Pacific Northwest
NATIONAL LABORATORY

PNNL-32413

Universal Utility Data Exchange (UUDEX) – Workflow Design – Rev 1

Cybersecurity of Energy Delivery Systems Research and Development

December 2021

SA Neumann
CM Schmidt
ML Cohen
S Sridhar
SR Mix

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-OE0000190

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

Universal Utility Data Exchange (UUDEX) – Workflow Design – Rev 1

Cybersecurity of Energy Delivery Systems Research and Development

December 2021

SA Neumann
CM Schmidt
ML Cohen
S Sridhar
SR Mix

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Revision History

Revision	Date	Deliverable (Reason for Change)	Release #
0	11/15/2019	Initial draft	PNNL-29417
1	12/2021	Updates based on implementation	PNNL-32413

Summary

This workflow design document describes the process of establishing a Universal Utility Data Exchange (UUDEX) Connection between two or more UUDEX Endpoints.

The existing processes required to establish a data link using Inter-Control Center Communications Protocol (ICCP) are very time consuming, from both the perspectives of effort and calendar time. The intent of UUDEX is to provide a more streamlined alternative.

The UUDEX workflow is also used to establish UUDEX Connections to exchange data other than that found in traditional ICCP data exchanges such as exchanges of power system model files, security events and mitigations, disturbance reports, and market data.

Terms, Acronyms, and Abbreviations

The following terms and acronyms are relevant to this specification:

ACL	Access Control List
Alert	A notification that conveys important information, typically where an action should be taken by a user
API	Application Programming Interface
Application	A software component that provides end use functionality for a participant, which may be a source or target of information conveyed through the UUDEX Framework
ASCII	American Standard Code for Information Interchange, as defined by ISO/IEC 646
CIM	Common Information Model, as defined by EPRI, the Utility Communications Architecture Users Group and as used by IEC 61968 and 61970 series of standards
CIP	Critical Infrastructure Protection
Consumer	A subscriber for information, subscribes to a subject and consumes information that has been published
CSV	Comma Separated Values, as defined by IETF RFC 4180
DOE	U. S. Department of Energy
ICCP	Inter-control Center Communications Protocol, also known as TASE.2 or IEC 60870-6
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standardization Organization
JSON	JavaScript Object Notation, as defined by IETF RFC 7159
NERC	North American Electric Reliability Corporation
Notification	Any message or signal that is generated asynchronously to report a condition of potential interest to users
OE-417	DOE Electric Emergency Incident and Disturbance Report
PDF	Portable Document Format, as specified in ISO 32000
Publish	To produce information by sending it to a subject
RFC	Request for Comment – Used in reference to published IETF standards, which are called RFCs
Subscribe	To consume information by receiving the information published to a subject
TASE	Telecontrol Application Service Element

TASE.2	Synonym for ICCP
Time series	A sequence of data values captured at different points in time that are telemetered, measured, or calculated that represent some aspect of the state of an object.
URL	Universal Resource Locator
UUDEX	Universal Utility Data Exchange
W3C	World Wide Web Consortium
XML	eXtensible Markup Language, as defined by the W3C

UUDEX Roles and Definitions

UUDEX Administrator	Administrative users that have global responsibility for a UUDEX Framework, and can authorize UUDEX Participants
UUDEX API (U-API)	A set of parameterized instructions that UUDEX Endpoints and UUDEX Infrastructure use to interact with each other. UUDEX APIs are abstract definitions, rather than detailed functions in a particular programming language.
UUDEX Component (U-Component)	An individual hardware or software element that supports the functioning of the UUDEX Infrastructure
UUDEX Connection (U-Connection)	A communication channel between a UUDEX Participant and the UUDEX Infrastructure that conforms to all UUDEX requirements (e.g., security, performance).
UUDEX Consumer (U-Consumer)	A consumer of information, receives information from a UUDEX Subject.
UUDEX Data Element (U-Data Element)	Any data collection conveyed over UUDEX Exchanges.
UUDEX Data Element Type (U-Data Element Type)	A defined structure and format for specific classes of UUDEX Data Elements. Each UUDEX Instance defines its own set of supported UUDEX Data Element Types.
UUDEX Endpoint (U-Endpoint)	An entity that produces or consumes UUDEX Data Elements through interactions with a UUDEX Subject.
UUDEX Exchanges (U-Exchanges)	A communication UUDEX Participants and the UUDEX Infrastructure where all communicants are acting as elements of a UUDEX Framework (i.e., excludes out-of-band exchanges between UUDEX Participants). The UUDEX Exchange will involve one or more UUDEX Connections and communications will only occur over UUDEX Connections.
UUDEX Framework (U-Framework)	Includes the totality of UUDEX, specifically UUDEX Infrastructure, UUDEX Endpoints, UUDEX APIs, UUDEX Participants, UUDEX Protocols, UUDEX Communication Fabric, and UUDEX Information Models.

UUDEX Header (U-Framework)	The portion of a UUDEX Message that contains metadata about the message exchanged between UUDEX Endpoints. The UUDEX Header controls behaviors associated with the delivery of the UUDEX Data Element. The UUDEX Header may be discarded when the UUDEX Data Element arrives at its destination, or its contents may be used to validate the UUDEX Message or other processing.
UUDEX Identity Authority (U-Identity Authority)	An entity that creates, certifies, manages, and revokes UUDEX Identity Objects. In effect, it serves as an identity authority within a UUDEX Instance.
UUDEX Identity Objects (U-Identity Objects)	A type of UUDEX Data Element that contains information necessary to authenticate the identity of a UUDEX Participant.
UUDEX Infrastructure (U-Infrastructure)	The servers, communication fabric and other hardware pertaining to UUDEX. Those UUDEX components that permit the management and flow of information to and from UUDEX Endpoints. These components provide a variety of services and are typically replicated for availability purposes.
UUDEX Instance (U-Instance)	A collection of connected UUDEX Participants that is closed with regard to its trust environment. A UUDEX Instance is defined by a set of identities within a UUDEX Infrastructure where those identities are only valid within that UUDEX Infrastructure and no other identities are valid within that UUDEX Infrastructure.
UUDEX Message (U-Message)	An instantiation of the data in a UUDEX Subject that is comprised of a UUDEX Header and a UUDEX Payload.
UUDEX Message Envelope (U-Message Envelope)	A structure of a UUDEX Message that is wrapped around a UUDEX Data Element while the UUDEX Data Element is in transit over a UUDEX Connection.
UUDEX Notification (U-Notification)	A response message sent by the UUDEX Infrastructure in response to a subscription match that indicates the presence of a UUDEX Data Element but does not contain the UUDEX Data Element's data.
UUDEX Participant (U-Participant)	An organization that is a onboarded member of a UUDEX Instance.
UUDEX Participant Administrator (U-Participant Administrator)	An administrative user that performs activities related to the to the publication and consumption of information for a given UUDEX Participant.
UUDEX Payload (U-Payload)	The portion of a UUDEX Message conveying the information exchanged between UUDEX Endpoints.
UUDEX Producer (U-producer)	A publisher of information, sends information to a UUDEX Subject.

UUDEX Protocol (U-Protocol)	The set of messaging patterns, message structures, UUDEX APIs, and common data structures outline in the UUDEX Protocol Design document.
UUDEX Server (U-Server)	A UUDEX Component that stores data, receives data from UUDEX Producers, delivers data to UUDEX Consumers, and maintains UUDEX Subjects and associated prioritization and access control policies. In general, the UUDEX Infrastructure abstracts the concept of the UUDEX Server, allowing UUDEX Endpoints to engage with the UUDEX Infrastructure without tracking individual UUDEX Servers.
UUDEX Subject (U-Subject)	A UUDEX Subject is the basic unit of storage, access. and organization in the U Infrastructure. Data is published by a UUDEX Producer to a UUDEX Subject and delivered to a UUDEX Consumer by queueing it to a UUDEX Subscription. The ability to publish or subscribe to a UUDEX Subject is controlled by access control policies
UUDEX Subscription (U-Subscription)	The means by which a UUDEX Consumer retrieves UUDEX Messages published to a UUDEX Subject.

These terms pertaining to UUDEX roles and definitions are defined in Section 4 of the *UUDEX Functional Design Requirements* document.

Contents

Revision History ii
Summary iii
Terms, Acronyms, and Abbreviations iv
Contents viii
1.0 Introduction 1
2.0 Principles 4
3.0 Scope 5
4.0 Processes 6
4.1 Configuration 6
4.2 Initialization 7
4.3 Security configuration 8
4.4 UUDEX Participant Onboarding 9
4.5 UUDEX Subjects and UUDEX Data Sets 10
4.6 Endpoint Definition 10
4.6.1 UUDEX Producers 12
4.6.2 UUDEX Consumers 15
4.6.3 UUDEX Infrastructure 16
4.7 Publication 16
4.7.1 Models 17
4.7.2 Measured Values 17
4.7.3 Documents 17
4.8 Discovery 18
4.9 UUDEX Subscriptions 18
4.10 Resiliency 21
4.10.1 Data Source Selection 21
4.10.2 Redundancy 21
4.10.3 Consensus 21
4.11 Monitoring and Management 22
4.12 Testing and Verification 23
5.0 User Interfaces 24
5.1 Roles 24
5.2 Core functionality (minimum requirements) 24
5.2.1 UUDEX Administrator 24
5.2.2 UUDEX Participant Administrator 25
5.3 Notifications 26
5.4 Third-Party User Interfaces 28
6.0 Application Programming Interfaces 29

7.0 Monitoring/Diagnostics/Testing....30
8.0 Extensions....31
9.0 References....32
Appendix A – Existing Industry Organizational and Personnel Vetting Procedures A.1

Figures

Figure 1-1: UUDEX Framework....2
Figure 4-1: UUDEX Infrastructure....7
Figure 4-2: Update of ACLs....8
Figure 4-3: UUDEX Participant Onboarding....9
Figure 4-4: Defining Endpoints....12
Figure 4-5: Simple UUDEX Producer....13
Figure 4-6: Publication by Peer Producers....14
Figure 4-7: UUDEX Consumers....16
Figure 4-8: Document Conveyance....18
Figure 4-9: UUDEX Subscriptions....19
Figure 4-10: UUDEX Endpoint Monitoring....23
Figure 5-1: UUDEX Administrator Actions....25
Figure 5-2: UUDEX Participant Administrative Actions....26
Figure 5-3: Notification Processing....27
Figure 7-1: Monitoring....30

1.0 Introduction

The purpose of this document is to describe the workflow required to implement a new Universal Utility Data Exchange (UUDEX) Connection or modify an existing UUDEX Connection (U-Connection) to enable the exchange of data that may be used for applications supportive of grid operations, market operations, distribution management, incident reporting, security notifications, or a wide variety of other utility-centric purposes. The focus is to provide perspective on the differences of the UUDEX workflow over the current workflow used in industry for the Inter-Control Center Communications Protocol (ICCP)[1]. The document also covers processes for onboarding new participants, data organization, resiliency, monitoring, and user interfaces.

Figure 1-1 provides an overview of the UUDEX Framework (U-Framework). UUDEX Infrastructure (U-Infrastructure) refers to the communications infrastructure used to connect UUDEX Endpoints (U-Endpoints) whether a shared multi-point communications infrastructure or a legacy point-to-point communications infrastructure.

[1] ICCP is also known as Telecontrol Application Service Element 2 (TASE.2), or IEC 60870-6, “Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations”.

