpenSEG offers a secure, private gateway that is designed to provide consistent, reliable access to real-time electric consumption data via proven industry standard messaging protocols.

CHAPTER 3: Open Smart Energy Gateway (OpenSEG)

OpenSEG provides near-real-time smart meter data in a readily usable form to consumer-owned devices without the delays or latencies associated with mechanisms such as Green Button.[1] To do this, the gateway establishes a secure local smart meter connection, then queries the meter to which it is bound to get energy consumption information at pre-defined intervals (a typical minimum interval is four seconds). OpenSEG stores the resulting data internally for retrieval by an external application via a well-defined API. The storage of the most recent 48 hours of data provides contextual usage information and allows a means for connecting the near-real-time measured data with historical data (e.g., Green Button data available via most utilities through a website). The full OpenSEG specification is included as Appendix A in this report.

Key points:

- OpenSEG provides a secure means for acquiring real-time energy consumption data from a smart meter without endangering the utility network (Searle and McParland, 2013).
- Historical data contains data from 48 hours immediately preceding the present time to provide context for each acquired data point. The cache is built to replace older data with newer data.
- Options are provided for the consumer to get data for a particular time or a relative time (e.g., pervious 60 seconds), or to get all the data in the cache.
- Consistent time stamps are used to allow synchronization of OpenSEG data with older data, as needed.

OpenSEG Characteristics

As described in the OpenSEG specification (Appendix B), the OpenSEG gateway is designed to act as an information gateway through which software applications can obtain information about residential energy consumption. It can be implemented on a small hardware platform designed to acquire power and energy data from a smart meter, develop context from the most recent 48 hours of consumption data, and present the information to the user via a well-defined API. In acquiring, formatting, and presenting the data, it maintains data security so that the data that belongs to the consumer remains in the control of the consumer.

[1] Green Button is a U.S. Department of Energy initiative (based on NAESB, 2011) by which utilities can provide consumers access to their own electric usage data after they have been reviewed, calibrated, and stored by the utility. In some cases this can take up to two days elapsed time.

OpenSEG has the following elements:

- **Meter data access:** ability to acquire ZigBee SEP 1.x data and to choose a time increment for those data (typically set to every 4 to 10seconds).
- **Data filter:** filter to gather only the data presented via the Simple Meter ZigBee cluster, to maintain system security (see Searle and McParland, 2013).
- **Data cache:** local circular data cache to store data from the most recent 48 hours.
- **Means for conveying data to consumers:** OpenSEG provides access to the data via the local network (typically WiFi using IP or via an Ethernet connection). OpenSEG is built to a well-defined software API describing how to acquire data.

OpenSEG Security

By design, ZigBee networks are composed of coordinators, routers, and end devices. According to the ZigBee Alliance (ZigBee Network topology), coordinators control the network structure (formation and security), routers extend the range, and end devices perform a particular task (e.g., sensing, metering, or controlling). ZigBee limits what devices that can join a particular network through the use of a ZigBee network key used by the network coordinator within the ZigBee architecture. Compromise of the network coordinator role, therefore, is a primary weakness of the system because it can become a pivot point for attacking other devices on the network. ZigBee coordinators usually assume the role of an SEP trust center and provide network management, device authentication, and device whitelisting. Any failure to authenticate with the trust center would likely block access to the rest of the home area network.

The SEP 1.x network formation contains several steps aimed at verifying devices before access is granted. First, a personal area network ID (PAN ID) and a network access password (ZigBee network key) are acquired by a device. Once verified, the device may join a network. For additional access to SEP services, including access to other SEP devices, a certificate-based key exchange (CBKE) authentication (using the elliptic curve cryptography certificate programmed into the device when created or introduced during a flash update) is required. Conceptually, a malicious user that gained access to this layer of the ZigBee program stack would be in a position to exploit program implementation shortcomings that had remained undetected by the manufacturer or compliance testing. In general, these malicious attempts would focus on any ZigBee services that are allowed to send data to one or more meter metrology functions. The actual risks are difficult to quantify since they would, in large part, depend on how well other areas of meter software had been implemented and tested. But, meter functions that present a *reasonably well-tested, read-only interface* to ZigBee services are considered immune to compromise. While analysis of this picture presents no absolutes, it is clear that the likelihood of successful malicious access to smart meters through the ZigBee interface is, essentially, the

product of a series of highly improbable and difficult-to-achieve actions, with the resulting probability of success far less than that of any single act. However, as long as such attacks are of concern to utilities, many consumers will see only limited benefits from system-wide investment in smart meters.

OpenSEG seeks to reduce both real and perceived risks by limiting the number and kind of devices that can communicate with the smart meter (through policy) and by limiting the kinds of requests that can be presented to smart meter ZigBee software stacks (through gateway implementation). As the gateway that controls meter access, OpenSEG limits the number of devices binding to the smart meter to just itself. It then provides a single point of access for all other HAN devices, preventing them from leveraging interPAN access to the meter. OpenSEG's design further limits the SEP clusters that can be accessed by HAN devices to those that are read-only.

OpenSEG Implementation Details

Lawrence Berkeley National Laboratory developed a proof-of-concept implementation of OpenSEG. Separately, a commercial firm, Rainforest Automation, developed and modified a device (EAGLE™) that also follows the OpenSEG specification. The text below provides general information about implementing OpenSEG, with primary focus on the LBNL proof-of-concept implementation.

