Green Button Data-Access Model for Smart Cities

Lessons Learned on Security, Transfer, Authorization, and Standards-Compliance in Sharing Energy & Water Usage Data

Cuong Nguyen
National Institute of Standards and Technology
Gaithersburg, Maryland, USA
cuong.nguyen@nist.gov

Jeremy J. Roberts
Green Button Alliance, Inc.
Raleigh, North Carolina, USA
jroberts@greenbuttonalliance.org

ABSTRACT

This paper provides a case study and lessons learned through the roll-out of the U.S. National Institute of Standards and Technology and U.S. Department of Energy Green Button electricity, natural gas, and water data-access initiative: to make readily available energy and water consumption data for consumers and third-party companies assisting mutual customers of utilities while protecting the security and privacy of the data. Energy and water usage data are important for smart cities in addition to individual consumers. Smart-city solutions rely heavily on the availability of such data to provide situational awareness as well as to inform control, actuation, and decision-making processes. However, the data need to be protected both for security and integrity. This paper presents a case study using the Green Button standard and the steps taken to ensure data security and privacy while enabling access to those consumption data by the consumer and third parties. Data security and privacy were achieved through use of the Green Button standard and subsequent implementation by the Green Button Alliance of a compliance-testing program. Considerations and solutions were needed for data in transit, data at rest, and the authorization mechanisms for allowing unregulated third-party companies to interface directly to utilities on behalf of the consumer while ensuring the consumer maintains complete control of what is to be shared and the ability to revoke that sharing at any time. The lessons learned from this approach could be applicable to other smart-city data.

CCS CONCEPTS

• Information systems → Data management systems → Data structures → Data access methods; • Information systems → World Wide Web → Web services → RESTful web services; • Security and privacy → Database and storage security → Data anonymization and sanitization

KEYWORDS

Green Button, Energy and Water Usage Data, Data Sharing, Data Security, Data Standard, Compliance Testing

SCC '19, September 10–12, 2019, Portland, OR, USA

ACM 978-1-4503-6978-7/19/09…$15.00
https://doi.org/10.1145/3357492.3358624

ACM Reference format:

Cuong Nguyen and Jeremy J. Roberts. 2019. Green Button Data-Access Model for Smart Cities: Lessons Learned on Security, Transfer, Authorization, and Standards-Compliance in Sharing Energy & Water Usage Data. In *Proceedings of The 2nd ACM/EIGSCC Symposium On Smart Cities and Communities, 10 September 2019 (SCC 2019). ACM, Portland, OR, USA, 6 pages.* https://doi.org/10.1145/3357492.3358624

1 INTRODUCTION

The Green Button initiative [1] was led and implemented by the U.S. National Institute of Standards and Technology (NIST), the U.S. Department of Energy (DOE), and industry partners in response to a White House call-to-action [2] to provide consumers with machine-readable energy-usage information in a standard electronic format. The ultimate goal of the initiative was to build an ecosystem that enables utility customers to have easy and secure access to their energy-usage information in a consumer-friendly and machine-readable format for electricity, natural gas, and water usage, and to readily and securely share this data with partners identified by the consumer. NIST identified energy usage information as a priority in its coordination effort with industry on smart grid interoperability standards under the Energy Independence and Security Act of 2007 [3]. The Green Button initiative leveraged the development of a standard for energy usage information. NIST led this effort with the public-private partnership known as the Smart Grid Interoperability Panel (SGIP)—now a part of the Smart Electric Power Alliance (SEPA)—that completed the North American Energy Standards Board (NAESB) REQ18/WEQ19 Energy Usage Information and REQ21 Energy Services Provider Interface (ESPI)/Green Button technical standards [4]. The Green Button standard(s) provided an extensible markup language (XML) format for data exchange. Beyond the standard, NIST (David Wollman, Martin Burns, and John Teeter) led the development team that worked on open-source reference implementations, test tools, and technical artifacts to support the creation of a Green Button ecosystem, and supported initial utility Green Button implementations in California and elsewhere. The next major step for the effort was to create an organization that would maintain the development and evolution of the standard and manage-and-grow the ecosystem. The Green Button Alliance (GBA) was formed as a non-profit organization with support from NIST, DOE, and industry partners.

