

**Pennsylvania Web Portal Working Group**

**Technical Implementation Standard**

**System-to-System Rolling 10-day**

**PUC Docket No. M-2009-2092655**

**Related Order Issued September 3, 2015**

# Table of Contents

[Table of Contents 2](#_Toc447196081)

[Version History 2](#_Toc447196082)

[Summary 3](#_Toc447196083)

[General Notes 4](#_Toc447196084)

[Secure Web Portal Standard 5](#_Toc447196085)

[StS Rolling 10-Day Usage File Examples 12](#_Toc447196086)

[Single & Multiple Meters (60 minute) 12](#_Toc447196087)

[Meter Change (60 minute) 12](#_Toc447196088)

[Meter Change w/Multiplier Change (60 minute) 12](#_Toc447196089)

[Net Metering (60 minute) 12](#_Toc447196090)

[Spring Daylight Savings Time (60 minute) 13](#_Toc447196091)

[Fall Daylight Savings Time (60 minute) 13](#_Toc447196092)

# Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of Change(s) |
| 0.1D | 3/17/2016 | Initial Draft Version |
| 0.2D | 3/31/2016 | Updated as follows:1. Corrected bullet numbering
2. Updated from 3/29 meeting discussion (1.2.10, 1.2.11, 1.2.15, 1.4.1)
3. Added requirement for EDCs to publish their specific data file formats in their user guide (1.2.18)
4. Added examples to end (p.12)
 |
| 1.0 | 4/5/2016 | No changes except version # and date. WPWG approved, final version for submission to PUC |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Summary

This document contains the technical standard developed by the Electronic Data Exchange Working Group’s (EDEWG) Web Portal Working Group (WPWG). The PaPUC required EDEWG to develop a standardized solution for the acquisition of historical interval usage and billing quality interval usage data via a secure web-portal, as specifically directed and detailed within the Pennsylvania Public Utility Commission’s (PaPUC’s) Smart Meter Procurement and Installation Order entered December 6th 2012 at Docket M-2009-2092655. Via Secretarial Letter dated 4/17/2014, in response to a request from EDEWG leadership, the PaPUC agreed that the contents herein would represent the minimally required standards to which each EDC’s solution must adhere, as opposed to standards applicable to a “standardized” solution common to all EDCs. Subsequently the PaPUC required EDEWG to develop standards for System-to-System (StS) functionality under Order entered and September 3rd 2015 at Docket M-2009-2092655.

This Technical Implementation Standard applies to the use of the StS Rolling 10-day method for sharing smart meter data. This method utilizes a “provide-and-park” approach, as opposed to a true system-to-system interface. The service allows an authorized user’s IT systems to communicate directly with the web portal system of the EDC (Electric Distribution Company) without requiring a user to manually log into the web portal itself and leverage the user interface. The EDC publishes a file that includes all available detailed bill-quality meter-level interval usage in hour-ending format for the set of accounts served by a particular EGS (Electric Generation Supplier) DUNS(+4) number on a specific usage delivery date. The EGS connects to the EDC’s system to retrieve the Rolling 10-day data file.

# General Notes

1. The following Electric Distribution Companies (EDCs) are required to support the System-to-System Web Interface:
	1. Duquesne Light Company
	2. First Energy (MetEd, Penelec, Penn Power, West Penn Power
	3. PECO
	4. PPL Electric Utilities
2. The web portal is intended for the following customer-authorized third parties: Licensed Electric Generation Suppliers (EGSs), Act 129 Conservation Service Providers (CSPs) contracted with the EDCs, and their contracted agents.   CSPs (either Curtailment or Conservation) desiring to access the web portals addressed by this framework either be provided access as agents of an existing EGS **OR** be licensed as EGSs themselves as a prerequisite to receiving access.
3. The PaPUC has not directed that this web portal use existing or potentially future EDC online customer communication platforms.
4. Any related items not specifically addressed by these standards are at the discretion of the individual EDCs.
5. Any change, modification or update to this data standard requires EDEWG approval via the change control process.

