Identity and Access Management for Electric Utilities

Protect Our Power | Best Practices in Utility Cybersecurity Conference

Harry Perper (NIST NCCoE | The MITRE Corporation)
January 27, 2020

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

harry.perper@nist.gov

NCCoE Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

harry.perper@nist.gov

NCCoE Model

Engagement & Business Model

harry.perper@nist.gov

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

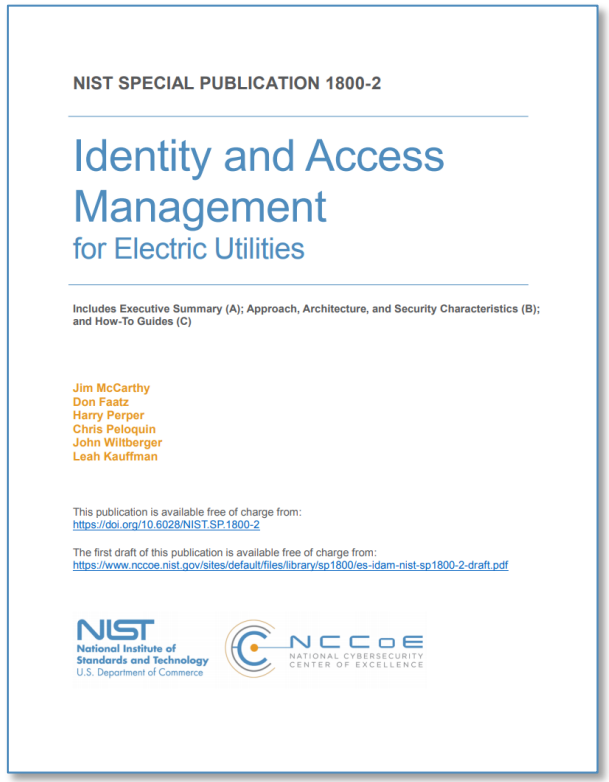
OUTCOME:
Advocate adoption of the example implementation using the practice guide