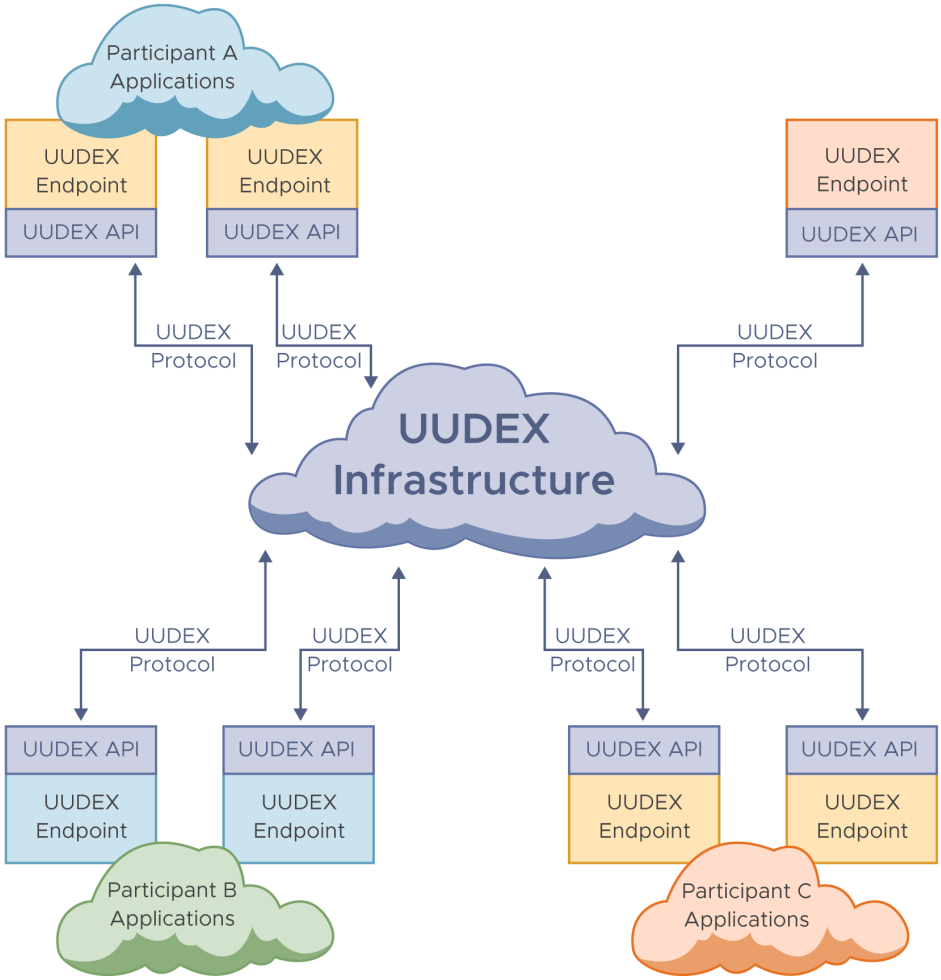

Figure 1-1: UUDEX Framework

The workflows needed to establish information exchanges within the U-Framework can be summarized as:

- Deployment of the U-Infrastructure, which involves servers, software, and a communications fabric.
- Registration of UUDEX Participants (U-Participants), representing organizations or companies (e.g., utilities, generator operators, independent system operators, and market participants) and government organizations (e.g., federal agencies and oversight authorities) that will allow information exchanges.
- Identification of the information a U-Participant will publish for consumption by other authorized U-Participants. These subjects are called “UUDEX Subjects (U-Subjects)”.
- Registration of U-Participant endpoints, where each endpoint can be assigned the rights to consume or publish specific information subjects (this includes creation and termination of UUDEX Subscriptions [U-Subscriptions]). Each of these is called a U-Endpoint and may be physically deployed at a site chosen by the U-Participant.
- Support real-time information exchanges, where endpoints may consume or publish specific subjects of information, and then transfer the information to or from specific applications that belong to a U-Participant.

- Support the management (including revocation) of information access rights for U-Participants.
- Support the management (including revocation) of U-Endpoint access to the U-Infrastructure.

2.0 Principles

While UUDEX is designed to be transport neutral, some aspects of this workflow may be impacted by the specific transport chosen for a specific UUDEX Implementation (U-Implementation). It is the intent of UUDEX to leverage existing technologies where possible, avoiding a “from-the-ground-up” implementation.

The following are key requirements that are effectively design principles for the workflow:

- Support key information exchanges currently supported by ICCP
- Support additional information exchanges not currently supported by ICCP
- Allow a variety of different types of documents to be exchanged
- Provide secure, reliable, performant transmission of information
- Provide rapid deployment of new U-Participants and U-Endpoints.

3.0 Scope

The scope of this document are workflows related to establishment of U-Connections and information exchanges using the UUDEX Framework (U-Framework).

Areas that are outside the scope of this specification include:

- The means by which organizations contractually agree to exchange information and associated controlled usage.
- Workflows related to software development.
- The details of the administrative user interfaces, beyond the description of their general usage within the UUDEX workflows.
- The details of the processes by which potential U-Participants and UUDEX Administrators (U-Administrators) are vetted for inclusion in a specific UUDEX Instance (U-Instance). These may vary between U-Instances and normatively dictating the nature of such vetting policies is therefore not specified. However, the sensitivity of the data exchanged over UUDEX may necessitate strong vetting practices in certain instances, often in accordance with industry standards and regulations. Appendix A provides suggested guidance for establishing vetting processes for organizations and individuals that participate in U-Instances.

4.0 Processes

4.1 Configuration

The process of configuration involves establishing a U-Framework. Details of this process are dependent on the transport technology used to implement a specific U-Instance.

Note that different U-Instances could be implemented using a variety of underlying transport technologies. These transport technologies may change and evolve over time. While a specific U-instance would use a particular transport technology, different U-Infrastructures within the same U-Instance can interoperate with each other if they use a common transport technology or if they are linked using a gateway capable of bridging between heterogeneous technologies.

One important aspect of UUDEX configuration is the selection of a network infrastructure. Organizations implementing a U-Infrastructure should select a network infrastructure based on their specific needs and risk profile. For many uses of UUDEX, the internet may be generically leveraged. However, for other uses it may be desirable to leverage a software defined network in order to achieve higher levels of security combined with improved quality of service. The basic principle is to avoid requiring the complexities and costs related to private network infrastructures, such as Multiprotocol Label Switching networks. However, if private network infrastructures already exist, UUDEX can use them to transport data.

The next aspect of configuration would be the deployment of the U-Infrastructure. The U-Infrastructure is a single logical entity consisting of multiple individual UUDEX Servers (U-Servers). These servers could be deployed in a variety of ways:

- Within a cloud infrastructure hosted and managed by a third party, with one or (preferably) more physical locations
- Within an enterprise network, with one or (preferably) more physical locations
- Using a federated, heterogeneous infrastructure at multiple locations, where each server could be managed by a different entity.

Given the anticipated uses of UUDEX, the servers that comprise the U-Infrastructure should optimally be deployed at a minimum of three physical locations, ideally each in separate geographic regions in a way that ensures that the loss of one or two locations does not result in data loss and minimizes the degree of service degradation. This allows for survival of the U-Infrastructure service in the event of network segmentation events, node failures, site failures, and some types of denial-of-service attacks.

A single organization might be a U-Participant in more than one U-Instance. In such a case, it could provide a “data transfer” function between these U-Instances, consuming data from one U-Instance and then publishing it in another U-Instance. These data transfers could occur in either direction. As data are published in the target U-Instance, the organization performing the data transfer would be responsible for establishing the relevant U-Subject and assigning access controls to that U-Subject. Such behavior would need to be contractually constrained, stipulating which U-Participants would be allowed to transfer data, what data could be transferred, and what access controls would need to be applied in the destination U-Instance.

4.2 Initialization

The process of initialization involves the set of activities required to enable the onboarding of U-Participants. This primarily involves seeding the U-Infrastructure with the information required to enable administrative activities. It also defines the standard set of data element types that may be conveyed using UUDEX.

The key data structures and their relationships in the U-Infrastructure are illustrated by the diagram of Figure 4-1.

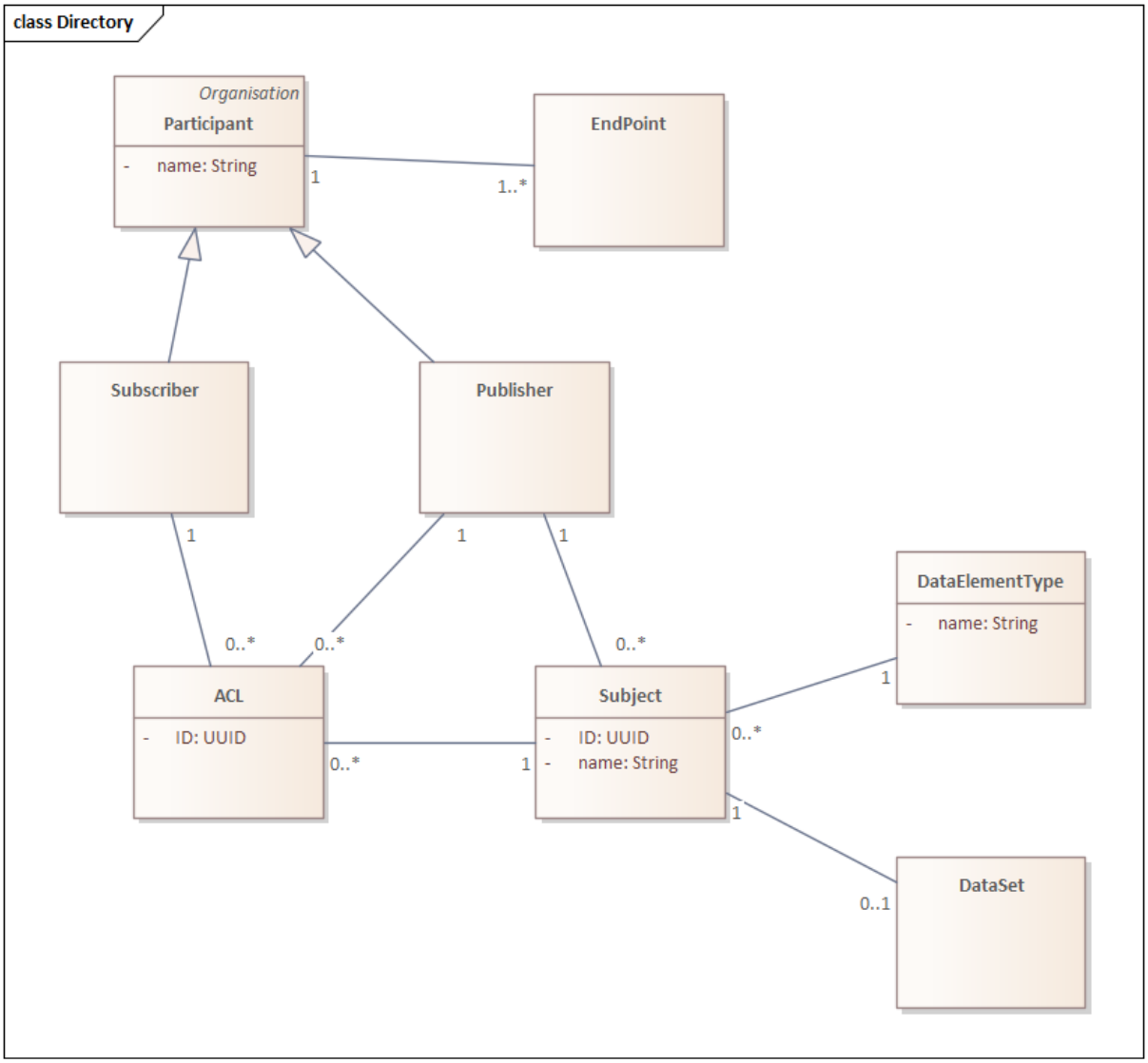

Figure 4-1: UUDEX Infrastructure

UUDEX will define a “standard” set of U-Data Element Types, where there may be an expanded set of U-Data Element Types that may be reflective of additional needs. Each U-Data Element Type has a defined data format and optionally a defined schema. U-Data Elements (of the same U-Data Element Type) are grouped into UUDEX Data Sets (U-Data Sets), which use a JavaScript Object Notation (JSON) format to describe their contents. One type of U-Data

Element Type is used to convey measured values, while other U-Data Element Types defined may include “documents,” such as for OE-417 forms or power system models. The set of U-Data Element Types can be extended as a consequence of standardization efforts or regulatory requirements. Defining new U-Data Element Types is an administrative activity.

4.3 Security configuration

The process of security configuration involves establishing access control lists (ACL) that would be applied to U-Subjects to constrain their access by U-Participants and U-Endpoints. The administrative users associated with given U-Subjects are able to change these controls at any time, including rescinding access to individuals who previously had access. Such an action would not impact any data those individuals had gathered already but would apply to all attempts to discover or collect data after the ACL change was applied.

