U.S. Department of Energy

PARS IIe – UCNI/OUO Solution Design

Solution Design Document

Igor Pedan

8/12/2014

Definitions

CIO – Chief Information Officer

CUI – Controlled Unclassified Information

DOE – Department of Energy

FIPS – Federal Information Processing Standards

HTTPS – Hypertext Transfer Protocol Secure

IP – Internet Protocol

NIST – National Institute of Standards and Technology

OUO – Official Use Only

PARS IIe – Project Assessment & Reporting System

SSL – Secure Sockets Layer

TFA – Two-Factor Authentication

TSL – Transport Layer Security

UCNI – Unclassified Controlled Nuclear Information

Document Scope

Identify proposed technology architecture and business processes for receiving, retaining, maintaining, and distributing UCNI/OUO documents within PARS IIe System.

UCNI/OUO Documents in PARS IIe

After completing preliminary discovery of multiple options available for encrypting and transmitting UCNI and OUO documents, PARS IIe team identified a possible solution for accepting and retaining UCNI and OUO documents within PARS IIe Document Management System powered by Microsoft SharePoint 2013 platform.

The key document security requirements that were identified for system are as follows:

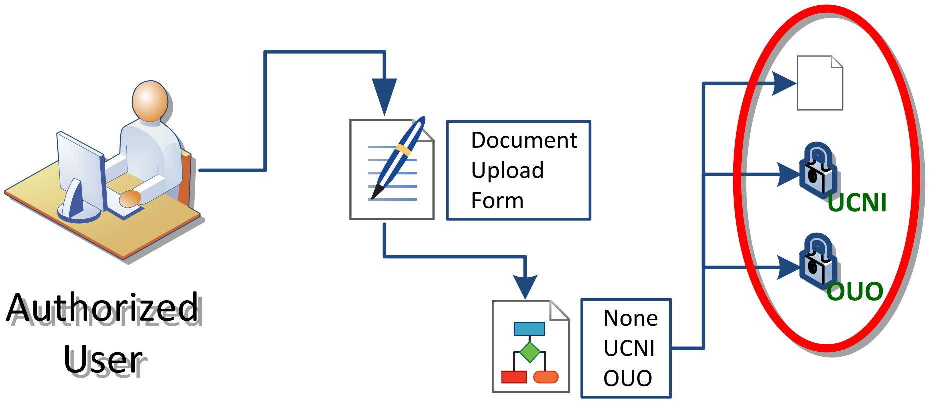
1. System shall allow users to identify documents as UCNI or OUO.
2. System shall protect all documents identified as UCNI or OUO by appropriate encryption method while in transit from user computer to PARS IIe server.
3. System shall protect all documents identified as UCNI or OUO by appropriate encryption method while at rest within the boundaries of PARS IIe system.
4. System shall provide appropriate access control to the documents identified as UCNI or OUO.

In addition, PARS IIe system was requested to accommodate the following business user requirements:

1. System shall allow user to download and view any UCNI and OUO document attached to the project they have read access to.
2. System shall allow temporary access to all UCNI and OUO documents associated with a project review (i.e. ICE, EIR, PPR, etc.) for users assigned to such project review.