Hardware

The OpenSEG open-source software can run on both general and embedded Linux platforms with processor speeds of at least 800 megahertz (MHz) and at least 500 megabytes internal random access memory. A USB host interface is needed on the platform to support communications with the meter via the Rainforest RAVEn™ dongle. OpenSEG also requires the availability of networking interfaces to support communications with external clients. These networking interfaces can support either wired or WiFi communications and may require additional USB ports for connection to the platform itself.

OpenSEG has been successfully deployed on various versions of the Intel Next Unit of Computing (NUC) platform and on an embedded platform (Beagle Bone Black). Deployment on smaller and less-capable Linux platforms may be possible, but has not yet been extensively tested. At the high end, a simple desktop or laptop system running a current version of the Debian Linux operating system would be ideal for OpenSEG. OpenSEG components are written in C, and the Linux execution environment need only support the C programming language. Figure 6 shows the current implementation of OpenSEG using a BeagleBone Black with WiFi and the Rainforest Radio Adapter for Viewing Energy (RAVEn™) attachments. In this

implementation, the overall device is approximately 6" x 4" x 1" in size. The OpenSEG should be placed within about 10 meters of the smart meter.

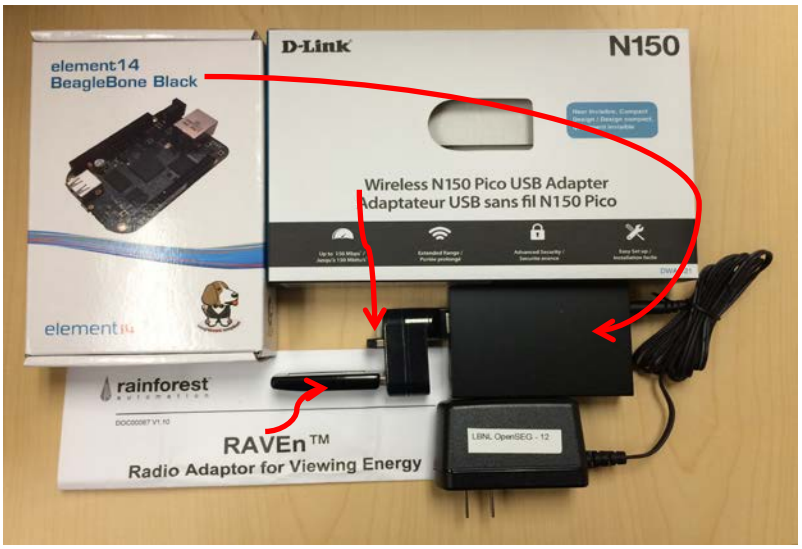


Figure 6. Current implementation of OpenSEG

Connection

The device with the OpenSEG software needs to be registered and linked to the utility smart meter using the ZigBee radio. That registration and linking process will be determined by each utility's specific rules. Typically this involves some form of registering the device into the meter. This may be done automatically, or by utility staff in response to a customer request. The meter joins the device using the media access control (MAC) address and installation code. Once that task is complete, any device within the customer premises or customer-designed service provider will access the meter data through the OpenSEG gateway. Those devices will not need to be registered with the utility or linked to the smart meter.

Data acquisition

OpenSEG uses local access to the smart meter ZigBee communications channel to obtain both power and integrated energy meter readings at finer time interval granularities than the 15-minute data available from most utility back office applications. As a result, meter data typically obtained through the OpenSEG gateway will contain time-structured information typically lost through data integration and averaging operations conducted by utility billing and archiving applications.

OpenSEG meter data access

OpenSEG is a gateway acting as a webserver responding to REST-based queries. The OpenSEG API uses a REpresentational State Transfer (REST) interface (Fielding, 2000) that is specifically intended to facilitate sharing of control information. The web service does not need to keep

external contextual information. Because a REST interface constrains messages to be self-descriptive, the communication is simplified because each query contains all the information needed to make a secure connection to get data. OpenSEG uses a Rainforest RAVEn™ dongle for acquiring data. Based on responses to a procurement held during this project, the RAVEn™ is the only commercially available equipment at this time that can acquire SEP 1.x data according to the needs of OpenSEG. **Error! Reference source not found.** summarizes distinguishing OpenSEG characteristics.

Table 2. Distinguishing characteristics: OpenSEG and other equipment

	OpenSEG (LBNL)
Acquires meter data in real time	✓
Filters for Simple Meter data cluster	✓
User-selected time intervals	✓
User-accessible data storage with interval data	✓
Length of local data cache	48 hrs.
Minimum smart meter sample time	4 sec.
Downloadable data formats	CSV, Green Button
Display data	On user-owned devices

The dongle itself is a necessary, but not sufficient, component of OpenSEG. The dongle is capable of distinguishing data from different ZigBee clusters, but is unable to filter except by explicit user selection of data clusters. The Simple Metering feature provides the ability to acquire just the consumption data after binding to the meter. The dongle has neither the ability to cache data nor does it inherently contain the ability to interact with a local network on its own. OpenSEG sends commands to the RAVEn™ to configure the data sampling interval, then stores the data retrieved from the meter via the RAVEn™.

In-Home Displays (IHD) produced by various vendors provide a running display of electric consumption at rates determined by manufacturers. At least one vendor (Rainforest Automation) has implemented web server features that provide similar data access semantics. We anticipate that, as the market for more detailed in-home energy displays grows, OpenSEG-like features will become more common.

Data storage

The OpenSEG data cache provides information about energy usage in the preceding 48 hours. Although the data rate can be selected by the user, incoming smart meter data are stored in a fixed-length data array that provides sufficient space to store two days of smart meter data read out at a maximum rate of one data read every four seconds. When this storage array is filled, the oldest data elements are discarded as new ones arrive—creating an "always present" cache of the last two days' data. Data are stored in the cache until it is requested by an authorized user (see Appendix B for details). The PULL architecture ensures that data are not widely published, but are instead "pulled" by authorized users.

