PERMANENT STANDARDS WORKING GROUP

APPENDIX F

DATA SECURITY IN DIRECT ACCESS

July 29, 1998

PSWG APPENDIX F: Data Security in DA

Introduction

A proposal was drafted by Ed Quiroz of the Office of Ratepayer Advocates (ORA) to discuss issues addressing the appropriate implementation of data security practices and related standards that may impact the PSWG. This proposal presented some ideas and concepts for further security policy and standards evaluation, consideration and recommendations.

Goal

Data is transferred at each interface in the data chain described as part of each subgroup in the PSWG. The new business environment of this new commerce is not risk free. As electric restructuring moves toward electronic commerce, many of the new risks are unique to this environment. The previous integrated monopoly structure created data flows that possessed little or no value to others. In a restructured competitive industries, the value of this data dramatically changes. The methods through which this data is secured must also change.

The proposal was intended to describe data security concerns pertinent to the PSWG. It is also intended to initiate discussion on ongoing national standards that address data security and whether the PSWG should be considering these standards as part of its evaluation process.

Vulnerability Potential and implications

Table 1 is presented as a simple tool to evaluate potential data vulnerabilities, their implications and potential impacts on the different PSWG subgroups. It is presented , not as an all inclusive list, but, rather as a way of assessing risks at different data interfaces. The discussion in the PSWG should focus on the whether vulnerabilities existing at these interfaces are even currently understood and what standards exist that might address these vulnerable points.

PSWG APPENDIX F: Data Security in DA

Table 1 - Vulnerability and Implications

Vulnerability Assessment	Implication	Hardware	Communication	Data Management	Installation
False Identity	false identity or copied identity	Minimal risk for residential, greater risks for commercial/industrial	medium risk	Affects who can access various parts of MDMA functions	Minimal risks for residential, some risks for commercial/industrial
Privacy/Confidentiality breach	Transactions duplicated, copied	low risk	medium risk	Higher risk	Low risk
Data Theft/Fraud (unaccounted for Data) .	transactions inserted or suppressed	Unauthorized meter programming	Greater risks at concentrator	Higher risk as data is aggregated and goes through VEE	Minimal risk, unique identifier should eliminate
Data integrity Violations	transactions altered or duplicated	Minimal risk for residential, greater risks for commercial/industrial	Possible signal access and interception	Higher risk as data is aggregated and goes through VEE	Depends on device programming
Service denial	transactions intercepted or delayed	Minimal risk for residential, greater risks for commercial/industrial	Possible signal blockage	Higher risk as data is aggregated and goes through VEE	NA
Malicious Action	unauthorized access and data attacks/corruption	Minimal risk for residential, greater risks for commercial/industrial	Possible intrusion and unauthorized service access	Higher risk as data is aggregated and goes through VEE	Low risk

Discussion of Standards

Little discussion relative to specific standards in use or under development addressing data security has occurred in the PSWG. A discussion by Tom Chen relative to the meter discussed data security from a meter manufacturer perspective. A separate presentation made by Diane Biegal of Enron included discussion of security from a perspective of its integration into an EDI - based transaction system.

Jointly, the UDCs are recommending a combined strategy of Secure Socket Layer (SSL) as a mechanism for secure data transmission from the MDMA server to other parties over a common carrier. Additionally, the integration of firewall technology (for unauthorized external access), encryption or some other reasonable security measure(s) are minimums recommended. The

presence of these elements are a reasonable step, but may not represent a completely secured solution. No discussion has been had in the PSWG or its MDM subgroup whether this set of recommendations represent a reasonable approach or if other standards exist to provide similar functions or better security.

There are draft standards for EDI related to EDI security standards (i.e. X12.58). Additional standards include format for digital certificate as specified by International Telecommunication Union (ITU) X.509. This standard relates to the digital ID that provides users with third-party evidence of the server's and user authenticity, establishing that the server is operated by an organization with the right to use the name associated with the server's digital ID. This safeguard's users from trusting unauthorized sites. Web browsers generally perform server authentication automatically-the user only is only notified if authentication fails due to an expired certificate, mismatched URL, or other problem.

Security Architecture

An architectural perspective is crucial if a market is going to able to identify changing risks to its data. Its also a useful tool in providing better understanding where the resources should be directed when the data's value demands an appropriate scale up. Basically, the architectural view should consider these components as part of the building blocks:

AUTHENTICATION establishing identity within a transaction

AUTHORIZATION establishing privileges within a transaction

SESSION INTEGRITY establishing a concept that none of the information involved in a transaction is modified in any manner not known or approved by all participants in the transaction, either while in progress or after the fact.

PRIVACY/CONFIDENTIALITY
establishing allowance for only the participants in a transaction to know the details of the transaction. A further definition might mean that only the participants know that a transaction is occurring.