As shown in Figure 4-2, there are two exchanges of interest regarding ACLs. The first involves the direct setting of an ACL attached to a U-Subject. In this case, the authorized UUDEX Participant Administrator (U-Participant Administrator) sends a message identifying the U-Subject, the action to take (add or remove the indicated permissions), and a set of permissions expressed as combinations of identities and access rights. The smallest unit of identity that can be specified would be an individual U-Participant, although groups of U-Participants might also be specified. The latter will depend on technical choices of access control paradigms. If the U-Infrastructure authenticates the U-Participant Administrator and recognizes them as authorized to alter the ACLs of the U-Subject, the action is executed. The updated ACL governs all actions U-Participants have with the U-Subject from then on. This includes fulfillment of U-Subscriptions.

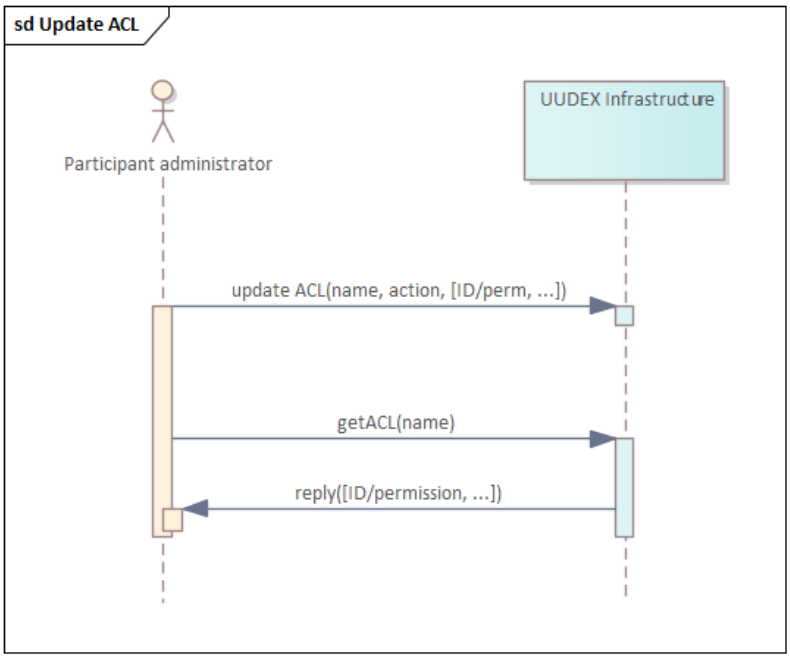

Figure 4-2: Update of ACLs

The second exchange involves the U-Participant Administrator collecting the complete ACL associated with the named U-Subject. In this case, if the U-Participant Administrator is

authenticated and authorized, the U-Infrastructure returns the complete ACL associated with the target of the query. This exchange allows the U-Participant Administrator to verify that their understanding of a U-Subject's ACL meets their expectations. If it does not, they can use the first exchange to make appropriate changes.

Some aspects of this are dependent upon the transport technology used for the U-implementation.

4.4 UUDEX Participant Onboarding

Within UUDEX, the onboarding of a U-Participant involves the processes listed below and shown in Figure 4-3.

- Out-of-band vetting of would-be participants. Appendix A provides guidance for vetting organizations and individuals.
- Registering an organization as a U-Participant.
- Identifying and vetting designated U-Administrators that can configure U-Endpoints, U-Subjects, or data element types on behalf of a U-Participant. The guidance in Appendix A may be applicable to this vetting process.

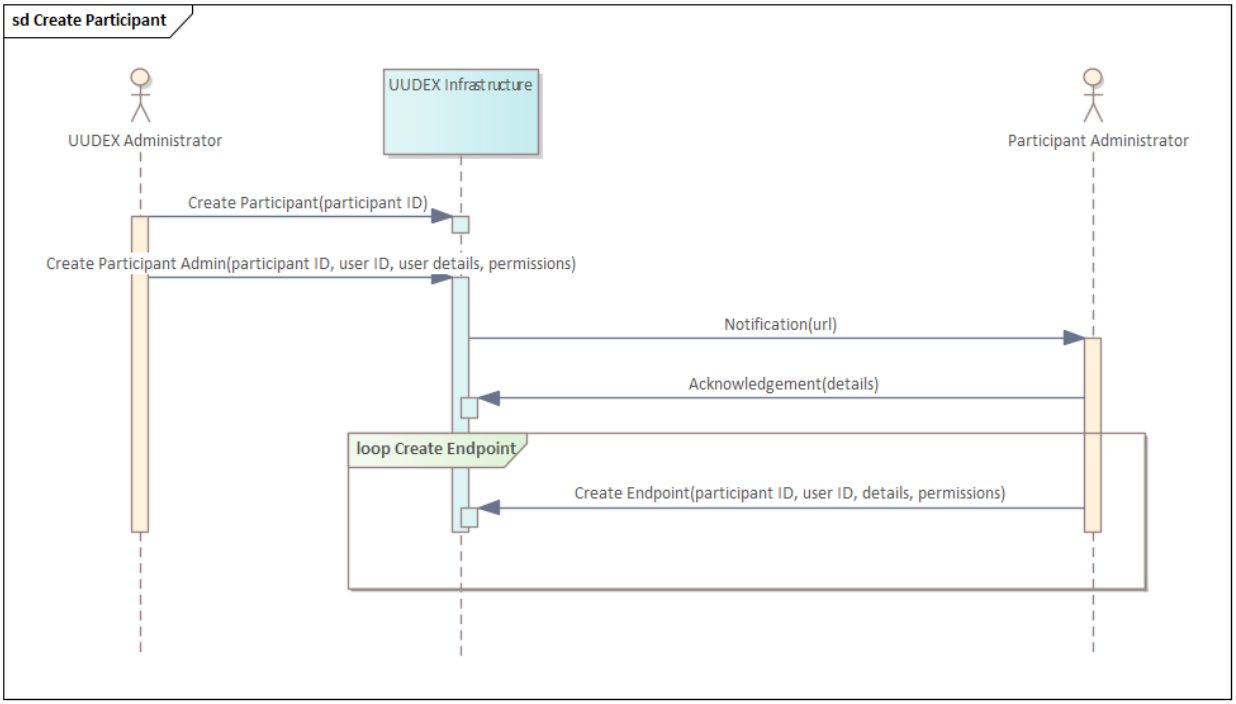

Figure 4-3: UUDEX Participant Onboarding

The initial steps of onboarding need to take place out-of-band from a UUDEX information flow, potentially over email or other mechanisms. Guidance provided in Appendix A might apply to this vetting process. This is because, until a U-Participant is onboarded, they will not have any credentials that allow them to engage in authenticated exchanges over UUDEX.

Organizations implementing a U-Instance will need to develop procedures for handling requests to become a U-Participant in that U-Instance. In the process of onboarding a U-Participant, the U-Participant (organization) is identified. U-Participants will need to determine what users are permitted to administer their interactions with a given U-Instance. These administrative users are responsible for all configuration of U-Endpoints and related information flows within the U-Framework. The notification for creating a U-Participant could be in the form of an email. After receiving a notification, the designated primary technical contact (i.e., the U-Participant Administrator) for the U-Participant would then provide additional details and register other users for access to the U-Instance.

When a U-Participant is registered, it is provided with credentials that will authenticate it to the U-Infrastructure of the U-Instance. The U-Participant will need to register specific U-Endpoints with the UUDEX Identity Authority (U-Identity Authority) employed by the U-Instance before it will be able to engage in regular UUDEX activities, such as publishing or subscribing to U-Subjects.

The U-Identity Authority is implemented using a secure, replicated database that is required for the operation of the U-Framework. Only a U-Administrator can make changes to the U-Identity Authority.

4.5 UUDEX Subjects and UUDEX Data Sets

Prior to enabling U-Endpoints for a U-Participant, the U-Subjects that a UUDEX Producer (U-Producer) publishes must be defined and created. Each U-Subject is associated with a specific UUDEX Data Element Type (U-Data Element Type) that contains individual UUDEX Data Elements (U-Data Elements).

For U-Subjects used for U-Data Sets, the contents of the U-Data Set is set by the U-Producer using a self-describing data model. This allows the U-Producer to publish U-Data Elements in an arbitrary order, and only requires the U-Producer to publish U-Data Elements that have changed since the last time they were published. This approach is significantly different than the legacy ICCP implementation, providing much greater flexibility in defining the exchanged data.

When defining a U-Subject, the following can be specified:

- Persistence, with a specified maximum lifetime
- Access controls, where U-Subscriptions are allowed to specific U-Subjects either as public or by specific U-Participants.

4.6 Endpoint Definition

U-Endpoints use the UUDEX application programming interface (API) to publish information (as U-Producers) and receive information (as UUDEX Consumers [U-Consumers], based on U-Subscriptions). U-Endpoints connect to the U-Infrastructure, not directly to other endpoints. U-Endpoints may be the result of:

- Third-party products that directly integrate with other components in a vendor’s product suite
- A custom integration that uses any one of a wide variety of integration technologies.

Defining U-Endpoints involves:

- Designating the U-Endpoint, where the U-Endpoint can be a U-Producer or a U-Consumer (or both) of information conveyed using U-Subjects
- Defining U-Subjects that will be used by producers
- Identifying U-Subjects of interest to consumers (i.e., discovery)
- Physically deploying and configuring the U-Endpoint, which includes UUDEX credentials (i.e., the digital certificate assigned to the U-Endpoint), and U-Connection information
- Connecting the U-Endpoint to the U-Infrastructure.

The process for defining U-Endpoints is shown in Figure 4-4.

Passing of credentials to a U-Participant for use in configuring a U-Endpoint would involve the user securely interacting as needed with the U-Infrastructure. This could involve notifications as described in Section 5.3.

U-Endpoints are validated for connections to the U-Infrastructure by a valid U-Participant. The result of the validation is a set of credentials that is used by the U-Endpoint when connecting to the U-Infrastructure. Each U-Endpoint may have peer instances, which are accessible at specific network addresses. In the case of peer instances, it is the responsibility of those peers to coordinate with each other for aspects of operation such as:

- Detection of startup or failure of peers
- Leader election
- Load balancing.

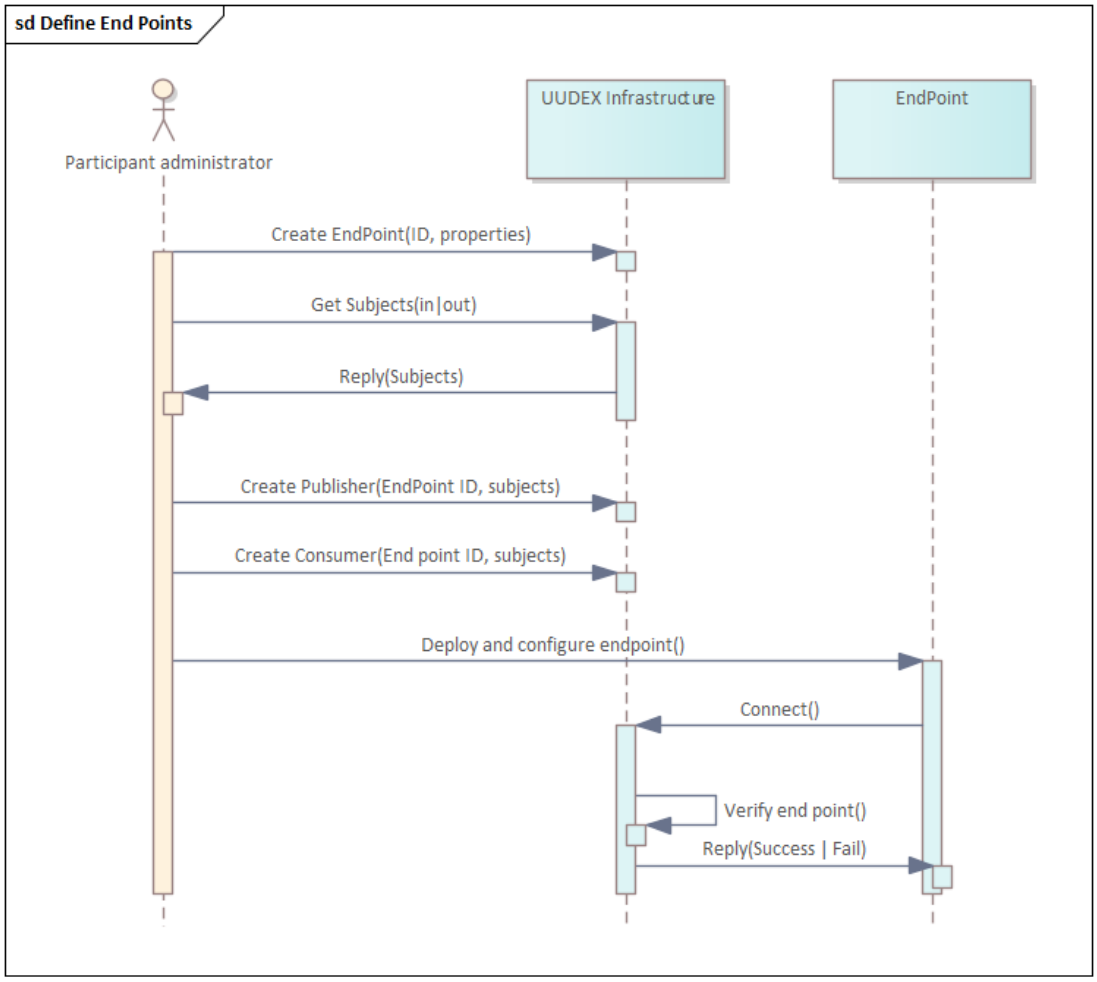

Figure 4-4: Defining Endpoints

The user would be provided a user interface that supports interactions with the U-Infrastructure. This would allow the user to:

- Locate U-Subjects “owned” by the U-Participant, and assign them to a U-Endpoint
- Identify U-Subjects owned by other U-Participants, where ACLs permit them to be consumed by U-Endpoints belonging to the U-Participant.

4.6.1 UUDEX Producers

A U-Producer is a U-Endpoint that can publish data elements to defined U-Subjects. *A U-Producer publishes data elements to U-Subjects.* A U-Producer is defined with the following properties:

- A set of one or more network addresses, allowing for “replicas” of each producer as needed for availability purposes.
- Designation of the endpoint as a valid U-Producer for a defined U-Subject.
- Control of which U-Participants can access which types of U-Subjects through use of ACLs.

The basic processing of a simple U-Producer is shown in Figure 4-5. This example has no redundancy. A more typical example of processing in which a U-Producer has peers is shown in Figure 4-6, where one instance will be active and responsible for publishing messages to one or more subjects. In the event of a failure, a peer instance will take over (usually through a consensus mechanism) and be responsible for publishing messages to reflect updates to data elements from a data source.

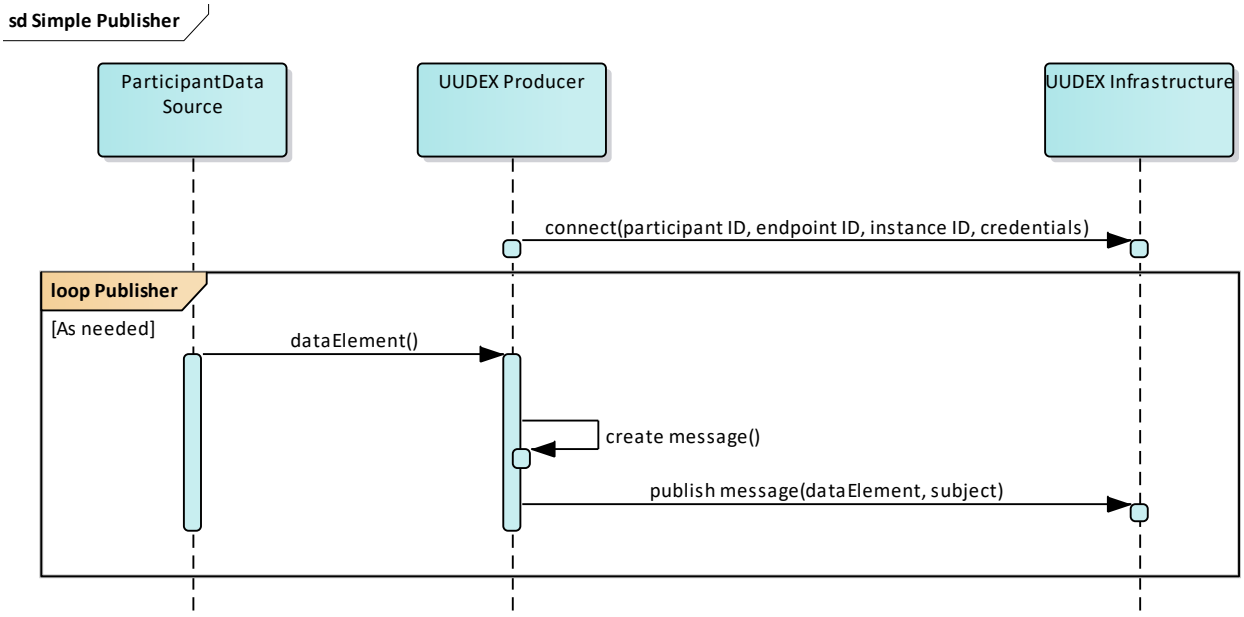

Figure 4-5: Simple UUDEX Producer

Where a U-Producer endpoint is implemented using a set of peers for availability purposes, it is the responsibility of the endpoint implementation to properly address coordination issues so information that must be published is published only once and in the proper order.

This process involves no user intervention.

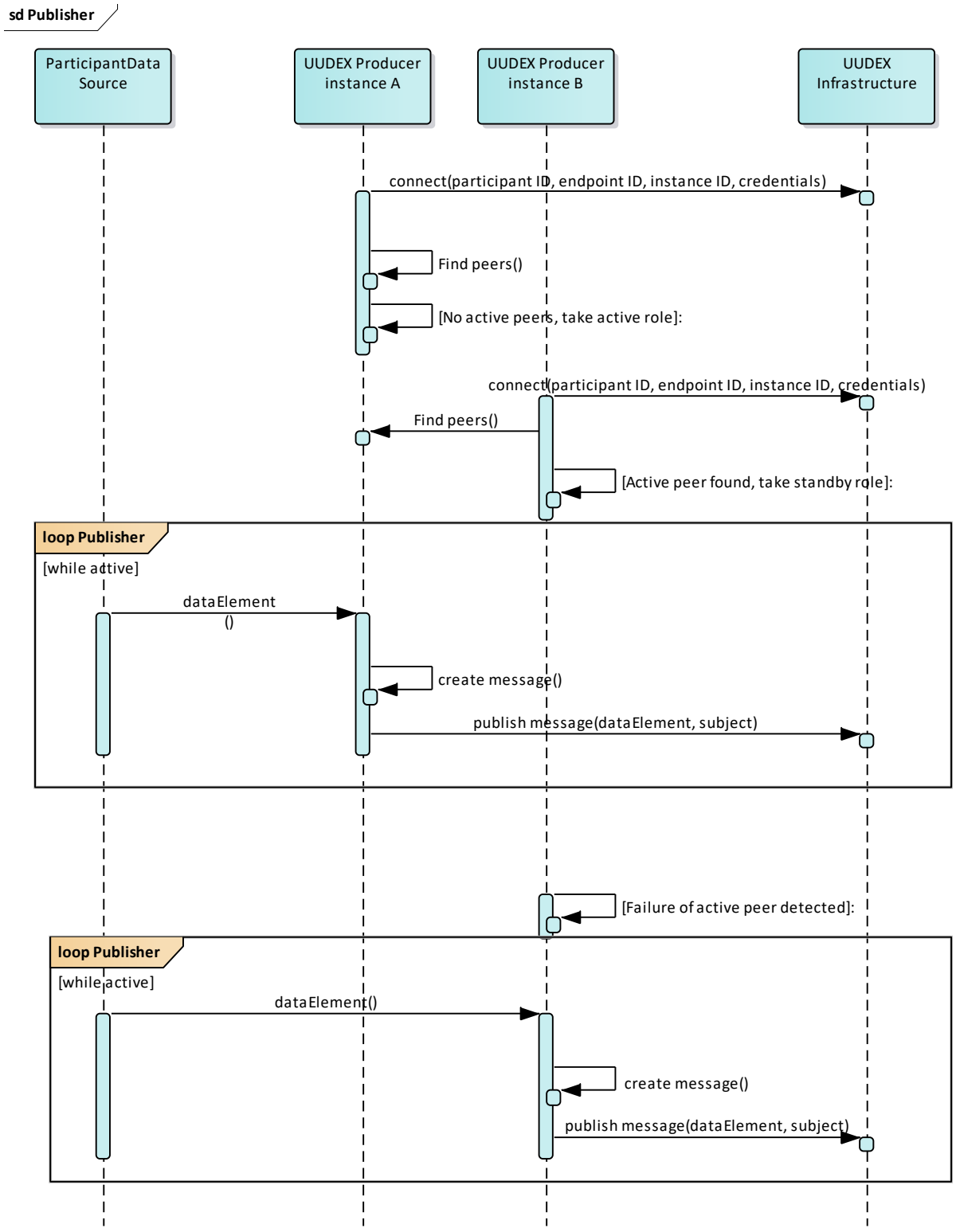

Figure 4-6: Publication by Peer Producers

4.6.2 UUDEX Consumers

A U-Consumer is a U-Endpoint that can subscribe to and consume information that was published to a U-Subject. *A U-Consumer subscribes to U-Subjects.* A U-Consumer is a U-Endpoint with the following defined properties:

- A set of one or more network addresses, allowing for “replicas” of each U-Consumer as needed for availability purposes.
- Designation of the U-Endpoint as a valid consumer for a defined U-Subject, where the U-Subjects are selected as a result of the discovery process.

Figure 4-7 shows the basic sequence for a U-Consumer to subscribe to a U-Subject and consume messages that were published to that subject.

Implementation of a U-Consumer allows several options:

- A standalone U-Consumer, without peer instances
- A U-Consumer with peers that all subscribe simultaneously, but potentially coordinates their actions
- A U-Consumer with peers that coordinate their U-Subscriptions, where only one peer consumes at a time.

In all cases, a U-Consumer is responsible for forwarding the information to upstream applications within its local enterprise as needed.

Where a U-Consumer endpoint is implemented using a set of peers for availability purposes, it is the responsibility of the endpoint implementation to properly address coordination issues, so that information that must be retrieved is made available to all U-Consumer endpoints.