There are two main methods for utility customer to obtain their Green Button data: Download My Data (DMD) and Connect My Data (CMD). DMD provides a mechanism for the customer to view and monitor their energy-usage information directly from a utility website or portal. CMD allows the customer to share their usage information with a third-party service provider, such as an application developer. One of the main focuses of the development was to ensure data security and privacy, to help address concerns that energy-usage data can be disaggregated to show the activities within a home; including whether the occupants are present [5]. Another focus of the effort was to create a testing program to assure that Green Button implementations conform to the standard, to improve interoperability within the Green Button ecosystem. The last major focus was to grow the Green Button ecosystem including to enhance the adoption and maintenance of the standard.

2 APPROACH TO PLATFORM STRUCTURE AND PLANNING

Significant planning and consideration went into determining the structure of energy-usage data. It was imperative to choose or create a format that would allow for future enhancements with backward compatibility. Electricity-usage data were the first data envisioned to be carried by Green Button, named after a government initiative for the sharing of Veteran Administration medical history information downloading known as the Blue Button [6]. Because the Green Button standards also included capability to handle other energy types, expansion of Green Button to include natural-gas data was quickly added, followed by water-usage data. Billing information and the concept of a split-and-parallel stream of data to carry personal information separate from the energy usage data were also implemented. Anticipating that there would be later additions—that were unknown at the time of inception—XML was deemed to be the most-flexible and readily available data-formatting language. It is one that could also be used with off-the-shelf tools and unaltered Web servers. The use of XML provided for a customer-friendly format, whereby the data are digital but can be read in a 'self-defining tag' system that allows people with an interest in the data to be able to see the data in a format that includes labels or tags without having to download or purchase a special parser. While XML is not visually friendly, it does allow for those who have an interest in understanding the underlying format to be able to view and interpret the data with an XML viewer or, with some difficulty, a text editor. Combined with XML Schema Definition (XSD) files—dictionary-like files that describe the format of the XML elements (tags), limits of values, and data types of values—most of the context of the data can be surmised.

The Atom Syndication Format, which acts as a wrapper to the Green Button -specific information, was selected to facilitate the ease of use in programming and conveyance of data using off-the-shelf tools that could already handle XML, since Atom itself is based on XML. Atom provided the ability to have data streamed without a need for defining a relational database structure or other non-flat file format but to still achieve the benefits of such non-flat relationships of data-to-other-data. XML transfers easily and can be parsed by most web servers without customization or need for add-on parsers. Atom parsers are readily available as well.

The U.S. Federal Government, along with some State and Canadian provincial governments, encouraged utilities and vendors to work together to make the Green Button a reality. The initial utility implementations of the standard were used to identify needed iterations in the standard. The advantage of this parallel activity was that the standard could be modified while it was being developed as things were discovered necessary or unnecessary in the implementations. The disadvantage was that there was no "gold standard" or "litmus test" for the implementations to mirror for interoperability. One lesson learned from this approach was that the latter disadvantage turned out to be greater than the advantage of parallel efforts due to the inability for third parties to create a single tool that would read and interpret data from multiple utilities without customization or tweaking of those data files. For most small companies, this proved too much of an effort to overcome with their limited resources.

Enhancements now (as then), come to the standard through an open workgroup known as the OpenADE Task Force (where ADE refers to automated data exchange) [7]. With industry and NIST leadership of OpenADE Task Force, both within the Utility Communications Architecture International Users Group (UCAIug) and its current home in the GBA, an effective forum was created to identify and track requested standards improvements. The OpenADE Task Force participation requires no membership, fees, commitments, or registrations by any company or individual. The results of these initial and subsequent enhancement efforts were given to the NAESB Energy Services Provider Interface (ESPI) Task Force (TF), a group of their Retail Electric Quadrant (REQ) and Retail Gas Quadrant (RGQ), which are focused on issues impacting the retail sale of energy to Retail Customers [8]. The ESPI TF was, and still is, used as the mechanism to standardize Green Button enhancements which are published and known officially as NAESB REQ.21 ESPI [9].