Publications

Practice Guides for the Energy Sector

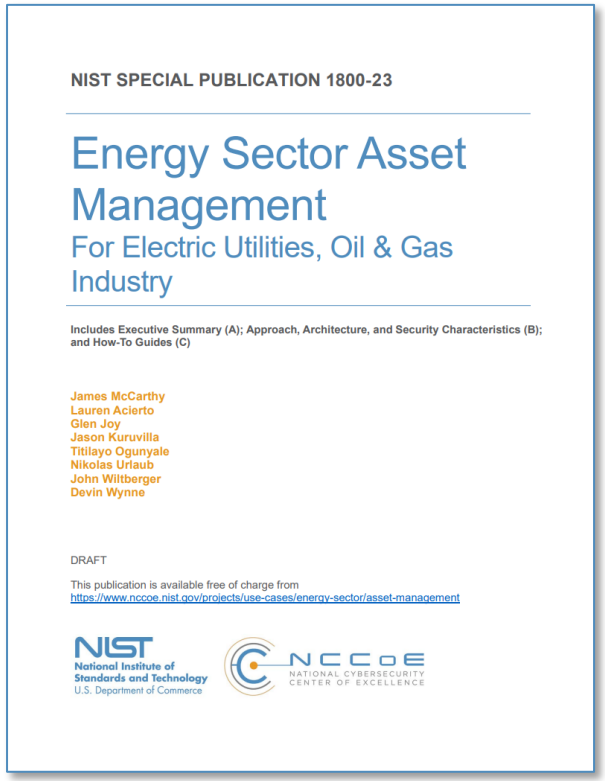
harry.perper@nist.gov

SP 1800-2: Identity and Access Management



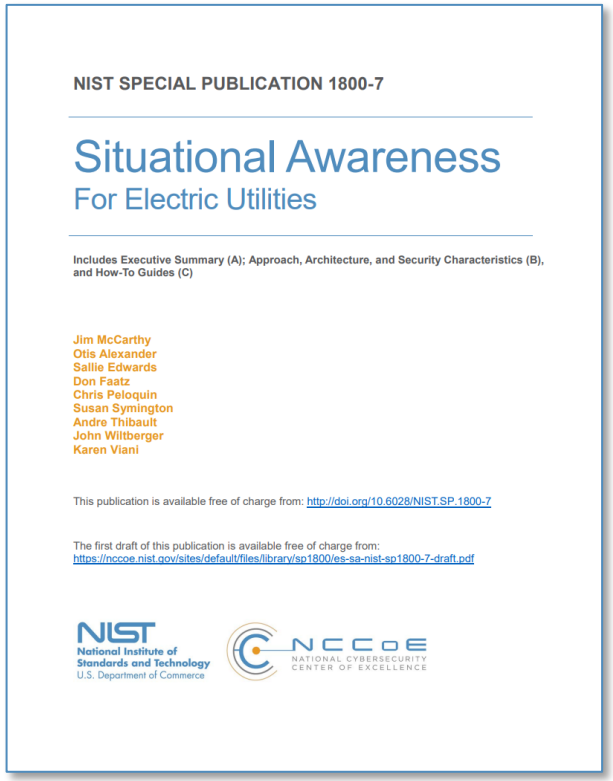
Control WHO is on your networks and in your facilities

SP 1800-23: Energy Sector Asset Management



Know WHAT is on your networks

SP 1800-7: Situational Awareness for Electric Utilities



Understand what the people and things on your networks are doing

Portfolio

- Attribute Based Access Control (SP 1800-3)
- Consumer/Retail: Multifactor Authentication for e-Commerce (SP 1800-17)
- Data Integrity: Identifying and Protecting
- Data Integrity: Detecting and Responding
- Data Integrity: Recovering (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Email Security (SP 1800-6)
- Financial Services: Access Rights Management (SP 1800-9)
- Financial Services: IT Asset Management (SP 1800-5)
- Financial Services: Privileged Account Management (SP 1800-18)
- Healthcare: Securing Electronic Health Records on Mobile Devices (SP 1800-1)
- Healthcare: Securing Picture Archiving and Communication Systems (PACS)
- Healthcare: Securing Wireless Infusion Pumps (SP 1800-8)
- Hospitality: Securing Property Management Systems
- Mitigating IoT-Based DDoS
- Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems

Portfolio (continued)

- Mobile Device Security: Cloud and Hybrid Builds (SP 1800-4)
- Mobile Device Security: Enterprise Builds
- Mobile Threat Catalogue
- Privacy-Enhanced Identity Federation
- Public Safety/First Responder: Mobile Application SSO (SP 1800-13)
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Mgmt (SP 1800-16)
- Transportation: Maritime: Oil & Natural Gas
- Trusted Cloud (SP 1800-19)

