




CALIFORNIA ISO

**Participating Load
Acceptance Test
(PLAT)
Procedures**

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

REVISION HISTORY

REVISION NO.	DATE	DESCRIPTION
0.0	4/6/2000	Initial release of PLAT document
2.1	7/12/00	Revised to enhance test parameters
2.2	7/18/2000	Added validation of real time data
2.3	8/16/2000	Finalize document
2.4	9/14/2000	Incorporate comments
2.5	01/22/2001	Remove references to "Summer 2000"

Proprietary Notice

The information and data contained in this document may not be transferred or used, in whole or in part, for any purpose whatsoever without the written consent of the California ISO.

The preceding restrictions are not intended to preclude the specified use of the information and/or data in the execution of the contract that is identified in this document.




 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

TABLE OF CONTENTS

Section	Title	Page
1.	INTRODUCTION.....	1
1.1	Methodology.....	1
1.2	Discrepancy Reports.....	2
1.3	Logistics.....	2
1.4	Unavailability and Exceptions	2
1.5	Definitions	2
1.6	SYSTEM TEST CONFIGURATION AND SYSTEM INSPECTION	4
1.7	Test Overview.....	4
1.7.1	Owner Responsibility	5
2.	TEST PROCEDURE	5
2.1	Perform Data check on all I/O values	5
2.1.1	Analog Values	5
2.1.2	Digital Values (if applicable).....	5
2.1.3	Calculations.....	5
2.2	Perform Alarm and Data Flagging on Each Point of Connectivity	5
2.3	Timing Check.....	5
2.4	Validation of Real Time Data.....	5
2.5	Connectivity Validation.....	5
APPENDIX A		
	DISCREPANCY REPORT FORM.....	A-1
ATTACHMENT B		
1.	PURPOSE.....	B-1
2.	TEST CASES	B-1

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

2.1	Secure communication with a Data Proc Gateway (DPG)	B-1
2.2	Certificates on the cryptographic hardware module	B-1
2.3	CAL ISO CRL	B-2
2.4	CRL Communication	B-3
2.5	certificate expiration	B-3
2.6	Certificate Renewal	B-4
2.7	communication with mmi, the brig	B-5
2.8	DPG soft-based certificates	B-5
3.	REFERENCES	B-6

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

1. INTRODUCTION

The tests contained in this document are intended to verify that the Participating Load-DPG solution supplied by each owner meets the requirements of the ISO Market Participating Load Technical Standard. These tests will be performed with the active participation of California Independent System Operator (ISO) personnel.

1.1 METHODOLOGY


In order to run a successful test, it is necessary to establish the methods and general procedures which will be followed throughout the test. It is important that these rules and procedures be agreed to, and followed, by all parties during the test. In those cases where either methods or procedures are violated or changed, all parties shall acknowledge the change, reach a mutually agreeable resolution, and document said violations or changes. This resolution may involve mutually agreed to changes being made to the test procedure or resumption of the previously agreed to methods and procedures. Any additional detailed testing required to further authenticate functionality and specifications of deliverables will be conducted with the owner and ISO personnel in a Site Acceptance Test conducted at Folsom.

The owner and the ISO will each appoint a Test Supervisor that is solely responsible for representing their respective companies during testing. The mutual agreement of these Test Supervisors is necessary for approving the tests, any departure from the procedure, and any documentation of errors or omissions. The individuals from the ISO and the owner conducting each series of tests will sign off on each test procedure before submitting to the Test Supervisors from both companies.

The ISO Test Supervisor may add or delete items from the test, redirect the test, skip sections, or review sections at any time during the test provided such changes are consistent with the terms of the Technical Standard and do not result in equipment damage.

The tests are designed to run in the sequence given in this document, except where noted. Proper sequencing of tests is necessary because of set up procedures that may have occurred in previous tests. However, it is recognized that circumstances often require that the sequence be interrupted. Such an interruption or rescheduling requires both Test Supervisors to agree, the impact of the sequence interruption be recognized, and said interruption or rescheduling be documented.

Successful testing involves the active participation and understanding of test procedures by both parties. Primarily, personnel will execute the tests in order to expedite them. This will provide the ISO with the opportunity to observe and question test results. Upon successful completion of each section, the Test Supervisors will sign off that section as complete and accepted.

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

1.2 DISCREPANCY REPORTS

There may be cases where test results are not satisfactory. Appendix A contains a Discrepancy Report (DR) form where all unsatisfactory results are to be recorded. Discrepancy reports will also be used to document any outstanding issues arising from the tests.

