Customer Communications Portal Management – Security Issues

1 Descriptions of Function

Issues confronting an Energy Company's Management Systems responsible for management of Telecommunications and Access Networks to support Customer Communications Portals.

1.1 Function Name

Customer Communications Portal Management: Security Issues

1.2 Function ID

IECSA identification number of the function

C-2.2

1.3 Brief Description

This scenario attempts to describe key issues relevant to the operation of Management Systems in a large Energy Company (Electric and/or Gas and/or Water with several million customers) that provide access to information from and access to control devices located at customer sites. Access to information from devices and access to control one or more devices on the customer premises is provided via Customer Communications Portals.

Here, we focus on security management issues.

1.4 Narrative

The key issue for the development of a security strategy and a set of policies that guide the development of a security plan is to clearly define the risks inherent in developing a network as described in this paper. This networking model is one that provides information and access to control actions involving significant numbers of Customer Communications Portals and many users both internal to the Energy Company and to outside entities.

In order to help frame the description of the security management issues, four major components of security; Confidentiality, Authentication, Nonrepudiation and Data Integrity, along with some examples of how they are pertinent to the Customer Portal environment will be reviewed:

Confidentiality deals with the need to keep information secret, i.e., keeping information from unauthorized users. In the context of the Customer Communications Portal there will be a great deal of information that will need to be kept confidential. For example, a particular customer's (say, a manufacturer of a certain type of widget) energy usage would be of great interest to a competitor as it would be an indication of inventory build up or increased sales of their product, likewise a reduced level of energy consumption could indicate problems. There are many other instances of similar situations. For each of these situations, it is imperative that no one other than the Energy Company, other authorized users and the particular customer should have access to energy usage and/or other information pertaining to that particular Customer. Given that there are many different Access Network components, data storage components, and internal Energy Company networks and perhaps several wirelesses network components, weakness in each or any of these components might enable someone desiring this information, access to the information.

Authentication in the context of the Customer Communications Portal environment is a mechanism that uniquely identifies who or what entity is trying to access information over the Customer Communications Portal networks and/or related databases. For example, is a Customer who accesses Customer Portal information over the Internet or the Customer Communications Portal Access Network(s) really the individual or entity that is implied by the transaction taking place? Or is it an imposter (perhaps an interested competitor) who is trying to obtain information valuable for his or her own purposes? There are many similar situations in a network and systems as complex as the Customer Communications Portal/Access Networks. Authentication is especially critical in those instances where the users need to access Customer Portal information over the Internet or via connections from another data communications network, as each network has it's own security domain, policies and thus, providing a common level of security integration will be a very difficult task. For example a Regulator accessing Customer Communications Portal information initiating a session from an agency network workstation accessing an Energy Company server via the Internet is bridging several networks with varying levels of security. Policies, access control mechanisms and security mechanisms must be in place to enable authenticated users access to the information that they need. But, mechanisms must be in place to ensure that imposters cannot obtain this access. Authentication is a key component of this capability.

Nonrepudiation is a mechanism that provides the means for a third party to verify the integrity and origin of data and the proof of delivery of this data. For example, if an authorized individual representing an ISO requests a large industrial customer to provide a certain level of auxiliary power services, and the customer agrees, the use of nonrepudiation services will provide a record of the request and response and the fact that the transaction took place. Neither the ISO representative nor the customer can at a later date deny that the request and its acceptance was made. In other words, it can be verified that the ISO representative indeed made the

request, the Customer indeed agreed to provide the services and that the request, the individuals were in fact the ones being represented in the transaction and that the requests and response did take place. In order to accomplish this, technologies such as public-key cryptography, digital signatures and digital notary or equivalent must be employed.

Data Integrity is protected if the Security Management System if it ensures that data conveyed over a network is complete and whole and that an unauthorized user or system has not modified it, added to it, or deleted it during its transmission or storage. In the context of the Customer Portal environment the Security Management System Data must ensure that data transmitted over the Customer Portal Access Network or data that has been stored in any Computer System or storage device that is part of associated systems is indeed whole and that it has not been modified or added to in any way. Maintaining Data Integrity is an essential element in the operation of the Customer Communications Portal, Access Network and related computing systems. For example, If there are ISO requests for local generation to meet system needs, it is critical that any records of the transaction, along with data relative to the energy flows, duration, etc. be accurately and transmitted in it's entirety across the network and accurately stored in appropriate databases. It will be essential that the data is complete and whole and that it has not been modified added to or deleted during its transmission and storage. As many of these transactions may be taking place in a semi or fully automated fashion, with little human interaction it is imperative that security mechanisms such as Data Integrity be in place to ensure accuracy and reliability of any critical data transmitted over the Access Data networks and stored in Customer Communications Portal/related databases.