Practice Guide

NIST NCCoE SP 1800 Series

Practice Guide Publication

Volume A: Executive Summary

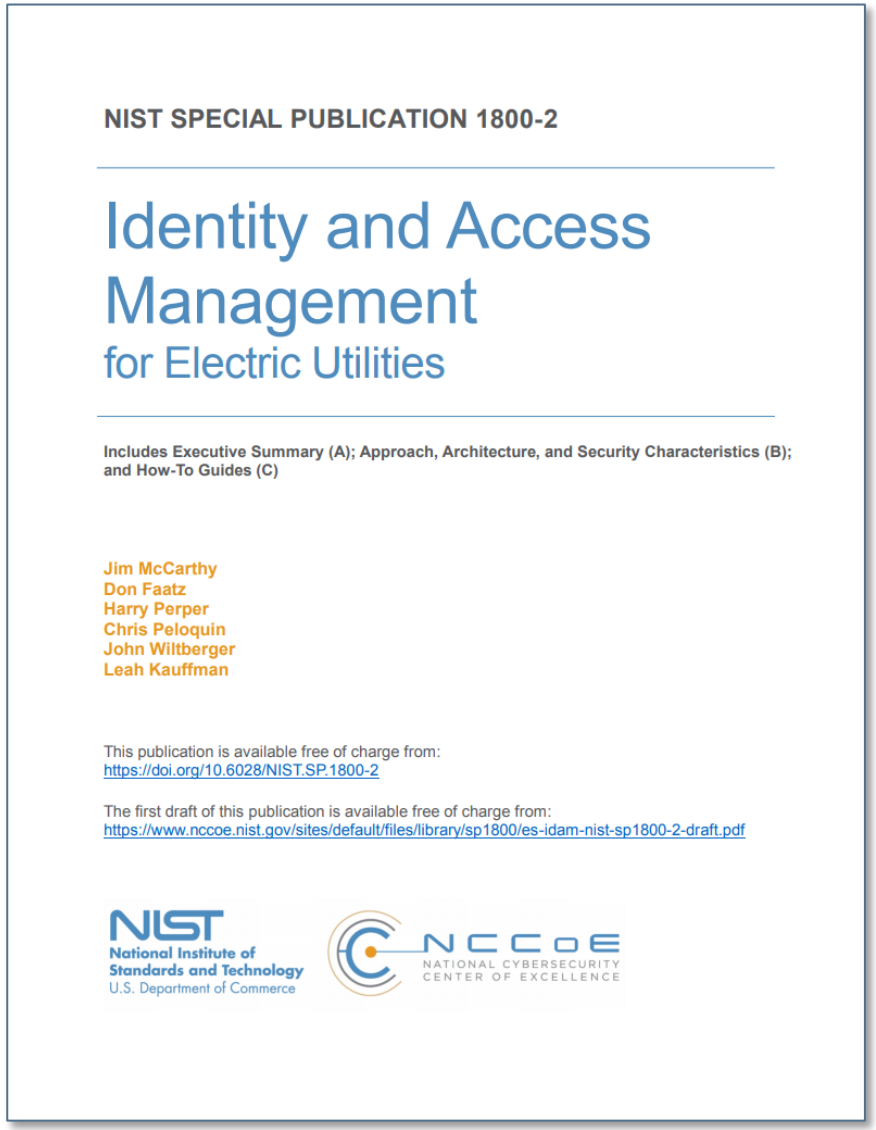
- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance


NIST SPECIAL PUBLICATION 1800-2

Identity and Access Management
for Electric Utilities

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jim McCarthy
Don Faatz
Harry Perper
Chris Peloquin
John Wiltberger
Leah Kauffman

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-2

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/es-idam-nist-sp1800-2-draft.pdf

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SP 1800 Series

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

Informative References								
Function	Category	Subcategory	CIS CSC 2016	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-2:** Threat and vulnerability information is received from information-sharing forums and sources.	4	4.2.3, 4.2.3.9, 4.2.3.12	A.6.14	A.6.1.4	SI-5, PM-15, PM-16	n/a
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-2:** Data-in-transit is protected.	13, 14	n/a	SR 3.1, SR 3.8, SR 4.1, SR 4.2	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8, SC-11, SC-12	CIP-005-5:R2 Part 2.2 CIP-011-2:R1 Part 1.2
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	2,3	n/a	SR 3.1, SR 3.3, SR 3.4, SR 3.8	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	SC-16, SI-7	CIP-010-2:R1, R2, R3