NONREPUDIATION
establishing the fact of participation in a particular transaction by all parties to the transaction, such that none of the parties can claim, after the fact, that they did not actually take part in the transaction

Proposed Security Policies Further Evaluation

Cryptography

Cryptography has made great strides over the past 20 years as computer networking has grown. There are now highly sophisticated ways to encrypt messages so that they can be decrypted and read only by the intended recipient. The entire set of technical and procedural rules for using keys, as well as the management structure for handling them, is called the public key infrastructure (**pki**).

The term "key" refers to a numerical algorithm used to encrypt a particular message or decrypt it so it can be read. In order for a cryptographic system to work, there must not only be a key, but a

secure way to distribute the key to the intended user. The safest way to distribute secret encryption keys is through public key systems, which use one key for encryption and a related but different key for decryption.

The public key infrastructure lets you:

- Receive a message and identify the only person who could have written it.
- Be sure that the message received is identical to the message sent.
- Establish these facts in a manner which should be enforceable in a legal setting such as a court.

Digital Signatures
This feature is currently supported as part of Secure Sockets Layer. Its implementation and practice has not been discussed.

Digital Certificates
A more industrial-strength and robust set of solutions involves digital certification. The electronic document binding a key to an individual or organization is called a digital certificate. In an electronic commerce setting, entities rely on the digital certificate to authenticate the identity of a party to a business transaction ("I trust that I'm buying from X because the digital certificate tells me so." Or "The digital certificate gives me confidence that I'm actually selling to Y and not to anyone else pretending to be Y.")

So why aren't more such systems in use? Because cryptography alone is not enough. It needs to be integrated as part of a set of data security process that provides:

- Key issuance;
- Certification;
- Revocation;
- Publication of revocation lists.

They are all crucial functions. A certificate is only as trustworthy as the organization that has issued it, and its willingness to take responsibility for its actions, as well as its ability to cover any liabilities that result if a certificate is issued in error.

Certificate Authorities
Institutions organized to issue certificates and manage the security system are called Certificate Authorities, or CAs. The CA binds an individual's identity to a unique public key.
The role of the CA is to:

- Own a unique public/private key pair for a particular user, and in some instances, for a particular transaction.
- Identify the individual who is seeking certification
- Provide secure management of its own private key
- Sign each certificate with its private key

- Provide repositories of revoked and valid certificates
- Provide client software as required
- Control access to private keys
- Properly identify subscribers
- Widely and securely distribute public key (used to verify signatures on certificates)
- Manage naming of subscribers in a robust fashion

(Remember, the safest way to distribute secret encryption keys is through public key systems, which uses one key for encryption and a related but different key for decryption. The public and private keys alternate in playing these roles.)

It should be noted that the California Independent System Operators (CAISO) has proposed a system of data security policies that recognizes levels of achievable security. This evaluation leaves room for scaling up to different levels of security and their attendant potential costs. The presence of digital certificates and certifying authorities are recognized as reasonable strategies toward achieving their data security objectives. The fact that an ITU standard such as X.509 exist that define this structure only lends further weight to evaluating its relevance to potential consideration in the PSWG.

PSWG APPENDIX F: Data Security in DA

Data Security Matrix Review

Table 2 Data Security Components and Deployment Strategy

Security component	Strategy	Meter Hardware	Meter Communica-tion	Meter Data Management	Meter installation
AUTHENTICATION establishing identity within a transaction	Password Encryption is a start. Future establishment of digital certification via certification authority	Low Requirement	Medium Requirement	High Requirement	Low Requirement
AUTHORIZATION	SSL feature. Future establishment of digital certification via certification authority	Low Requirement	Medium Requirement	High Requirement	Low Requirement
SESSION INTEGRITY	PGP	Low Requirement	Medium Requirement	High Requirement	Low Requirement
PRIVACY/CONFIDENTIALITY	PGP	Low Requirement	Medium Requirement	High Requirement	Low Requirement
NONREPUDIATION	Password Encryption provides no basis. Need establishment of digital certification via certification authority	Low Requirement	Medium Requirement	High Requirement	Low Requirement

The Strawman Proposal

Choice 1 - Business as usual - SSL3.0 and password and encryption of data on MDMA server is sufficient. The current system does not address the concerns of data integrity and non repudiation and thus may not be fully secure as the electric market moves forward.

Choice 2 - Evaluate further standards to develop Security policy that emphasizes scalability based on vulnerability potential. In moving to EDI based systems, develop security policies based on an architecture that integrates S/MIME , PGP and digital signatures.

Choice 3 - Evaluate further standards to develop Security policy that includes choices 1 and 2 and integrates Digital Certification and Certifying Authority (CA) practices.

Choice 4 - Recognize that data security policy cuts across the entire market place and a working group that has been created to look at data flow and integrity issues is a more appropriate home for further discussions rather than the PSWG.

PSWG Recommendations

Data security has a significant impact on the overall confidence in market data quality and integrity. As such, its perspective should be a complete market view. There is a working group currently evaluating market issues that address the areas of information flows, gaps and overall data integrity. This working group is the Data Quality and Integrity Working Group (DQIWG).

By unanimous vote, the PSWG adopted a recommendation to handoff further discussion and security policy evaluation, development and coordination to the DQIWG.