1.3 LOGISTICS

The test period will begin with an orientation meeting of all personnel involved in the testing. The purpose of this meeting is to review testing procedures and to set forth what is to be accomplished by the end of the test period. The test period will conclude with a review meeting. In the case where unsatisfactory test results are obtained, this meeting will be used to determine the proper course of action to obtain satisfactory results.

1.4 UNAVAILABILITY AND EXCEPTIONS

All items or features that are a part of this system, but for one reason or another are not available at the time of the tests must be documented on the Discrepancy Report (DR) form located at Appendix A.


1.5 DEFINITIONS

Unless the context otherwise indicates, any word or expression defined in the Master Definitions Supplement, Appendix A to the ISO Tariff, and capitalized herein, has the same meaning where used in these principles with initial capitalization have the meanings set forth below:

Aggregated Loads: Multiple Loads represented as a Participating Load that meet ISO standards specified in this technical document, and that are approved by the ISO to schedule and bid Supplemental Energy and Ancillary Services as a single resource using some combination of individual Loads.

Aggregating Load Meter Data Server (ALMDS): a Meter Data acquisition and processing system, which is capable of passing Operational Data to the ISO SCADA interface for means of telemetry for one or more Aggregated Loads, within the parameters set forth in the ISO's standards for Participating Loads.

Bridge Remote Intelligent Gateway (BRIG): a device used to connect soft certificate DPGs to the Master IOC. Its purpose is to "bridge" the basic assurance afforded by the soft certificate to the high assurance represented in the hard card certificate of the Master IOC.

 CALIFORNIA ISO		Revision Date Revision No.	1/24/01 2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

Data Processing Gateway (DPG) equipment and software installed by a Generator that can interface to the ISO via the Energy Communications Network (ECN), or via a secured Internet connection, as a means for providing required tele-metered values from the Generating Unit to the ISO. The equipment and software implements TCP/IP compliant protocols (DNP 3.0 and Modbus) and conforms to ISO X.509v3 security mechanisms and protocols.

DNP 3.0: Distributed Network Protocol, Version 3.0, Data processing application that runs on master and remote devices and is used for data exchange.


Energy Communications Network (ECN): The overall ISO digital network architecture comprised of multiple sub-net, wide area, and local network segments.

EMS Telemetry: A process for measuring a quantity (amps, volts, MW, etc.) and transmitting the result via a communication system (radio, microwave, etc.) to a remote location for indication or recording.

ISO Supervisory Control and Data Acquisition Intelligent Interface (SCADA INTERFACE): An Internet or ECN enabled host that will receive Operational Data from the various Load data reporting devices. The ISO SCADA INTERFACE will be capable of retrieving Operational Data in various SCADA protocols and will be secured using X.509v3 Digital Certificates and Secure Socket Layer (SSL) for authentication and encryption.

ModBus: A data processing application that runs on master and remote devices and is used for data exchange. Modicon ModBus Protocol was developed originally for use with Modicon Programmable Logic Controllers.

Operational Data: Data (such as, but not limited to kV, MW, MVAR, MWh, MVARh, status) collected at defined periods by ISO EMS Telemetry that is

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

immediately available for ISO system operator's use in determining system conditions.

Ramp Rate: The measured rate, expressed in MW per minute, of a resource's ability to adjust its output or consumption.

Report by Exception: A data collection method that involves only retrieving data that has changed by predetermined parameters since the last scan period when the data was actually retrieved and is used to reduce the amount of data that must be retrieved during each scan.

Remote Intelligent Gateway (RIG) A device specified by the ISO to directly telemeter operational data from generator to the EMS. A RIG is required to be used by generators wishing to participate in the regulation market , as well as other ancillary services

Scan Rate: Predefined rate for receiving or sending data.

Secure Socket Layer (SSL): A security protocol that uses symmetrical and public key cryptography to secure communication over the Internet.

Transmission Control Protocol / Internet Protocol (TCP / IP): IP is used at the network layer of the Objective Systems Integrators (OSI) stack for routing packets. TCP is used at the transport layer of the OSI stack and works with IP for packet routing.


X.509v3: Digital certificate public key format defined by the International Telecommunications Unit (ITU) X.509 Standard.

1.6 SYSTEM TEST CONFIGURATION AND SYSTEM INSPECTION

This section is intended to verify that the system is assembled and ready for test. It is also intended to familiarize the test personnel with the various system components, the overall system configuration, and how the various components are interconnected.