harry.perper@nist.gov

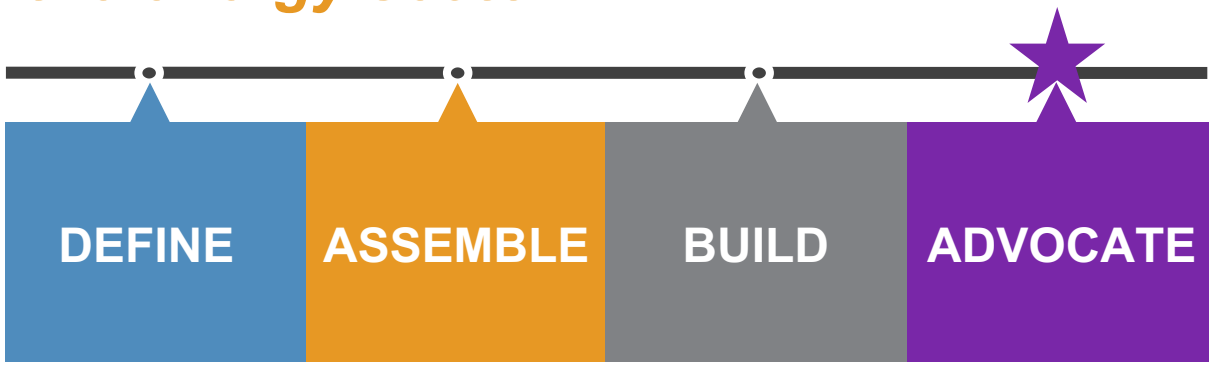
Identity and Access Management for the Energy Sector - SP 1800-2

Identity and Access Management: SP 1800-2

Securing networked infrastructure for the energy sector

Overview

- Electric companies need to be able to control access to their networked resources
- Identity and Access Management (IdAM) implementations are often decentralized and controlled by numerous departments within a company
- The IdAM Practice Guide shows how an electric utility can implement a converged IdAM platform to provide a comprehensive view of all users within the enterprise across all silos, and the access rights they have been granted



Project Status

Final published July 2018

Collaborate with Us

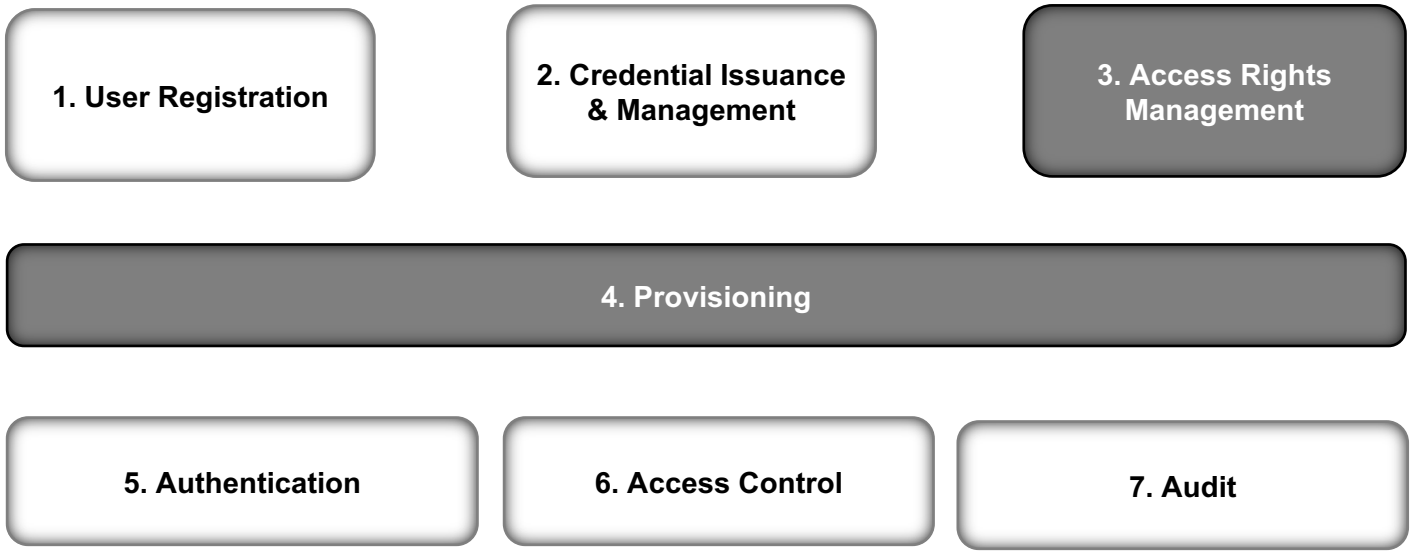
- Download NIST SP 1800-2, Identity and Access Management for Electric Utilities
- Email energy-nccoe@nist.gov to join the Community of Interest for this project

What is Identity and Access Management?

