voltus

BETTER ENERGY • MORE CASH

NYISO Transmission Owner Integrations

Straw Proposal

April 2022

Agenda

- Issue Statement
- Networking Solution
- Telemetry Protocol
- Appendix

Issue Statement

- NYISO's DER Participation Model requires that participating **aggregators communicate directly with the Transmission Owners (TOs)**, either exclusively or in addition to the NYISO.
  - Ancillary Services Manual Section 6.2.3.9 allows up to 200 MW within NYCA to directly communicate with NYISO.
  - This 200 MW cap was hit in March 2022.
  - Now, resources must directly communicate with the TO.

- There are **two main issues to resolve to enable** Direct Communication with the TO:
  - **Networking Solution:** how does the data **travel** from DER/Aggregation to the TO?
  - **SCADA Protocol Choice: what content** is transmitted and how is it structured?
- Administrative tasks like **outage** and **offer management** are **outside the scope of this proposal**
- If adopted, this proposal could be rolled out **within 6 months**.

Do you agree with this scope?

Networking Solution: Proposal

- Proposed Networking Solution: **Encrypted TCP over the Public Internet**
  - All traffic would be going over the public internet using the TCP/IP stack.
- **Why?**
  - This would be the **most straight-forward option** for DERs to implement, since the option requires no custom hardware and minimal (compared to other solutions) setup.
  - Eliminate the **single point of failure** of relying on a single piece of hardware (MPLS node)
  - To **ensure secure communication**, TCP will be encrypted with certificates signed by the TO.
  - This is the approach **currently taken by the California ISO**

Networking Solution: Details

- Based on the approach in CAISO, the **process roughly breaks down:**
  - TO manages a custom root CA
  - TO provides a custom root certificate for DER to trust
  - DER would generate a private/public key pair
  - DER submits a CSR to the TO, signed certificate is used as the server certificate for the telemetry endpoint communicating with the TO
- Read more about PKI (public key infrastructure) CAISO public/private key instructions example
- More details on the CAISO setup are provided in the "CAISO Example" in the Appendix.

Telemetry Protocol: Proposal

- Proposed Telemetry Protocol: **DNP3**
- Why?
  - DNP3 is a lighter-weight protocol, compared to ICCP (currently used by NYISO)
  - DNP3 is a choice for some TOs communicating with the generators already
- TOs could standardize on usage of the DNP protocol and expose the point structure on the following slide
  - If individual TOs have a different set of points/point types, they can propose their own DNP3 configuration.

Telemetry Protocol: DNP3 Configuration

DER → TO

- Object 30/32, var 2 - 16 bit analog MW value, every 6 seconds
  - no deadband value, COMM_LOST flag set
  - **load (MW)**
  - **performance (MW)**
  - **baseline (MW)**

- Object 1/2, var 2 - binary input all variations, every 6 seconds
  - **breaker status** - on/off may not be required for DER or Demand response)

TO → DER

- Object 41, var 2 - 16 bit analog output, polled every 6 seconds
  - **6 sec baseline (MW)**
  - **5 min baseline (MW)**

Questions or Comments?

email regulatory+nyiso@voltus.co

Appendix

CAISO Example: Background

- Voltus completed our interconnection with CAISO in summer 2021.
- We believe that CAISO leads by example and removes significant boundaries for DER participation by using modern technologies.
- We are certain that CAISO requirements for direct telemetry implementation are compliant with CIP-012.
- At a high level, CAISO telemetry allows for the approach advocated above: DNP3 over encrypted TCP/IP secured with PKI.

CAISO Example: Networking

All traffic would be going over the public internet using the TCP/IP stack.
To ensure secure communication, TCP will be encrypted with client certificates signed by the TO.

- TO manages a custom root CA

CyberTrust-issued SHA2 custom root CA (read more about CAISO use of certificate authorities here)

- TO provides a custom root certificate for DER to trust
- DER would generate a private/public key pair

Read more about PKI (public key infrastructure)
CAISO public/private key instructions example

Key Generation Requirements:

- The participant must use RSA keys with a key length must be a minimum of 2048 bits.
- The participant must store the private key securely, i.e. using AES-256 encryption.
- DER submits a CSR to the TO, signed certificate is used as the server certificate for the telemetry endpoint communicating with NYISO

Certificate Signing Request (CSR) Requirements:

• The common name (CN) should reflect the server's DNS host name. In the case of a RIG, the common name of the RIG is provided in the RIG database documentation
• The CSR must be generated according to the Public Key Cryptography Standard #10 (PKCS #10).

CAISO Example: Business Practice Manual Quotes

- CAISO recommends the following security considerations for integrating assets (section 4.7)

- **Section 2.2.3**

  The ISO is open to any way of connecting to a Participating Generator's current control system and communication infrastructure to communicate to the ISO EMS as long as the Participating Generator meets the security and operational objectives for direct telemetry.

- They outline improvements of reliability over the public internet and the choice to make communications accessible to open the market to more DER participation

CAISO Example: Business Practice Manual Quotes

- **Section 4.2**

  Over time, the reliability of the public Internet has improved but cyber threat to public networks has increased. Concurrently, the operational cost of leasing use of semi-private networks such as the ECN has increased relative to the cost of employing the various software-defined security overlays now available on public networks for connecting remote locations. **Driven by Cloud computing, public networks continue to evolve to support secure and cost-efficient interconnection.** The ISO continues to adapt to provide increasingly more cost-effective communications options that reduce barriers to participating in ISO markets.

  …

  In 2016, the FERC approved a new type of ISO market participant called a Distributed Energy Resource (DER) Aggregate (DERA). The aggregation point is a market resource. Participants in the market asked the ISO to evaluate new options for securing DERA telemetry in order to reduce barriers to entering ISO markets. Specifically, prospective participants sought to use their existing Internet broadband, instead of the ECN, to the ISO; these participants also requested an alternative to participant-managed PKI. The ISO has responded by adding two communications options secured on the public Internet, one of which continues to require use of digital certificates.

CAISO Example: Business Practice Manual Quotes

The following are outlined as acceptable modes of network solutions for direct telemetry

Section 5.3.2

The ISO supports three transport options for direct telemetry:

1. ECN with T1 leased circuit.
2. Public Internet with ANIRA IPsec VPN backhaul to ECN.
3. Public Internet.

…

Option three requires the Participating Generator to provide a broadband circuit to the Public Internet. The Participating Generator **does not need to lease** a T1 circuit but **does need to manage an ISO-issued digital certificate** to secure the communication link.

References:

- [1] CAISO Digital Certificates Page
- [2] Business Practice Manual - Direct Telemetry