1.7 TEST OVERVIEW

After the DPG has been connected and powered up, connectivity with the ISO interface shall be verified. Once communication has been verified, the test of inputs and outputs (I/O) will commence. A point to point check validating the correct scaling of the signal from the meter side through each device to the EMS display at the ISO will be conducted. . All analog inputs will be verified using a three-point check (0, mid-scale, and full scale). There should be no security problems and data will be validated, as scaled correctly through each device.

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

1.7.1 Owner Responsibility

The owner is solely responsible for supplying the means to drive the appropriate signals through the meter that reflect 0%, 50% and 100% output to the ISO EMS System. At the ISO's discretion, a field engineer may audit such test.

The owner is also solely responsible for supplying the ISO the scaling factors for each meter, along with test documentation. This applies to multiple meters making up one aggregated value. For aggregated loads, the value will be tested from the ALMDS device as a 0%, 50% and 100% value.

2. TEST PROCEDURE

2.1 PERFORM DATA CHECK ON ALL I/O VALUES

2.1.1 Analog Values

Input a manual value. Verify that the correct value and mapping is displayed at the workstations and the EMS displays. All analog inputs will be verified using a three-point check (0, mid-scale, and full scale).

2.1.2 Digital Values (if applicable)

Toggle each digital value. Verify that the correct value and mapping is displayed at the workstations and the EMS displays.

2.1.3 Calculations

Any points that are utilized as calculations in the DPG need to be demonstrated as to correct inputs and result. Logic results supplied to the EMS must be verified (i.e. data quality).

2.2 PERFORM ALARM AND DATA FLAGGING ON EACH POINT OF CONNECTIVITY

Test loss of communications alarms and bad data quality flags by disconnecting connections starting from the meter, then the DPG, and the Master Interface. Each one should alarm appropriately. Note any exceptions.


2.3 TIMING CHECK

Perform a timing check by inputting an analog step change in the meter output and verify the ISO SCADA display reflects the change within one minute and four seconds (per the Participating Load Technical Standard).

2.4 VALIDATION OF REAL TIME DATA


The ISO will validate the accuracy of real time data by comparing real time data with historical revenue metered data.

2.5 CONNECTIVITY VALIDATION

 CALIFORNIA ISO		Revision Date Revision No.	1/24/01 2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

After the PLAT testing to verify the correct values and performance, the DPG will remain connected to the ISO for 5 contiguous days to ensure connectivity stability. During that time, any failure to maintain the transmission of data will discredit the site from participating. This will require a retest once the problem has been resolved. Any configuration that causes the production system to fail will require a connectivity validation test to be successfully run on ISO's development system before reconnection to the production system.

Note: Once a site has completed Acceptance Testing and Validation, they may proceed with the process of applying for A/S Certification Testing. Owners should refer to G-213 and the attachments to the procedure at: <http://www.caiso.com/thegrid/operations/opsdoc/gcp/> for A/S certification information.

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.4
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

APPENDIX A

DISCREPANCY REPORT FORM

This Discrepancy Report (DR) form incorporates the necessary information for entering variances into the CAISO Variance Tracking System. Please familiarize yourself with this form. Please complete **all** sections of the form. Submission of incomplete DRs will result in a delay entry into the system. After completing the form, please submit hard copies to Diana Sarubbi (ISO Building 151 [ext. 2240], or by Fax to 916-351-2181). Variance Numbers are automatically assigned by the system and all hard copies are kept in the SAT binder for future reference.

A-1 Variance Tracking Classifications

Following is a description of the Variance Classification. Each Variance **MUST** be assigned a classification before it can be entered into the Variance Tracking System.

Emergency – Class 1 (Showstoppers)


Testing must stop. The Supplier/Owner must evaluate and correct the variance immediately before testing continues, but no longer than two (2) working days.

High Priority – Class 2

Testing can continue but with major workaround(s) and/or reduced functionality. The supplier/ Vendor must evaluate the variance and correct it system can be validated.

Medium Priority – Class 3

Testing can continue but with minimal workaround(s) and/or operator intervention. The system can be validated, but a commitment to resolve within two weeks must be agreed to.