Auditability in the context of the Customer Communications Portal environment is a mechanism that provides records of activities that can attest to the security services. In other words a security audit tool or set of tools will enable logging of any attempted security breach from within or outside of the Energy Company networking environment. The audit trail should include information on the type of breach such as host break-in, network break-in, multiple incorrect passwords and user ID attempts, etc.

A Security System Manager through the use of a Security Management System faces many difficult tasks in order to provide access to Customer Communications Portal data in a manner that ensures that only authorized uses have access to the data, and have the capability to download software or issue commands to Customer Portals. There are several broad concerns and actions the Security Manager must undertake, to initially get the system up and running and then to effectively operate the system on an ongoing basis. The Security Management System must be configured to implement the appropriate operating and security policies as determined and agreed to by the key business entities and as defined in the System Manager by:

1) Defining the risks to the Energy Company, external entities, Government Agencies and Regulators and other users of Customer Portal data. Each Energy Company will have different networking and computing environments, so there will be different levels of risk depending on each company's particular environment. Following is a listing of some of the risks that are common to many corporate organizations. It is by no means intended to be a comprehensive listing:

a) Data Theft. Any data stored on a computing device or routed or transmitted through a network (and especially if the data can be accessed via the Internet) is vulnerable to theft. The key issue to consider is how valuable is the data and how much effort and cost is it worth expending to protect this data. In an Energy Company environment data theft can result in significant financial costs, some data is protected by Regulatory statues the disclosure of this data could result in fines or other penalties, competitive advantage could be lost for it's customers and there can be exposure to fraud for both the company and its customers. It is critical that the owner(s) of this data make an evaluation of how valuable the data is to them before developing security plans. Security systems used to implement Authentication and Data Integrity in the Customer Portal systems will help mitigate Data Theft.

b) Data Destruction: It is possible that data can be deleted through some action of a user. This will require that backup media be scanned to retrieve the data or in a worst-case scenario, that the data must be recreated (if possible). In Energy Company environments data destruction could lead to serious consequences. The key issue again, is how valuable is the data and how much effort and cost is it worth expending to protect this data. Security systems used to implement Authentication and Data Integrity in the Customer Portal systems will also help mitigate Data Destruction.

c) Loss of Network or System integrity: It is possible that by various means that hackers have at their disposal (Trojan Horse, etc.) the integrity of a key host or other device is compromised or disabled. This can be a very serious problem that can take a significant amount of time to analyze and repair, the cost of which can be quite expensive. There is no one tool that can address these threats. Use of firewalls and other perimeter defense mechanisms, Tools that uncover and disable viruses, worms, Trojan horse software and other attack software are critical to minimizing these risks.

d) Loss of Network or System accessibility and availability: If key components of the Network are disabled by intruder action or by configuration changes, accessibility and availability of the network and access to the data can be lost for some time. There is no one tool that can address these threats. Use of firewalls and other perimeter defense mechanisms, Tools that uncover and disable viruses, worms, Trojan horse software and other attack software are critical to minimizing these risks. It is critical that access to any controlling software residing in any portion of the Customer Portal Access Networks be restricted to only authorized users. Authentication mechanisms should be employed to enable access. Computing systems should to the extent possible utilize access control mechanisms on any network interface. Auditing tools should be provided on these computing systems as well as integrity checking tools so that any unauthorized activity can be quickly identified.

2) Assigning and managing Access Classes and authorization levels that reflect the policies defined by the System Manager, including but not limited to the following tasks:

a) Assigning User Identifications and Passwords and monitor password usage to ensure that they are changed on a periodic basis by all users,

b) Ensuring that application log-in procedures are followed by all users,

c) Ensuring that appropriate encryption mechanisms (Triple DES, AES, Private Key, etc) are employed on a per entity, per user and application basis

d) Implement a Security Key Management system for those situations that make it appropriate to utilize Public Key Encryption in order to meet the security requirements defined by the System Manager.

   i) Provide mechanisms to recover lost keys. This could take the form of a Key Escrow System where several parties hold portions of specific encryption keys. For example if data from a Customer Portal is especially sensitive and it was encrypted and the Customer Key was lost, then the parties that held portions of the key can be enlisted to provide their portions of the key in order to ensure that the Customer's data can be recovered. The portions of the key held by other parties would not be sufficient to individually decrypt the data, but when combined the key and the encrypted data can be recovered. Note that this is only an example of what mechanisms might be employed to cover this type of contingency.