Data access

By storing retrieved meter data locally on the OpenSEG platform, consumers can retrieve high-fidelity (i.e., frequent) energy consumption data for the most recent 48 hours. The amount of data and the length of time over which it is cached inside the gateway can be adjusted. Forty-eight hours was selected as a reasonable amount of time to provide a bridge between real-time data and archived Green Button formatted data available from most utilities via a website access. By choosing to record data in a circular cache so that more recent data writes over older data, we also eliminate data custodianship issues, which could arise if the data were pushed to the cloud for permanent storage.

OpenSEG data access mechanisms are intentionally simple: Access to archived meter data can be by absolute time, by reference to the current time, as a complete dump of cache contents, or as a single data point. Details are provided in Appendix B.

> **Absolute Time**. Data can be requested in absolute time by providing time values that represent the starting and ending time of the data measurement series of interest. This method provides the capability to extract data samples that correspond to the time surrounding a particular event or time of interest (e.g., "7 AM").
>
> **Current State**. Data can be requested for times relative to the present by providing time interval values that describe the time interval of interest relative to the present time. As expected, this access mechanism provides a convenient way to request data for the "past three hours" or the "previous 60 seconds."

Full Cache. An OpenSEG user may also request all data in the cache from the oldest data still remaining in the storage array to the present time.

Single Current Point. A request can be made to identify the smart meter electric data for the current time. This is the default if no time interval is specified.

Time stamps

Since unanticipated communications dropouts and/or smart meter/OpenSEG communications problems can create time intervals with missing data, measurement times are recorded explicitly. As a result, OpenSEG stores all consumption data measurements as value pairs that contain both a measurement value and a time stamp indicating the time of its acquisition.

Time information in the OpenSEG cache is unambiguously recorded using a well-understood and efficient format that is based on that commonly used in all Linux or Unix operating systems. This format represents time as a single 32-bit unsigned value that indicates the number of *seconds past the time of midnight January 1, 1970* (also known as Unix Epoch time). This time stamp can be readily formatted into more human readable representations that allow specific measurements to be displayed as values in the recent past (e.g., "2 hrs. 32 min. ago") or viewed as part of a historical timeline (e.g., "April 3, 2014, 2:30:45 PM"). Although the SEP 1.x firmware uses the same data representation for time stamps (namely, a 32-bit, unsigned number of seconds from an agreed-upon epoch data), the ZigBee Alliance/SEP 1.x group has chosen a different epoch date from that universally accepted within the Unix/Linux community. The SEP 1.x epoch reference time is midnight January 1, 2000. However, as long as these two reference dates remain unchanged, the OpenSEG platform can apply a simple correction to the smart meter time stamp data stream to allow it to be synchronized with data collected and reported by utilities. For example, midnight GMT October 1, 2014, would be represented as 1412121600. Table 3 shows sample data pairs from an actual OpenSEG monitoring of a small load. The first value of the data pair is typically power, measured in watts. Interpretation of the second (time) value is discussed below.

Table 3. Sample OpenSEG data and conversion

Sample OpenSEG data pairs		Converted time (second point)
4	1414444868	Oct 27 2014 14:21:08
4	1414444874	Oct 27 2014 14:21:14
5	1414444879	Oct 27 2014 14:21:19

5	1414444884	Oct 27 2014 14:21:24
5	1414444889	Oct 27 2014 14:21:29

With a reliable mechanism that allows storage and retrieval of second-based time stamps for measurement data, there is a need for a stable reference time source. While all computing platforms considered for implementing the OpenSEG platform have internal clocks capable of generating suitable time stamps, none were considered sufficiently stable to provide accurate readings that will not drift by fractions of an hour over the course of several months time. It is possible to configure operating systems to periodically query stable timeservers over wide area network connections and produce globally accurate time information, but this would require continuous internet access. Furthermore, during internet communications outages, the backup operational mode for these services is to use inaccurate local clocks with no reliable indication of when time synchronization was lost or regained.

Fortunately, the utility-connected smart meter itself provides consistent time synchronization to the OpenSEG platform. In addition to providing accurate digitization of instantaneous and integrated power consumption, the metrology portion of the modern smart meter maintains an accurate time base that allows each measurement to be properly time stamped. While these internal clocks can suffer the same long-term inaccuracies found on other computing platforms, all utility AMI systems have been designed to provide synchronization mechanisms that allow all meter time bases to function in lockstep. ZigBee SEP 1.x provides the means of communicating this same time reference with OpenSEG as is communicated to the utility back office billing programs over the AMI channel.

Conveying energy usage data with OpenSEG

OpenSEG supports energy usage data exchange using two data formats. The primary format is that sponsored by the U.S. Department of Energy: the Green Button format (www.greenbuttondata.org). Green Button is used by a large number of utilities to convey historical energy consumption information to end-user applications. This XML-based format intentionally contains a significant amount of metadata that describes the exact origin of the accompanying data, as well as information about its sample rate and measurement times. The inclusion of Green Button metadata in the OpenSEG output stream is intended to facilitate the comparison of local usage data with historical consumption data received from utility websites.

While the general acceptance of the Green Button data format is increasing due to widespread utility acceptance, it is fairly complex, and creates sizeable memory resource requirements for

applications using it. For simple devices, such as "refrigerator-magnet" energy displays, OpenSEG also supports a simple CSV (comma separated value) data format.