# Secure Web Portal Standard

**System-to-System (StS) Rolling 10-Day**

The Web Portal solution standard can be broken down into the following processes:

1. **Certification, Access, and Customer Privacy**
2. **Data Request**
3. **Data Response**
4. **Security and Technical**
5. **Tracking and Reporting**
6. **Certification, Access, and Customer Privacy**
7. Portal user eligibility
	1. Each request will be logged into a unique Web Portal for each EDC.
	2. The portal is “primarily intended for licensed EGSs and customer-authorized third parties”.
	3. Entities licensed by the PUC as an EGS are eligible to access the web-portal. (Licensee status is available on the PaPUC’s website at <http://www.puc.state.pa.us/consumer_info/electricity/suppliers_list.aspx>. )
		1. These include EGSs themselves, Conservation Service Providers (considered by PaPUC as “CSPs”), and demand response / load management providers (also known as Curtailment Service Providers, considered by PJM as “CSPs”). (Other third parties not considered PUC-licensed entities in this regard include but are not limited to researchers, public agencies with subpoenas, PaPUC-licensed Natural Gas Suppliers (NGSs), customers themselves, and other customer-authorized entities.)
		2. CSPs (either Curtailment or Conservation) desiring to access the web portals addressed by this framework either be provided access as agents of an existing EGS **OR** be licensed as EGSs themselves as a prerequisite to receiving access.
			1. The PUC has the authority to penalize EGSs for fraudulent operations.
			2. CSPs contracted with EDCs for Act 129 work are governed by PaPUC regulations over the EDC and the principal/agent relationship between the EDC and CSP.
		3. Unlicensed subcontractors or agents of licensed EGSs, such as Electronic Data Interchange (EDI) and billing providers, are eligible to receive access to the web portal on behalf of licensees that they represent, but their use must be directly associated with those licensees under the assumption that users are only accessing the portal in support of service to a specific licensed entity. For example, a provider obtaining usage for an account on behalf of fictitious supplier “ABC Energy” must be logged in such that the “ABC Energy” licensee is associated with and held accountable for associated use of the portal by that provider on ABC Energy’s behalf. *(This is covered in more detail in Section 2.5, Tracking and Reporting.)*
		4. The capability for other 3rd parties (entities not licensed by the PaPUC as EGSs) to access this information is outside the scope of the WPWG effort. Such entities are **NOT** eligible for access to the web portal and must obtain customer data via other means.
			1. Alternative means of obtaining customer data include contacting the customer directly or – at the discretion of the EDC – submitting requests to the EDC accompanied by proper Letters Of Authorization, or “LOAs” (i.e. Duquesne’s current process).
8. Access Management
	1. EDCs may provide access to the web portal for said EGS after verifying that the EGS is PaPUC-licensed. (Completion of EDI certification testing is not a prerequisite.)
	2. The EDC and EGS must complete and document a pre-production connectivity test, during which the EGS calls the EDC web service for at least one account number specified by the EDC and receives a successful response from the EDC.
		1. The EDC reserves the right to require EGSs to conduct more comprehensive testing and to require use of both test URLs and test credentials as part of that testing.
	3. 3rd parties that require Web Portal access but not full certification or treatment as an EDI-capable trading partner will have to submit a request to that EDC directly for web portal access. (The EDC must verify that the party is PaPUC-licensed as an EGS or broker/marketer prior to granting access.)
	4. The minimal requirement is for a single non-human system level user ID per PaPUC-licensed EGS entity.
		1. Each use of the portal is directly associated with exactly one PaPUC-licensed entity.
		2. EDCs will associate a unique non-human system level ID with an entity’s name and DUNS+4 number(s). (The user ID cannot be the user’s e-mail address.)

***NOTE:*** *EDCs may elect to implement system level IDs at the organizational level, meaning one system level ID per user regardless of the number of DUNS+4 entities associated with that user, dependent upon the feasibility and cost-effectiveness of this option.*

* + 1. The system user ID must be associated with a **non-public** e-mail address directly associated with either the licensed entity or the associated subcontractor/agent. (Examples of forbidden public e-mail addresses include but are not limited to Gmail, Yahoo, Hotmail, and AOL.)
		2. The EDC must document their process for maintaining the non-human system level ID credentials in the user guide.
			1. Scheduled interval of system level ID password resets. EDC must provide notice no earlier than 15 days prior to the reset event. In the event of a breach in security, the EDC may immediately reset the system level ID password and notify the EGS.
1. The EDC must publish and communicate availability of a System-to-System user guide for all portal users which covers the following:
2. Functional use of the solution
3. Any EDC-specific administrative or security conditions more stringent than the standards published in this document
4. The EDC must maintain, re-publish, and re-communicate the availability of the user guide as changes occur
5. The PaPUC will audit and if necessary pursue licensee organizations, not individuals.
6. Customer Privacy
	1. Prior PaPUC regulatory mandates require that the EDC make this data available to EGSs and place the burden of customer authorization on licensed EGSs and their agents, who are subject to PUC audit for the same.
	2. The Web Portal will adhere to the privacy standards mandated by the PaPUC regardless of the customer’s preference for release of information on file with the EDC.
7. **Data File Requirements**

Once an EDC has established System-to-System access to the Web Portal, the requestor will be able to access available data via an online, system based process.