3) Implementing firewalls and building perimeter protection systems that will block unauthorized users from gaining access to networks, databases and other resources that may impair the operation of the Customer Portal System and integrity of the data. Note this is a task that cannot be predefined, in any given Energy Company environment there may be several computer systems and databases that must be protected from unauthorized access from both internal and external entities and individuals. Unfortunately, the more segmentation the higher the engineering and maintenance costs.

4) Implementing Virtual Private Network connectivity for outside entities and individuals Regulators, Governmental Agencies, etc. outside of the Energy Company networking environment to enable access to data they are authorized to obtain. Authentication mechanisms will need to be used in many cases to enable adequate levels of security protection.

1.5 Actor (Stakeholder) Roles

Describe all the people (their job), systems, databases, organizations, and devices involved in or affected by the Function (e.g. operators, system administrators, technicians, end users, service personnel, executives, SCADA system, real-time database, RTO, RTU, IED, power system). Typically, these actors are logically grouped by organization or functional boundaries or just for collaboration purpose of this use case. We need to identify these groupings and their relevant roles and understand the constituency. The same actor could play different roles in different Functions, but only one role in one Function. If the same actor (e.g. the same person) does play multiple roles in one Function, list these different actor-roles as separate rows.

Grouping (Community)		*Group Description*
Actor Name	*Actor Type (person, device, system etc.)*	*Actor Description*

Replicate this table for each logic group.

1.6 Information exchanged

Describe any information exchanged in this template.

Information Object Name	*Information Object Description*

1.7 Activities/Services

Describe or list the activities and services involved in this Function (in the context of this Function). An activity or service can be provided by a computer system, a set of applications, or manual procedures. These activities/services should be described at an appropriate level, with the understanding that sub-activities and services should be described if they are important for operational issues, automation needs, and implementation reasons. Other sub-activities/services could be left for later analysis.

Activity/Service Name	*Activities/Services Provided*

1.8 Contracts/Regulations

Identify any overall (human-initiated) contracts, regulations, policies, financial considerations, engineering constraints, pollution constraints, and other environmental quality issues that affect the design and requirements of the Function.

Contract/Regulation	*Impact of Contract/Regulation on Function*

Policy	*From Actor*	*May*	*Shall Not*	*Shall*	*Description (verb)*	*To Actor*

Constraint	*Type*	*Description*	*Applies to*

2 Step by Step Analysis of Function

Describe steps that implement the function. If there is more than one set of steps that are relevant, make a copy of the following section grouping (Preconditions and Assumptions, Steps normal sequence, and Steps alternate or exceptional sequence, Post conditions)

2.1 Steps to implement function

Name of this sequence.

2.1.1 Preconditions and Assumptions

Describe conditions that must exist prior to the initiation of the Function, such as prior state of the actors and activities

Identify any assumptions, such as what systems already exist, what contractual relations exist, and what configurations of systems are probably in place

Identify any initial states of information exchanged in the steps in the next section. For example, if a purchase order is exchanged in an activity, its precondition to the activity might be 'filled in but unapproved'.

Actor/System/Information/Contract	*Preconditions or Assumptions*

2.1.2 Steps – Normal Sequence

Describe the normal sequence of events, focusing on steps that identify new types of information or new information exchanges or new interface issues to address. Should the sequence require detailed steps that are also used by other functions, consider creating a new "sub" function, then referring to that "subroutine" in this function. Remember that the focus should be less on the algorithms of the applications and more on the interactions and information flows between "entities", e.g. people, systems, applications, data bases, etc. There should be a direct link between the narrative and these steps.