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.4
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

DISCREPANCY REPORT			
California Independent Systems Operator			
Project No. _____			
Author _____		Variance No. _____	
Software <input type="checkbox"/>	Hardware <input type="checkbox"/>	Communications <input type="checkbox"/>	RTU <input type="checkbox"/>
Variance Class			
Emergency <input type="checkbox"/>	High <input type="checkbox"/>	Medium <input type="checkbox"/>	Low <input type="checkbox"/>
Description of Problem:			
Resolution:			
Corrected/Repaired By _____		Date _____	Author's Concurrence _____

ATTACHMENT B



CALIFORNIA ISO

**Participating Load Program
Security Subsystem**

**Information Technology Division
Technology Risk Management**

**Version 2.2
06/12/2000**



 CALIFORNIA ISO		Revision Date	06/12/00
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

TABLE OF CONTENTS

1.	INTRODUCTION	1
1.	PURPOSE	1
2.	TEST CASES	1
2.1	Secure communication with a Data Proc Gateway (DPG)	1
2.2	Certificates on the cryptographic hardware module	1
2.3	CAL ISO CRL	2
2.4	CRL Communication	3
2.5	certificate expiration	3
2.6	Certificate Renewal	4
2.7	communication with mmi, the brig	5
2.8	DPG soft-based certificates	5
3.	REFERENCES	6

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

1. PURPOSE

The purpose of this document is to define the Acceptance Test plan for the security subsystem of the Participating Load Program (PLP). The PLP team can use these test cases to ascertain that the PLP system meets the Application Security Policy and Compliance Test Criteria, section 4.1, Minimum Tests.

The test cases described in this document are additions to the tests that were completed during the Site Acceptance Testing (SAT) Test Cases. The test cases in this document are also in addition to the completed RIG Site Acceptance Tests (SAT), specifically the following Security Subsystem tests:

2. TEST CASES

2.1 SECURE COMMUNICATION WITH A DATA PROC GATEWAY (DPG)

This test demonstrates that a DPG unit can establish secure communication using a strong cryptographic algorithm and key length.

Procedure


1. Place a *snoop* process or device between the two communicating units.
2. Establish a secure telnet session with the DPG.
3. View the cipher suite and note the algorithm.
4. Enter 50 characters.
5. Using the *snoop*, verify that the characters are encrypted.
6. Enter the same 50 characters as in Step 5.
7. Verify that the encrypted stream is different than what was viewed in Step 6.

Acceptance:

Visual inspection of the data flow between the communicating unit confirms that the communication is encrypted. A print out of the cipher suite confirms usage of 3DES with 128-bit key or similar strength.

2.2 CERTIFICATES ON THE CRYPTOGRAPHIC HARDWARE MODULE

This test demonstrates that the SCADA Interface will only use the certificates on its cryptographic module for establishing sessions. This test must be administered after the unit has received the pass phrase of its cryptographic.

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

Procedure:

1. Establish a session with the SCADA Interface using its assigned cryptographic module
2. End session
3. Attempt to establish a session with the SCADA Interface using a different cryptographic module.

Acceptance:

In Step 3, the session will not be successful due to wrong module.

2.3 CAL ISO CRL


This test demonstrates that communicating parties consult an authentic CRL before establishing a secure session.

Procedure:

1. Issue a CRL that does not include a revocation for the certificates of the communicating parties.
2. Establish a session between the two parties.
3. Verify that a session is successfully established.
4. Terminate the session.
5. Issue a CRL that contains a revocation for the certificate of one of the communicating parties.
6. Load the CRL into the system of each communicating party.
7. Establish a session between the two parties.
8. Verify that a session cannot be established.

Acceptance:

In Step 3, the communicating parties successfully establish a session. In Step 7, the session cannot be established and the reason for failure is noted as *revoked certificate*. An audit record shows a failed attempt to establish a session using a revoked certificate.

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

2.4 CRL COMMUNICATION

This test demonstrates that each BRIG will correctly receive the most up-to-date CRL.

Procedure:

1. Issue a CRL that contains a revocation for the certificate of a communicating party.
2. Determine the MMI system and the port number where the CRL *listener* process resides.
3. Communicate a CRL to the listener process via authenticated FTP.
4. Use the credentials of a party whose certificate was revoked in Step 1 and attempt to establish a session with a BRIG.
5. Verify that a session cannot be established.

Acceptance:

In Step 3, the CRL is successfully communicated to the listener process. The CRL is propagated to each BRIG unit. In Step 5, the session cannot be established and the reason for failure is noted as revoked certificate.

2.5 CERTIFICATE EXPIRATION

This test demonstrates the BRIG generates an alarm starting 60 days before the expiration of the unit's certificate.