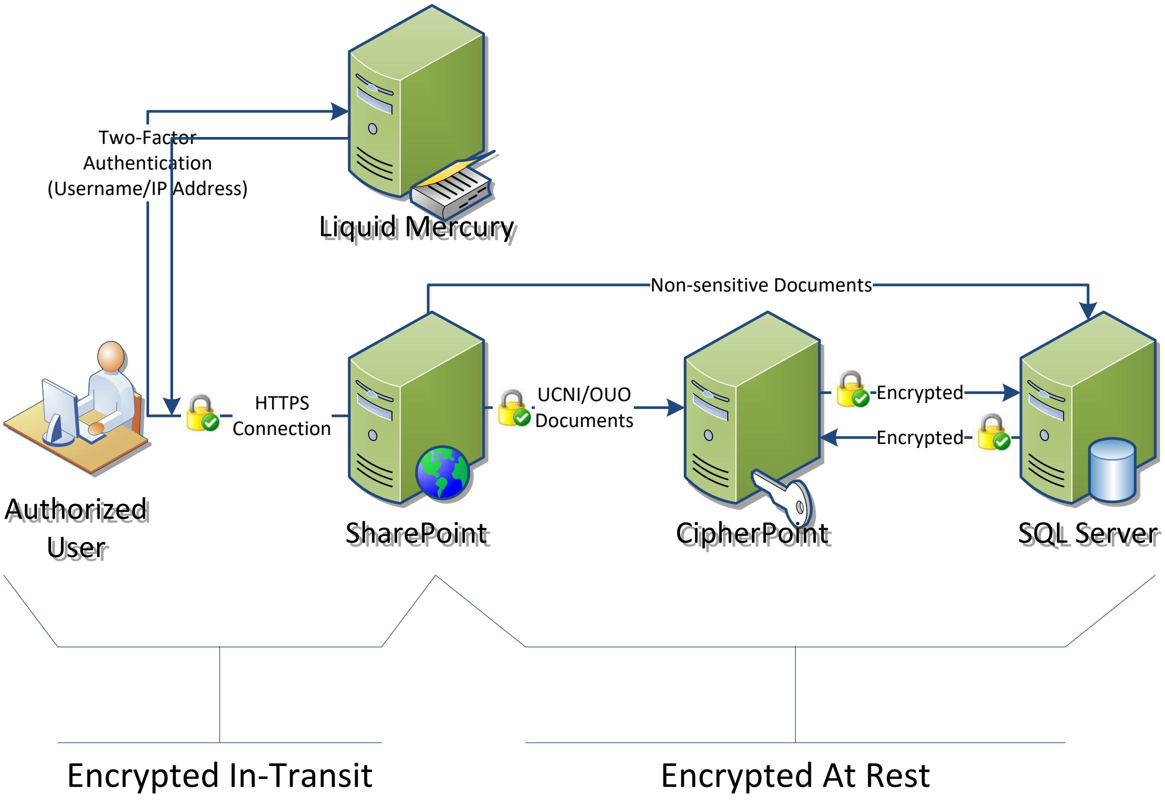
Based on these identified requirements, the following solution meets both cyber security and business user requirements.

SharePoint Marking of UCNI and OUO documents



User uploading documents to project, contractor, or review libraries will be required to make a selection for document to select Document Control status in order to mark it as None, UCNI, or OUO. Upon selection, document will be displayed within SharePoint libraries marked according to the user selection.

At Rest and In Transit Encryption & Two-Factor Authentication

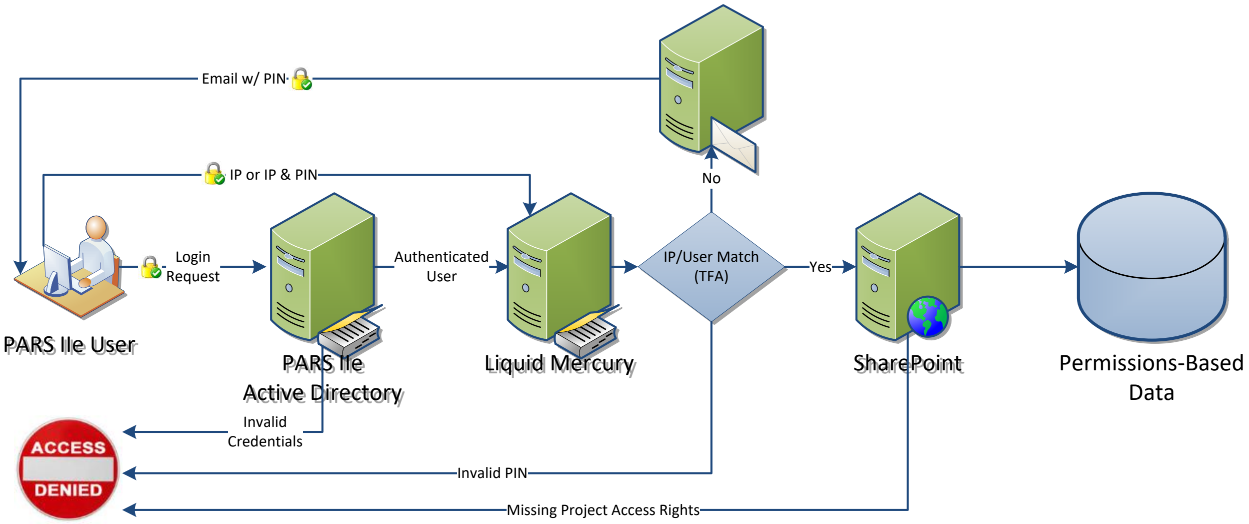


All of PARS IIe system uses HTTPS secure transfer protocol. This will allow users to transmit/upload documents to PARS IIe securely via encrypted HTTPS connection. Once the document reached PARS IIe server, CipherPoint Eclipse encryption software will encrypt the file to ensure it is securely stored in SharePoint SQL Server database.