OpenSEG testing and installation

We tested OpenSEG and confirmed that it reliably binds to smart meters typically deployed in California (Silver Spring™ and Itron™), and conveys data consistently over extended time periods. Installation tests identified the need to "unbind" the RAVEn™ device from any previous settings before engaging with an IOU network. The general robustness of OpenSEG has been confirmed over an extended time (months). OpenSEG compares the periodic recorded energy data with the time integral of recorded power data as a check of data validity. Discrepancies between the two values would indicate missing data points.

We have been able to confirm the ability of OpenSEG to monitor and record appliance state changes in real time, provide reliable access to acquired data, and monitor for data dropouts. In the lab, reported data dropouts were determined to be minimal over periods of up to two weeks. As a practical matter, OpenSEG platforms placed approximately 25 feet from the meter to which they were bound but separated by plaster, wood, or glass window office wall materials had less reliable data transfer. Over 24 hours, we found approximately eight power consumption messages were lost via communications errors (< 0.05 percent). Despite these infrequent data losses, the communications channel recovered quickly, and normal operations resumed over the testing period.

CHAPTER 4: Summary and Next Steps

As discussed above, historically, digital near-real-time energy consumption data have not been widely available for electric energy users. Recently, digital smart meters have been installed in California to provide two distinct mechanisms for transmitting energy consumption data. This report describes the development of an Open Smart Energy Gateway that can securely collect high-frequency (to four-second intervals) electric use data using the ZigBee SEP 1.x capability installed in existing smart meters. The acquired data are available for display on user-owned devices via an application included in the OpenSEG deployment. OpenSEG has been designed and tested using smart meters in the lab and in homes in California by the major California utilities to confirm that it can reliably convey real-time energy and demand data to users over an extended time period.

Future work will include installation of these systems in a number of residential and small commercial settings, where more detailed tests of the ability of OpenSEG to work in different local area network setups and in different environments will be tested. Additional tests are contemplated to examine OpenSEG's capability to record energy use and storage data related to

electric vehicle charging. Future research is also needed to evaluate the use of OpenSEG in the use cases described above. These are:

- **Energy Use Monitoring.** OpenSEG provides a mechanism for consumers to collect near-real-time energy consumption data without the delays or latencies associated with it being transported to the utility data center and then back to the consumer's application.
- **HAN Architecture Enhancement.** OpenSEG provides a single point of access from the meter to the home, with all other home-based devices accessing meter data via OpenSEG. As such, it provides a clear distinction between utility-controlled assets and those controlled by consumers, while establishing a reliable, secure communication path between the two for further develop in HAN systems.
- **Verification of Aggregate Load Changes.** Signaling DR events was originally proposed via meter communications into a home. However, the OpenSEG architecture assumes that a more reliable and secure method for conveying DR signals is via IP. OpenSEG provides time-stamped energy consumption data that can provide (a) a commonly agreed-upon clock against which responses can be scheduled, and (b) confirmation of aggregate response to a demand-response event.
- **HAN Network Performance Monitoring.** Through a continuous comparison of time integrated power measurements with periodically reported energy measurements, OpenSEG provides a means by which the state of the HAN network can be directly monitored locally. Data dropouts can be seen via a lack of continuity in the comparison.
- **Aggregating Electric Metering for Ancillary Services and Fast DR Programs.** OpenSEG collects 10-second data that could be used to evaluate changes in electric load shapes. These data may be compliant with requirements by the California Independent System Operator for high-resolution electric load shape monitoring. Many buildings with these smart meters use over 100 kW, and the aggregation of a dozen or more small commercial buildings may provide a significant DR resource.

REFERENCES

California Public Utilities Commission. California Smart Grid, Annual Report to the Governor and the Legislature. May 2014. http://www.cpuc.ca.gov/NR/rdonlyres/2F5149C6-885A-4211-8CBA-A4F88F02CEA7/0/SmartGridAnnualReport2013final.pdf

Centerpoint Energy. Technical Overview of CenterPoint Energy's Interim HAN Interfaces. June 30, 2009.

Cleveland, F. White Paper for NIST CSWG: Home Area Network Cyber Security Requirements. Xanthus Consulting International. November 2009. http://xanthus-consulting.com/Publications/documents/HAN_Interface_Category_Cyber_Security_Requirements.pdf

Cooper, Adam. IEE (Institute for Electric Efficiency) Report, Utility-Scale Smart Meter Deployments, Plans, and Proposals. The Edison Foundation. May 2012. http://www.edisonfoundation.net/iee/Documents/IEE_SmartMeterRollouts_0512.pdf (retrieved 24 September 2014)

Dawson-Haggerty. S. sMAP: The Simple Measurement and Actuation Profile. 2012. http://pythonhosted.org/Smap/en/2.0/

Edison Smart Connect public information brochure. 2008.

Fielding, R. T. REST: Architectural Styles and the Design of Network-based Software Architectures. Doctoral dissertation, University of California, Irvine. 2000.

Gunther, Erich W. Edison SmartConnect™: Utility to Home Area Network Interface. May 24, 2007. https://docs.zigbee.org/zigbee-docs/dcn/07-5073.pdf

Lee, Annabelle, and Glen Chason. Smart Energy Profile (SEP) 1.x Summary and Analysis. National Electric Sector Cyber Security Organization Resource. October 2011.

Lewin, Doug, Bob King, Tony Marsh. An Update on Smart Energy in Texas. South-Central Partnership for Energy Efficiency as a Resource (SPEER). July 2014.