The numbering of the sequence steps conveys the order and concurrency and iteration of the steps occur. Using a Dewey Decimal scheme, each level of nested procedure call is separated by a dot '.'. Within a level, the sequence number comprises an optional letter and an integer number. The letter specifies a concurrent sequence within the next higher level; all letter sequences are concurrent with other letter sequences. The number specifies the sequencing of messages in a given letter sequence. The absence of a letter is treated as a default 'main sequence' in parallel with the lettered sequences.

Sequence 1:

```
1.1 - Do step 1
1.2A.1 - In parallel to activity 2 B do step 1
1.2A.2 - In parallel to activity 2 B do step 2
1.2B.1 - In parallel to activity 2 A do step 1
1.2B.2 - In parallel to activity 2 A do step 2
1.3 - Do step 3
1.3.1 - nested step 3.1
1.3.2 - nested step 3.2
```

Sequence 2:

```
2.1 - Do step 1
2.2 – Do step 2
```

#	Event	Primary Actor	Name of Process/Activity	Description of Process/Activity	Information Producer	Information Receiver	Name of Info Exchanged	Additional Notes	IECSA Environments
#	*Triggering event? Identify the name of the event.*[1]	*What other actors are primarily responsible for the Process/Activity? Actors are defined in section0.*	*Label that would appear in a process diagram. Use action verbs when naming activity.*	*Describe the actions that take place in active and present tense. The step should be a descriptive noun/verb phrase that portrays an outline summary of the step. "If …Then…Else" scenarios can be captured as multiple Actions or as separate steps.*	*What other actors are primarily responsible for Producing the information? Actors are defined in section0.*	*What other actors are primarily responsible for Receiving the information? Actors are defined in section0.* *(Note – May leave blank if same as Primary Actor)*	*Name of the information object. Information objects are defined in section 1.6*	*Elaborate architectural issues using attached spreadsheet. Use this column to elaborate details that aren't captured in the spreadsheet.*	*Reference the applicable IECSA Environment containing this data exchange. Only one environment per step.*

2.1.3 Steps – Alternative / Exception Sequences

Describe any alternative or exception sequences that may be required that deviate from the normal course of activities. Note instructions are found in previous table.

#	Event	Primary Actor	Name of Process/Activity	Description of Process/Activity	Information Producer	Information Receiver	Name of Info Exchanged	Additional Notes	IECSA Environments

[1] Note – A triggering event is not necessary if the completion of the prior step – leads to the transition of the following step.

2.1.4 Post-conditions and Significant Results

Describe conditions that must exist at the conclusion of the Function. Identify significant items similar to that in the preconditions section.