At this time current configuration of PAR SIIe SharePoint does not support the use of files on SharePoint server and files are either at rest or in transit from the PARS IIe environment perspective. However, CipherPoint Eclipse software has built in “in use” encryption capabilities for SharePoint that would allow easy expansion of the functionality into allowing viewing and modifying controlled documents on the server in encrypted state by the authorized user(s).

Additional level of security is expected to be provided by the Liquid Mercury Two-Factor Authentication (TFA) Module. Additional protection with this method is ensured by the attacker needing to compromise not only username and password combination of a user with access to controlled information, but also that user’s registered PC and email account registered and controlled by DOE CIO.

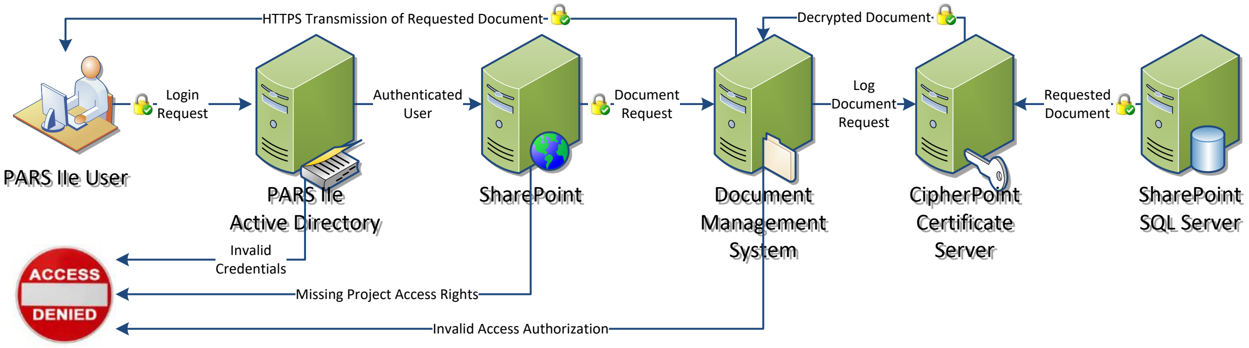
Two-Factor Authentication



The authentication will be performed based on IP address of a computer the user is using to connect to PARS IIe and username/password combination. Once user is authenticated through PARS IIe Active Directory, combination of IP address and Username is done at Liquid Mercury server. Initially, no user will have IP associated with username and therefore an email to an email address registered within MIS and PARS II Active Directory will be sent containing special one-time-use PIN information. User will then have to login providing this PIN in order to associate username with IP. If incorrect PIN is entered, user will be denied access to the system. If PIN is entered correctly, or this is a follow-on attempt by the user to enter the system after IP has been associated with the username, user will be placed in the system where he/she will be granted access to data based on the permissions managed through Access Management practices. This TFA module utilizes:

1. something user knows (username/password combination), and
2. something user has (registered email address and registered equipment with unique IP address).

Access Management & File Retrieval



Access to documents marked as UCNI and OUO will be managed through PARS IIe User Access Management Policies. In order for a user to gain access to UCNI or OUO document, user has to:

1. **successfully authenticate into PARS IIe system;**
   Only users with active DOE MIS account, approved by Program Office, authorized by Office of Management, and active in the system within the last 90 days are able to access PARS IIe domain.
2. **have access to a project or project review that contains controlled documents;**
   Only users approved by appropriate project official (FPD, Program Manager, Project Review Lead, etc.), authorized by Office of Management are able to access specific projects.
3. **be identified as needing routine (i.e. project analyst) or temporary (i.e. project review contractor) access to controlled information.**

Users who do not meet one or more access authorizations are denied access to protected information. Users who successfully pass all three authorization checks are able to download protected documents via HTTPS secure transfer protocol. Each request for access to controlled information is logged and logs will be reviewed on a regular basis.

<u>Additional Benefits of Proposed Solution</u>

1. Processes and technology selected for the solution are in full compliance with requirements prescribed by NIST 800-111 (protecting files at rest), FIPS PUB 140-2 (protecting files in use and in transit), and DOE O 471.1B (marking and accessing controlled information).
2. Server-based encryption and decryption of files supports web-based nature of the PARS IIe system, introduces significant cost savings, and provides much needed flexibility to the business users in area of document access control.
3. Solution is designed specifically to address requirements set forth for UCNI documents. With OUO requirements being more relaxed, adhering to UCNI standards provides sufficient controls for handling of both UCNI and OUO documents.