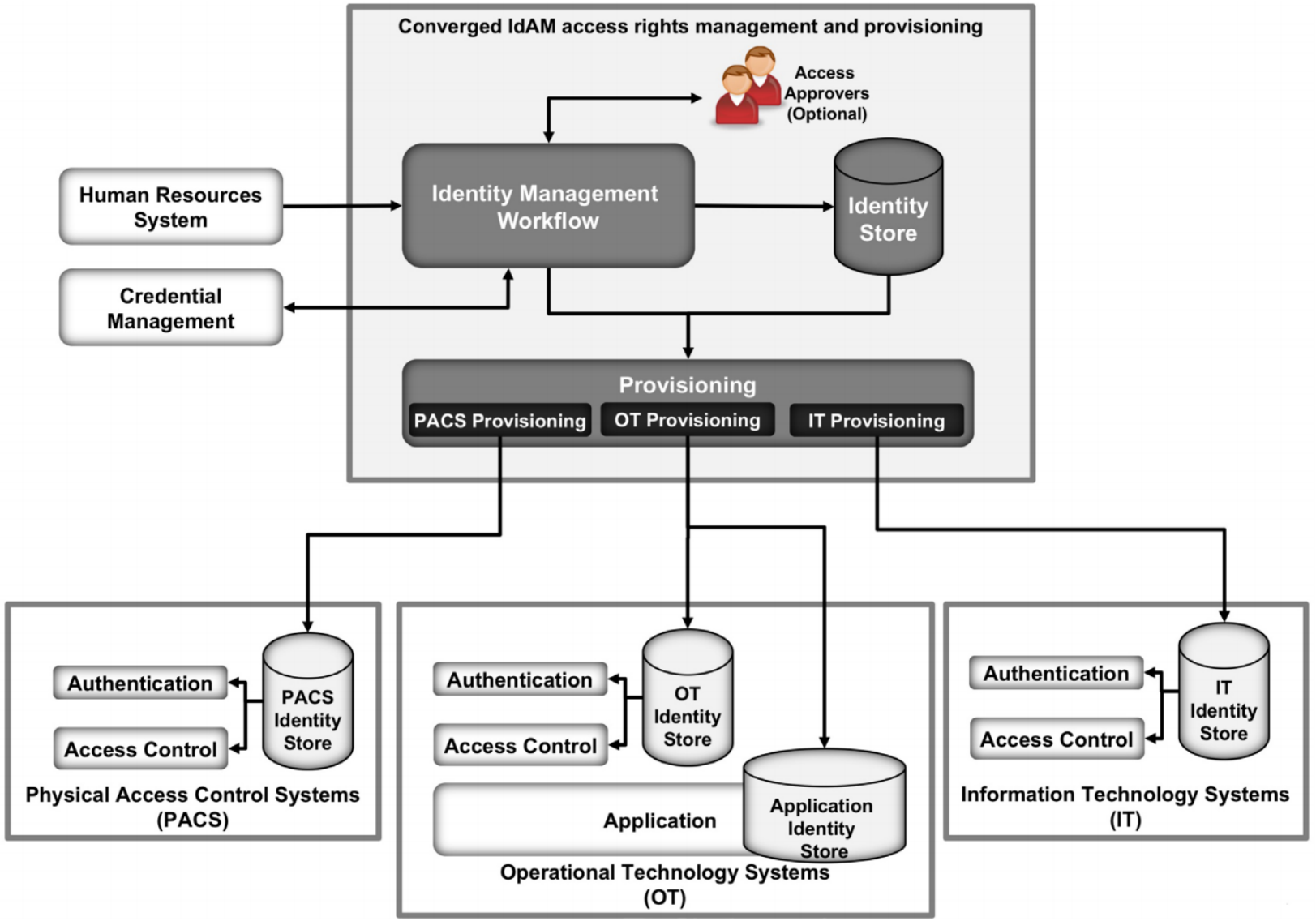
IdAM is the discipline of managing the relationship between a person and the resources the person needs to access to perform a job.