Montoya, Michael D., and Janet S. Combs. Southern California Edison Company's (U-338-E) Application for Approval of Advanced Metering Infrastructure Pre-Deployment Activities and Cost Recovery Mechanism. Filed December 21, 2006 with California Public Utilities Commission.

NAESB (North American Energy Standards Board). 2011. Energy Services Provider Interface (ESPI). https://www.naesb.org//ESPI_Standards.asp

O'Flynn, C. P. "Message denial and alteration on IEEE 802.15.4 low-power radio networks." 4th IFIP international conference on new technologies, mobility and security. February 2011.

Roche, Jim. "AMR vs. AMI" *Electric Light and Power* Vol. 13, No. 10. 2008. http://www.elp.com/articles/powergrid_international/print/volume-13/issue-10/features/amr-vs-ami.html

Searle, Justin, and Chuck McParland. HAN Attack Surface and the Open Smart Energy Gateway Project. Lawrence Berkeley National Laboratory Report. LBNL-6013E. May 2013.

Smart Meter Texas. Understanding Smart Meter Texas, Version 1.0, November 1, 2013 (See also Utility-Scale Smart Meter Deployments, Plans, Proposals, IEE Report, May 2012)

Sokullu R., O. Dagdeviren, and I. Korkmaz. "On the IEEE 802.15.4 MAC layer attacks: GTS attack." Second international conference on sensor technologies and applications. August 2008.

ZigBee Alliance. Smart Energy Profile Specification Revision 16, Version 1.1. 23 March 2011.

APPENDIX A: Software Specification for an Open Smart Energy Gateway (OpenSEG) Device

January 2015

Introduction and Overview

The Open Smart Energy Gateway (OpenSEG) facilitates the capture and display of near-real-time electricity consumption data acquired directly from smart meters. OpenSEG can stream data (energy- or power-consumption) from a ZigBee network interface card incorporated within an electronic interval power meter using industry standards for data security.

> *Electronic interval power meters (also known as* smart meters*) contain two radios for transmitting data acquired by the metrology component of the device: the AMI radio transmits over a secure line directly to the utility, and the ZigBee radio provides a signal that can be acquired by an appropriately configured Home Area Network (HAN) device. OpenSEG communicates with the ZigBee radio.*

OpenSEG is a software system typically implemented on a small hardware platform such as BeagleBone Black running Debian Linux. It is designed to acquire power and energy data from a smart meter, archive the most recent 48 hours of electrical consumption data, and present information, on demand, to users via a well-defined Application Programming Interface (API). In acquiring, formatting, and presenting the data, OpenSEG uses standard secure communications protocols—thus ensuring that access to consumer data remains under consumer control.

OpenSEG has the following elements:

- **Meter data access:** ability to acquire ZigBee SEP 1.x data and to choose the time increment for that data (typically set to 4 to 10 seconds, depending on the meter).
- **Data filter:** filter the SEP 1.x data model to gather only the data presented via the Simple Meter ZigBee cluster in order to maintain system security.
- **Data cache:** local circular data cache to store data from the most recent 48 hours.
- **Means for conveying data to consumers:** OpenSEG contains a webserver application to allow data access via the local web (typically WiFi using IP). Data can alternately be acquired via an Ethernet connection. A sample application built to this API is included in each OpenSEG device to allow a consumer to view their electricity consumption data.

Functionality

OpenSEG acts as a gateway between a utility-controlled ZigBee-based HAN and a local area network (LAN). The OpenSEG gateway contains an acquisition program and web server that

regularly polls the meter, stores acquired time and power or energy values locally in a 48 hour circular cache, and responds to web-based user requests for archived data.

The OpenSEG gateway, once properly configured, queries the meter via the ZigBee radio at programmed intervals. In support of this, an OpenSEG's ZigBee radio interface must be properly registered with the ZigBee network coordinator (typically the smart meter itself). This registration process is typically performed in coordination with utility customer support staff.

While much of OpenSEG's behavior is determined by its two required protocol stacks (ZigBee Pro and TCP/IP), the OpenSEG application provides the following functionality:

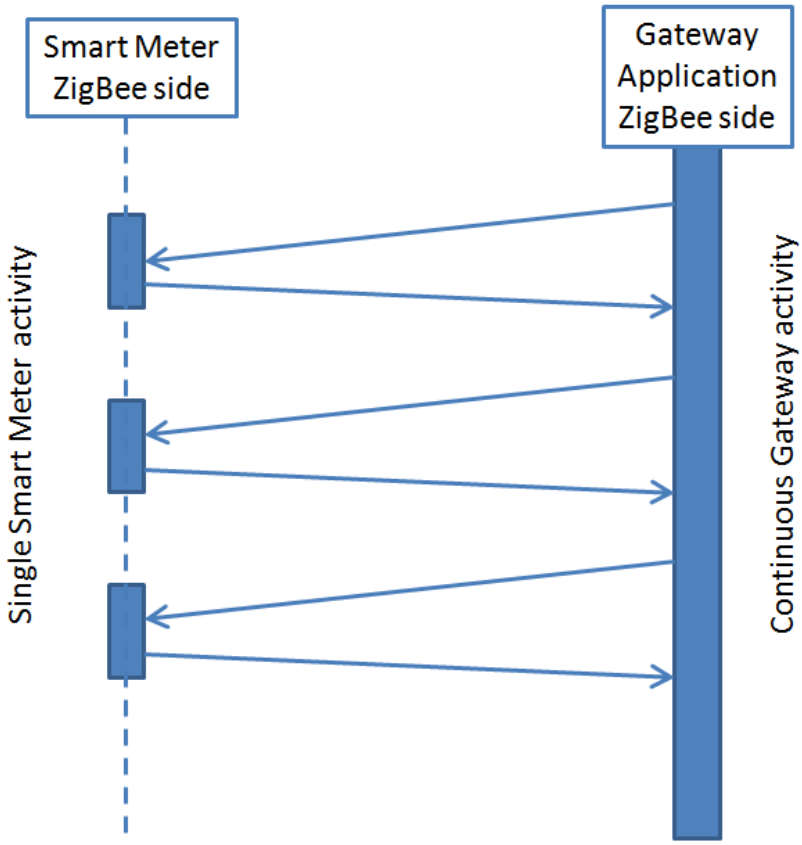
- The OpenSEG continuously polls the smart meter via the ZigBee radio for the current value of two specific C12 table entries. These entries correspond to instantaneous power demand (i.e., kilowatts) and current integrated energy (i.e., kilowatt-hours) as seen by the meter's metrology circuitry. These data are retrieved from internal meter tables and formatted for transmission by meter-specific ZigBee SEP 1.x programs. But, in all revenue meters investigated, values received by OpenSEG correspond directly to those contained in metrology tables.
- Data request rates are limited only by ZigBee SEP 1.x specifications and the capability of the Rainforest RAVEn™ dongle (currently one read every four seconds).
- Data resulting from each query is stored with a matching date/time tag acquired simultaneously from the smart meter's clock.
- Time tags for acquired data are provided by smart meter metrology circuits. Therefore, data time tags provided by OpenSEG will be consistent with utility-acquired data that flows from the smart meter back to utility billing centers over meter AMI communications networks. While there is no attempt to synchronize the time base of the OpenSEG computing platform (e.g., Linux) to that of the smart meter, the use of Network Time Protocol on the computing platform and utility-based time synchronization of smart meters typically results in system-level synchronization of better than 40 seconds.
- There is no requirement that the OpenSEG provide capability for long-term data logging or the ability to query readings for time intervals greater than 48 hours in the past (viz. the time of the actual data query): historical logging is supported only for the past 48 hours within the local OpenSEG cache.
- Once installed and in use, OpenSEG as designed should operate continually and reliably without user intervention. If power to the OpenSEG device is lost, then once it is restored, OpenSEG automatically attempts to reboot itself, attempts to rejoin the utility HAN, and (if successful) resumes meter query operations (as configured) on the restoration of power to the device and/or the smart meter.

To maintain data and network security, by design OpenSEG reads only a selected subset (Simple Metering Cluster) of the read operations implemented in the ZigBee SEP 1.x (ZigBee 1.0 specification, Document 075356r15, Annex D.3). No other SEP 1.x operations are required or

allowed by the firmware executing the OpenSEG application, except for meter data queries and ancillary messages needed for device and service discovery, and support of a limited number of Simple Metering Cluster read operations.

While OpenSEG can be implemented using a variety of ZigBee SEP 1.x communications platforms, all HAN activity except for those ZigBee Pro and SEP 1.x messaging activities required by this application should be disabled to maintain network security.

Missing Data: The HAN protocol stack within the meter is ultimately responsible for correctly responding to missed or corrupt packets. OpenSEG accumulates statistics for total and lost smart meter queries and indicates missing data via adjusted data time tags and the absence of a meter value for a given interval.



Acquiring Data via OpenSEG

Data acquired by OpenSEG is stored in the local circular 48-hour cache, with newer data overwriting older data. An OpenSEG API has been developed to describe how to access data in this cache. The API developed for OpenSEG assumes a PULL architecture, in which data are requested from the local cache. A PUSH architecture has been demonstrated for OpenSEG, but is not yet fully developed.

The API specification essentially defines the URL patterns (see REST API below) to which the gateway will respond. The current addressing scheme assumes that an OpenSEG gateway will contain data for, at most, one meter of a given type. At present, the OpenSEG gateway is assumed to only access the single electrical meter to which it is bound. (This restriction can be lifted if the case can be made for accessing multiple meters on a single gateway. To date, we have not identified such a case.)

Specifying Data to Be Acquired

Two options for acquiring data are available:

1. To obtain real-time energy consumption data (demand) measured by the meter to which the OpenSEG is bound via reading its ZigBee radio, use:

   GET meter/electricity/interval_reading/<format>/[<interval-sec>]

   Where

   - **<format>** is
     - csv for comma separated variable formatted data or
     - gb for Green Button formatted data (see section below)
   - ***<interval-sec>*** indicates the time interval, in seconds, for which data are requested. If present, the OpenSEG gateway will return data from the time interval between the time the request is received and the **<interval-sec>** seconds earlier.
     - Note that the enclosing brackets (**[]**) indicate the **<interval-sec>** argument is optional. If this argument is missing, a single value—the current meter reading—will be returned.

2. To obtain energy metadata for a particular energy consumption data stream, use:

   GET meter/electricity/meta_data/kvp/<key>

   If a request is made for metadata, the requesting REST message indicates the key for which the corresponding value is requested. Current valid metadata keys for the parameter <key> is one of the following character strings (without quotes).

   - "DateTimeInterval"
   - "Commodity"
   - "Kind"
   - "FlowDirection"
   - "PowerOfTen"
   - "UnitsOfMeasurement"

Metadata are returned in the form key=value. Note that keys and their respective values are character strings. Returned value strings are consistent with those contained in the NAESB "Energy Services Provider Interface Standard" (available at http://www.naesb.org/).

External Interfaces

The OpenSEG gateway has two primary external interfaces: the utility HAN and a local area network .