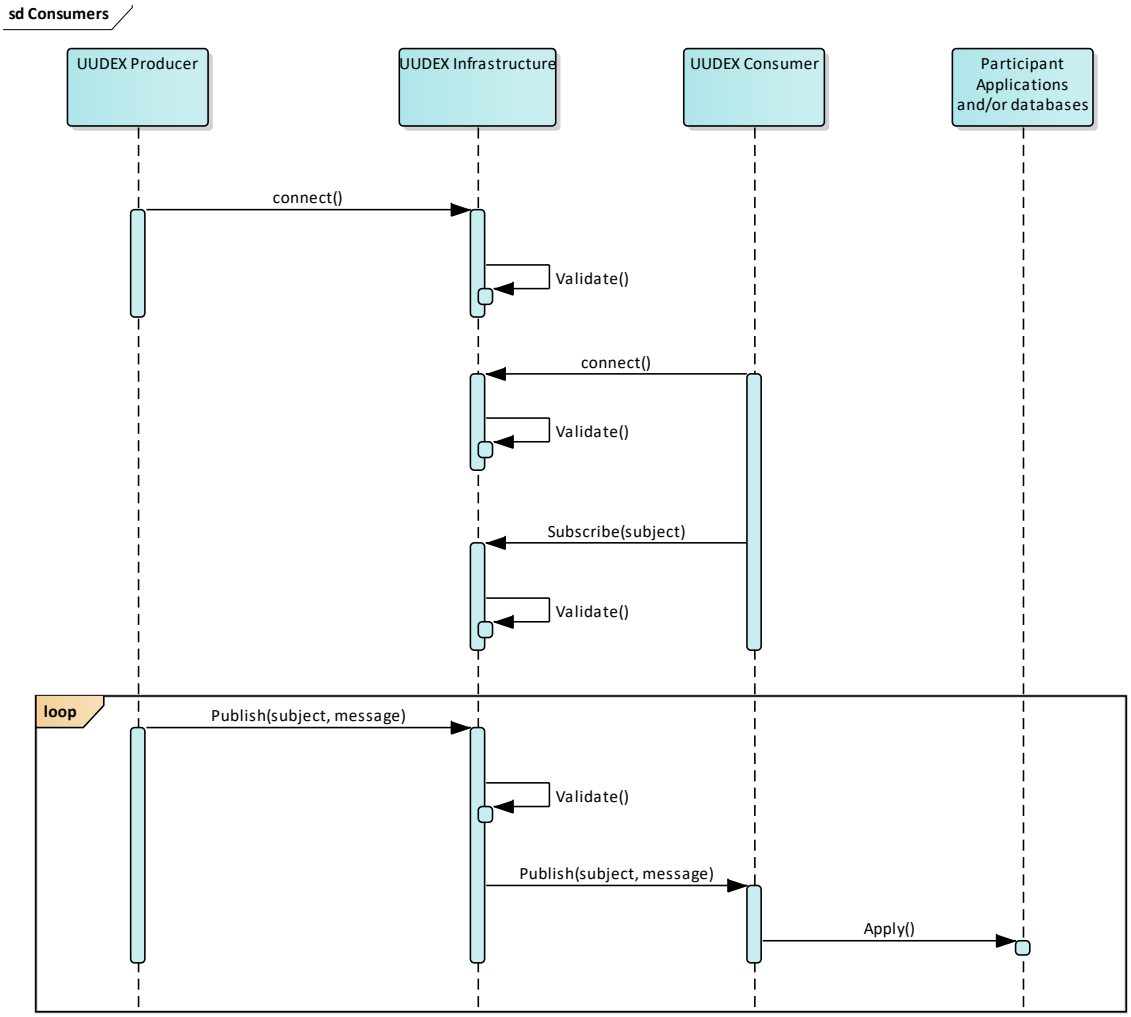

Figure 4-7: UUDEX Consumers

4.6.3 UUDEX Infrastructure

A prerequisite for a U-Participant to deploy U-Endpoints is to establish connectivity through the chosen network infrastructure to be used by the specific U-Framework deployment.

U-Participants also are responsible for establishing a secure hardware and network infrastructure for the deployment of endpoint software.

4.7 Publication

Publication involves a U-Producer and one or more U-Consumer endpoints. The U-U-will send a data element of a given data element type to a defined U-Subject. Where a U-Producer may have a set of peer instances, only one instance of the U-Producer should publish a data element instance; that is, information published to a given U-Subject is unique and is not sent redundantly.

The process flow for publication is shown in both Figure 4-5 and Figure 4-6.

4.7.1 Models

Models are descriptions of an electricity network that are consumed by applications and simulate, analyze, and or assist the operation of the real-world electricity network. Industry standard data formats are used to convey these models. These are typically defined in non-JSON formats. They will be compressed and encoded for conveyance using the JSON formatted UUDEX Message Envelope (U-Message Envelope). The payload metadata will describe the specific format.

4.7.2 Measured Values

Measured value U-Data Sets are U-Data Elements that are used to convey time series data. The creation of a U-Data Set involves determining a set of data points and identifying the nature of the point and typically its relationship to objects defined in a model. Data points may represent measured, calculated, or entered values. Publication of a U-Data Set involves sending the most recent values for each data point, which includes:

- The measured, calculated, or entered value
- A timestamp to indicate when the value was last obtained
- A quality code.

A set of measured values is essentially a snapshot of a set of values for a given period of time. It is expected that measured values will make up a significant amount of all messages. The description of the individual U-Data Elements that comprise a set of measured values are:

1. Measured values are identified by a common identifier, expected to be the IEC Common Information Model (CIM) Master Resource Identifier (mRID) as defined by the model referred to in Section 4.7.1. If mRIDs are not used, an equivalent unique identifier may be used in its place. Additional information about a specific measured value may also be described.
2. The current value for each data point with timestamp and quality code. These typically will be conveyed in real time to reflect the current state or may be sent periodically or on an exception basis.

4.7.3 Documents

The definition of documents involves defining a data element type with the following properties:

- A data element type name
- A data format
- A schema specification (optional, but common to structured documents).

Documents can be classified as structured (where specific data elements can be readily extracted (e.g., JSON, XML or CSV files) or unstructured (e.g., image, Microsoft® Word document, PDF document, text file, or binary file).

Documents can often be conveyed through UUDEX with source formatting being non-JSON, in which case they will be compressed and encoded for conveyance using the U-Message Envelope. The payload metadata will describe the specific format so the object can be readily

reconverted to its original form by the receiver. This flow is shown in Figure 4-8. Upon receipt, the documents will be decoded and uncompressed to return them to their original format.

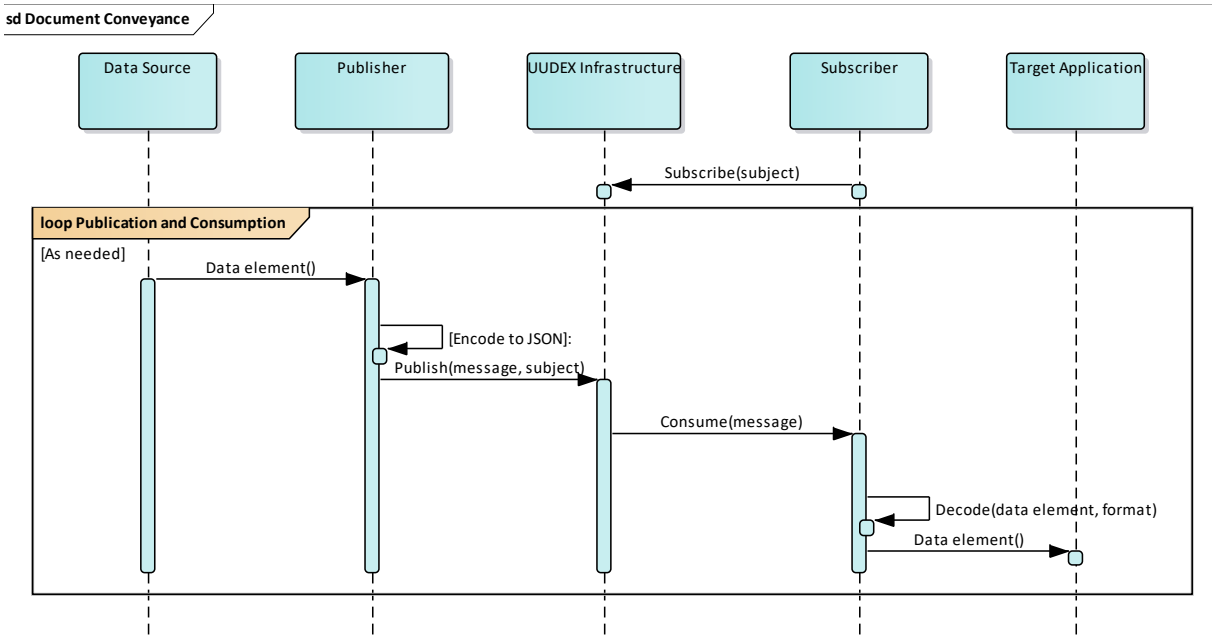

Figure 4-8: Document Conveyance

4.8 Discovery

Discovery occurs when a U-Participant wants to access information that may be provided by other U-Participants. ACLs defined by the “owning” U-Participant will identify whether or not a U-Participant is able to:

- Discover the existence of a U-Subject
- Publish to a specific U-Subject
- Subscribe to a specific U-subject
- Manage a specific U-Subject

4.9 UUDEX Subscriptions

U-Subscriptions are the mechanism by which one U-Participant collections information from U-Subjects. The following are basic statements about U-Subscriptions:

- A U-Subscription must contain at least one U-Subject but may contain multiple U-Subjects.
- A given U-Subject may be in multiple U-Subscriptions.
- U-Endpoints subscribe to U-Subjects.
- Many U-Endpoints may subscribe to the same U-Subject and a single U-Endpoint may subscribe to multiple U-Subjects.
- Each subscribing U-Endpoint will receive a copy of any message published to a specific U-Subject.

- The U-Subject's publisher's ACLs control which U-Participants may configure U-Endpoints to subscribe to a given U-Subject.

Figure 4-9 shows the U-Subscription to a U-Subject by U-Endpoints, after which U-Data Elements published by a U-Producer to the subject can be consumed by those U-Endpoints.

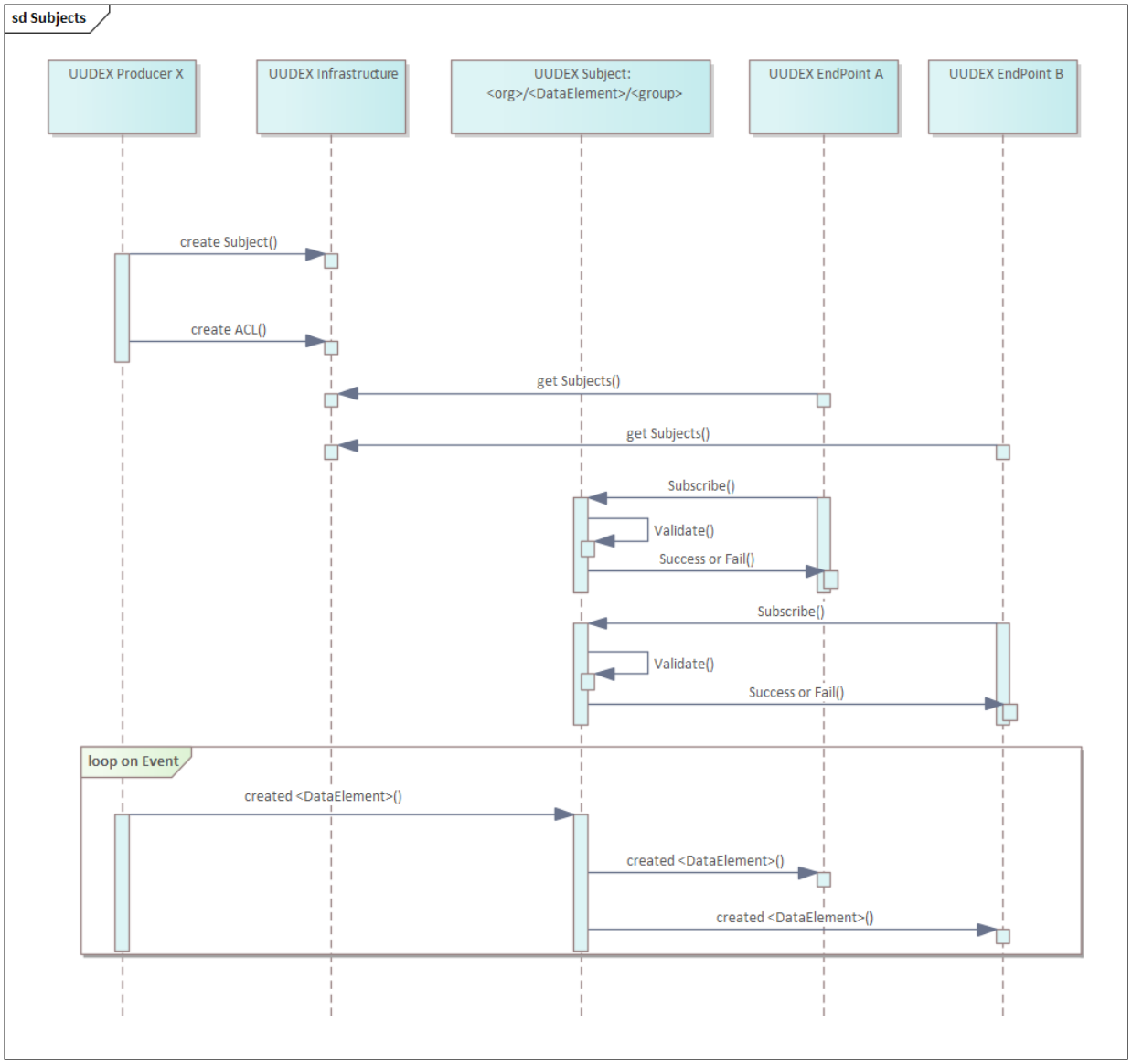

Figure 4-9: UUDEX Subscriptions

As noted in Section 4.6, U-Endpoints may have peers to support redundancy and resiliency. As such, when a particular U-Endpoint submits a request to create a U-Subscription, there may be other U-Endpoints belonging to the associated U-Participant that are treated as peers of the requesting U-Endpoint for the purpose of this U-Subscription. Should a given U-Endpoint become unavailable, its peers need to be able to receive U-Subscription fulfillment messages. It is the responsibility of the U-Infrastructure to ensure this happens, and as a result, when a U-Subscription is established, the requesting U-Endpoint will identify the U-Endpoints that should be treated as peers from the perspective of the U-Subscription. Similarly, all peer

U-Endpoints would be considered “owners” of the U-Subscription, with the power to manage that U-Subscription as described below. Regarding Figure 4-9 and the following descriptions, we will refer to “the U-Endpoint” that created and manages the U-Subscription. However, note that it may be the case that this “logical U-Endpoint” is actually a peer group of U-Endpoints, all with equivalent rights and roles with regard to the U-Subscription.