1. The EDC must publish each file to a specified FTP site within its secure web portal, allowing only web portal users registered under that specific DUNS(+4) to have access to that particular set of usage data.
2. The EDCs reserve the right to publish multiple data sets with predefined volumes (i.e. X accounts per file) based upon their existing infrastructures
	1. The data set structure parameters must be included and maintained in the EDC’s user guide
3. The EDC must provide the usage data at the METER level.
4. On a daily basis (processing days only), the EDC must publish all available detailed bill-quality meter-level interval usage in hour-ending format for the set of accounts served by a particular DUNS (+4) number on a specific usage delivery date.
	1. The daily file publish schedule must be included and maintained in the EDC’s user guide.
5. Publication occurs over a rolling 10-day period with the EDC making best efforts to publish data for a given date as close to 48 hours following the last interval on that date as technically possible.
6. The EDC must remove older data in favor of more recent data as the rolling 10-day period renews itself over time.
7. The EDC must publish each file as a compressed, comma-delimited file (zipped CSV) based on the interval usage increments provided.
	1. For instance, an EDC with a portion of meters capturing 60-minute increments and another set of meters capturing 15-minute increments will publish the associated interval usage in a minimum two separate files, one presenting accounts for which 60-minute intervals are available and another presenting accounts for which 15-minute intervals are available.
8. Each file published will have a unique filename adhering to the following standard:

[EDC DUNS (+4)]\_[EGS DUNS(+4)]\_P[Publication Date]\_IU[Usage Date]\_[Interval Increment]\_[File #].zip

* 1. For instance, the first PECO 60-minite file for usage delivery date of 9/2/2014 that corresponds to EGS DUNS “123-45-6789-0123”, if published on 9/8/2014, would be named as follows: 007914468\_1234567890123\_P20140908\_IU20140902\_60\_01.zip
1. The same eligibility rules leveraged in providing historical usage in response to EDI-based requests apply when providing usage via the portal. (Example: PECO does not honor EDI-based historical usage requests on finalled accounts.)
2. For each account number where the EDC has data available the EDC will provide the usage data.
	1. Each file must include the following data elements:
		1. Customer identifier (varies by EDC; EDC account number is an example)
		2. Meter Number
		3. Usage Delivery Date (identical for all records)
		4. Multiplied Hour-Ending meter-level interval usage values. Detailed usage data, aka consumption or kWh, consisting of one day of bill-quality interval data available within 48 hours of the read that the EDC has not yet billed.
			1. EDCs will sign net metered (generation) values as negative.
3. Interval usage data shared that pertains to the standard originally required by March of 2014 must be billed data, defined as data from a billing cycle for which the EDC has already billed the customer.
4. This data is subject to change in the event that the EDC cancels and rebills those periods.
5. Data within 48 hours of the read must be “bill-quality”, defined as “data that is sourced from an EDC’s meter data management system that has completed the process of being verified, estimated, and edited” as cited from Page 16 of the PaPUC Final Order. This means that the EDC has not necessarily billed the associated period yet.
6. All timestamps presented in the portal should be presented in 24-hour Eastern Time.
7. All intervals must be presented in hour-ending format.
8. End of day hour ending label will be 2359
9. **NOTE:** The solution assumes that all EDCs bill a 24-hour period of usage on a midnight-to-midnight basis.
10. The Interval Usage data must accommodate Daylight Savings Time (DST) events on the appropriate date.
11. Spring DST – For the short DST usage delivery date only, the interval reading during the time event will be null. The DST intervals will be reported as follows:
	1. 60 minute – 0300 interval null
	2. 30 minute – 0230 and 0300 intervals null
	3. 15 minute – 0215, 0230, 0245 and 0300 intervals null
12. Fall DST – For the long DST usage delivery date only, additional interval usage values will be populated in the columns at the end of each record as a second set of data for hour-ending 0200, labeled 0200D (0115D, 0130D, 0145D). These columns will include null values for all other usage delivery days. The DST intervals will be repeated as follows:
13. 60 minute – 0200 interval repeated
14. 30 minute – 0130 and 0200 intervals repeated
15. 15 minute – 0115, 0130, 0145 and 0200 intervals repeated.
16. Precision of usage values will be dictated by the degree of precision available from each EDC’s AMI network. This solution will not dictate usage precision standards.
17. On-peak and off-peak characteristics of usage and demand are ***not*** necessary to include in the web portal, as these elements are typically tied to EDC tariffs. EGSs may calculate such components at their own discretion.
18. The EDC will document their individual data file formats for both the online and downloadable CSV responses in their web portal user guide.
19. **Security and Technical**

Customer data must be delivered with the highest integrity and privacy. The Security standards cover the standards, tools, and policies that will be considered for the exchange of this data.