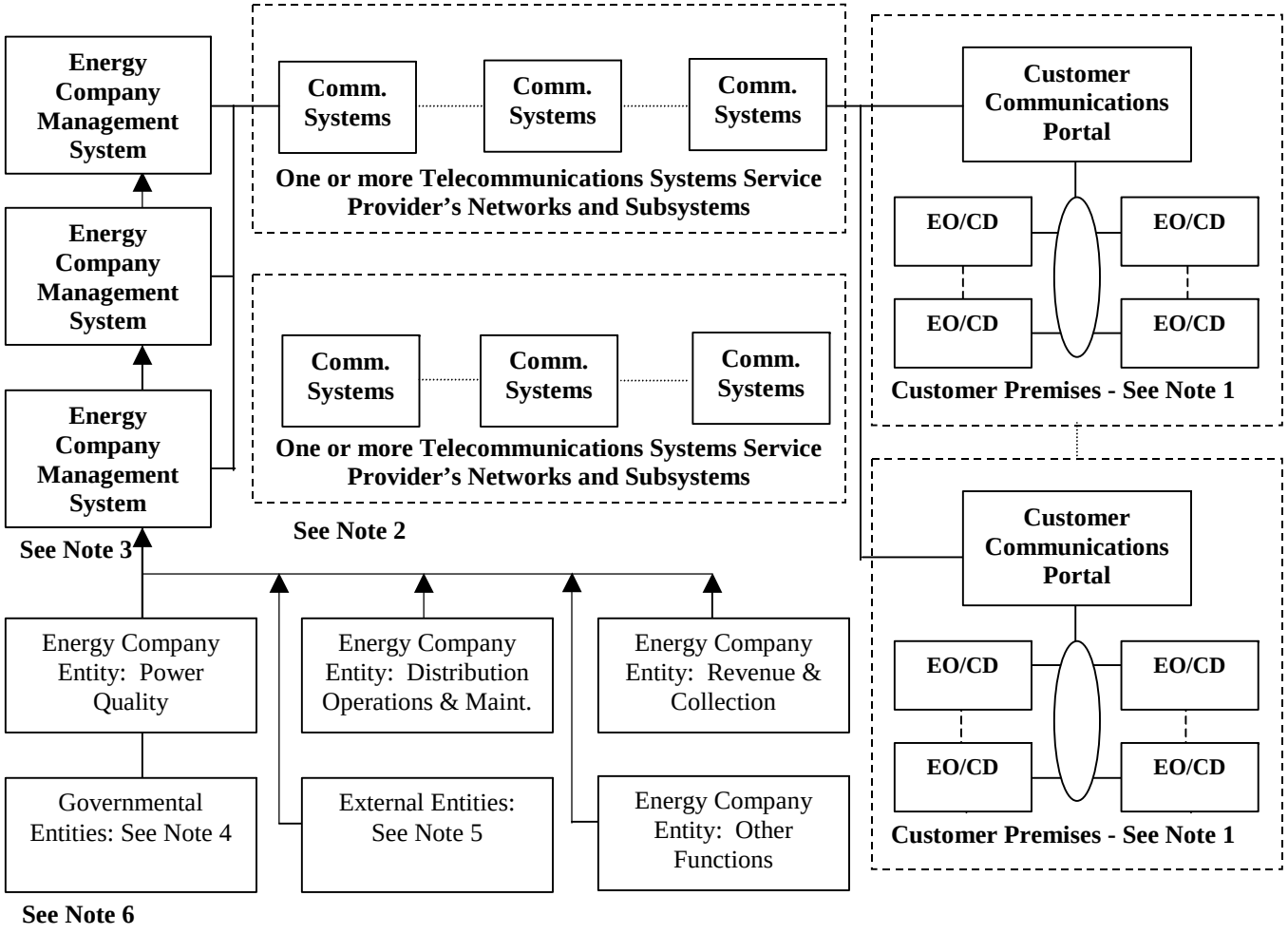
Describe any significant results from the Function

Actor/Activity	*Post-conditions Description and Results*

2.2 Architectural Issues in Interactions

Elaborate on all architectural issues in each of the steps outlined in each of the sequences above. Reference the Step by number..

2.3 Diagram



Legend:

EO/CD Energy Company Observable/Controllable Devices

(Systems, Hardware, Software, Applications, etc.)

Notes:

1. EO/CD's may be interconnected to the Customer Communications Portal by various LANs or wired/wireless systems
2. Many diverse Telecommunications Access Networks may be used to connect to Portals
3. Several different Energy Management Systems may be required including an overall "System Manager" (that deals with overall policies, views of various business entities, etc.) a Security Management System (that deals with authorization, security, reporting and related issues) and a Network Management System (that deals with the Customer Portal Access Networks and data communications issues)
4. Several Governmental Entities will need to access certain information that will be obtained via the Customer Communications Portals. Some of these are: PUC's, FERC, FTC, FCC, FBI, DHS, NIST, various State and Local Governmental Agencies, etc.
5. Several Entities outside of the Energy Companies will need to access certain information that will be obtained via the Customer Communications Portals. Some of these are: ISO, RTO, Independent Power Generators, various appliance manufacturers, etc
6. All of the Entities shown in the boxes are routed through the various Key Management Systems. This is meant to signify that the policies, procedures, access control rights, security and other enablers and constraints of these Management Systems will tailor the views of the data that these entities can access and the control messages that they are authorized to initiate. This does not imply that there will actually be individual computer/software systems that these entities must be routed through. The diagram represents a logical view , not a physical view.

3 Auxiliary Issues

3.1 References and contacts

Documents and individuals or organizations used as background to the function described; other functions referenced by this function, or acting as "sub" functions; or other documentation that clarifies the requirements or activities described. All prior work (intellectual property of the company or individual) or proprietary (non-publicly available) work must be so noted.

ID	Title or contact	Reference or contact information
[1]		

[2]		

3.2 Action Item List

As the function is developed, identify issues that still need clarification, resolution, or other notice taken of them. This can act as an Action Item list.

ID	Description	Status
[1]		
[2]		

3.3 Revision History

For reference and tracking purposes, indicate who worked on describing this function, and what aspect they undertook.

No	Date	Author	Description
0.			

This page intentionally left blank.