Utility HAN

The OpenSEG gateway device must be able to join the utility HAN as a conforming ZigBee Pro and SEP 1.x network device. This implies the following:

1. The gateway uses ZigBee/SEP 1.x communications devices that have been fully certified by the ZigBee Alliance and have received production-level ZigBee SEP 1.x security certificates from Certicom, Inc. It must be capable of being provisioned by the participating utility using their approved device installation procedure and be able to join and participate in their field-deployed HAN networks.
    a. To achieve enhanced levels of security associated with the OpenSEG design (e.g., reduced levels of functionality described above), the utility meter should only allow one HAN device—namely, the OpenSEG device—to be provisioned and join its ZigBee network.
2. The gateway device application-level firmware is capable of originating SEP 1.x-compliant queries for one or more elements of the smart meter's Simple Metering Cluster and successfully interpreting smart meter response messages.

Effectively this means that OpenSEG gateway ZigBee devices must be accepted by participating utilities for use within their networks. The typical OpenSEG gateway interacts directly with smart meters using a Rainforest RAVEn™ dongle that has been accepted by all California IOUs and many utilities outside of California.

Local Area Network (LAN)

OpenSEG can function as part of an 802.3 (Ethernet) or 802.11 (WiFi) network within the local area network. Given the relatively low expected data rates, minimal data rates for either of these media standards are adequate. OpenSEG functions with both static and dynamic IP addresses and is capable of auto speed negotiation (for 802.3 media) or acting as a secure (WPA2 PSK) wireless supplicant (for 802.11). OpenSEG interfaces comply with a number of widely used standards needed to function in a modern LAN environment such as TCP/IP, HTTP, and HTML.

OpenSEG Design Constraints

If the functionality described in this document is extended (e.g., data logging to a "cloud" application), these functions must be implemented in a way that does not impair the ability of the OpenSEG device to continually perform the actions described here. In particular, functions not related to those described in this document should not impair the device's ability to poll the meter at well-defined intervals and respond to data requests from sources within the local area network. If any added functionality introduces additional cyber-security risks, those risks are considered out of scope for this specification.

Data flow

By design, the OpenSEG program code makes a clear distinction between data acquisition + caching from the fulfillment of data requests from the cache. From a security perspective, the OpenSEG application follows the "only read from, never write to the smart meter" principle. At no time should the gateway application be permitted to transmit to the meter an SEP packet that will be interpreted as a "write" operation (as interpreted by any SEP cluster).

Electrical

OpenSEG's design aims to minimize power consumption. However, a battery-powered OpenSEG is discouraged because of the unpredictable processing load—and subsequent power consumption—that may be presented by certain display platform interactions.

OpenSEG Relationship to Existing Standards

ZIGBEE SEP 1.x

OpenSEG complies with published ZigBee Pro and SEP 1.x specifications for all communications on the utility side of the platform as known at the time of the OpenSEG development. Given the frequent changes of these documents, demonstrated compliance (i.e., ZigBee certification) with published specifications at the time of OpenSEG development cannot ensure interoperation with all utility smart meters. Specific local lab and field testing of OpenSEG with a particular utility's SEP 1.x implementation is the ultimate indication of compliance.

Transport Layer Security (TLS)

Once data are acquired from a meter and transmitted to a consumer, they become the property of the consumer and their protection is no longer a utility concern. However, OpenSEG provides tools that allow consumers to protect energy usage data within their own security domain.

OpenSEG supports TLS (Transport Layer Security) connections (e.g., HTTPS) for securing connections between the gateway and other nodes on the residential LAN. OpenSEG

communications containing energy usage data are encrypted at levels consistent with levels found in general e-commerce internet transactions. To eliminate the potential for non-authorized clients to access the gateway device, transactions between OpenSEG and an IP client should also implement appropriate authentication schemes. For example, such a scheme would require client nodes to present a known, correct user/password phrase pair as part of the HTTPS/REST request. Note, the OpenSEG specification does not require the use of client-side certificates to uniquely identify the requesting user. If required, user identity can be verified through the combination of server-side certificates (via HTTPS) and HTTP basic authentication.

REST Web Services

Representational State Transfer (REST) web services represent a simplified, lightweight methodology for implementing client/server web service transactions. Although REST services are built using standardized HTTP/1.0 elements, their syntax is not formally standardized. SSL/HTTPS is recommended to maintain data security. OpenSEG REST web service implementations are consistent with existing "best practices" as described in appropriate W3C documents (e.g., http://www.w3.org/TR/ws-arch), as known at the time of development.

Green Button Initiative

The ESPI-REQ.21 (NAESB) standard, which defines the underlying Uniform Resource Identifier (URI) and data formats for Green Button messages, was originally defined for generalized data exchange between data servers and multiple authorized third-party applications. It provides a secure process by which end users can give specific third parties authorized access to their energy consumption data. These standard developed authorization mechanisms assume large, enterprise-like IT environments that differ from those found in typical settings where OpenSEG is expected to be used.

Given the widespread encouraged use of the Green Button Initiative, OpenSEG provides an option to make acquired data available using published Green Button data formats and query semantics. In recognition of the different environment in which the smaller OpenSEG platform is expected to operate, the following adaptations are made:

1. **No specific mechanism is required for the exchange of an Authorized Third-Party ID with OpenSEG.** Authorized Third-Party IDs, which should conform to the published Green Button specification, can be exchanged between the OpenSEG and client application through any suitable—and secure—out of band mechanism. For example, gateways and client applications can be manually configured with suitable IDs. Or IDs can be based on client platform MAC or IP addresses.