IdAM encompasses the processes and technologies by which individuals are identified, vetted, credentialed, authorized access to resources, and held accountable for their use of these resources.

IdAM processes and technologies create digital identity representations of people, bind those identities to credentials, and use those credentials to control access to resources.

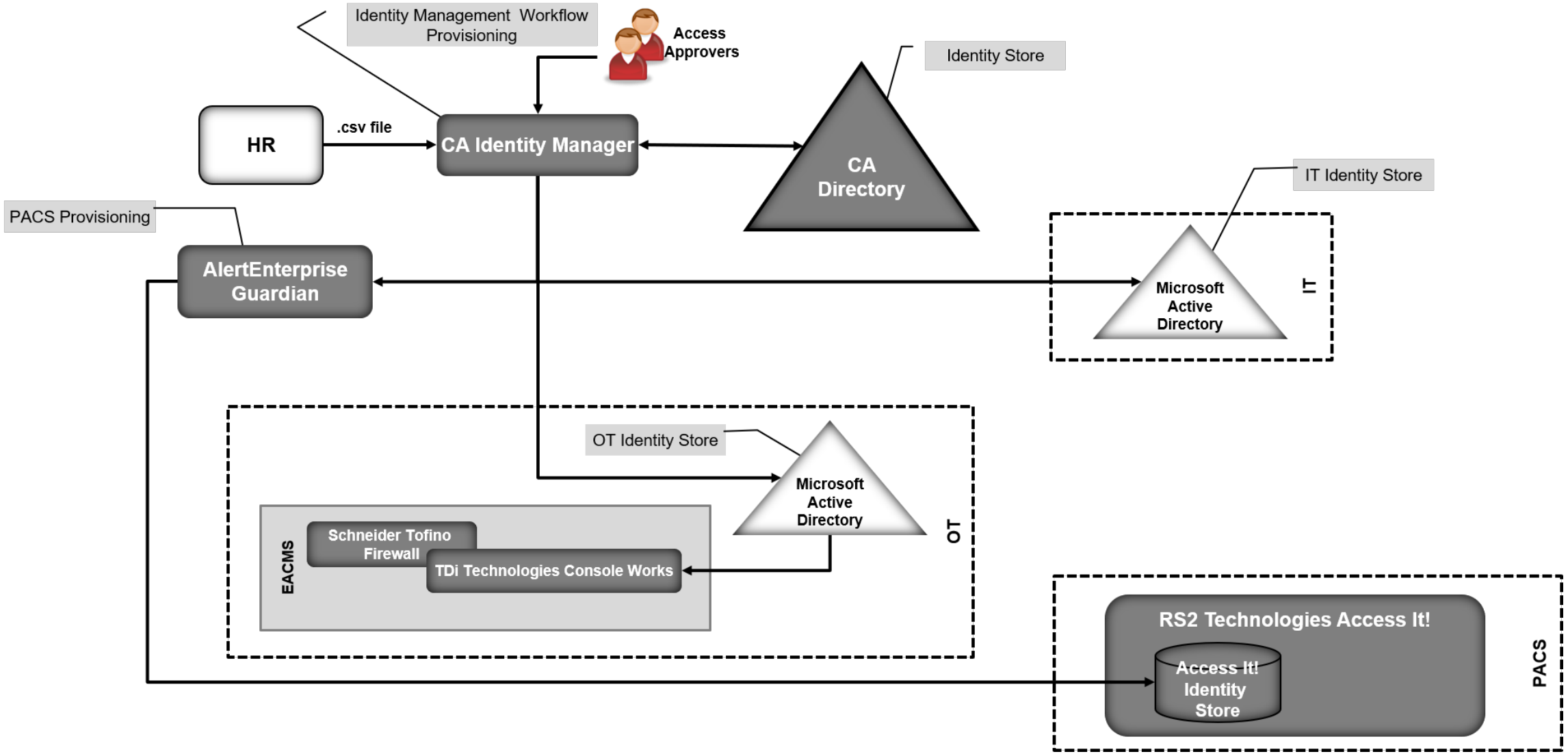


Identity and Access Management: Architecture



IdAM Lab Implementation

harry.perper@nist.gov



SP 1800-2: Potential Outcomes

harry.perper@nist.gov

Adopting all or part of the example implementation can:

- Reduce the risk of malicious or untrained people gaining unauthorized access to critical infrastructure components and interfering with their operation
- Allow rapid provisioning and de-provisioning of access from a converged platform
- Simplify regulatory compliance by automating generation and collection of access information
- Improve situational awareness: proper access and authorization can be confirmed via the use of a single, converged solution
- Improve security posture by tracking and auditing access requests and other IdAM activity across all networks
- Enhance the productivity of employees, support oversight of resources, and speed delivery of services

IdAM Best Practices (partial list*)

Leverage a converged IdAM solution

- Centrally manage and monitor authentication, authorization, and access-control requirements for all OT and IT users

Apply the principle of least privilege to (at a minimum):

- the central identity and authorization store
- the authorization workflow management system

Log all activity that is performed on IdAM components

Deploy all components on securely configured OSs that use 2FA

Segregate IdAM components onto their own network

Require super-administrators to use a console access manager when accessing the console of all devices on the IdAM network

* View the full list at SP 1800-2, Volume B, Section 5.9.6, *Evaluation of Security Characteristics*

Identity and Access Management: SP 1800-2

Project Collaborators

Questions?

Harry Perper

harry.perper@nist.gov

301-975-0367

http://nccoe.nist.gov

301-975-0200

nccoe@nist.gov

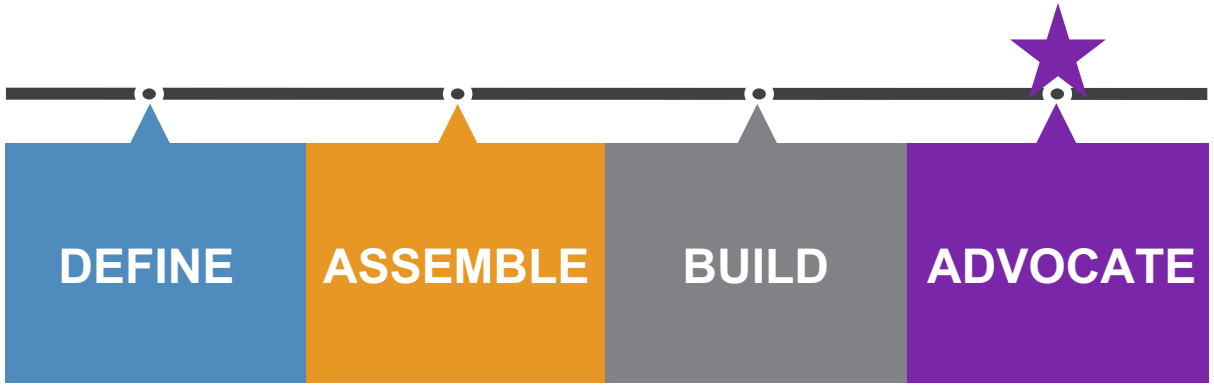
Back-up Slides and Additional Information

Energy Sector Asset Management: SP 1800-23

Assessing cyber risk on OT networks

Overview

- Industrial control system assets provide command and control information as well as key functions on OT networks, therefore any vulnerabilities in these assets can present opportunities for malicious actors
- To properly assess cybersecurity risk within the OT network, energy companies must be able to identify all assets, especially those that are most critical
- This project provides a reference architecture and an example solution for managing, monitoring, and baselining assets, and includes information to help identify threats to these OT assets