U-Subscription fulfillment refers to the process by which new data is added to a U-Subject, and the logical U-Endpoint is alerted to this action. As shown in Figure 4-9, the U-Framework supports two methods of fulfillment—Data Push and Data Notification.

- Data Push – This mode of fulfillment causes new data to be sent to the logical U-Endpoint directly and is useful in sharing information such as measurement sets to which the U-Endpoint is subscribed.
- Data Notification – In this mode of fulfillment, the U-Infrastructure sends a notification message alerting the logical U-Endpoint to the presence of new data and providing a pointer to the data (i.e., a message ID) so the logical U-Endpoint can directly query and retrieve that data. This method is useful in conveying changes or updates to data, such as power system models, that may then be retrieved by the U-Endpoint.

Each U-Subscription will contain one or more U-Subjects. A U-Subscription will specify whether the fulfillment method, either Data Push or Data Notification. The same U-Subject may be in different U-Subscriptions with different fulfillment types allowing an individual U-Subscriber control over how data is delivered to it.

Logical U-Endpoints control their U-Subscriptions. They can Create, Pause, Resume, and Delete each U-Subscription for which they are the subscriber. These controls are described below:

- Create – Requests that the U-Infrastructure establish a U-Subscription to the named U-Subject. If the logical U-Endpoint's U-Participant is allowed to consume the data from the U-Subject according to the U-Subject's ACL, the U-Subscription will be permitted.
- Pause – Temporarily pause notifications/delivery related to U-Subscription fulfillment. The U-Subscription remembers the last data that the logical U-Endpoint received.
- Resume – Pick up U-Subscription fulfillment, starting with the first available data added to the U-Subject following the Pause request. (Note, however, that if a U-Subscription is paused for an extended period of time and if the U-Subject's data is of ephemeral value and periodically deleted, some data between the Pause and Resume action might be lost.)
- Delete – remove the U-Subscription from the U-Infrastructure. If, at some later point, the logical U-Endpoint creates a new U-Subscription to the U-Subject, fulfillment will start with the first material to arrive at the U-Subject following the new U-Subscription.

After connecting to the U-Infrastructure, U-Consumer endpoints will subscribe to one of more U-Subjects, where each U-Subscription is validated based on ACLs defined for that U-Subject by the “owning” participant.

There might be situations that cause a U-Subscription to be cancelled other than through a direct request from a logical U-Endpoint. In such a case, the U-Infrastructure must immediately inform the logical U-Endpoint of this cancellation. This avoids a situation in which the logical U-Endpoint believes it will receive timely messages, but this is not the case. It is possible that a single U-Participant might have multiple U-Subscriptions to the same U-Subject. These

U-Subscriptions will be identified differently and managed separately (i.e., pausing one U-Subscription would not pause the other). The U-Infrastructure must not try to unify multiple U-Subscriptions from the same U-Participant into a single U-Subscription for either fulfillment or U-Subscription management.

4.10 Resiliency

4.10.1 Data Source Selection

U-Endpoints are responsible for the selection of data sources. This is usually done through the process of development or configuration of endpoint software. Typically, redundant data sources would exist that could be leveraged for an endpoint that is responsible for publishing information on behalf of the data source.

4.10.2 Redundancy

Redundancy is accomplished in several ways:

- Redundancy within the U-Infrastructure, where UUDEX services are provided by a set of servers and a primary network that has at least one backup network to which the primary network fails over
- Definition of peer instances for U-Endpoints (producers or consumers)
- Existence of redundant data sources and sinks from which U-Endpoints read or write data.

Redundancy within the U-Infrastructure is accomplished by replicating UUDEX Components (U-Components), where those U-Components form a coordinated cluster that ensures continued operation through a variety of failure and recovery scenarios. It is the responsibility of a U-Endpoint and other uses of the UUDEX API to use a specified set of candidate connection addresses when connecting to the U-Infrastructure, at which point the active set of underlying sites, servers and services are transparent to the U-Endpoints. Ideally, to achieve the highest levels of availability, the underlying servers that support the U-Infrastructure would be deployed across a minimum of three geographically separated physical locations.

U-Participants can decide on the level of redundancy that is needed for given information flows and can deploy an appropriate number of peer endpoints. Where a high level of availability is needed, peer endpoints would typically be deployed at different sites and would use more than one physical network path to the U-Infrastructure.

The proper access and update of redundant data sources and sinks is the responsibility of the U-Participant Infrastructure and U-Endpoint implementation.

4.10.3 Consensus

Redundancy brings on the need to avoid confusion. A key concern is to avoid a “split-brain” scenario, where U-Components within the U-Framework continue to operate while isolated from other U-Components, resulting in a diverging view of state. This scenario is avoided by having U-Components operate through “consensus.” There are two key situations for which a consensus mechanism is needed:

- Where a U-Participant has peer U-Endpoints that are configured for redundancy
- By replicas of servers and their associated services within the U-Infrastructure.

In the case of a U-Endpoint that is configured with peer U-Servers for redundancy, it is the responsibility of those peers to employ an appropriate consensus mechanism such as a quorum calculation. Within the U-Infrastructure, there should be *N* U-Servers where *N* is an odd number, minimally three of each U-Component, to achieve some level of fault tolerance while avoiding the ability to segment the peers into two partitions each assuming it is functional and the other has failed. Ideally, *N* should be an odd number greater than four. The servers should be configured to avoid a segmentation or other failure event that would leave an equal number of U-Servers in each resulting partition. This allows the calculation of a quorum, where quorum is achieved when the number of U-Servers aware of each other in a U-Instances is greater than half of the number of U-Servers that are configured in the U-Instance.

In the event of a loss of quorum (e.g., a transition from three peers to one, or five peers to two), the remaining peers should transition to a down state in order to avoid a split-brain scenario. Transitions that involve an increase in the number of peers (e.g., from three instances to four) or a loss of a minority of peers (e.g., transition from three peers to two or five peers to three) would not impact UUDEX functionality. When a quorum is lost from the perspective of a given peer, there is no ability to participate in the determination of a consensus, which then requires the peer to transition to a down state.

Peers in a down state should continually monitor other peers to determine if quorum can be regained, and the peers can exit the down state. U-Producer peers entering the up state should resynchronize with other U-Producers before fulfilling a U-Subscription by allowing existing U-Producers to fulfil U-Subscription requests.

4.11 Monitoring and Management

Each U-Endpoint should periodically publish a health and statistics message that can be captured and recorded by the U-Infrastructure for the purposes of monitoring. This message would provide information such as:

- The time duration the endpoint has been active (a measure of the reliability of the endpoint)
- A timestamp[1] with the current time (useful to identify message latencies)
- The time of last report
- The number of messages/data elements published and consumed since last report
- The number of bytes published and consumed since the last report.

Figure 4-10 shows the process for a U-Endpoint to periodically report its health and other operational statistics. The *Monitoring Agent* function shown in the figure is a service deployed within the U-Infrastructure that is responsible for capture of U-Endpoint health and related statistics. The *Monitoring Tool* function shown in the figure would provide the ability for a user to view U-Endpoint current state and performance history. This is further described in Chapter 7.0.

[1] Note – this assumes that time is synchronized between the two endpoints

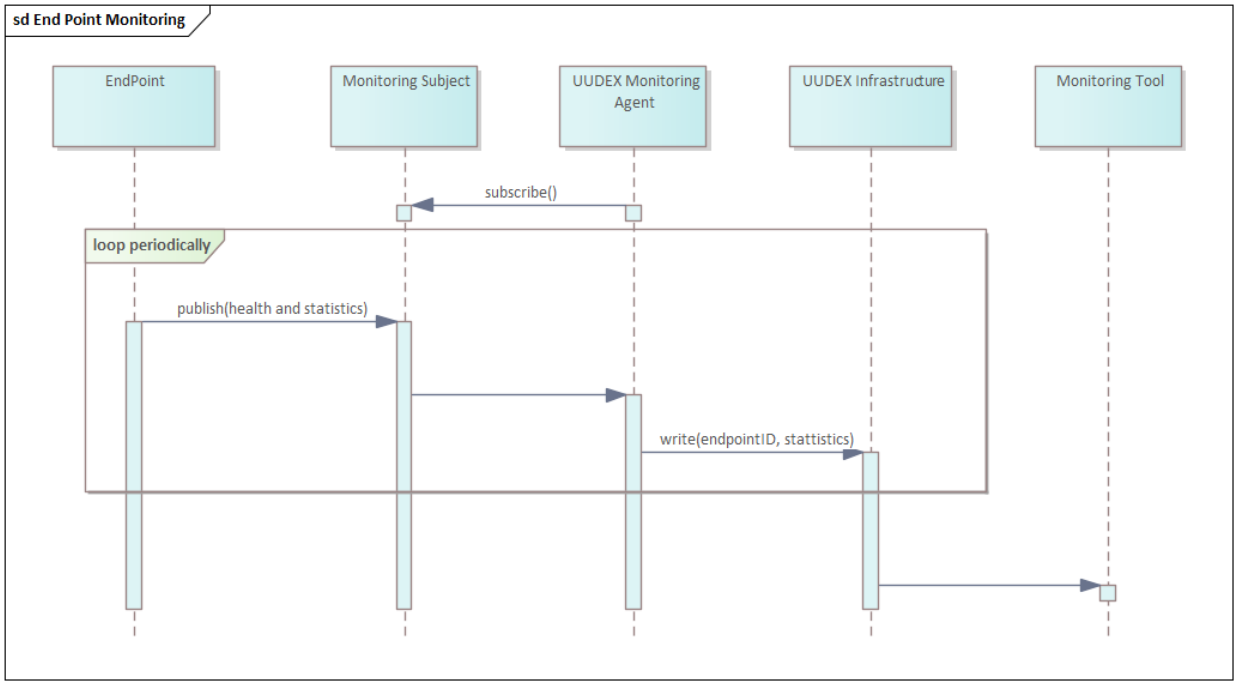

Figure 4-10: UUDEX Endpoint Monitoring

4.12 Testing and Verification

When a new U-Endpoint is connected to the U-Infrastructure, some level of testing and verification is needed. Key aspects of this are essentially automated, as U-Endpoints are required to issue periodic messages for the purpose of monitoring. When a U-Endpoint is deployed, the following should be visible:

- The U-Participant can access the U-Endpoint and determine if it has successfully connected to the U-Infrastructure using interfaces provided by the specific U-Endpoint product.
- U-Administrators and the U-Participant Administrators can see that the U-Endpoint is connected to the U-Infrastructure and is providing periodic health and state information.

Provisions would also be put in place to “test” U-Subjects, where information could be published and subscribed for testing and verification purposes.

5.0 User Interfaces

The nature of UUDEX user interfaces is described in this chapter. The user interfaces are not intended to provide any end-user functionality, rather they provide administration and monitoring capabilities.

These user interfaces are not to be confused with the API used to publish and subscribe to U-Subjects using the U-Framework.