2. **The historical database for OpenSEG is limited.** OpenSEG implementations are not required to provide historical data archiving capabilities beyond the 48-hour archive

inherent in its data cache. OpenSEG queries for times outside of this range will return a simple "data not found" response. As indicated above, when queried for smart meter data with a URI that *does not contain any time interval parameters*, all conforming OpenSEG implementations will respond with a single value that represents the current instantaneous value of the queried data value.

Green Button syntax[2] requires the query to indicate the (past) time interval for which data are being requested. Although we do not strictly follow the Green Button URL syntax, we remain conceptually consistent via some simplifying assumptions. The Green Button usage point is equivalent to the base URL of the OpenSEG gateway itself. For example, if the URL points to an OpenSEG gateway (Typical URLs might be of the form https://192.168.1.34 or, if DNS naming is supported, https://my_gateway.my_domain.org), that base URL represents the address of a Green Button usage point that can provide resource metering information. At present, minimal interest in accessing real-time metering information using Green Button formats has been seen, and this capability remains a program build-time configuration option.

Additional data formatting and query semantics between nodes on the LAN and the OpenSEG device should follow the patterns described in the Green Button initiative. Details on this specification can be found at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/GreenButtonInitiative. Additional information concerning the supporting ESPI-REQ.21 (NAESB) standard can be accessed at http://www.naesb.org/ESPI_Standards.asp.

Performance

OpenSEG and its associated application firmware are capable of the following:

- Through the use of ZigBee SEP1.x, continual, successful smart meter C12 table queries for a single table value at rates up to one query every four seconds.
- Responses to REST web service queries received from the residential LAN at rates of approximately one query every second.

[2] Green Button's data hierarchy—or "data tree" —starts with a "usage point" that defines the location at which commodities are "consumed." An example location could be a single residence identified by utility account information. From this root usage point, the hierarchy then specifies the particular commodity being measured and details about the measurement technology—for example, "electrical energy measured with revenue meter." Below this level lie metadata descriptions of various data measurement features (e.g., time interval between measurement values, units, etc.) and, separately, the actual interval data itself.

APPENDIX B: REST API Design

The OpenSEG is based on a PULL architecture, whereby data are requested from the cache. Since the OpenSEG acts as a web server that returns data in response to a simple REpresentational State Transfer (REST)-based web query, the API specification essentially defines the URL patterns to which the gateway will respond.

For simplicity's sake, the current addressing scheme assumes that an OpenSEG gateway will contain data for, at most, one meter of a given type. While a request will typically need to indicate interest in reading data from an electrical meter, there is no need to identify the particular electrical meter to be read; the OpenSEG gateway can only access the single electrical meter to which it is bound. (Note that this is a design choice. This restriction can be lifted if the case can be made for accessing multiple meters on a single gateway. To date, we have not identified such a case.)

Specifying Data to be Acquired

To obtain energy consumption data (i.e., real-time demand) from the single electrical meter serviced by an OpenSEG gateway, one of the two following APIs can be used, determined by the desired data format.

For comma separated variable (CSV) data:

> ***GET meter/electricity/interval_reading/csv/[<interval-sec>]***

For Green Button format data:

> ***GET meter/electricity/interval_reading/gb/[<interval-sec>]***
>
> **In both cases, <interval-sec>** indicates the time interval, in seconds, for which data are requested. If present, the OpenSEG gateway will return data from the time interval between the time of receiving the request and **<interval-sec>** seconds earlier. If this argument is missing, a single value—the current meter reading—will be returned. Note that the parameters **csv** and **gb** are used to identify the desired format for returned data, and the enclosing brackets (**[]**) indicate the optional **<interval-sec>** argument.

To obtain energy metadata for a particular energy consumption data stream, the following API can be used.

> ***GET meter/electricity/meta_data/kvp/<key>***

If a request is made for metadata, the requesting REST message indicates the key for which the corresponding value is requested. Current valid metadata keys for the parameter <key> are one of the following character strings (without quotes).

- "DateTimeInterval"
- "Commodity"
- "Kind"
- "FlowDirection"
- "PowerOfTen"
- "UnitsOfMeasurement"

Metadata are returned in the form key=value. Note that keys and their respective values are character strings. Returned value strings are consistent those contained in the North American Energy Standards Board (NAESB) "Energy Services Provider Interface Standard" (available at http://www.naesb.org/).

Green Button Data

Green Button's data hierarchy—or "data tree"—starts with a "usage point" that defines the location at which commodities are "consumed." An example location could be a single residence identified by utility account information. From this root usage point, the hierarchy then specifies the particular commodity being measured and details about the measurement technology—for example, "electrical energy measured with revenue meter." Below this level lie metadata descriptions of various data measurement features (e.g., time interval between measurement values, units, etc.) and, separately, the actual interval data itself. Green Button syntax requires the query to indicate the (past) time interval for which data are being requested.

Although we do not strictly follow the Green Button URL syntax, we remain conceptually consistent via some simplifying assumptions. For one thing, the Green Button usage point is equivalent to the base URL of the OpenSEG gateway itself. For example, if the URL points to an OpenSEG gateway (typically using URLs of the form https://192.168.1.34 or, if DNS naming is supported, https://my_gateway.my_domain.org), that base URL represents the address of a Green Button usage point that can provide resource metering information.

In the future, within the Green Button data model, additional parameters may be needed to specify the precise meter for which consumption data are being requested (at present it is only the specific meter to which OpenSEG is formally attached). These parameters would be added to the base URL to provide a complete specification (also referred to as "the path") to the requested data.