Project Status

Published draft on 09/23/2019
Comments being accepted through November 25, 2019

Collaborate with Us

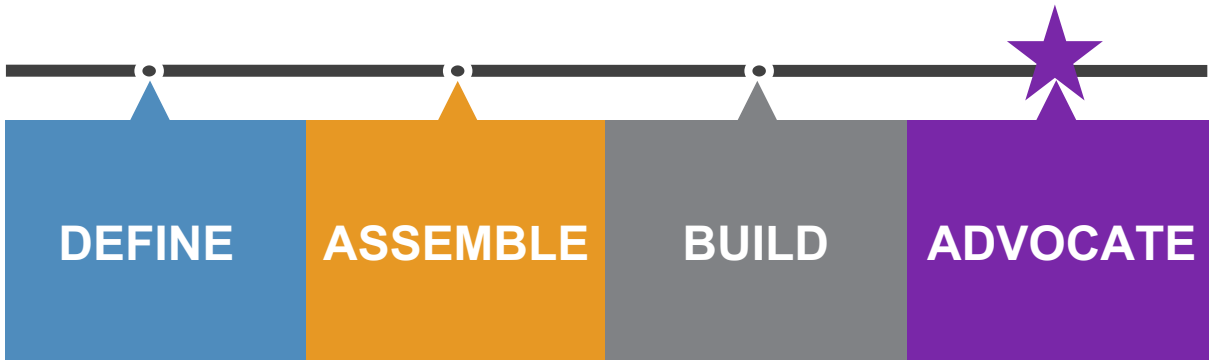
- Read Energy Sector Asset Management Practice Guide
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

Situational Awareness: SP 1800-7

Improving security for electric utilities

Overview

- Energy companies rely on operational technology to control the generation, transmission, and distribution of power
- A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots
- This project explores methods energy providers can use to detect and remediate anomalous conditions, investigate the chain of events that led to the anomalies, and share findings with other energy companies



Project Status

Final SP 1800-7 released in August 2019

Collaborate with Us

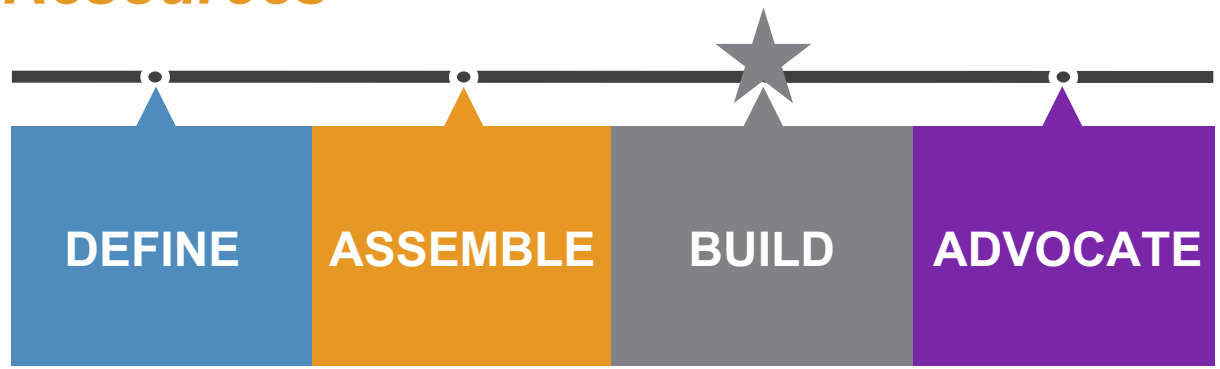
- Download SP 1800-7 Situational Awareness for Electric Utilities
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

Securing the Industrial Internet of Things

Cybersecurity for Distributed Energy Resources

Overview

- As an increasing number of distributed energy resources (DERs) are connected to the grid, there is a need to examine the potential cybersecurity concerns that may arise from these IIoT connections.
- This project focuses on demonstrating data integrity and malware prevention, detection, and mitigation for scenarios in which information exchanges occur between DERs and the distribution grid.



Project Status

Project Kickoff: December, 2019

Collaborate with Us

- Read Project Description: Securing the Industrial Internet of Things
- Email energy_nccoe@nist.gov to join the Community of Interest for this project