Note:


This test requires a cryptographic module whose user certificate will expires 60 days and 1 to 23 hours after the date of this test.

Procedure:

1. Insert the cryptographic module in the RIG.
2. Note the expiration date of the certificate.
3. Verify that an alarm is generated no later than 1 hour after certificate is 60 days from expiration.

Acceptance:

The BRIG unit generates a continuous alarm no later than 1 hour after certificate is 60 days from expiration.

 CALIFORNIA ISO	Revision Date	1/24/01
	Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure	Print Date	1/24/01
	Effective Date	

2.6 CERTIFICATE RENEWAL


This test demonstrates that a remote operator can remotely renew the certificate of the BRIG unit.

Procedure:

1. Use an MMI unit with its cryptographic module inserted in the bottom slot of the reader. The top slot should be empty.
2. Establish a remote session with BRIG.
3. Attempt to invoke the *SPYRUS tools*.
4. Verify that the invocation fails and that an audit record reflects the failed attempt.
5. At the MMI station insert the cryptographic module of an authorized operator in the top slot of the reader and log into it.
6. Invoke the *SPYRUS tools* script to create a key pair and a Certificate Signing Request (CSR) in PKCS 10 format.
7. Take the PKCS 10 file from the MMI unit and store it on a removable media (e.g., floppy disk).
8. Terminate the remote session and remove the cryptographic module from the top slot.
9. Obtain a digital certificate for the new public key and store the certificate on a removable media.
10. Terminate all sessions with the BRIG.
11. Attempt to establish a new session with the BRIG.
12. Verify that a session can be established and note the DN of the BRIG as recorded in the audit logs.
13. Verify that the DN of BRIG matches the DN in the current certificate.
14. Take the removable media that contains the certificate to the MMI unit.
15. Insert the cryptographic module of the authorized operator into the top slot of the MMI's reader.
16. Establish a remote session with the BRIG and invoke the *SPYRUS tools* script to import the new certificate chain to the card and to *activate* the key.
17. Terminate all sessions with the BRIG.
18. Attempt to establish a new session with the BRIG.
19. Note the new DN of the BRIG as recorder in the audit logs.

Acceptance:

An authorized operator can remotely change the key and the certificate of a slave BRIG. After successful re-keying, the BRIG will use its new key and certificate.

 CALIFORNIA ISO		Revision Date	1/24/01
		Revision No.	2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

2.7 COMMUNICATION WITH MMI, THE BRIG

This test demonstrates that communication with the MMI, the master, the DPG and the BRIG is only allowed via approved protocols and ports

Procedure:

1. Verify that all systems (DPGs, MMIs and BRIGs) are connected to the network.
2. Bring the systems up to their full functional state (i.e., all required services must be turned on).
3. Provide the IP addresses of the systems to the ISO Information Security Services.
4. Wait until ISO information security engineers run all their scanning tests and inform you of the result

Acceptance:

ISO information security engineers are satisfied that the BRIG only communicates via allowable ports and protocols.

2.8 DPG SOFT-BASED CERTIFICATES


This test will demonstrate the proper use of soft-based certificates by the DPG.

Procedure:

1. Test that an expired certificate is not honored.
2. Test that a revoked certificate is not honored.
3. Test that the session does not last beyond the validity period of the certificate.
4. Test that the session is dismantled if the certificate is revoked

Acceptance:

In Step 1, a session was not connected due to expired certificate. In Step 2, the session cannot be established and the reason for failure is noted as *revoked certificate*. In Step 3, the session ended when the certificate expired. In Step 4, when the certificate is revoked and the CRL is updated to the BRIG and DPG, the session terminates.

 CALIFORNIA ISO		Revision Date Revision No.	1/24/01 2.2
Participating Load Program Security Subsystem Site Acceptance Test Procedure		Print Date	1/24/01
		Effective Date	

3. REFERENCES

- 1) Remote Intelligent Gateway Prototype, Security Subsystem Functional Specification; version 2.3.2; CUDA Technical Team, 12/16/98.
- 2) Remote Intelligent Gateway Prototype, Security Subsystem Operational Specification; version 1.1; CUDA Technical Team, 1/7/99.
- 3) *RIG Security Subsystem: Specification for Key Rollover*, Version 1.1, CUDA Technical Team, 4/14/99.
- 4) Remote Intelligent Gateway (RIG) Security Subsystem Site Acceptance Test, version 0.4, CUDA Technical Team, 5/6/99