3 APPROACH TO THE PROTECTION OF PRIVACY/SECURITY

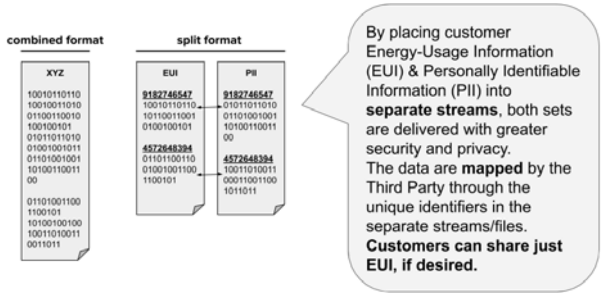
Security of customer energy-usage data and any personally identifiable information (PII) was a key and critical component of defining the solution for data in transit. While the Green Button standard scope of effort does not cover how data are to be stored at the utility nor at the third-party providing services for a mutual customer (data in situ), Green Button focuses on the security of these data in terms of their authorization and deliverance.

Green Button emphasizes five core tenets:

- multiple streams of data,
- adherence to modern web-transit standards,
- verification of party identity,
- the authority of the data custodian for customer verification, and
- the concept of customer consent and control.

3.1 MULTIPLE STREAMS OF DATA

As part of an approach to ensure that man-in-the-middle attacks do not breach entire sets of data, data in transit are separated into two streams: energy-usage information (EUI) and PII. In this way, any breach on one of the two data streams would not reveal the content of the other data stream. The information is obtained out of context of the other and usage data without context to whom it belongs, or personal information, like an address, without the associated usage values. Figure 1 below illustrates the separate streams of data. Security of customer energy-usage data and any personally identifiable information was a key and critical component of defining the solution for data in transit.



By placing customer Energy-Usage Information (EUI) & Personally Identifiable Information (PII) into **separate streams**, both sets are delivered with greater security and privacy.
The data are **mapped** by the Third Party through the unique identifiers in the separate streams/files.
Customers can share just EUI, if desired.

Figure 1: Split Data Format

3.2 ADHERENCE TO MODERN WEB-TRANSIT STANDARDS

In addition to the separation of data streams, security transit is ensured by the reference of NIST Federal Information Processing Standards (FIPS) 140-2 L1 cybersecurity standards [10] and use of the latest cipher suites on both ends—sending and receiving—and through the use of TLS 1.2 (or greater) and Certificate Authority - issued web certificates for the transfer of data. Figure 2 below illustrates the protection scheme for the data transfer.

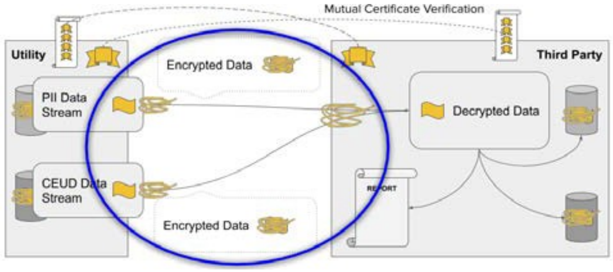


Figure 2: Encrypted Transfer

3.3 DOWNLOAD VS. CONNECT

As mentioned in an earlier section, the Green Button ecosystem is comprised of two different methods for obtaining data: (1) for a customer to download their data after defining the parameters of the scope of that data set and (2) for a customer to connect their data directly from the utility to a third- party provider after defining the scope of the data set. In the former method, DMD, there is no Alliance- or standards-defined way for obtaining these data; only for the format of these data in terms of the file structure. In the latter method, CMD, the Green Button defines the handshaking and exchange of these data in addition to the file (or stream) structure. While the workflows are different, the end goal is the same: that the customer is provided their data—either before analysis in the case of DMD or after analysis in the case of CMD.

Since DMD is nearly a subset of CMD, verification of party identity and the use of authorization are only necessary for CMD. There are inherent benefits of both methods—with DMD being easier from the standpoint of security and conveyance of data and CMD being more robust for continued access to data—but overall, CMD provides for an easier user experience at the expense of a greater development effort on the side of both the utility and the third-party provider for CMD deployment. Further, the workflows have different starting and ending paths, which must be considered in the development of a Green Button platform.

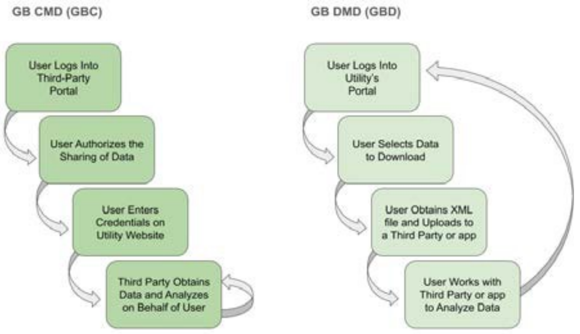

GB CMD (GBC)
User Logs Into Third-Party Portal
User Authorizes the Sharing of Data
User Enters Credentials on Utility Website
Third Party Obtains Data and Analyzes on Behalf of User
GB DMD (GBD)
User Logs Into Utility's Portal
User Selects Data to Download
User Obtains XML file and Uploads to a Third Party or app
User Works with Third Party or app to Analyze Data

Figure 3: Workflow of CMD and DMD

As shown in Figure 3, the workflow for CMD begins with a customer starting at a third-party provider's website where they would select their utility from a menu of utilities for which the third-party provider has a relationship; what is known as the third-party provider being already on-boarded with that utility (having met the technical and legal requirements set forth by the utility and/or jurisdictional authorities). The third-party provider would then direct the customer to the utility website with an application programming interface (API) call: essentially a web link and associated parameters. The API call would include the desired scope (the type of data, historical amount, interval, etc.). Subsequently, the utility would present the customer with verification screens for authentication (proof of the customer identity) and authorization (agreement to share the data scoped by the parameters in the API call). When complete (successful), the customer would then be sent back to the third-party provider's website using the provided return web link to complete the relationship with that provider.

Everything else is handled behind the scenes: the sharing of unique "tokens" for the establishment of the relationship in addition to the subsequent and ongoing data exchanges (more on that later). The customer would then utilize the services of the third-party provider for understanding their data.

The workflow for DMD begins by the customer/user logging into a utility's customer portal where they would select the data they wish to download, would obtain that data set as an XML file (or multiple XML files), and would then leave the utility's customer portal to go to a third-party providers portal or application where they would upload these data sets for their desired analysis and interpretation of their data.

3.4 VERIFICATION OF PARTY IDENTITY

Because the workflow for CMD includes the handshaking between utilities and third-party providers, verifying the identity of the other party can be an important addition to the security toolbox. Both utilities and third-parties can verify and prove the identity of their interfacing party by keeping repositories of each other's public certificates to ensure that the certificate chain is intact and that the entity interacting with them is that which is expected. This repository or databasing of certificates (or the databasing of digital signatures/thumbprints of a certificate) is an out-of-band exercise and thus by being out of band, can provide additional security at the expense of a manual process when those certificates change and need to again be shared with the interfacing party. The party-identity verification, as shown in Figure 4, would take place before any transfer of data between the utility and third-party to help in ensuring that the data in transit are in fact between those two entities.

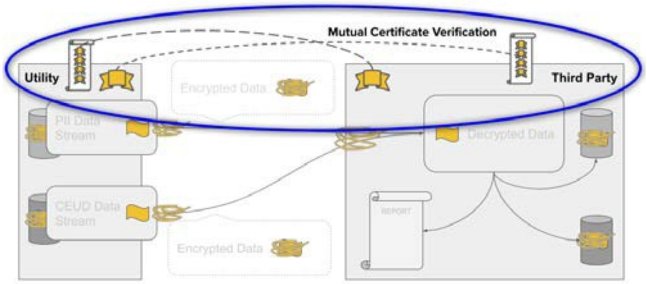


Figure 4: Mutual Certificate Verification

While data-at-rest is out of scope for Green Button, GBA and NIST have worked closely with the U.S. Department of Energy's DataGuard Energy Data Privacy Program [11] as a partner in promoting their *à la carte* menu of options available to utilities and third parties—as well as to commissions and jurisdictions—for ensuring the safeguarding of data in situ. GBA also recommends the separated EUI and PII in transit be kept separated in situ to keep a potential security breach of EUI confined to EUI without ownership (PII) and a potential security breach of PII confined to PII without context (EUI). Further, GBA recommends encryption- at-rest at both the utility and the third party; with independent, non-shared keys. That is, third-party providers would have no keys to the utilities' databases and utilities would have no keys to the third-party providers' databases.

3.5 THE AUTHORITY OF THE DATA CUSTODIAN FOR CUSTOMER VERIFICATION

In consideration of authorization for access, it was determined that the primary relationship for data sharing is between the utility (the Data Custodian) and the customer; more so than between the customer and the third-party, because the utility already has pre-established relationships with customers that include knowledge of their verified physical domicile and contact information. Therefore, it was decided for Green Button that the utility would act as an identity authority for data-sharing authorization by the customer; certainly, for DMD (as it is the utility's portal that the customer navigates) but as well for CMD representing the sharing of data with a third-party provider.

It has become commonplace for Google, Facebook, LinkedIn, and other online, identity-based companies to act as identity authorities for the ease and security of creating online accounts with disparate companies across the web; that is, to use, for example, LinkedIn credentials to create an account, log into that account, and share information with a website unrelated to LinkedIn—a website of a third-party provider—rather than creating a brand-new and separate account with that provider. The method for doing that is the Open Authorization (OAuth) [12] where authorization is granted by the customer for a defined scope of access and that authorization/scope combination is represented by a unique "token" used for subsequent reference of the authorization and its scope. OAuth 2.0 (the latest OAuth version at the time of this paper) is an ongoing effort of the Internet Society's Internet Engineering Task Force (IETF) OAuth Working Group [13].

3.6 THE CONCEPT OF CUSTOMER CONSENT AND CONTROL

Similar to the online identity-based social-media companies, utilities act as identity authorities for the sharing of electricity, natural gas, and water information with third-party companies that will be serving their mutual customers. Therefore, a customer can request the sharing of information with the third-party by authorizing that third-party access data on their behalf; data that are restricted by a given scope that can include the type of data (electricity, natural gas, and/or water), the interval of reading (e.g., monthly, daily, hourly), the level of personal information (e.g., service address, meter number, only usage data), and the duration of the authorization (e.g., one year, two years) if customer-initiated or utility-initiated revocation does not take place sooner. The result of that OAuth authorization is the unique token that is shared between the utility and the third-party provider of services—and no utility's customer-login information is shared. Thus, the sharing of data is always subject to customer consent and the customer always retains the right to determine the level of that sharing with the ability to revoke that relationship at any time. Revocation of third-party-provider access by the mutual customer occurs at the utility via OAuth.

Use of OAuth allows for yet-another-set of off-the-shelf tools in the Green Button ecosystem; making deployment on implementations easier and the user experience across the web more consistent [14]. However, today, not all methods of creating OAuth tokens are secure: The Green Button standard does not allow the use of the OAuth 2.0 "Implicit" method of token creation; a method which has enabled several known cybersecurity breaches. Further, no use of the OAuth "Resource Owner" method is allowed for Green Button; a method which allows the use of User ID and Password for authorization of tokens—a potential insecurity.

3.7 DESTRUCTION AND BACKUP OF DATA

Although not within the scope of Green Button, it is also important to consider the full data lifecycle including destruction and backup of data: Any customer- initiated destruction of third-party provider collected data would need to be ensured via local regulation or via third-party provider contract with the utility at the time the third-party provider was on- boarded as a viable party to transact with the utility's mutual customer. The availability/ability for a customer to download a backup of data—from either the utility or the third-party provider— should be instituted by local regulation and set forth to be made available in the standardized Green Button XML file format to allow comparison and/or porting of the data.

4 GREEN BUTTON TESTING AND CERTIFICATION PROGRAM

Testing and certification (T&C) program development is another critical component of the Green Button ecosystem. The standard provides the specifications and requirements for implementation. However, testing is needed to ensure that the product is implemented correctly in accordance with the standard's requirements. There are three types of T&C programs [15]. First-party certification is often known as "self-certification," where a manufacturer will attest that the product meets the requirements of the standard. Second-party certification is when a user tests and certifies the product; and in the case of the smart grid, it is mostly the utility that serves this role. Third-party certification is done through an independent authority that includes a certification body and associated test lab. The Green Button T&C was developed under the third-party structure with the UCAIug as the certification authority (administered by the GBA) and UL serving as both the certification body and the test lab. Most recently, GBA has taken the role of the certification authority and can also conduct testing, with the goal of the program being a cost- sensitive examination of implementations for compliance to the standard.

The T&C program-development effort was conducted in parallel with the standard development-and-enhancement to ensure that feedback from initial implementations could be incorporated into the standard. One effective approach was to develop the testing tools in an open-source environment that allowed the interested parties to contribute and use them. This has helped to speed up the testing of initial implementations. Also beneficial in driving the need for T&C development was information coming from hack-a-thons—gatherings of application programmers with the goal of determining interoperability between suppliers of data and readers of data.

4.1 LESSONS LEARNED

As mentioned in the discussion of the standardization effort, utilities (and vendors to utilities) were developing their Green Button implementations in parallel with the initial standardization effort. This resulted in DMD implementations that were producing customer usage files that were inconsistent with the format proposed in the standard XSD and inconsistent with the output of other utilities. In concert with the DOE and NIST, hack-a-thons were held to see how communities of interested parties would build the Green Button ecosystem.

The hack-a-thons had demonstrated that there needed to be more than standardization to ensure interoperability among implementations so that customization per utility was not necessary. While utilities were producing a file that would be used in a limited capacity geographically, third parties were expecting that their solutions could be rolled out to numerous customers in multiple geographies across North America and this was proven to be onerous without a way to ensure similar implementations by the utilities and the utilities' vendors.

It was upon the realization that there needed to be (a) a concerted and singular place for standardization efforts, (b) a way to verify and certify that implementations were compliant to the standard, and (c) a go-to place for finding reference implementations, technical support, educational materials, and collaboration, that the idea of a nonprofit organization to support the Green Button was conceived.

5 ECOSYSTEM DEVELOPMENT

Having a robust ecosystem is very important for any technology to maintain development and enhance adoption of that technology. Through the efforts of the initial participants, and those that were interested in unified implementations, the GBA was launched in February 2015 to provide these services. The Green Button ecosystem was conceived to be a public-private initiative that would serve as an initial model for subsequent public-private initiatives for the collective benefit of American citizens and be a part of smart-city solutions. The Green Button initiative is seen as a way to take private, corporate and individual goals under the wing of the government to foster the efforts into a single focus and then to spin it out into its own initiative of self-preservation and growth. The creation of the nonprofit GBA was the culmination of those efforts and the handoff of government assistance; allowing the industry to grow in the hands of the corporate and individual participants in a concerted and unified manner. The GBA continues these initial missions through the support of grants and primarily, through the membership of interested parties.

To date, the Green Button ecosystem has grown to include the United States, Canada, and the Republic of Korea; and it is being considered by other countries as a model for their own energy-data-sharing programs. Figure 5 below shows the geographic extent of the Green Button ecosystem. The GBA and its partners continue to work with interested parties to grow the ecosystem and encourage further adoptions.

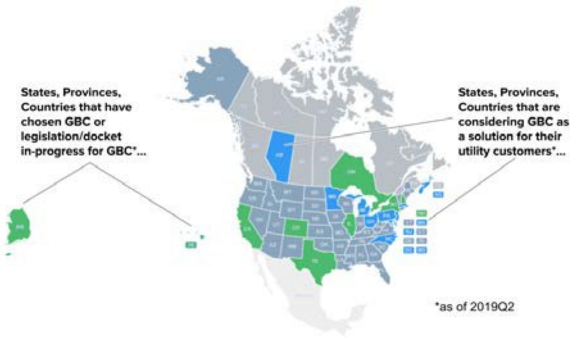

States, Provinces, Countries that have chosen GBC or legislation/docket in-progress for GBC*...
States, Provinces, Countries that are considering GBC as a solution for their utility customers*...
*as of 2019Q2

Figure 5: Ecosystem Map

6 CONCLUSION

The Green Button initiative for electricity, natural gas, and water data-access focused on freeing up consumption data. It provides a case study for the development and maintenance of a data-centric ecosystem. The first step of the initiative was a focus on the platform through the selection of XML as the data format. The next step was to standardize the requirements. This has helped with the initial implementation of products. A key aspect of the design was to ensure data security and privacy. The approach taken in Green Button is effective in ensuring security and privacy for the sharing of consumption data. The next important step was to develop a T&C program to assure that the implementation would be conformant to the standard. The last step was to form an ecosystem with a lead organization to further develop the technology and encourage further adoption. The lessons learned from this approach could be applicable to other smart-city data efforts as a model that addresses authorization, consent, and control in addition to cybersecurity when data access involves regulated and non-regulated entities' handling and sharing of data.

ACKNOWLEDGMENTS

Portions of this publication and research effort are made possible through the help and support of NIST via cooperative agreement 70NANB18H271. Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States. Certain commercial products are identified in order to adequately specify the procedure; this does not imply endorsement or recommendation by NIST, nor does it imply that such products are necessarily the best available for the purpose. The authors also acknowledge the significant contributions of NIST colleagues David Wollman and Martin Burns in their leadership of the Green Button initiative.

REFERENCES

[1] M.J. Burns, J.A. Teeter, and D.A. Wollman. Green Button: Building an Interoperable Ecosystem. Energybiz, 2014.

[2] National Science and Technology Council, A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

[3] Energy Independence and Security Act of 2007 [Public Law No: 110-140], Sec. 1305, http://www.gpo.gov/fdsys/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf.

[4] North American Energy Standards Board (NAESB) ESPI/Green Button Standard, http://www.naesb.org/ESPI_Standards.asp.

[5] F.G. Mármol, C. Sorge, O. Ugus, and G.M. Pérez. Do not snoop my habits: preserving privacy in the smart grid. IEEE Communications Magazine, 2012, 50(5), 166-172.

[6] Health IT Blue Button. https://www.healthit.gov/topic/health-it-initiatives/blue-button.

[7] OpenADE. http://osgug.ucaiug.org/sgsystems/OpenADE/default.aspx.

[8] The North American Energy Standards Board (NAESB) Retail Electric Quadrant. https://www.naesb.org//naesb-req.htm.

[9] NAESB Energy Services Provider Interface Model Business Practices. https://www.naesb.org/ESPI_Standards.asp.

[10] Federal Information Processing Standard (140-2). https://csrc.nist.gov/publications/detail/fips/140/2/final.

[11] DataGuard Energy Data Privacy Program. https://www.smartgrid.gov/data_guard.html.

[12] Open Authorization Framework. https://oauth.net/.

[13] Internet Engineering Task Force. https://www.ietf.org/.

[14] M.J Burns. How The Green Button Initiative Secured Its APIs With OAuth. ProgrammableWeb. https://www.programmableweb.com/api-university/how-green-button-initiative-secured-its-apis-oauth.

[15] ANSI/NEMA SG-IPRM 1-2016, Smart Grid Interoperability Process Reference Manual. https://www.nema.org/Standards/Pages/Smart-Grid-Interoperability-Process-Reference-Manual.aspx.