**DER Aggregator-Distribution Utility Bidirectional Market Based Information Communications Use Case**

**Description:**

This use case addresses the bidirectional market-based electronic information exchanges between a DER Aggregator and a Distribution Utility to conduct transactions for sales of distribution grid services that fall under state or local jurisdiction. Based on the NAESB Base Contract for the Sale and Purchase of Distributed Grid Services from DER Aggregations, which includes provisions for parties to use secure electronic communications (ECS) to exchange applicable information under the contract, and the Enabling Distribution Non-Wires Solutions Use Case in the NARUC Grid Data Sharing Playbook, the participants identified broad categories of information that these parties will likely need to communicate using known communication and security standards and protocols currently used by industry, and cybersecurity considerations related to the protection of the data in transit and the communication itself.

The participants used this feedback to create the Bilateral Market Based Information Communications use case between a Distribution Utility and DER Aggregator Use Case. Additional information is needed regarding business requirements and processes to help identify specific cybersecurity protections and protocols that should be considered for inclusion in any developed NAESB Business Practice Standards.

|  |  |  |  |
| --- | --- | --- | --- |
| **DER Aggregator-Distribution Utility Bidirectional Market Based Information Communications** | | | |
| Cybersecurity Considerations/Goals | Comm & Security Standards/Protocols | Comments | Related Business Processes and Requirements |
| * Confidentiality of sensitive information, including entity identifiers and account information * Availability of communications infrastructure * Integrity of data * Identification and authentication of parties (e.g., X.509 v3 certs for authentication) * Authorization of parties (e.g., OAUTH) * Validated delivery of message, including a time stamp * Expected duration of cybersecurity protection (e.g., key size, key duration, key lifetime) (Need to distinguish between symmetric and asymmetric cryptography. Symmetric may require longer key sizes *when quantum computing is a reality*. The asymmetric quantum algorithms have been defined by NIST.) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN * TLS * IPSec * VPN | * May be variety of implementations that are not consistent * Uniformity and consistency in standards use * Standardized approach creates efficiency and benefits stakeholder * Investigate real-time versus non-retail communication differences and cybersecurity needs * Need understanding of business requirements |  |

**Discussed Categories of Potential Data Exchanges between Parties:**

| *Category of Information* | *Data Owner/Controller* | *Receiving Party* | *Cybersecurity Considerations* | *Communication/Security Protocols in Use* | *Comments* |
| --- | --- | --- | --- | --- | --- |
| **Billing & Payment Information Communications** | Distribution Utility | Aggregator | * Confidentiality of sensitive information, including entity identifiers and account information * Availability of communications infrastructure * Integrity of data * Identification and Authentication of parties (e.g., X509 certs for authentication) * Authorization of parties (e.g., OAUTH) * Validated delivery of message, including a time stamp * Expected duration of cybersecurity protection (e.g., key size, key duration, and key lifetime) ((Need to distinguish between symmetric and asymmetric cryptography. Symmetric may require longer key sizes when quantum computing is a reality. The asymmetric quantum algorithms have been defined by NIST.) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN * TLS * IPSec * VPN | * May be variety of implementations that not consistent * Uniformity and consistency in standards use * Standardized approach creates efficiency and benefits stakeholder |
| Aggregator | Distribution Utility |
| **System/Outage Information Communications** | Distribution Utility | Aggregator | * Availability and integrity of data * Confidentiality of sensitive information, including entity identifiers and account information * Disruptive activities (e.g., denial of service) * Timeliness and time sensitivity (e.g., timestamps) * Authentication of parties * Authorization of parties * Reliable delivery of message * Expected duration of cybersecurity protection (e.g., key size) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN | * Investigate real-time versus non-retail communication differences and cybersecurity needs * Need understanding of business requirements |
| Aggregator | Distribution Utility |
| **Aggregation Information Communications** | Aggregator | Distribution Utility | * Availability and integrity of data * Confidentiality of sensitive information, including entity identifiers and account information * Timeliness and time sensitivity (e.g., timestamps) * Disruptive activities (e.g., denial of service) * Authentication of parties * Authorization of parties * Reliable delivery of message * Expected duration of cybersecurity protection (e.g., key size) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN | * Investigate real-time versus non-retail communication differences and cybersecurity needs * Need understanding of business requirements |
| **Aggregation Availability Communications** | Aggregator | Distribution Utility | * Availability and integrity of data * Confidentiality of sensitive information, including entity identifiers and account information * Timeliness and time sensitivity (e.g., timestamps) * Disruptive activities (e.g., denial of service) Authentication of parties * Authorization of parties * Reliable delivery of message * Expected duration of cybersecurity protection (e.g., key size) | * REQ.21 ESPI * Secure FTP / SSH / HTTPS * HTTPS posts * FTP * EDI / VAN * SD WAN | * Investigate real-time versus non-retail communication differences and cybersecurity needs * Need understanding of business requirements |