Several of these standards are varied adaptations of the Guidelines for Smart Grid Cybersecurity published by the National Institute of Standards and Technology, or NIST. (NIST also refers to these guidelines as Interagency Report 7628, or NISTIR 7628.)

*NOTE: EDC policies and procedures, including but not limited to those governing information security and configuration management, may be more stringent than the standards identified in this section. In the event of contradictions between these standards and EDC policies and procedures, the more restrictive of the two shall govern.*

1. No data governed within the scope of these standards will be publicly accessible.
	1. Valid user login to an EDC’s secure web portal is required to access all related data.
	2. All other access must be denied.
	3. The user must log on each and every time they access the portal. (Any capability designed to “remember” the user should not preclude user logon.)
2. At a minimum, EDC portal solutions must be compatible with the two most recent major versions of Microsoft’s Internet Explorer web browser.
3. Each EDC’s portal solution requires the use of a non-self-signed SSL certificate issued by a Microsoft-trusted authority for governance of secure user connections via HTTPS, both before and after user authentication at logon. Both requestors and EDCs would be responsible for transmitting all data – both calls and responses – using SSL encryption.
4. The web portal will limit system level user to one concurrent session per credential.
5. The portal will lock out the system level user credential and prevent access if the system fails to successfully login with the same credential five times within a 30-minute period.
6. The EDC must notify portal users of any planned changes no later than two weeks prior to the planned implementation of those changes. (NOTE: This does not apply to implementation of added functionality that would have no impact on existing portal functions.)
7. If an EDC’s secure web portal experiences either technical problems or a cybersecurity incident (as defined by EDC information security procedures) which substantially disrupts portal operations OR increases the risk of compromising portal information (inadvertently allowing unauthorized users access to either customer usage data or user credentials), then the EDC must immediately perform the following:
	1. Deny all new attempts to access the portal by default.
	2. Communicate status to portal users and stakeholders as appropriate given the nature of the issue or incident.
		1. Avoid disclosing restricted details that could aid cybersecurity attackers.
		2. Consider EDEWG Leadership and PaPUC liaisons to EDEWG as impacted stakeholders.
	3. Leave the above restrictions in place until deeming that the issue has been resolved and that any associated risk has been sufficiently mitigated. (This will vary based on several factors, potentially including but not limited to identification of the source of the issue and the degree to which any collateral damage has been contained.)
	4. This standard does not supersede pre-existing EDC cybersecurity incident response plans. EDCs will always execute their own plans and rely on their own definitions with regard to cybersecurity incidents.
8. Data-at-Rest
	1. Defined as stored electronic information that is not in motion/transit, regardless of storage medium. Storage mediums include but are not limited to databases, file systems, storage networks, memory (temporary / cached or otherwise), and other writeable media.
	2. EDCs and third parties authorized to use these solutions (as well as their agents) will employ reasonable technological measures to properly secure related customer, account, and usage data-at-rest within the scope of these solutions. Such protections may include the use of encryption for rendering such data unusable, unreadable, and/or indecipherable to unauthorized individuals. Existing measures in place for this or other sensitive customer information procured via other means may also be sufficient.
9. **Tracking and Reporting**

*NOTE: The PA WPWG is not aware of any specific PaPUC reporting requirements relative to portal use and therefore assumes that the following standards would support any necessary ad hoc reporting for either EDCs or market participants on portal use and administration.*

1. The EDC must track the following portal-related event information on a per-user basis:
	1. User changes (user ID, associated entity, last updated date/time, add/update/terminate)
	2. User login attempts (user ID entered, login attempt date/time, successful/failed)
	3. Quarterly review status of licensed entities (user ID, attestation date/time)
2. The portal must perform all logging on the server-side.
3. The portal must retain all of the above portal-related event information for a period of at least three years.
4. Each EDC’s portal must provide the capability for users associated with each licensed entity to query and download any of the above portal-related event information within a specified date range for one or more users associated with that specific entity (but no others).
5. The EDC must have the capability to query and download any of the above portal-related event information for one or more users and/or licensed entities.
6. The portal must not allow any user, including EDC users, to directly edit the above log data.

# StS Rolling 10-Day Usage File Examples

**Example provided as reference only. Each EDC must provide individual data file format(s) in their user guide.**

## Single & Multiple Meters (60 minute)





## Meter Change (60 minute)





## Meter Change w/Multiplier Change (60 minute)





## Net Metering (60 minute)





## Spring Daylight Savings Time (60 minute)





## Fall Daylight Savings Time (60 minute)