5.1 Roles

The two primary roles for UUDEX administrative users are U-Administrators and U-Participant Administrators. Their roles are briefly described below:

- U-Administrators have global responsibility for the U-Framework and can authorize U-Participants.
- U-Participant Administrators can perform activities related to the publication and consumption of information for a given U-Participant and also can access monitoring tools.

There may be needs to define other roles over time. The following are examples of potential additional roles:

- An auditor who could view the information needed to adequately audit the operation and management of the U-Infrastructure
- A monitor who could view the current state of the U-Infrastructure, logs, and related performance metrics.

An individual can be assigned to one or more roles.

Individuals designated to fulfill these sensitive U-Infrastructure roles should be vetted. Guidance provided in Appendix A might apply to this vetting process.

5.2 Core functionality (minimum requirements)

5.2.1 UUDEX Administrator

The user interface should provide the following capabilities for a U-Administrator:

- Create, authorize, and de-authorize U-Participants
- Update U-Participant details
- Define valid U-Data Element Types, beyond the standard set defined by UUDEX.

These capabilities are shown in Figure 5-1.

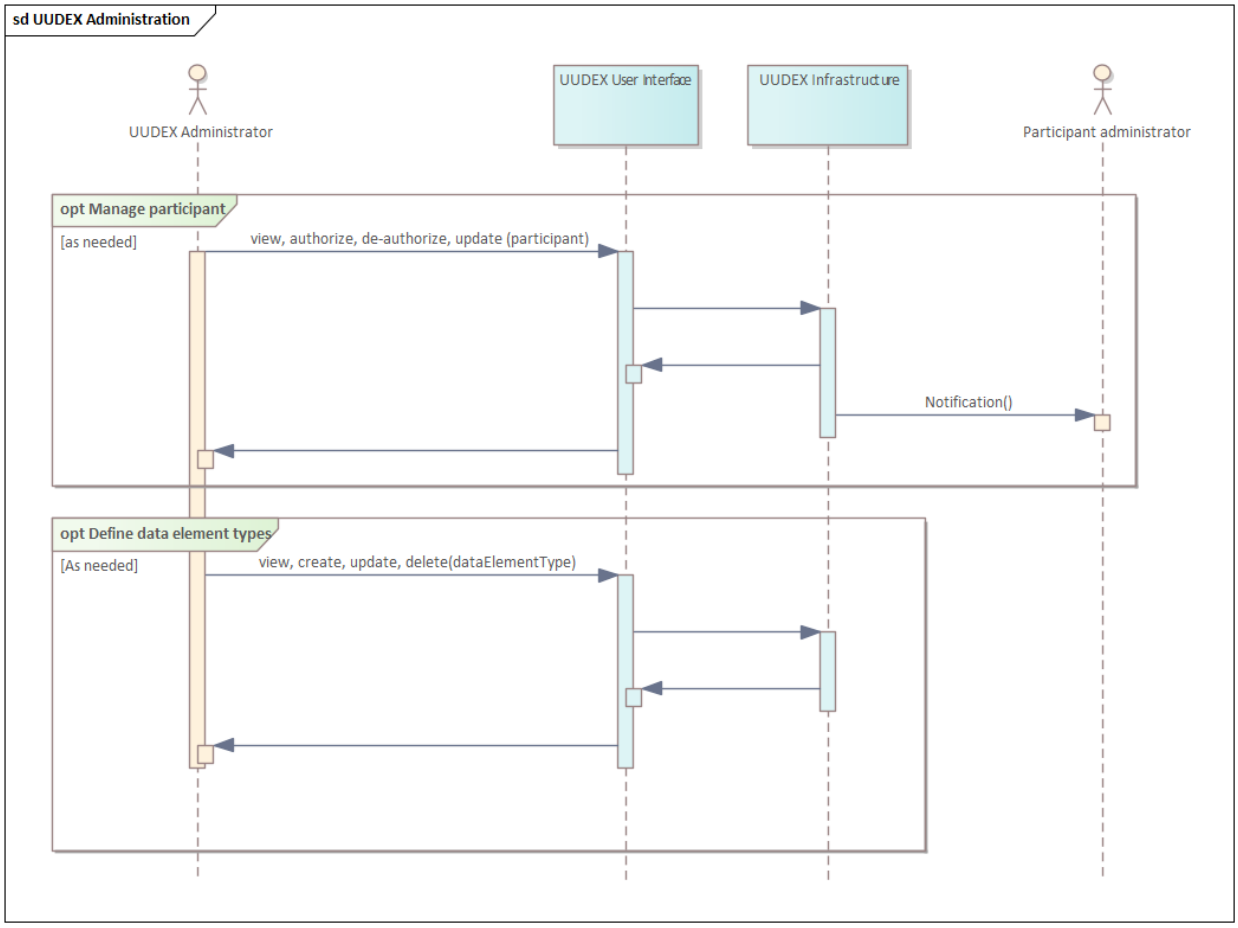

Figure 5-1: UUDEX Administrator Actions

5.2.2 UUDEX Participant Administrator

The user interface would provide the following functionality for a U-Participant Administrator whose role is different from that of a U-Administrator:

- Create and delete U-Subjects (for publications)
- Discover (view) available U-Subjects (for U-Subscriptions)
- Create, authorize, and de-authorize U-Endpoints
- Associate U-Subjects to U-Producer U-Endpoints
- Set U-Subscriptions for U-Consumer U-Endpoints.

These capabilities are shown in Figure 5-2.

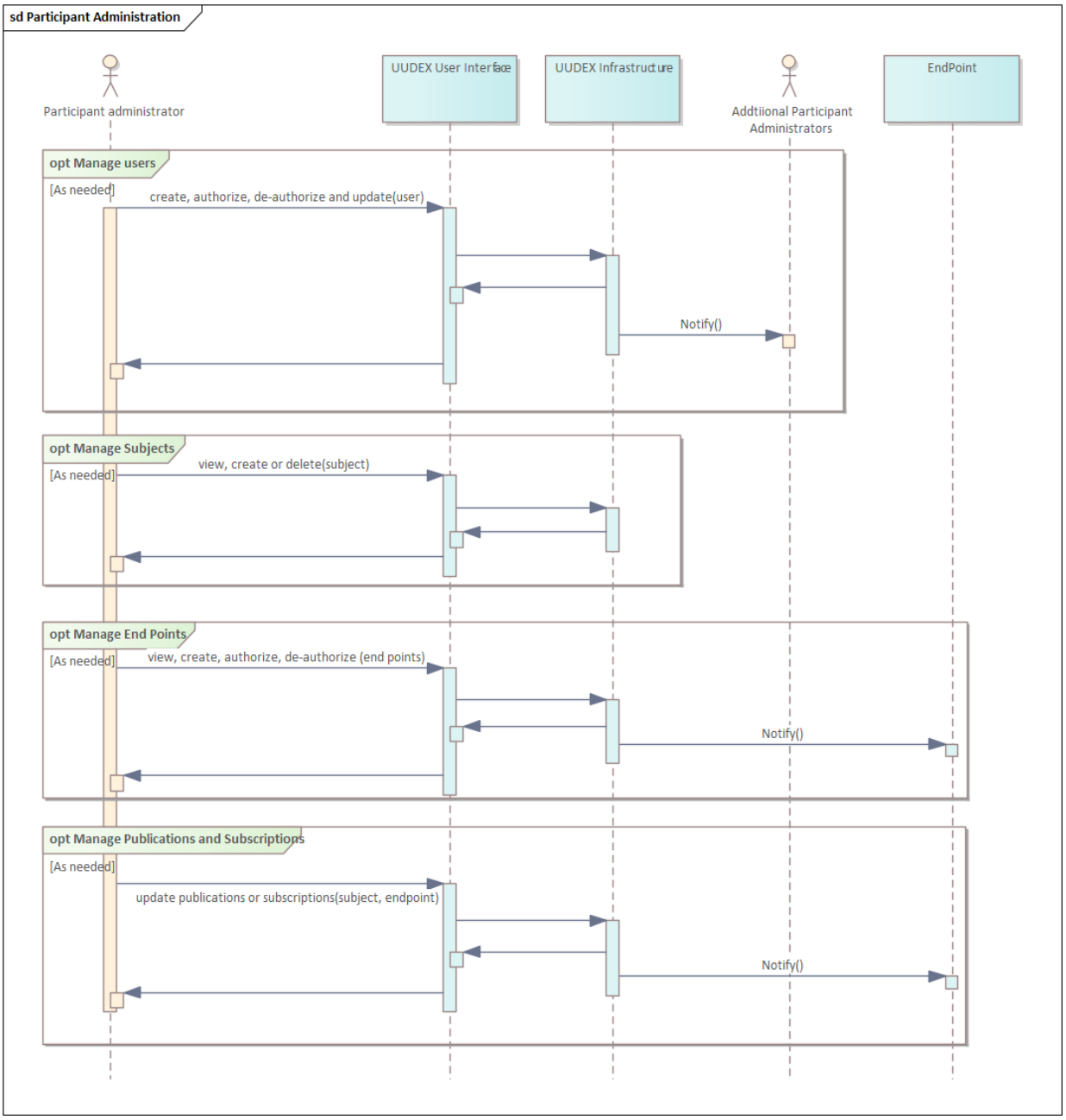

Figure 5-2: UUDEX Participant Administrative Actions

5.3 Notifications

A key aspect of the user interface is to provide the means to issue notifications and alerts to users, such as U-Administrators or U-Participant Administrators. These notifications would normally be issued “out-of-band,” using mechanisms such as email or text messages.

When a condition of interest is detected by the U-Infrastructure, it is reported to the U-Infrastructure for recording and generation of notifications to potentially interested users. Conditions of interest can be defined in two ways:

- Hard coded into U-Components, typically as a part of exception handlers
- Rules that would identify thresholds (e.g., message rates) upon which notifications are issued.

Given security concerns, only a summary of the notification is provided with a URL that would enable the user to securely authenticate in order to get details or take consequential actions. This is shown in Figure 5-3.

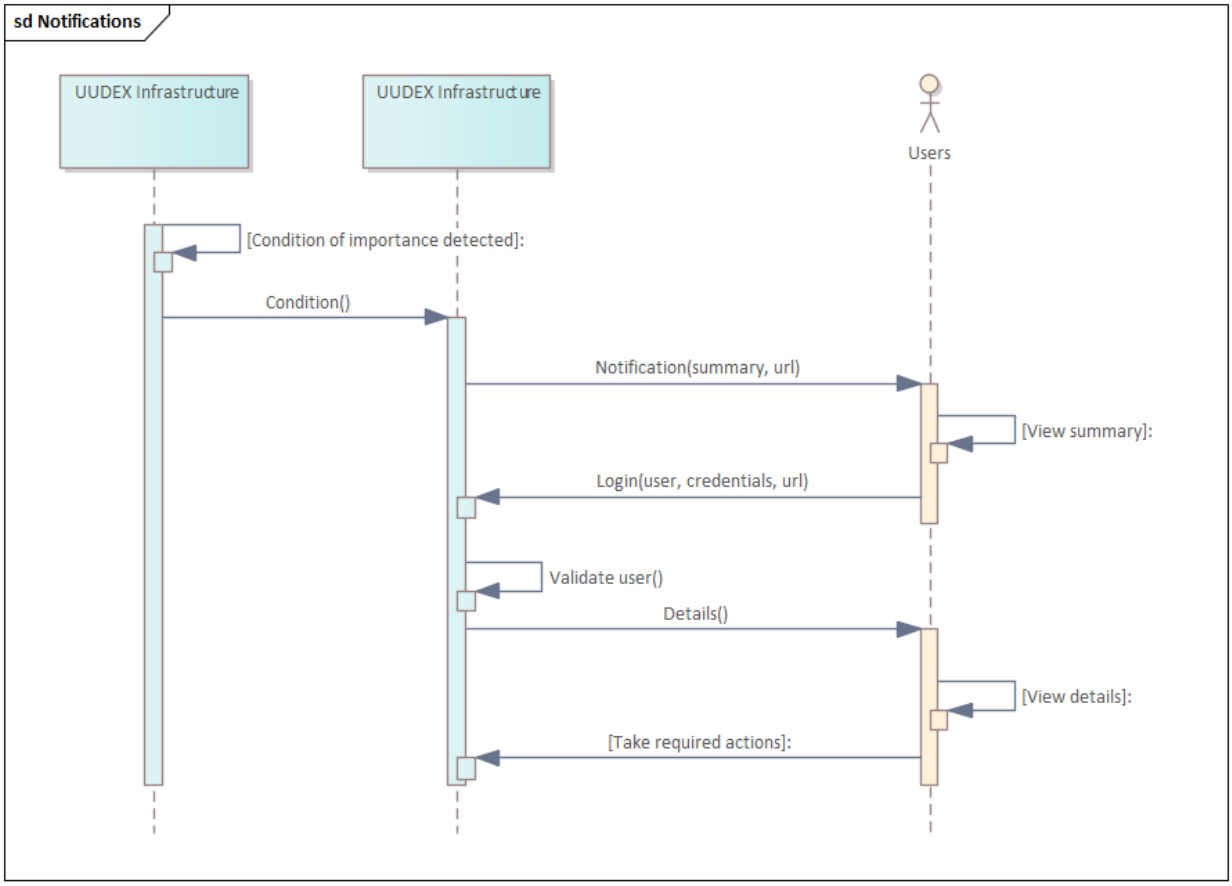

Figure 5-3: Notification Processing

As examples, notifications could be generated as a consequence of:

- User authorization
- U-Endpoint authorization
- UUDEX monitoring (e.g., alerts of U-Endpoint or U-Infrastructure “health” issues, see Chapter 7.0)

It is important to note that alerts are notifications that typically require some action by a user. For example, a notification would be generated if a U-Endpoint was created or a configuration updated, but an alert would be generated to indicate that a U-Endpoint has failed.

5.4 Third-Party User Interfaces

Given that the U-Framework is intended to be transport neutral, there may be user interfaces that are needed to manage and monitor aspects of the transport layer as well as the underlying communication fabric. These would be supplemental to UUDEX-specific user interfaces as described earlier in this chapter. These would likely be leveraged by U-Administrators as opposed to U-Participant Administrators.

6.0 Application Programming Interfaces

APIs are used to construct U-Endpoints and administrative interfaces. The API may be versioned, where the U-Infrastructure will respect a given set of versions. Implementation of an API would have the following characteristics:

- A transport technology
- A version identifier
- Bindings for one or more programming languages.

The APIs would be leveraged by:

- Administrative user interfaces, as used by the U-Administrator or U-Participant Administrator
- U-Endpoints at U-Producers
- U-Endpoints at U-Consumers.

Before using an API, the user or application needs to be authenticated. Once authenticated, only authorized API calls or data may be accessed.

Each of the workflows described in the preceding sections leverages APIs. Workflows related to the development of UUDEX software components are outside the scope of this specification.

A key aspect of APIs is to hide as much of the underlying implementation details as possible. This allows increased simplicity when implementing clients and enables the underlying implementation to evolve more easily.

7.0 Monitoring/Diagnostics/Testing

The U-Framework will provide mechanisms for monitoring, testing, and general problem diagnosis. Some of these mechanisms may be specific to the transport layer or communication fabric. Other mechanisms will be more specific to the tracking and analysis of U-Connections and information flows. This is shown in Figure 7-1.

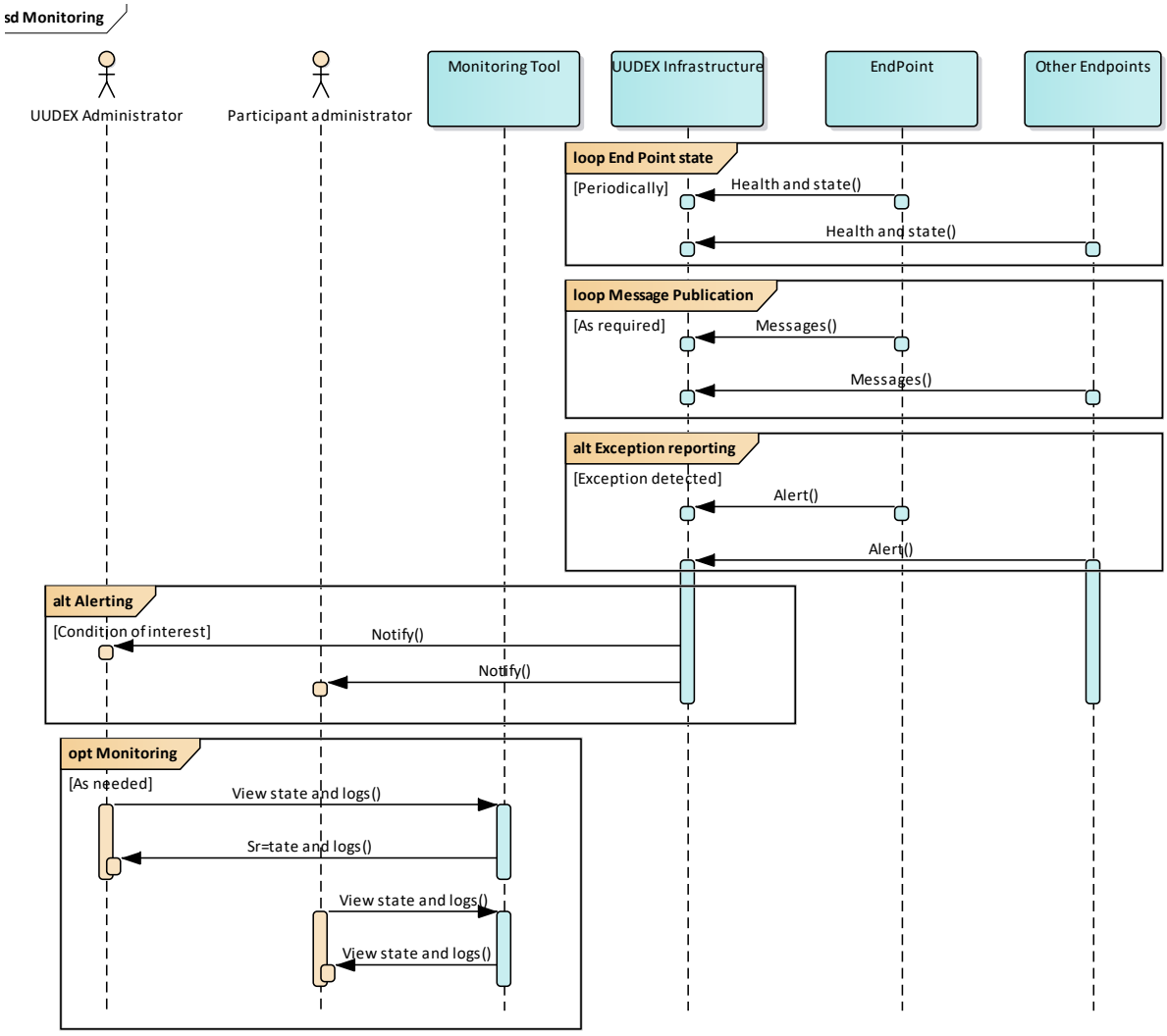

Figure 7-1: Monitoring

Notifications (including Alerts) are discussed in Section 5.3.

Additionally, notifications could be sent as simple network management protocol (SNMP) traps or logged via Syslog messages for use by third-party management tools and enterprise event management software.

8.0 Extensions

UUDEX is designed to allow for both evolution and extension. In the case of evolution, there could be new versions of data element types that need to be accommodated. For extensions, new data element types might be defined, or information might be added for existing data element types. Extensions also could be provided in the form of APIs that would be used by endpoints.

9.0 References

The following informative references are applicable to this document:

- UUDEX Functional Requirements
- UUDEX Protocol Design
- IEC 61970-301 (CIM)
- IEC 60870-6 (TASE.2, a.k.a. ICCP)
- IETF RFC 4180 (csv) (https://tools.ietf.org/html/rfc4180)
- IETF RFC 7159 (JSON) (https://tools.ietf.org/html/rfc7159
- XML Standard (http://www.w3.org/standards/xml/)
- Java Message Service (JMS) 2.0 (https://jcp.org/en/jsr/detail?id=343)
- Data Distribution Service (DDS) (https://www.omg.org/omg-dds-portal/)
- MQTT Standard (https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html)
- OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0 (http://docs.oasis-open.org/amqp/core/v1.0/amqp-core-complete-v1.0.pdf)
- Pesonen, Lauri IW, David M. Eyers, and Jean Bacon. "Access Control in Decentralised Publish/Subscribe Systems." J. Networks 2, no. 2 (2007): 57-67.
- Pesonen, Lauri IW. A capability-based access control architecture for multi-domain publish/subscribe systems. No. UCAM-CL-TR-720. University of Cambridge, Computer Laboratory, 2008.
- Hohpe, Gregor, and Bobby Woolf. Enterprise integration patterns: Designing, building, and deploying messaging solutions. Addison-Wesley Professional, 2004.
- Birman, Kenneth P. Guide to Reliable Distributed Systems: Building High-Assurance Applications and Cloud-Hosted Services. Springer Science & Business Media, 2012.
- North American Electric Reliability Corporation (NERC) CIP-004-6: Cyber Security — Personnel & Training (https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States)

Appendix A – Existing Industry Organizational and Personnel Vetting Procedures

Before two Universal Utility Data Exchange (UUDEX) Endpoints can establish a connection to share information, a reason for sharing information needs to be established. In some cases, the reason is based on regulatory obligations (e.g., in North America. the electricity sector sharing of information between a transmission owner and a reliability coordinator as mandated by North American Electric Reliability Corporation [NERC] Standards), contractual obligations (e.g., sharing of market-related data among market participants), or for public benefit (e.g., sharing of outage information to a public website or with first responders). In each case, the information publisher needs to be sure that the consumer: 1) needs to have access to the information, and 2) will use it only for the purposes for which it is shared. This requires that the two organizations either have established a level of trust or are mandated to "trust" each other under penalty of regulatory sanctions. The specific procedures for establishing trust are beyond the scope of this document.

Individuals designated to fulfill roles of high responsibility within a U-Instance need to be thoroughly vetted to ensure that they are trustworthy. U-Administrators will be able to view all data in the U-Instance and control who receives information exchanged over UUDEX. U-Instances might exchange information that is the subject of national regulations, commercial contract agreements, and/or other limitations on use. The sensitivity of this data might require the application of certain vetting requirements for U-Administrators (e.g., access to information controlled by national regulation might require, by law, background checks performed by a national law enforcement body).

The identification of parties to serve in sensitive UUDEX roles needs to be informed by an understanding of relevant regulations and other agreements that might stipulate limitations on access and ensure that the vetting process accounts for these limitations. Failure to adequately vet individuals for these roles could be very costly and damaging to all the organizations using the U-Instance in question. Even if an inadequately vetted administrator is not actively seeking to leverage their authority to compromise the security of the U-Instance, they are unlikely to be aware of data-use constraints that were not identified as part of the vetting process, which could lead to accidental misuse of data. For these reasons, the vetting process for individuals with authority over aspects of U-Instances, especially the U-Administrators, needs to be thorough and comprehensive, and including an ongoing and periodic training component so that vetted individuals understand their role in protecting the U-Infrastructure and the data communicated through it.

In the United States, there are several existing frameworks for performing this increased scrutiny. These frameworks are briefly described below:

- For North American organizations that support reliable operations of the bulk electric system and are required to comply with NERC Standard CIP-004, the Personnel Risk Assessment process provides a framework for establishing and conducting a risk assessment for staff who have access to the control systems that operate the bulk electric system. This framework could be adapted and adopted by other organizations.

- The Transportation Worker Identification Credential[1], also known as TWIC®, is a U.S. government identification credential and is required for workers who need access to secure areas of maritime facilities and vessels. Many of these maritime facilities are located at power plants, so many electric utilities are familiar with the credential and the approval process. The process involves filling out an application, and after the application has been processed, an in-person interview to complete the process.

Organizations may also have additional vetting procedures that can be adapted or used—for example, as part of the hiring process or for internal transfers. Governmental organizations such as municipal utilities may have more stringent requirements that include criminal background checks.

Individual organizations that are establishing a U-Infrastructure for internal purposes (e.g., synchronizing data between a primary and backup control center) may have specific requirements or procedures that are different than those for administrators of external U-Connections.

[1] See https://www.tsa.gov/for-industry/twic

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov