NIST SPECIAL PUBLICATION 1800-2B

Identity and Access Management

for Electric Utilities

Volume B:
Approach, Architecture, and Security Characteristics

Jim McCarthy
National Cybersecurity Center of Excellence
Information Technology Laboratory

Don Faatz
Harry Perper
Chris Peloquin
John Wiltberger
The MITRE Corporation
McLean, VA

Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

July 2018

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-2B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-2B, 99 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at energy_nccoe@nist.gov.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mail Stop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework [1] and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

To protect power generation, transmission, and distribution, energy companies need to control physical and logical access to their resources, including buildings, equipment, information technology (IT), and operational technology (OT). They must authenticate authorized individuals to the devices and facilities to which the companies are giving access rights with a high degree of certainty. In addition, they need to enforce access-control policies (e.g., allow, deny, inquire further) consistently, uniformly, and quickly across all of their resources. This project resulted from direct dialog among NCCoE staff and members of the electricity subsector, mainly from electric power companies and those who provide equipment and/or services to them. The goal of this project is to demonstrate a converged, standards-based technical approach that unifies identity and access management (IdAM) functions across OT networks, physical access control systems (PACS), and IT systems. These networks often operate independently, which can result in identity and access information disparity, increased costs, inefficiencies, and a loss of capacity and service delivery capability. Also, these networks support different infrastructures, each with unique security risks. The converged IdAM solution must be constructed to effectively address the highest-risk infrastructure. This guide describes our collaborative efforts with technology providers and

electric-company stakeholders to address the security challenges that energy providers face in the core function of IdAM. This guide offers a technical approach to meeting the challenge and also incorporates a business-value mindset by identifying the strategic considerations involved in implementing new technologies. This NIST Cybersecurity Practice Guide provides a modular, open, end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and levels of IT sophistication. It shows energy providers how we met the challenge by using open-source and commercially available tools and technologies that are consistent with cybersecurity standards. The use-case scenario is based on a normal day-to-day business operational scenario that provides the underlying impetus for the functionality presented in this guide. While the reference solution was demonstrated with a certain suite of products, this guide does not endorse these specific products. Instead, this guide presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with an energy provider's existing tools and infrastructure.

KEYWORDS

cyber, physical, and operational security; cybersecurity; electricity subsector; energy sector; identity and access management; information technology

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Jasvir Gill	AlertEnterprise
Srini Kakkera	AlertEnterprise
Srinivas Adepu	AlertEnterprise
Pan Kamal	AlertEnterprise
Mike Dullea	CA Technologies
Ted Short	CA Technologies
Alan Zhu	CA Technologies
Peter Romness	Cisco Systems
Lila Kee	GlobalSign
Sid Desai	GlobalSign
Paul Townsend	Mount Airey Group (MAG)
Joe Lloyd	Mount Airey Group (MAG)
Paul Timmel	National Security Agency
Victoria Pillitteri	NIST
Jonathan Margulies	Qmulos
Ayal Vogel	Radiflow

Name	Organization
Dario Lobozzo	Radiflow
Steve Schmalz	RSA
Tony Kroukamp (The SCE Group)	RSA
Kala Kinyon (The SCE Group)	RSA
Ulrich Schulz	RSA
Dave Barnard	RS2 Technologies
David Bensky	RS2 Technologies
Rich Gillespie (IACS Inc.)	RS2 Technologies
George Wrenn	Schneider Electric
Michael Pyle	Schneider Electric
Bill Johnson	TDi Technologies
Pam Johnson	TDi Technologies
Clyde Poole	TDi Technologies
Nadya Bartol	Utilities Telecom Council (UTC)
Danny Vitale	XTec

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
AlertEnterprise	User access authorization provisioning
CA Technologies	IdAM workflow, provisions identities and authorizations to Active Directory instances
Cisco Systems	Network Access control
GlobalSign	Provides North American Energy Standards Board (NAESB)-compliant X.509 certificates
Mount Airey Group (MAG)	Manages attributes that control access to high-value transactions
Radiflow	Controls communication among industrial control system (ICS) devices

Technology Partner/Collaborator	Build Involvement
RSA	IdAM workflow, provisions identities and authorizations to Active Directory instances
RS2 Technologies	Controls physical access
Schneider Electric	Controls access to devices in the ICS / Supervisory Control and Data Acquisition (SCADA) network
TDi Technologies	Controls and logs access to ICS devices by people (ICS engineers and technicians)
XTec	Provides Personal Identity Verification Interoperable (PIV-I) smart-card credentials and a physical-access-control capability using the smart card

Contents

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

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

List of Figures

List of Tables

1 Summary

When the National Cybersecurity Center of Excellence (NCCoE) met with electricity subsector stakeholders, they told us they need a more secure and efficient way to protect access to networked devices and facilities. The NCCoE developed an example solution to this problem by using commercially available products.

The NCCoE's approach provides a converged access management system that reduces the risk of disruption of service by reducing opportunities for cyber attack or human error.

This example solution is packaged as a "How-To" guide that demonstrates how to implement standards-based cybersecurity technologies in the real world, based on risk analysis and regulatory requirements. This guide helps organizations to gain efficiencies in identity and access management (IdAM), while saving them research and proof of concept costs.

1.1 Challenge

As the electric power industry upgrades older infrastructure to take advantage of emerging technologies, utilities are also moving toward greater operational technology (OT) and information technology (IT) convergence. This allows greater numbers of technologies, devices, and systems to connect to the grid to improve efficiency, provide access to data often held in silos, and enhance productivity.

This convergence increases the challenge to OT and IT departments in efficiently and effectively managing identities and access. Many utilities run IdAM systems that are fragmented and controlled by numerous departments. Several negative outcomes can result from this: a lack of overall traceability and accountability regarding who has access to both critical and noncritical assets, an increased risk of attack and service disruption, and an inability to identify potential sources of a problem or attack.

To better protect power generation, transmission, and distribution, electric utilities need to be able to control and secure access to their resources, including OT systems, buildings, equipment, and IT systems. IdAM systems for these assets often exist in silos, and employees who manage these systems lack methods to effectively coordinate access to devices and facilities across these silos. This is inefficient and can result in security risks for electric utilities, according to our electric subsector stakeholders.

In collaboration with experts from the energy sector (mainly electric power companies) and those who provide equipment and services to them, we developed a use-case scenario to describe a security challenge based on normal day-to-day business operations. The scenario centers on a utility technician with access to several substations and to remote terminal units connected to the utility's network in those substations. The technician moves out of the region and resigns. A converged IdAM system can quickly and consistently remove the technician's access to all facilities and systems. This provides the timely management of access and reduces the potential for errors. Electric utilities need this ability to provide the right person with the right degree of access to the right resources at the right time.

1.2 Solution

To help the energy sector address this cybersecurity challenge, we developed an example solution that electric utilities can use to more securely and efficiently manage access to the networked devices and facilities on which power generation, transmission, and distribution depend. Our solution uses commercially available products to demonstrate a converged IdAM platform. This platform provides a comprehensive view of users across all of the entity's business and utility operations silos, and the access rights granted those users. This converged IdAM platform is described in this National Institute of Standards and Technology (NIST) cybersecurity Identity and Access Management practice guide.

Electric utilities can use some or all of this guide to implement a converged IdAM system by referencing related NIST guidance and industry standards, including the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Version 5 standards. Commercial, standards-based products, like the ones that we used, are readily available and interoperable with commonly used IT infrastructure and investments.

In our lab at the NCCoE, which is part of NIST, we built an environment that simulates an electric utility's architecture. This architecture includes the typical technology silos found in a utility (such as OT, IT, and physical access control systems [PACS]).

This practice guide includes three versions of an end-to-end identity management solution that provides access-control capabilities to reduce opportunities for cyber attack or human error. It also takes into account the risks that converged control can present. In this guide, we show how an electric utility can implement a converged IdAM platform, using multiple commercially available products, to provide a comprehensive view of all users within the electric utility, across all silos, and of the access rights that they have been granted.

This guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations, including NERC CIP Version 5 standards
- provides a detailed example solution with capabilities that address security controls
- includes a demonstrated approach that is modular and can be implemented using different products to achieve the same results
- includes instructions for implementers and security engineers, including examples of all of the necessary components and installation, configuration, and integration

- uses products that are readily available and interoperable with your existing IT infrastructure and investments
- can meet the needs of electric utilities of all sizes, including corporate and regional business offices, power generation plants, and substations

We used a suite of commercial products to address this challenge; however, this guide does not endorse these particular products, nor does implementing the reference design in this guide guarantee regulatory compliance. Your utility's information security personnel should identify the standards-based products that will best integrate with your existing tools and infrastructure. Your company can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

1.3 Benefits

The NCCoE's practice guide to Identity and Access Management for Electric Utilities can help your organization:

- adopt products and capabilities on a component-by-component basis, or as a whole, thereby minimizing impact to the enterprise and existing infrastructure
- reduce the risk of malicious or untrained people gaining unauthorized access to critical infrastructure components and interfering with their operation, thereby lowering the overall business risk
- allow for rapid provisioning and de-provisioning of access from a converged platform, so that personnel can spend more time on other critical tasks
- improve situational awareness: proper access and authorization can be confirmed through the use of a single, converged solution
- improve the security posture by tracking and auditing access requests and other IdAM activity across all networks
- enhance the productivity of employees and speed delivery of services, and support oversight of resources

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and provides users with the information that they need to replicate this approach to IdAM for electric utilities. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST Special Publication (SP) 1800-2A: *Executive Summary*
- NIST SP 1800-2B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-2C: *How-To Guides* – instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

Energy utility leaders, including chief security and technology officers will be interested in the *Executive Summary (NIST SP 1800-2A)*, which describes the:

- challenges enterprises face in implementing and using IdAM systems
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk, will be interested in this part of the guide, *NIST SP 1800-2B*, which describes what we did and why. The following sections will be of particular interest:

- Section 4.4.3, Risk, provides a description of the risk analysis we performed
- Section 4.4.4, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary*, *NIST SP 1800-2A*, with your leadership team members to help them understand the importance of adopting standards-based IdAM for electric utilities.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-2C*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution for OT systems, PACSs, and IT systems. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 4.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov

3 Introduction

The NCCoE initiated this project because technology practitioners in the electricity subsector, including those focused on OT, IT, and telecommunications, told us that IdAM was a concern to them. As we developed the original problem statement, or use case, on which this project is based, we consulted with electric-company chief information officers, chief information security officers, security management personnel, and others with financial decision-making responsibility (particularly for security).

The individuals that we consulted told us that they need to control physical and logical access to their resources, including buildings, environmental applications, energy management system (EMS) control and data centers, equipment, IT, and OT systems. They need to authenticate only designated individuals and devices to which they are giving access rights. In addition, they need to enforce access-control policies (e.g., allow, deny, inquire further) consistently, uniformly, and quickly across all of their resources. Current IdAM implementations can often be fragmented and controlled by numerous departments within an electric utility or by individual equipment owners. Several negative outcomes can result from this situation: an increased risk of attack and service disruption, an inability to identify potential sources of a problem or attack, and a lack of overall traceability and accountability regarding who has access to both critical and noncritical assets. While the example solution presented here is motivated by a problem identified by electric utilities, it can be adapted to utilities that have multiple OT silos, such as utilities that handle electric and water, or electric and gas. Another key consideration is the need for companies to demonstrate compliance with industry standards and/or government regulations.

We, at NCCoE, constructed two versions of an end-to-end identity management solution that provides access-control capabilities across the OT, PACS, and IT networks. We used the same approach for each build, in that we only interchanged two core products that contained the same functionality and capability. Section 5.3.1 and Section 5.3.2 detail these two example solutions. Our build collaborator, AlertEnterprise, independently constructed a third version of the solution; Section 5.5 details this solution. The end result is that a user's access to facilities and devices can be provisioned from a single console. Access privileges can be modified by adding new users and assigning access for the first time, modifying existing user access privileges, or disabling user access privileges. Our goal was to provide the electricity subsector with a solution that addresses the key tenet of cybersecurity—access management/rights—based on the principle of least privilege, which is defined as providing the least amount of access (to systems) necessary for the user to complete his or her job [2].

4 Approach

4.1 Audience

This guide is intended for technology practitioners (including those focused on OT, IT, and telecommunications) who are responsible for implementing security solutions in electricity subsector organizations.

4.2 Scope

This project began with a detailed discussion between NCCoE and members of the electricity subsector community, about their main security challenges. The risk of unauthorized access to facilities and devices, and the inability to verify if user access had been properly established, modified, or revoked, quickly became the focus of the discussion.

In response, the NCCoE drafted a use case that identified numerous desired solution characteristics. After an open call in the Federal Register, we chose technology collaborators based on their ability to provide these characteristics. In the scope, we initially thought that it would be feasible to include federated identity management services [3], or "arrangement[s] that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access to the networks of all enterprises in the group." As we progressed through the initial stages of solution development, we realized that access, authentication, and authorization through federated identity means would vastly increase the amount of time needed to complete a build. We narrowed the scope to providing identity management of energy company employees, including a converged provisioning capability to the OT, PACS, and IT networks. The scope became successful execution of the following provisioning functions:

1. enabling access for a new employee
2. modifying access for an existing employee
3. disabling access for a former employee

The objective is to perform all three actions from a single interface that can serve as the authoritative source for all access managed within an energy provider's facilities, networks, and systems.

4.3 Assumptions

This project is guided by the assumptions identified in the following subsections.

4.3.1 Security

All network and system changes have the potential to increase the attack surface within an enterprise. In Section 4.4, Risk Assessment, we provide detailed recommendations on how to secure this reference solution.

4.3.2 Modularity

This example solution is made of many commercially available parts. You might swap one of the products that we used for a product that is better suited for your environment. We also assume that you already have some IdAM solutions in place. A combination of some of the components described here, or a single component, can improve your identity and access/authorization functions, without requiring you to remove or replace your existing infrastructure. This guide provides both a complete end-to-end solution and options that you can implement based on your needs.

4.3.3 Human Resources Database/Identity Vetting

This build is based on a simulated environment. Rather than recreate a human resources (HR) database and the entire identity vetting process in our lab, we assumed that your organization has the processes, databases, and other components necessary to establish a valid identity.

4.3.4 Identity Federation

We initially intended to work with energy providers to demonstrate a means for sharing selected identity information across organizational boundaries. While we assumed that the NCCoE could implement some type of identity federation mechanism to authenticate and authorize individuals who are both internal and external to the organization, this capability exceeded the scope of the build.

4.3.5 Technical Implementation

This guide is written from a "how-to" perspective. Its foremost purpose is to provide details on how to install, configure, and integrate components. We assume that an energy provider has the technical resources to implement all or parts of the build or has access to companies that can perform the implementation on its behalf.

4.3.6 Limited Scalability Testing

We did not attempt to replicate the user-base size that would be found at medium and large energy providers. We do not identify scalability thresholds in our IdAM builds, as those depend on the type and size of the implementation and are particular to the individual enterprise.

4.3.7 Replication of Enterprise Network

We were able to replicate the three silos: (1) PACS, (2) IT or corporate networks, and (3) the OT network, in a limited manner. The goal was to demonstrate, both logically and physically, that provisioning functions could be performed from a converged IdAM system, regardless of its location in the enterprise. In a real-world environment, the interconnections between the OT, PACS, and IT silos depend on the business needs and compliance requirements of the enterprise. We did not attempt to replicate these interconnections. Rather, we acknowledge that implementing our build or its components creates new interfaces across silos. We focused on providing general information on how to remain within the bounds of compliance, should you adopt this example solution. In addition, we provide guidance on how to mitigate any new risks introduced to the environment.

4.4 Risk Assessment

We performed two types of risk assessment: the initial analysis of the risk posed to the electricity subsector as a whole, which led to the creation of the use case and the desired security characteristics, and an analysis to show users how to manage the cybersecurity risk to the components introduced by the adoption of the solution.

4.4.1 Assessing Risk Posture

NIST SP 800-30, Risk Management Guide for Information Technology Systems [4][4] states, "Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of the NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems [5] material available to the public. The risk management framework (RMF) guidance as a whole proved invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

Using the guidance in NIST's series of publications concerning the RMF, we performed two key activities to identify the most-compelling risks encountered by energy providers. The first was a face-to-face meeting with members of the energy community to define the main security risks to business operations. This meeting identified a primary risk concern—the lack of converged IdAM services, particularly on OT networks. We then identified the core risk area, IdAM, and established the core operational risks encountered daily in this area. We deemed the tactical risks to be as follows:

- lack of authentication, authorization, and access-control requirements for all OT in the electricity subsector
- inability to manage and log authentication, authorization, and access-control information for all OT using converged or federated controls
- inability to centrally monitor authorized and unauthorized use of all OT and user accounts
- inability to provision, modify, or revoke access throughout the enterprise (including OT) in a timely manner

Our second key activity was conducting phone interviews with members of the electricity subsector. These interviews gave us a better understanding of the actual business risks, as they relate to the potential cost and business value. NIST SP 800-39, Managing Information Security Risk [6], focuses particularly on the business aspect of risk, namely at the enterprise level. This foundation is essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. A summary of the strategic risks is provided below:

- impact on service delivery: Ensuring that people have access to the systems needed to perform their job functions, and do not have access to the systems not needed to perform their job functions, reduces the risk of inappropriate or unauthorized use of access to affect availability.
- cost of implementation: Implementing IdAM once, and using it across all systems, may reduce both system development costs and operational costs.
- budget expenditure, as it relates to investment in security technologies
- projected cost savings and operational efficiencies to be gained as a result of new investment in security
- compliance with existing industry standards: NERC CIP Version 5 requires deliberate and timely control of both logical and physical access to assets.
- high-quality reputation or public image
- risk of alternative or no action
- successful precedents

Undertaking these activities in accordance with the NIST RMF guidance yielded the necessary operational and strategic risk information, which we subsequently translated to security characteristics. We mapped these characteristics to the NIST SP 800-53 Revision4 [7] controls, where applicable, along with other applicable industry and mainstream security standards.

4.4.2 Managing Security Risk from Converged IdAM

As mentioned previously, a foundation of cybersecurity is the principle of least privilege, defined as providing the least amount of access (to systems) necessary for the user to complete his or her job [2]. To enforce this principle, the access-control system needs to know the appropriate privileges for each user and system. An analysis of the IdAM solution reveals two components that need to be protected from both external and internal threat actors: the central identity and authorization store and the authorization workflow management system. The authorization workflow management system is trusted to make changes to the central identity and authorization store. Therefore, any inappropriate or unauthorized use of these systems could change authorization levels for anyone in the enterprise. If that occurred, the enterprise would experience a lack of integrity of the identity and authentication stores. The central identity and authorization store is the authoritative source for the enterprise and holds the hash for each user password, as well as the authorizations associated with each user. Access to this information would enable an unauthorized user to impersonate anyone in the organization. In this situation, the enterprise would lose control over access to resources. Security controls to mitigate this risk are discussed in Section 5.9.5.1.1.

To protect the build components, we implemented the following requirements in our lab environment: access control, data security, and protective technology. Section 5.9 provides a security evaluation of the example solution and a list of the security characteristics. Please note that we addressed only the core requirements appropriate for the IdAM build.

4.4.3 Risk

While risk is addressed in current industry standards, such as NERC CIP Version 5, our sector stakeholders told us about additional risk considerations at both the operational and strategic levels.

Operationally, a lack of a converged IdAM platform can increase the risk of people gaining unauthorized access to critical infrastructure components. Once unauthorized access is gained, the risk surface increases and the opportunity for the introduction of additional threats to the environment, such as malware and denial of service (especially oriented toward OT), is realized.

At the strategic level, you might consider the cost of mitigating these risks and the potential return on your investment in implementing a product (or multiple products). You may also want to assess if a converged IdAM system can help enhance the productivity of employees and speed delivery of services and explore if it can help support oversight of resources, including IT, personnel, and data. This example solution also addresses imminent operational security risks and incorporates strategic risk considerations.

Adopting any new technology can introduce new risks to your enterprise. We understand that this example solution to mitigate the risks of fragmented IdAM may, in turn, introduce new risks. By converging IdAM functions, we decrease the risk that inconsistencies, errors, and omissions across multiple, independent IdAM systems can be used to gain unauthorized access to networked devices. We recognize, however, that converging IdAM functions provides a point of single infiltration of multiple critical systems (OT, PACS, and IT). We address this key risk in detail in Section 5.9.5.1, and provide a comprehensive list of mitigations in Section 5.9.6.

4.4.4 Security Control Map

As explained in Section 4.3.1, we derived the security characteristics through a risk analysis process conducted in collaboration with our electricity subsector stakeholders. This is a critical first step in acquiring or developing the capability necessary to mitigate the risks as identified by our stakeholders. Table 4-1 maps the desired security characteristics and example capabilities of the use case to the Framework for Improving Critical Infrastructure Cybersecurity, also known as the NIST Cybersecurity Framework (CSF); relevant NIST standards; industry standards; and controls and best practices.

Table 4-1 Use-Case Security Characteristics Mapped to Relevant Standards and Controls

Example Characteristic		Sector Specific Compliance Guidance					
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 Revision 4**	**IEC/ISO 27001**	**NERC CIP Version 5**
Authentication for OT	Authentication mechanisms	Protect	Access Control	AC-2, IA Family		ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-007-5 R2, CIP-007-5 R5
Access Control for OT	Access control mechanisms	Protect	Access Control and Protective Technology	PR.AC-2: Physical access to assets is managed and protected PR.AC-3: Remote access is managed PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC-3, AC-17, AC-19, AC-20, CM-7, PE-2, PE-3, PE-4, PE5, PE-6, PE-9	ISO/IEC 27001:2013 A.6.2.2, A.9.1.2A, 11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.13.1.1, A.13.2.1	CIP-003-5 R1, CIP-004-5 R2, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R1

Example Characteristic		Sector Specific Compliance Guidance					
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 Revision 4	IEC/ISO 27001	NERC CIP Version 5
Authorization (provisioning) OT	Access policy management mechanisms	Protect	Access Control	PR.AC-4 Access Permissions are managed, incorporating principles of least privilege and separation of duties.	AC-2, AC-3, AC-5, AC-6, AC-16	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-007-5 R5
Centrally monitor use of accounts	Log account activity	Detect, Protect	Continuous Monitoring & Protective Technology	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events PR.PT-1: Audit/log records are determined, documented, implemented...	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11, AU family	ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R4, CIP-007-5 R5, CIP-008-5 R2, CIP-010-5 R1, CIP-011-5 R2

Example Characteristic		Sector Specific Compliance Guidance						
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 Revision 4	IEC/ISO 27001	NERC CIP Version 5
Protect exchange of identity and access information	Encryption	Protect	Data Security	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected	SC-8, SC-28	ISO/IEC 27001:2013 A.8.2, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	CIP-011-5 R1
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access	Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16, IA Family	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-007-5 R4, CIP-007-5 R5

The relationship of NERC CIP requirements to the security characteristics is derived from a mapping between the NIST 800-53 Revision 4 [7] security controls and NERC CIP requirements. These mappings are for reference only. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance.

4.5 Technologies

Table 4-2 provides information about the products and technologies that we implemented to satisfy the security control requirements. This table describes only the product capabilities that were used in our builds. Many of the products have significant additional security capabilities that were not used in our builds. The “Product” column of the table contains links to vendor product information that describes the full capabilities.

Table 4-2 Products and Technologies Used to Satisfy Security Control Requirements

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
Authentication for OT	Authentication mechanisms	PR.AC-1: Identities and credentials are managed for authorized devices and users	Identity Management Platform	CA	Identity Manager	R12.0 SP14 Build 9140	Implements workflows for creating digital identities and authorizing them access to physical and logical resources, including authoritative source

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
				RSA	Identity Management and Governance (IMG) Governance Lifecycle	6.9.74968	Implements workflows for creating digital identities and authorizing them access to physical and logical resources
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access		Virtual Directory		Adaptive Directory	7.1.5 R29692	Authoritative source for digital identities and authorized access to resources
			Credential Management	GlobalSign	Enterprise PKI	N/A	Provides North American Energy Standards Board (NAESB)-compliant X.509 certificates to OT personnel

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
			Credential Management / Physical Access Control	XTec	Credential Issuance Solutions	N/A	Provides Personal Identity Verification Interoperable (PIV-I) smart-card credentials and physical-access-control capability using the smart card
Access Control for OT	Access control mechanisms	PR.AC-2: Physical access to assets is managed and protected	Credential Management / Physical Access Control	XTec	Physical Access Control Logical Access Control Authentication and Validation	N/A	Provides PIV-I smart-card credentials and physical-access-control capability using the smart card
			Physical Access Control Enforcement	RS2 Technologies	Access It!	4.1.15	Controls physical access to power facilities, buildings, etc.
Authorization (provisioning) OT	Access policy management mechanisms	PR.AC-4: Access permissions	Provisioning	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the IdAM

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access	are managed, incorporating the principles of least privilege and separation of duties					workflow to Access It Universal
Authorization (provisioning) OT	Access policy management mechanisms		Identity Management Platform	CA	Identity Manager	R12.0 SP14 Build 9140	Provisions identities and authorizations to Active Directory (AD)
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access			RSA	IMG	6.9.74968	
			Secure Attribute Management	Mount Airey Group	Ozone Console and Ozone Authority Secure Attribute Management Public Key Enablement Ozone Mobile	Ozone Authority 4.0.1, Ozone Server 2.1.301, Ozone Envoy 4.1.0, Ozone Console 2.0.2	Manages attributes that control access to high-value transactions

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
Centrally monitor use of accounts	Log account activity	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Industrial Control System (ICS) User Access Management	TDi Technologies	ConsoleWorks	4.9-0u0	Controls access to industrial control system (ICS) devices by people (ICS engineers and technicians)
Access Control for OT	Access control mechanisms	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Industrial Control System (ICS) User Access Management	TDi Technologies	ConsoleWorks	4.9-0u0	Creates an audit trail of access to ICS devices by people
			ICS Device-to-Device Access Management	Radiflow	Industrial Control System Firewall and iSIM Software OT Security Substation Security	iSIM 3.6.07	Controls communication among ICS devices

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
			Access Gateway	Cisco	Identity Service Engine (ISE)	1.4.0.253	Controls access to resources in OT by users in IT based on both user identity and device identity
			Access Gateway	Schneider Electric	ConneXium Tofino Ethernet Firewall	2.10	Controls access to devices in the ICS/SCADA network

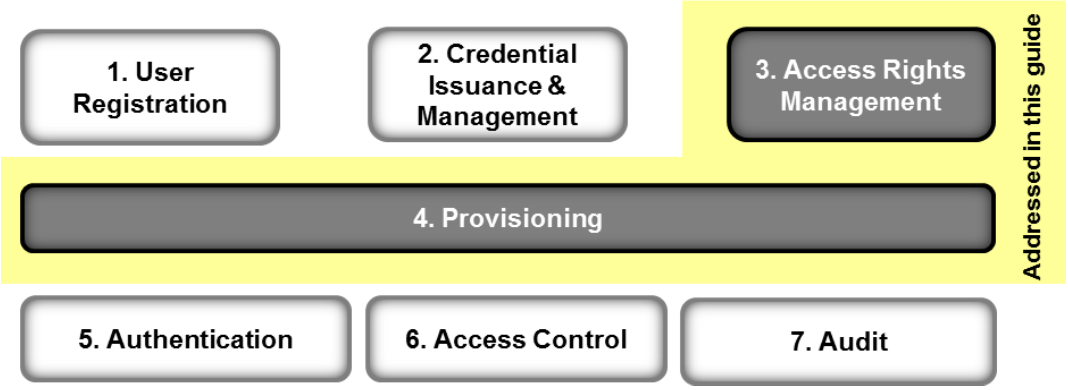
RSA IMG is now known as RSA VIA Governance and RSA VIA Lifecycle.

5 Architecture

5.1 Architecture Description

IdAM is the discipline of managing the relationship between a person and the resources that the person needs to access to perform a job. It encompasses the processes and technologies by which individuals are identified, vetted, credentialed, and authorized access to resources, and held accountable for their use of these resources. These processes and technologies create digital identity representations of people, bind those identities to credentials, and use those credentials to control access to resources. IdAM is composed of the capabilities illustrated in Figure 5-1, which are detailed, by number, in the text that follows.

Figure 5-1 IdAM Capabilities



1. User registration determines that a reason exists to give a person access to resources, verifies the person’s identity, and creates one or more digital identities for the person.
2. Credential issuance and management provides life-cycle management of credentials, such as employee badges or digital certificates. Additional information on credential issuance and management, as well as authentication, can be found in NIST SP 800-63-2, Electronic Authentication Guideline [8].
3. Access rights management determines the resources that a digital identity is allowed to use.
4. Provisioning populates digital identity, credential, and access rights information for use in authentication, access control, and audit.
5. Authentication establishes confidence in a person’s digital identity.
6. Access control allows or denies a digital identity access to a resource. NIST Interagency/Internal Report (NISTIR) 7316, Assessment of Access Control Systems [9], explains commonly used access-control policies, models, and mechanisms.
7. Audit maintains a record of resource access attempts by a digital identity.

The top three capabilities are administrative capabilities, in that they involve human actions or are infrequently used. For example, verifying identity typically involves physically reviewing documents, such as a driver's license or passport. Credential issuance and management is invoked when an employee is hired, changes jobs, leaves the company, loses a credential, or when a credential expires.

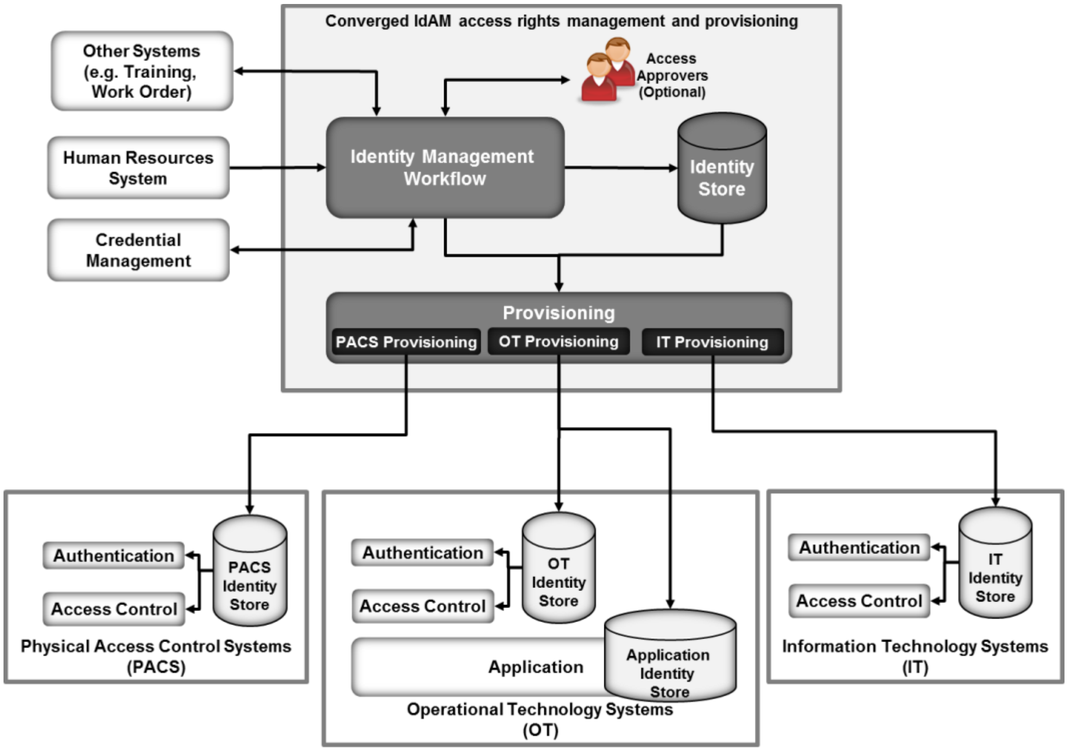
The bottom three capabilities are "run-time" capabilities, in that they happen whenever a person accesses a resource. Authentication, access control, and audit are typically automated activities that occur every time that a person enters a facility by using a badge, or logs into a computer system. A directory, such as Microsoft AD, is often used in the implementation of run-time functions.

Provisioning connects the administrative activities to the run-time activities by providing the run-time capabilities with the information needed from the administrative activities.

In the electricity subsector today, some or all of these IdAM capabilities are frequently replicated at least three times—once for a person's access to OT, again for physical access, and then to access IT. Additionally, these capabilities may be independently replicated for each system within OT or IT. Replication makes it difficult to ensure that employees have access to the resources that they need to perform their jobs, and only those resources. Newly hired employees may not have access to all of the resources they need. Employees who change jobs may retain access to resources they no longer need. Terminated employees may retain access long after they have left. Further, multiple independent IdAM processes make it difficult to periodically review who has access to what resources.

The example solution described here addresses these problems by creating a converged implementation of the IdAM access rights management and provisioning capabilities that is used across OT, PACS, and IT. This converged implementation does not change the run-time capabilities of authentication, access control, and audit, leaving them replicated and distributed. The converged implementation depends on a utility's existing processes, such as employee on-boarding and badge issuance, to provide both user registration and credential issuance and management capabilities. Figure 5-2 illustrates the example solution.

Figure 5-2 IdAM Example Solution


Converged IdAM access rights management and provisioning
Access Approvers (Optional)
Other Systems (e.g. Training, Work Order)
Human Resources System
Credential Management
Identity Management Workflow
Identity Store
Provisioning
PACS Provisioning
OT Provisioning
IT Provisioning
Authentication
Access Control
PACS Identity Store
Physical Access Control Systems (PACS)
Authentication
Access Control
OT Identity Store
Application
Application Identity Store
Operational Technology Systems (OT)
Authentication
Access Control
IT Identity Store
Information Technology Systems (IT)

The converged IdAM capability implements the following items:

- an IdAM workflow to manage the overall process
- an identity store, which is the authoritative source for digital identities and their associated access rights to resources
- a provisioning capability to populate information from the workflow and identity store into the run-time capabilities. The provisioning capability is further decomposed into OT provisioning, IT provisioning, and PACS provisioning

Each of the three silos, OT, IT, and PACS, may have its own identity stores that contain digital identities and access rights for use in controlling access to systems within the silo. Further, some applications in a silo may have their own application identity stores that are used by the application to control access to the information and to the services that it provides. The converged IdAM capability, through provisioning, manages the information in these other identity stores.

The combined capabilities can reduce the time to update access in the OT, PACS, and IT systems from days to minutes. They also improve the audit trail capture by integrating the three audit logs into one. Provisioning may also verify that authorizations stored locally in the run-time capabilities are consistent with those in the identity store. If locally stored authorizations are inconsistent with authoritative values in the identity store, provisioning may raise an alarm or change locally stored authorizations to be consistent with the identity store.

The example solution implements three basic transactions:

- creating all required credentials, authorizing access, and provisioning access for a new employee
- updating credentials and access for an existing employee who is changing jobs or requires a temporary access change
- destroying credentials and removing accesses for a terminated employee

The IdAM workflow receives information about employees and their jobs from the HR system. For a new employee, HR is responsible for performing initial identity verification. Based on a new employee's assigned job, the IdAM workflow creates one or more digital identities and determines the credentials and resource accesses required. The workflow triggers credential management capabilities to create physical identification badges, physical access cards, and any logical access credentials, such as X.509 public key certificates, that may be needed. The workflow records information about these credentials in the identity store.

The example solution does not assume that each person will have a single digital identity. A current employee is likely to have several distinct digital identities because of independent management of digital identities in physical security, business systems, and operational systems. Requiring a single digital identity would create a significant challenge to the adoption of the example solution.

Instead, the identity store associates all of an employee's digital identifiers so that all of the person's accesses can be managed together. Once the example solution is in place, an organization can continue issuing multiple digital identifiers to new employees or can assign a single digital identifier that is common to physical security, business systems, and operational systems.

The workflow automatically authorizes some physical and logical accesses that are needed either by all employees or for an employee's job. The workflow stores information about credentials and authorized accesses in the identity store. The workflow then invokes provisioning to populate silo-specific and application identity stores with credential information and access authorizations. This allows the employee to access facilities and systems.

Access to some resources, both logical and physical, will require explicit approval before being authorized. For these, the workflow notifies one or more access approvers for each such resource, and then waits for responses. When the workflow receives approvals, it stores the authorized accesses in the identity store and provisions them to the silos. All information about approved, pending, and provisioned physical and logical access authorizations is maintained in the identity store. Pending access authorizations may be either authorizations that have been approved, but not yet provisioned, or time-bounded authorizations to be provisioned/de-provisioned at a future time. Explicit approval is used to ensure that OT managers and supervisors retain control over access to critical operational systems.

While the system to manage access authorizations is converged, the authority to make access authorizations remains distributed across IT, OT, and physical security management.

When the HR system notifies the workflow that an employee is changing jobs, the workflow performs similar actions. First, it identifies resource accesses and credentials associated only with the employee's former job. It revokes those resource accesses in the identity store and de-provisions them from the silos. It directs that associated credentials be invalidated and destroyed. It removes information about those credentials from the identity store and de-provisions credential information from the silos. Workflow actions are programmable and can be customized to meet organization-specific needs. It then identifies the resource accesses needed for the employee's new job, authorizes them in the identity store, and provisions them to the silos. The workflow identifies any new credentials that will be needed in the new job, triggers the creation and issuance of those credentials, waits for them to be created, updates the identity store, and provisions new credential information to the silos.

When the HR system notifies the workflow that an employee has been terminated, the workflow removes all of the employee's resource accesses from the identity store and de-provisions them from the run-time functions. It triggers the invalidation and destruction of the employee's credentials, removes credential information from the identity store, and de-provisions credential information from the silos.

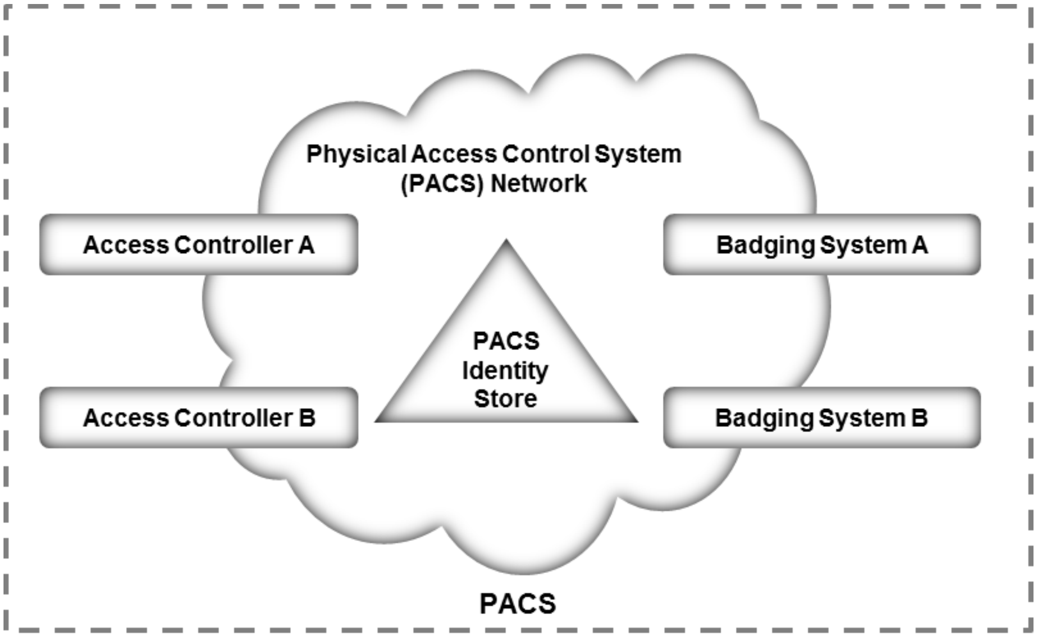
In addition to input from the HR system to process personnel actions, the workflow can provide a portal for employees to request access to resources, which can be reviewed and approved. Also, systems other than HR can be integrated with the workflow to initiate resource access requests. These capabilities reduce overhead and administrative downtime.

5.1.1 Physical Access Control System Silo

The PACS silo hosts both access controllers and badging systems. The badging systems implement a credential issuance capability that creates the badges that employees use to gain access to facilities and other physical resources. The access controllers read information from badges and check authorization information to determine if a person should be allowed access. If access is allowed, the access controller unlocks a door, allowing the person to enter the facility.

Figure 5-3 shows the architecture of the PACS silo.

Figure 5-3 Notional PACS Architecture



The PACS identity store contains identities and access-control information for the people who operate the badging systems and the people who manage the access-control systems. This access-control information is provisioned into the PACS identity store instance from the converged IdAM system.

Access controllers may also use the PACS identity store to check authorization information to determine physical access. If the access controllers use the PACS identity store, then the IdAM system will provision authorization information to the PACS identity store. If the access controllers use their own internal identity store, then authorization information will be provisioned directly to the access controller. Build #1 provisions directly to the access controller, and Build #2 provisions to the PACS identity store.

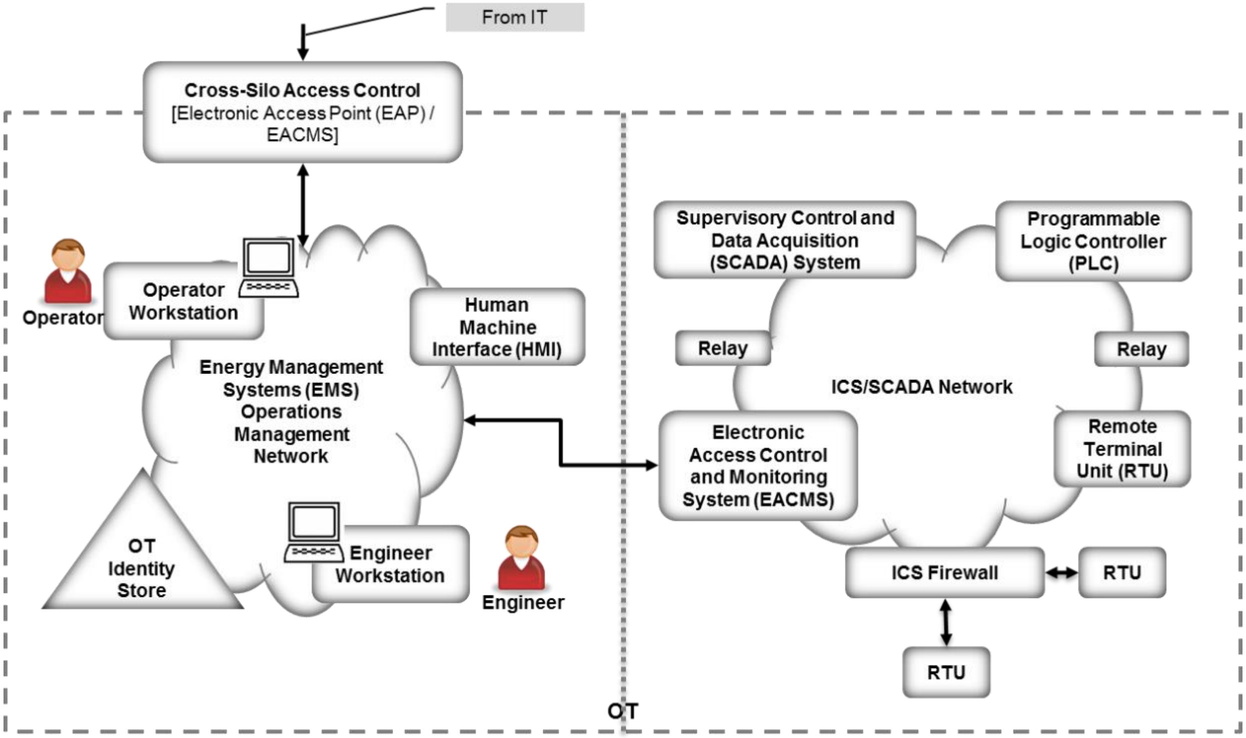
5.1.2 Operational Technology Silo

The OT silo is composed of two types of systems:

- operational management systems that operators and engineers use to monitor and manage the generation and delivery of electric energy to customers
- industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems that provide real-time and near-real-time control of the equipment that produces and delivers electric energy

Figure 5-4 shows the notional architecture of the OT silo.

Figure 5-4 Notional OT Silo Architecture


From IT
Cross-Silo Access Control [Electronic Access Point (EAP) / EACMS]
Operator
Operator Workstation
Human Machine Interface (HMI)
Energy Management Systems (EMS) Operations Management Network
OT Identity Store
Engineer Workstation
Engineer
Supervisory Control and Data Acquisition (SCADA) System
Programmable Logic Controller (PLC)
Relay
Relay
ICS/SCADA Network
Electronic Access Control and Monitoring System (EACMS)
Remote Terminal Unit (RTU)
ICS Firewall
RTU
RTU
OT

The operations and management network within the OT silo has an identity store that contains identities and access authorizations for operational management systems. These identities and authorizations are provisioned from the converged IdAM system. A cross-silo access-control capability allows some access to operational management systems from the IT silo. The converged IdAM system provisions authorizations to access OT resources from the IT silo into the OT identity store.

An electronic access control and monitoring system (EACMS) controls access to ICS/SCADA devices on the ICS/SCADA network, from the operations management network. The EACMS allows operators and engineers to have terminal access to the programmable logic controllers, relays, and remote terminal units (RTUs) that provide real-time control of energy production and delivery. Authorizations allowing access via the EACMS may be provisioned into the OT identity store or directly into the EACMS by the converged IdAM system. The converged IdAM system can provide time-bounded authorizations that will allow access during a limited time period. When the period expires, a workflow is triggered that revokes the authorization in the identity store and de-provisions the authorization from the OT identity store.

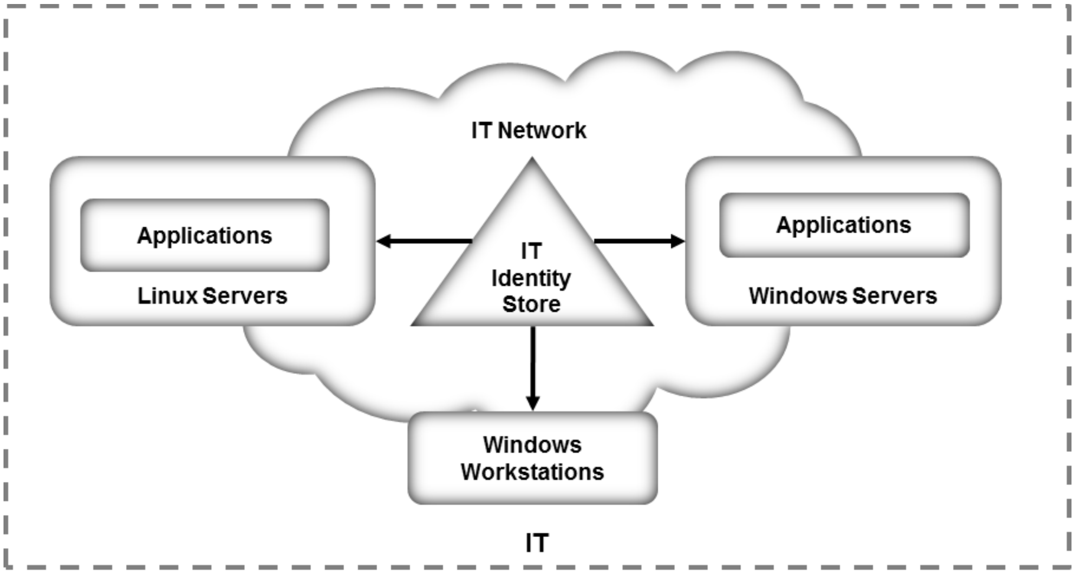
An ICS/SCADA firewall controls communication among ICS/SCADA devices. The converged IdAM system does not currently manage or provision authorizations that control device-to-device communications. Authorizations for device-to-device communications are either learned by the firewall in training mode or configured using a vendor-supplied application. This capability could be added in a future version of the converged IdAM system.

5.1.3 Information Technology Silo

The IT silo hosts business systems. These systems consist of user workstations and business applications running on Microsoft Windows or Linux servers. An IT identity store contains identities and access authorizations for both business system users and system administrators who manage the applications and servers. These authorizations are provisioned from the converged IdAM system. Applications that are not able to use an external identity store can be provisioned directly by the converged IdAM system.

Figure 5-5 shows the notional architecture of the IT silo.

Figure 5-5 Notional IT Silo Architecture



5.2 Example Solution Relationship to Use Case

When we first defined this challenge in collaboration with industry members, we wrote the following scenario [10]:

> *"An energy company technician attempts to enter a substation. She is challenged to prove her identity in a way that provides a high degree of confidence and is not onerous (i.e., does not require a significant behavior change). Her attempt at entry initiates an authentication request that, if possible, connects to the company's authentication and authorization services to validate*

> *her identity, ensure that she is authorized to access the substation, and confirm that a work order is on file for that substation and that worker at that time.*
>
> *Once she gains access to the substation, she focuses on the reason for her visit: She needs to diagnose a remote terminal unit (RTU) that has lost its network connectivity. She identifies the cause of the failure as a frayed Ethernet cable and replaces the cable with a spare. She then uses her company-issued mobile device, along with the same electronic credential she used for physical access, to log into the RTU's web interface to test connectivity. The RTU queries the central authentication service to ensure the authenticity and authority of both the technician and her device, then logs the login attempt, the successful authentication, and the commands the technician sends during her session."*

The first portion of the scenario deals with physical access to a substation. Unlike the description in this scenario, the example solution provides the management of identities and authorizations in a single system but assumes that the decision to allow a particular technician to have access to a particular facility at a particular time may be distributed. Distributing the access decision-making capability helps ensure that access control continues to function in the event of communication failures. Utilities have indicated that communication failures with substations are common. Therefore, authorization to allow the technician to have access to the substation will be created centrally by the IdAM workflow, placed in the identity store, and then provisioned to the PACS responsible for the substation. Accomplishing this requires integrating the work order management system with the IdAM workflow. Assigning a work order, to a technician, that requires access to a substation triggers actions within the IdAM workflow to authorize access to the substation and to provision that authorization to the substation PACS. When the technician presents his/her physical access credential at the substation, the PACS uses the provisioned authorization to determine if he/she should be allowed to have access. Likewise, while not explicitly stated in the example, completion of the work order triggers the IdAM workflow to remove the technician's substation access authorization and de-provision it from the substation PACS.

The second portion of the scenario deals with logical access to ICS/SCADA devices within the substation. Again, unlike the description in the scenario, the example solution centralizes the management of identities and authorizations, but assumes that run-time functions, such as authenticating a user and granting the user to have access to specific ICS/SCADA devices, are distributed functions. In this case, the example solution assumes that the substation contains an EACMS to which the technician connects his/her mobile device. The EACMS authenticates the technician and controls his/her access to ICS/SCADA devices within the substation. Assigning the technician to this work order triggers an IdAM workflow that authorizes him/her to have access to ICS/SCADA devices in the substation, stores these authorizations in the identity store, and provisions both the authorizations and any needed authentication credentials to the substation's EACMS. Completion of the work order triggers the removal of the access authorization, and de-provisioning of authorizations and credentials, from the substation EACMS.

5.3 Core Components of the Reference Architecture

To verify the modularity of the example solution and to demonstrate alternative provisioning methods, we created two builds of the converged IdAM capability. Both builds used the following products:

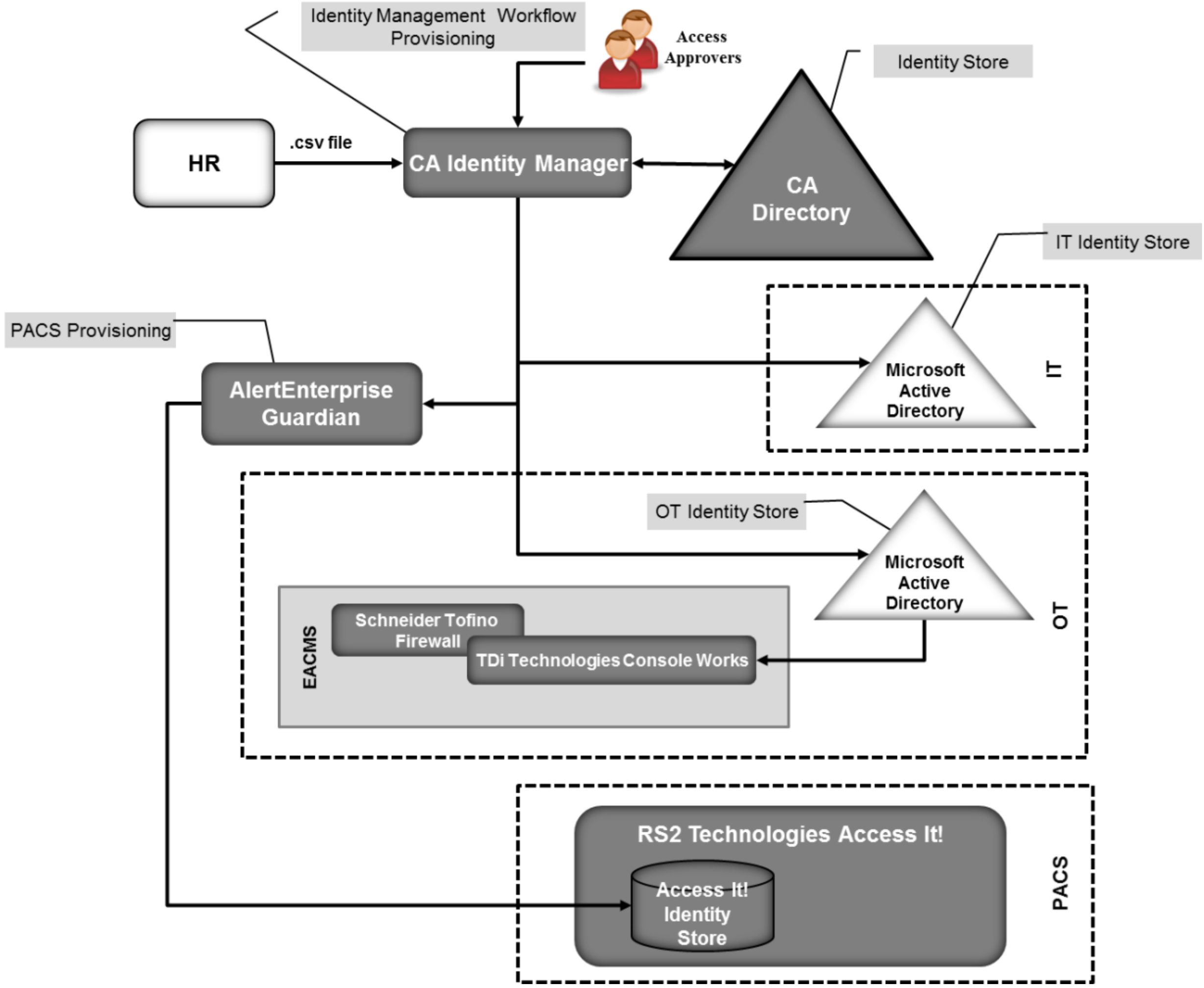
- AlertEnterprise Guardian implements provisioning to an RS2 Technologies (RS2) Access It! PACS.
- TDi Technologies ConsoleWorks and a Schneider Electric Tofino firewall serve as an EACMS.
- A Radiflow ICS/SCADA firewall controls interactions between two Modbus-speaking RTUs—a Schweitzer Engineering Laboratories (SEL) RTU and an RTU emulated by a Raspberry Pi single-board computer.

Build #1 used CA Technologies (CA) Identity Manager to implement the IdAM workflow and aspects of provisioning, and CA Directory to implement the identity store. Build #2 used the RSA IMG (now known as RSA VIA Governance and RSA VIA Lifecycle) to implement the IdAM workflow and the RSA Adaptive Directory to implement the identity store and aspects of provisioning.

5.3.1 Build #1

Figure 5-6 illustrates Build #1. See legend in Appendix B.

Figure 5-6 Build #1


Identity Management Workflow Provisioning
Access Approvers
Identity Store
HR
.csv file
CA Identity Manager
CA Directory
IT Identity Store
PACS Provisioning
AlertEnterprise Guardian
Microsoft Active Directory
IT
OT Identity Store
Microsoft Active Directory
EACMS
Schneider Tofino Firewall
TDi Technologies Console Works
OT
RS2 Technologies Access It!
Access It! Identity Store
PACS

CA Identity Manager implements the IdAM workflow. It receives input from an HR system, in the form of comma-separated value (CSV) files. We simulated the HR system by using manually produced CSV files because the NCCoE lab does not have an HR system. A mutually authenticated, integrity-protected connection between an HR system and CA Identity Manager is the preferred solution. CA Identity Manager also provisions information to Microsoft AD instances in business systems (IT) and in the operational system (OT). No relationship among these AD instances is assumed.

IT applications are assumed to be integrated with the IT identity store implemented by Microsoft AD and use credential information and authorization information in this AD instance. If there are IT applications that are not integrated with AD, the provisioning capabilities of CA Identity Manager would be used to directly provision the applications.

AlertEnterprise Guardian provisions physical access authorizations into the RS2 PACS. It is also capable of implementing workflow and provisioning ICS devices; however, those capabilities were not used in this build. CA Identity Minder supports call-outs within a workflow that can be used to invoke external programs. A call-out is used to connect with AlertEnterprise Guardian and to provide information to be provisioned to the RS2 PACS.

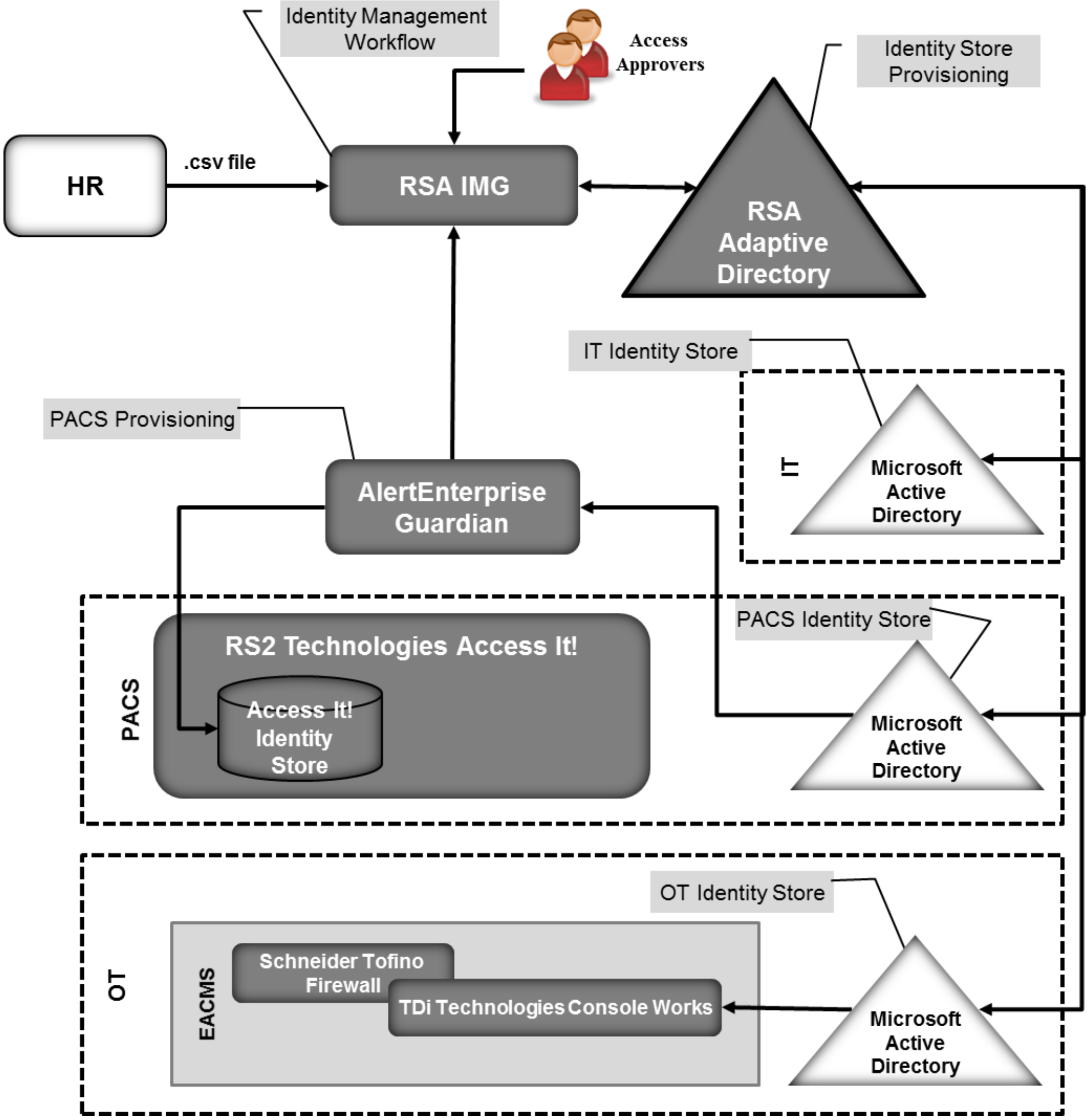
An instance of TDi Technologies ConsoleWorks is installed in the OT silo and integrated with the OT identity store that is implemented by a Microsoft AD instance. Identity Manager provisions ICS/SCADA access authorizations into this AD instance. ConsoleWorks uses the access authorizations in AD to control user access to ICS/SCADA devices. ConsoleWorks also captures an audit trail of all user access to the ICS/SCADA network.

A Schneider Electric Tofino firewall is installed between ConsoleWorks and the ICS/SCADA network. The firewall determines which Internet Protocol (IP) addresses within the ICS/SCADA network are accessible through ConsoleWorks and which network protocols can be used when accessing those addresses, but these are not managed by the converged IdAM solution. The combination of ConsoleWorks and the Tofino firewall implement an EACMS between the EMS / Operations Management Network and the ICS/SCADA network.

5.3.2 Build #2

Figure 5-7 illustrates Build #2. See legend in Appendix B.

Figure 5-7 Build #2


Identity Management Workflow
Access Approvers
Identity Store Provisioning
HR
.csv file
RSA IMG
RSA Adaptive Directory
IT Identity Store
IT
Microsoft Active Directory
PACS Provisioning
AlertEnterprise Guardian
PACS Identity Store
PACS
RS2 Technologies Access It!
Access It! Identity Store
Microsoft Active Directory
OT Identity Store
OT
EACMS
Schneider Tofino Firewall
TDi Technologies Console Works
Microsoft Active Directory

RSA IMG implements the IdAM workflow. It receives input from an HR system, in the form of CSV files. In Build #2, RSA IMG stores information in RSA Adaptive Directory, which subsequently provisions the information to the silo identity stores implemented with Microsoft AD instances.

RSA Adaptive Directory implements the identity store and provisioning portions of the example solution. RSA Adaptive Directory is a virtual directory that acts as a proxy in front of multiple back-end directories. The build assumes that each silo—OT, PACS, and IT—hosts a Microsoft AD instance. No relationship among these AD instances is assumed. When an IMG workflow stores information in Adaptive Directory, that information is actually stored in one or more of the underlying AD instances. In this way, storing information in Adaptive Directory provisions that information into one or more AD instances.

AlertEnterprise Guardian provisions physical access authorizations into the RS2 PACS. RSA IMG writes these authorizations into Adaptive Directory, which stores them in the PACS AD instance. AlertEnterprise Guardian monitors the PACS AD instance for updates, such as changed physical access authorizations for an existing user, the addition of a new user with physical access authorizations, or the removal of an existing user and associated access authorizations. When changes are detected, Guardian provisions them into the RS2 PACS.

As in Build #1, TDi Technologies ConsoleWorks and a Schneider Electric Tofino firewall are used in the OT silo to provide an EACMS between the EMS / Operations Management Network and the ICS/SCADA network. ConsoleWorks utilizes the AD instance in OT for the authorization of users in this build as well.

5.3.3 Implementation of the Use-Case Illustrative Scenario

This section explains how each of the two builds implements the scenario in Section 5.2.

A work order management system assigns a technician to resolve an issue with an RTU at a substation. The system initiates a workflow in either CA Identity Manager or RSA IMG that authorizes the technician to have physical access to the substation. In Build #1, this authorization is sent to AlertEnterprise Guardian via a call-out in the workflow in CA Identity Manager. Guardian provisions the authorization into the RS2 PACS. The authorization is also stored in the CA directory. In Build #2, this authorization is written to Adaptive Directory and stored in the PACS AD instance. AlertEnterprise Guardian detects the authorization change for the technician and provisions it to RS2. When the technician arrives at the substation and scans his/her credentials at the door, RS2 allows him/her to enter the facility.

The workflow also authorizes access to ICS/SCADA devices in the substation. In Build #1, CA Identity Manger stores this authorization in the CA directory and provisions it to the OT AD instance. In Build #2, IMG writes this authorization to Adaptive Directory, which stores it in the OT AD instance. When the technician connects his/her mobile device to ConsoleWorks in the substation, he/she is authenticated, and ConsoleWorks checks the OT AD instance, sees that he/she is authorized, and allows him/her to access the ICS/SCADA devices in the substation.

When the work order is closed, the work order management system triggers another workflow that removes the technician's access authorizations. In Build #1, the authorizations are removed from the CA directory. Substation physical access is de-provisioned from RS2 via a call-out from the workflow to AlertEnterprise Guardian. Identity Manager de-provisions ICS/SCADA access from the OT AD.

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

ConsoleWorks detects the change in the OT AD instance and de-provisions the technician's access to the RTU.

In Build #2, IMG removes the authorizations from Adaptive Directory. This removes the authorizations from the PACS and OT AD instances. AlertEnterprise Guardian detects the change in the PACS AD instance and de-provisions the technician's substation physical access. ConsoleWorks detects the change in the OT AD instance and de-provisions the technician's access to the RTU.

Without an active assigned work order, the technician has no physical or logical access to the substation.

The reference architecture requires substations to have power and communications to receive provisioned authorizations. The reference architecture does not address crisis or emergency situations where this requirement is not met. The reference architecture assumes that existing energy-company procedures for crisis or emergency response will be used/updated to address this challenge.

5.4 Supporting Components of the Reference Architecture

In addition to the products used to build an instance of the core example solution (the build), several products provide supporting components to the build, as shown in Figure 5-8. These products implement IdAM capabilities that, while necessary to completely implement IdAM within an organization, are not an integral part of the converged IdAM capability.

XTec AuthentX and GlobalSign demonstrate the outsourcing of some credential issuance and management capabilities. XTec AuthentX also demonstrates the outsourcing of some physical access-control capabilities.

The XTec AuthentX Identity and Credential Management System (IDMS/CMS) provides a PIV-I smart-card credential, based on NIST standards, that can be used for logical and physical access, as well as the description of the XTec product and its role in supporting the implementation of the example solution. AuthentX demonstrates the outsourcing of some aspects of user registration, credential issuance and management, authentication, and access-control capabilities. These capabilities are provided using a cloud-hosted solution with identity vetting workflows, credential issuance stations, and full life-cycle maintenance tools. AuthentX produces Homeland Security Presidential Directive 12–compliant smart cards that are interoperable with, and trusted by, federal counterparts.

The components of the XTec solution in our lab included XNode, card readers, and compliant PIV-I cards. The XTec product places the XNode, an IP-addressable RS232/RS485 controller within close range of the reader and door strike, as opposed to a typical, central control-panel deployment. The XNode can also control SCADA devices and send them encrypted instructions.

AuthentX IDMS/CMS can also provide a web-based implementation of the IdAM workflow in the example solution, as well as credential management and provisioning. AuthentX IDMS/CMS can control, log, and account for identity vetting, credential issuance, and credential usage with AuthentX PACS and logical access controls, as well as immediately control credential revocation to all interoperable resources.

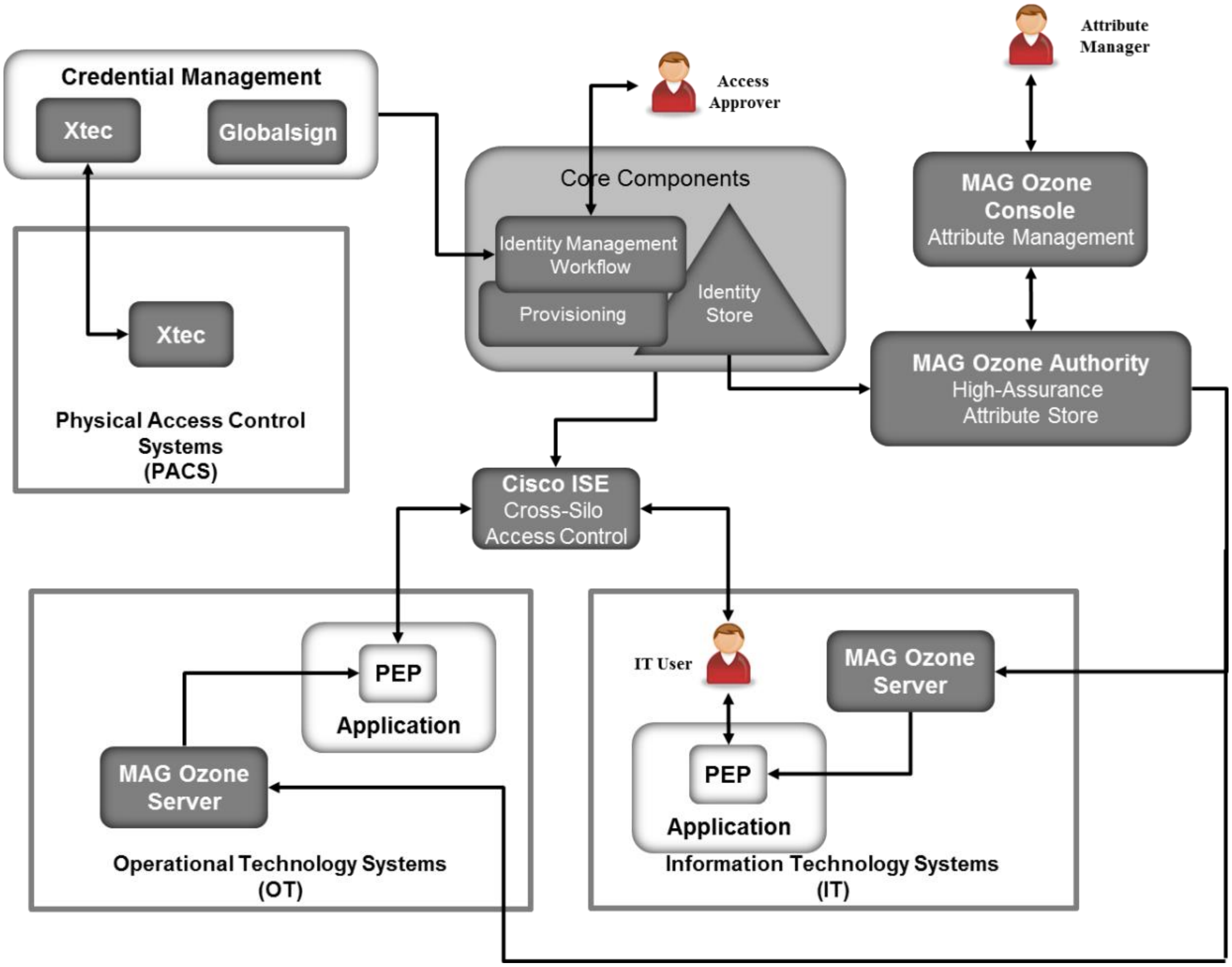
GlobalSign operates an NAESB-accredited software-as-a-service Certificate Authority. It illustrates an outsourced credential issuance and management capability that provides NAESB-compliant X.509 digital certificates. NAESB-compliant digital certificates are required credentials for authenticating Open Access Same-Time Information Systems (OASIS) transactions and access to the Electronic Industry Registry—the central repository for information related to energy scheduling and management activities in North America [11].

Mount Airey Group's (MAG's) Ozone and Cisco's Identity Services Engine (ISE) demonstrate access-control decision and enforcement capabilities that the converged IdAM capability can provision. MAG Ozone can also provide authorization management capabilities.

The MAG Ozone product provides a high-assurance attribute-based access control (ABAC) implementation [12]. ABAC controls access to resources by evaluating access rules using attributes associated with the resource being accessed, the person accessing the resource, and the environment. Ozone Authority provides a high-assurance attribute store. Attributes stored in Ozone Authority are managed using Ozone Console. Ozone manages attributes that control access to high-value transactions, such as high-dollar-value financial transactions.

Ozone Authority pulls attributes either from Adaptive Directory in Build #2 or from an AD instance in Build #1. Once Ozone Authority pulls the attributes, the attribute values are managed through Ozone Console.

Figure 5-8 Supporting Components



Ozone Server uses these attributes, in either the OT or IT silo, to decide if a user is allowed to perform a transaction. Ozone Server provides its decision to the policy enforcement point associated with the application.

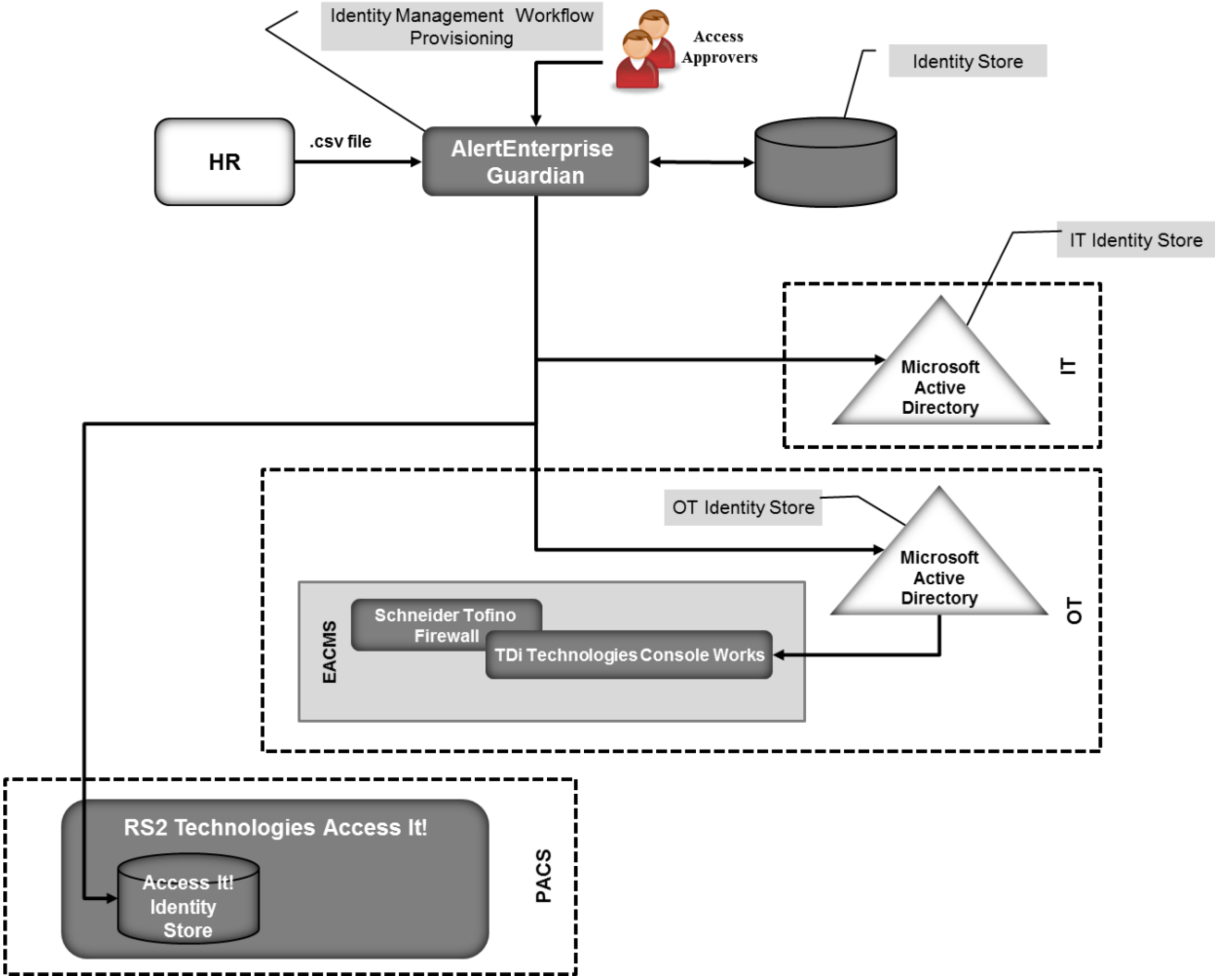
MAG provided an application for the IT silo to demonstrate some of Ozone's capabilities. Other than the MAG demonstration application, a full ABAC capability was not included in the architecture. A separate NCCoE project is creating an ABAC building block that could be used in IT or OT. The application is described in Appendix A [13].

Cisco ISE controls the ability of devices to connect over the network. ISE expands on basic network address-based control to include the identity of the person using a device. ISE is used in the builds to provide a gateway function between OT and IT, limiting which users and devices are allowed to connect from IT to resources in OT.

5.5 Build #3 – An Alternative Core Component Build of the Example Solution

RSA, CA, and AlertEnterprise all provide products that can implement the IdAM workflow, identity store, and provisioning. Our initial builds of the example solution used RSA and CA products to implement the IdAM workflow, the identity store, and AD provisioning. AlertEnterprise Guardian was used to provision the RS2 PACS; however, Guardian can also implement the IdAM workflow, identity store, and both OT and IT provisioning. To illustrate Guardian's full capabilities, AlertEnterprise created this independent build of the example solution in their labs, using the Guardian product (Figure 5-9). See legend in Appendix B.

Figure 5-9 Build #3


Identity Management Workflow Provisioning
Access Approvers
Identity Store
HR
.csv file
AlertEnterprise Guardian
IT Identity Store
Microsoft Active Directory
IT
OT Identity Store
Microsoft Active Directory
OT
EACMS
Schneider Tofino Firewall
TDi Technologies Console Works
RS2 Technologies Access It!
Access It! Identity Store
PACS

AlertEnterprise Guardian implements the IdAM workflow. It receives input from an HR system in the form of CSV files. We simulated the HR system by using manually produced CSV files because the NCCoE lab does not have an HR system. The preferred solution is a mutually authenticated, integrity-protected connection between an HR system and AlertEnterprise Guardian. Guardian provisions information to Microsoft AD instances in OT and IT. No relationship among these AD instances is assumed.

IT applications are assumed to be integrated with AD, and use credential information and authorization information in the IT AD instance. If there are IT applications that are not integrated with AD, the provisioning capabilities of Guardian would be used to directly provision the applications.

Guardian provisions physical access authorizations into the RS2 PACS. Physical Access and Cardholder life-cycle functions are supported through Guardian workflow to ensure that the right level of access is granted to the right people, based on training, compliance, and security requirements.

An instance of TDi Technologies ConsoleWorks and a Schneider Electric Tofino firewall are installed in the OT silo to implement an EACMS between the EMS / Operations Management network and the ICS/SCADA network. ConsoleWorks is integrated with the OT AD instance. Guardian provisions ICS/SCADA access authorizations in the OT AD instance. ConsoleWorks uses the access authorizations in OT AD to control user access to ICS/SCADA devices.

Additional information about Build #3 is available from the AlertEnterprise website [14].

5.6 Build Implementation Description

The infrastructure was built on Dell model PowerEdge R620 server hardware. The server operating system (OS) was the VMware vSphere virtualization operating environment. In addition, we used a 6-terabyte Dell EqualLogic network attached storage (NAS) product, Dell model PowerConnect 7024, and Cisco 3650 physical switches to interconnect the server hardware, external network components, and the NAS.

The NCCoE built two instantiations of the example solution to illustrate the modularity of the technologies. Build #1 uses the CA Identity Manager product. Build #2 uses the RSA Identity Management and Governance (IMG) (now known as RSA VIA Governance and RSA VIA Lifecycle) and RSA Adaptive Directory products.

The lab network is connected to the public internet via a virtual private network (VPN) appliance and firewall to enable secure internet and remote access. The lab network is not connected to the NIST enterprise network. Table 5-1 lists the software and hardware components that we used in the build, as well as the specific function that each component contributes.

Table 5-1 Build Architecture Component List

Product Vendor	Component Name	Function
Dell	PowerEdge R620	Physical server hardware
Dell	PowerConnect 7024	Physical network switch
Dell	EqualLogic	NAS
VMware	vSphere vCenter Server Version 5.5	Virtual server and workstation environment
Microsoft	Windows Server 2012 r2 AD Server	Authentication and authority
Microsoft	Windows 7	Information management
Windows	Windows Server 2012 r2 Domain Name System (DNS) Server	DNS
Windows	Structured Query Language (SQL) Server	Database
AlertEnterprise	Enterprise Guardian	Interface and translation between the IdAM central store and the PACS management server
CA	Identity Manager Release 12.6.05 Build 06109.28	Identity and access automation management application, IdAM provisioning
Cisco	ISE Network Server 3415	Network access controller
Cisco	Catalyst 3650	TrustSec-enabled physical network switch
GlobalSign	Digital Certificates	Cloud certificate authority
MAG	Ozone Authority	Central attribute management system
MAG	Ozone Console	Ozone administrative management console
MAG	Ozone Envoy	Enterprise identity store interface
MAG	Ozone Server	Ozone centralized attribute-based authorization server

Product Vendor	Component Name	Function
Radiflow	iSIM – Industrial Service Management Tool	SCADA router management application
Radiflow	SCADA Router RF-3180S	Router/firewall for SCADA network
RSA	Adaptive Directory Version 7.1.5	Central identity store, IdAM provisioning
RSA	IMG Version 6.9 Build 74968	Central IdAM system (workflow management)
TDi Technologies	ConsoleWorks	Privileged user access controller, monitor, and logging system
RS2	Access It! Universal Release 4.1.15 Physical-access-control components	Configures and monitors the PACS devices (e.g., card readers, keypads)
Schweitzer Engineering Laboratories	SEL-2411	Programmable automation controller
Schneider Electric	Tofino Firewall model number TCSEFEA23F3F20	Industrial Ethernet firewall
XTec	XNode	Remote access control and management

5.6.1 Build Architecture Components Overview

The build architecture consists of multiple networks that mirror the infrastructure of a typical energy industry corporation. The networks are a management network and a production network (Figure 5-10). The management network was implemented to facilitate the implementation, configuration, and management of the underlying infrastructure, including the physical servers, vSphere infrastructure, and monitoring. The production network (Figure 5-11) consists of the following components:

- the demilitarized zone (DMZ)
- IdAM
- IT network – business management systems
- OT network – ICS/SCADA industrial control system and EMS
- PACS network

These networks were implemented separately to match a typical electricity subsector enterprise infrastructure. The network diagrams and descriptions presented here illustrate and explain the laboratory environment that was used at NCCoE to build proof-of-concept implementations of the example solution. This lab architecture is not intended as security guidance. Firewalls block all traffic, except required internetwork communications. The primary internetwork communications are the user-access and authorization updates from the central IdAM systems between the directories and the OT, PACS, and IT networks.

Figure 5-10 Management and Production Networks

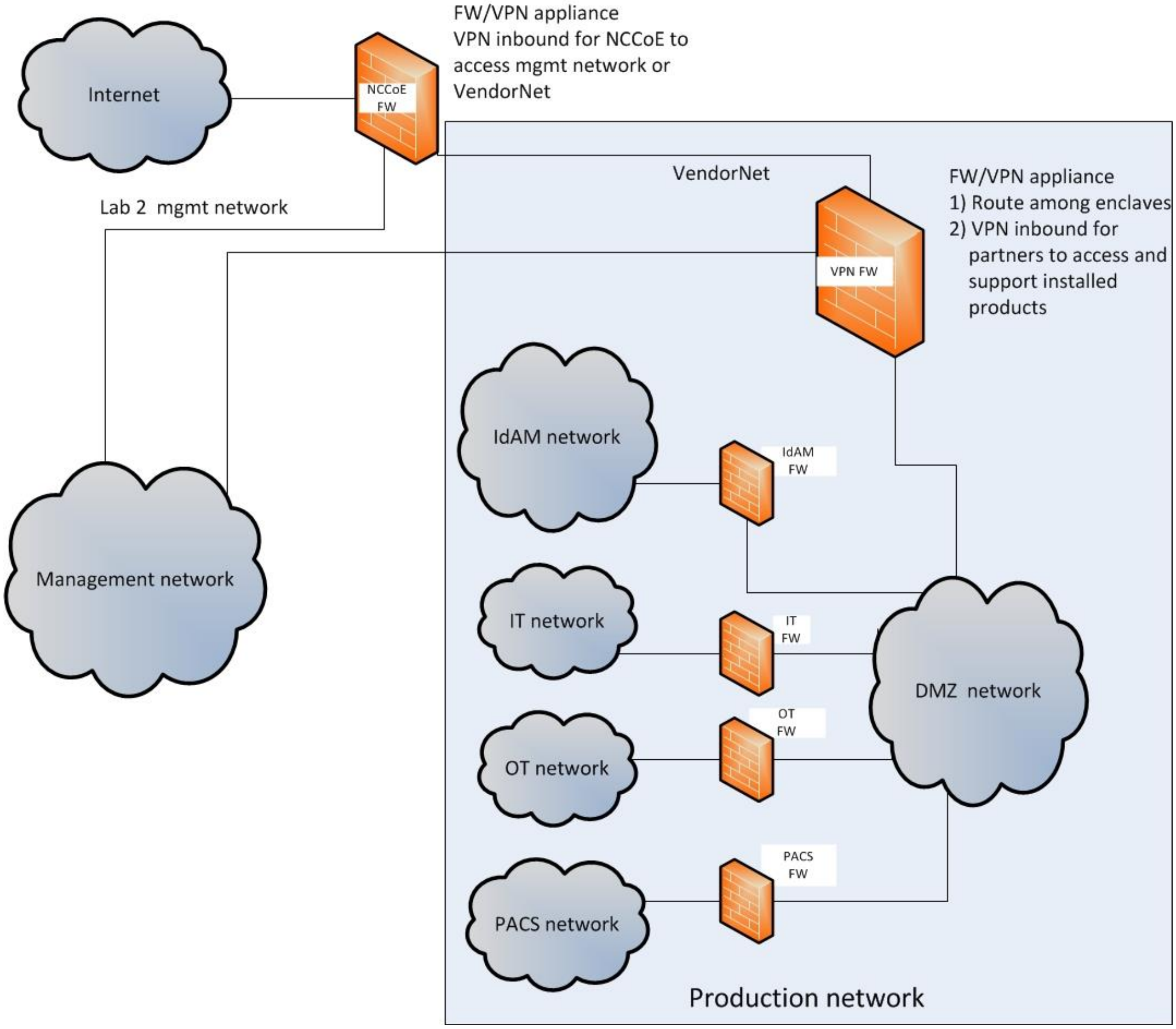
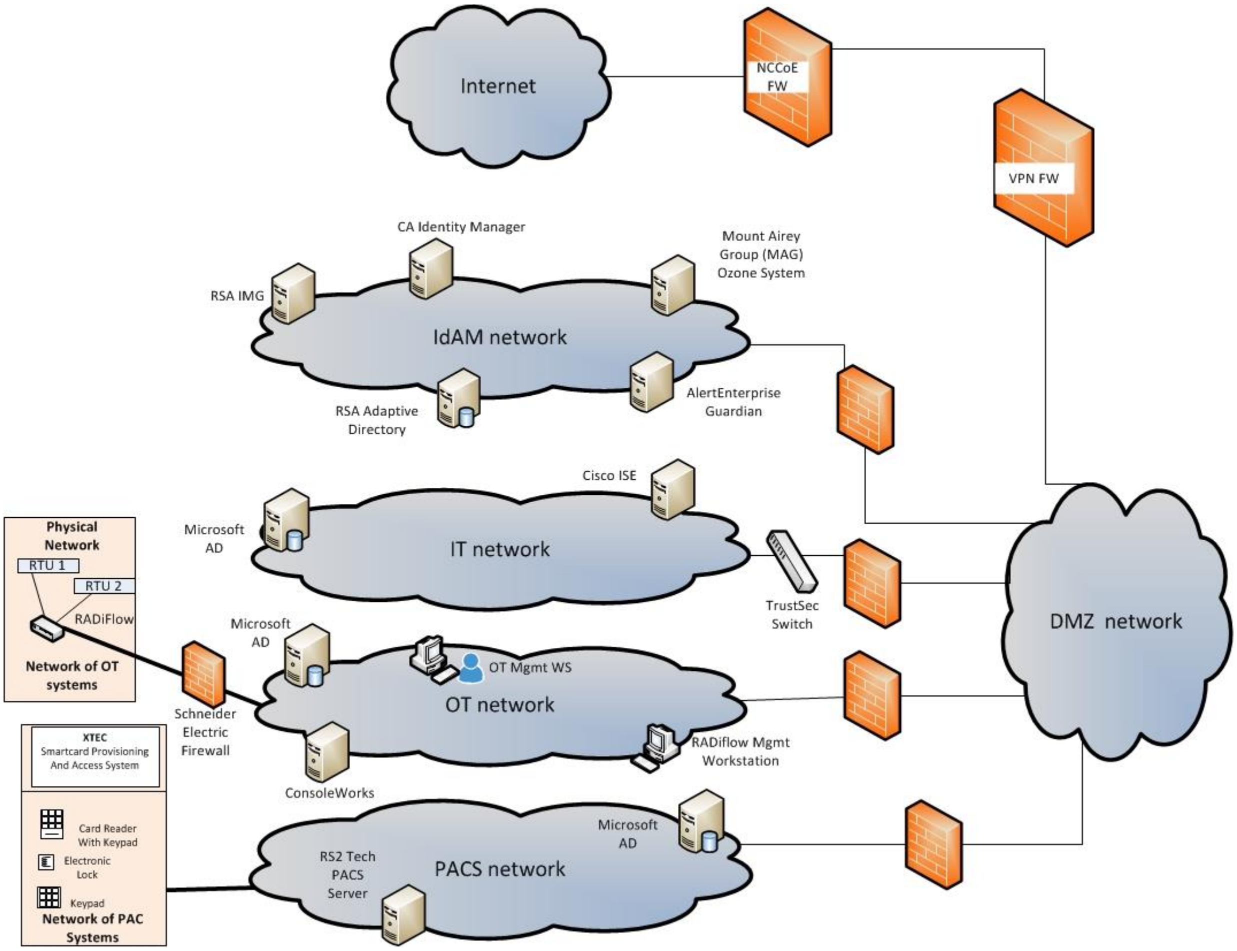


Figure 5-11 IdAM Build Architecture Production Network



The IdAM network represents the proposed converged IdAM network/system. This network was separated into OT, PACS, and IT to highlight the unique IdAM components that were proposed to address the use-case requirements.

The IT network represents the business management network that typically supports corporate email, file sharing, printing, and internet access for general business-purpose computing and communications.

The OT network represents the network that is used to support the EMSs and ICS/SCADA systems. Traffic is allowed into and out of the OT network via the OT firewall, for specific ports and protocols between specific systems identified by IP address.

The PACS network represents the network that supports the PACS across the enterprise. Typically, this network uses the enterprise IT network, and is segmented from the user networks by virtual local area networks (VLANs), which provide traffic and management segregation in the NCCoE Energy Sector lab.

VLANs, alone, should not be considered a security separation mechanism. In our architecture, a firewall allows limited access to and from the PACS network to facilitate the communication of access and authorization information. Technically, this communication consists of user role and responsibility directory updates originating in the IdAM system.

5.6.2 Build Network Components

5.6.2.1 Internet

The public internet is accessible by the lab environment to facilitate both cloud services and access for vendors and NCCoE administrators.

5.6.2.2 VPN Firewall

The VPN firewall is the access-control point for vendors, to support the installation and configuration of their components of the architecture. We used this access to facilitate product training and implementation support. This firewall also blocks unauthorized traffic from the public internet to the production networks. We used additional firewalls to secure the multiple domain networks (OT, PACS, IT, and IdAM).

5.6.2.3 Switching and Routing

Switching in the architecture is executed using a series of physical and hypervisor soft switches. VLANs are implemented to segment the networks shown in Figure 5-10 and Figure 5-11. VLAN switching functions are handled by physical Dell switches and the virtual environment. Routing was accomplished using the firewall.

5.6.2.4 DMZ

The DMZ provides a protected neutral network space that the other networks of the production network can use to route traffic to/from the internet or each other. The DMZ presented here is designed to support the NCCoE laboratory environment. Organizations should construct DMZs by using the appropriate guidance for their environment, such as NERC Guidance for Secure Interactive Remote Access.

5.6.3 Operational Technology Network

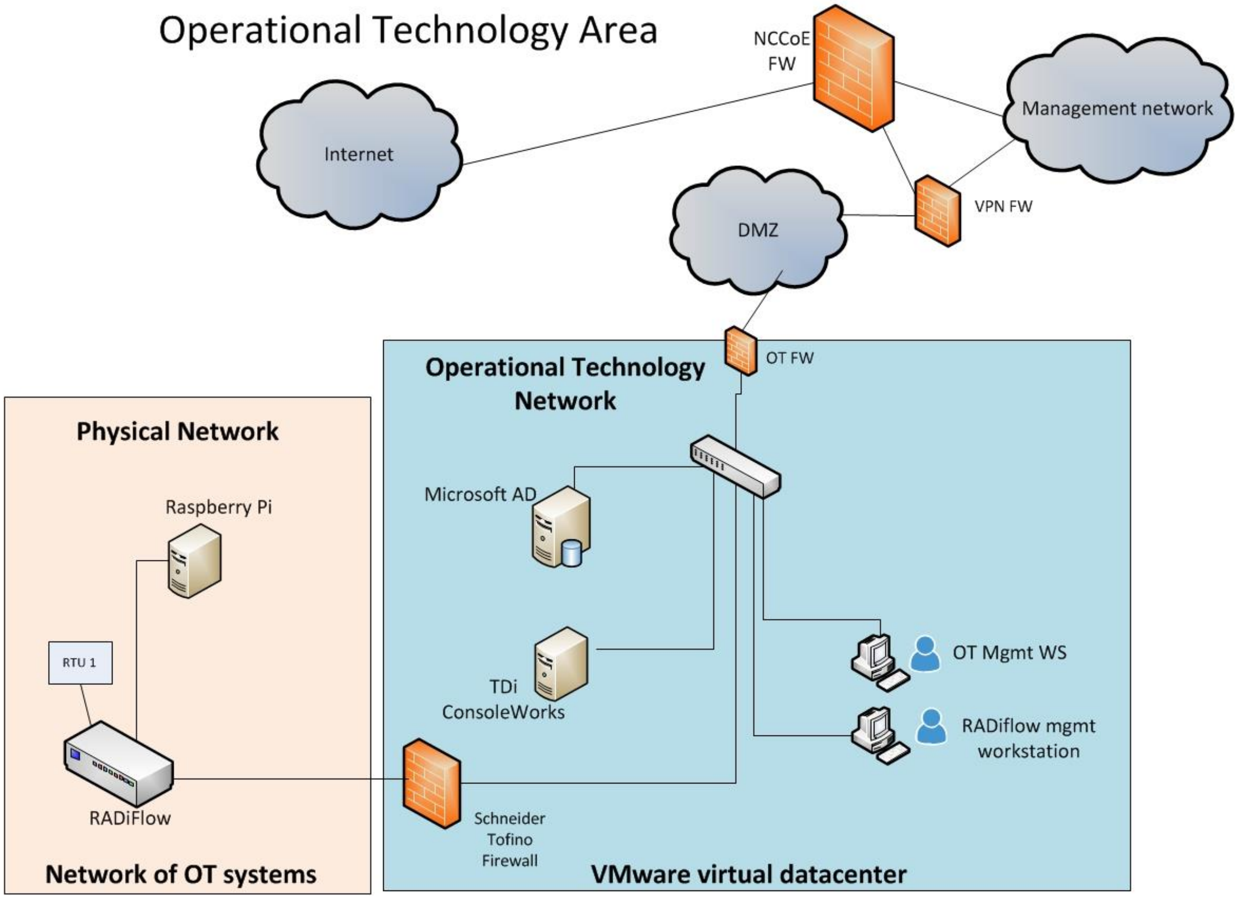
The builds include the following OT network components:

- directory instance
- OT management workstation
- RTU with IP interface
- RTU with serial interface

- ICS/SCADA router
- router management workstation
- ICS/SCADA gateway / access-control system

This network emulates an energy enterprise OT network and systems. The specific vendor products used in this network are identified in Table 5-1 (refer to Section 5.6) and Figure 5-12.

Figure 5-12 OT Network



In the OT network, the Radiflow router performs the ICS/SCADA network firewall function. The ConsoleWorks product provides the access-control/gateway function. The build used the gateway function to manage access to the OT router and RTU management/console interface. The interface can be used to configure the RTU and to issue real-time function commands (e.g., open/close relays). The access-control/gateway function uses the OT directory to obtain access authority for each user requesting access to an RTU.

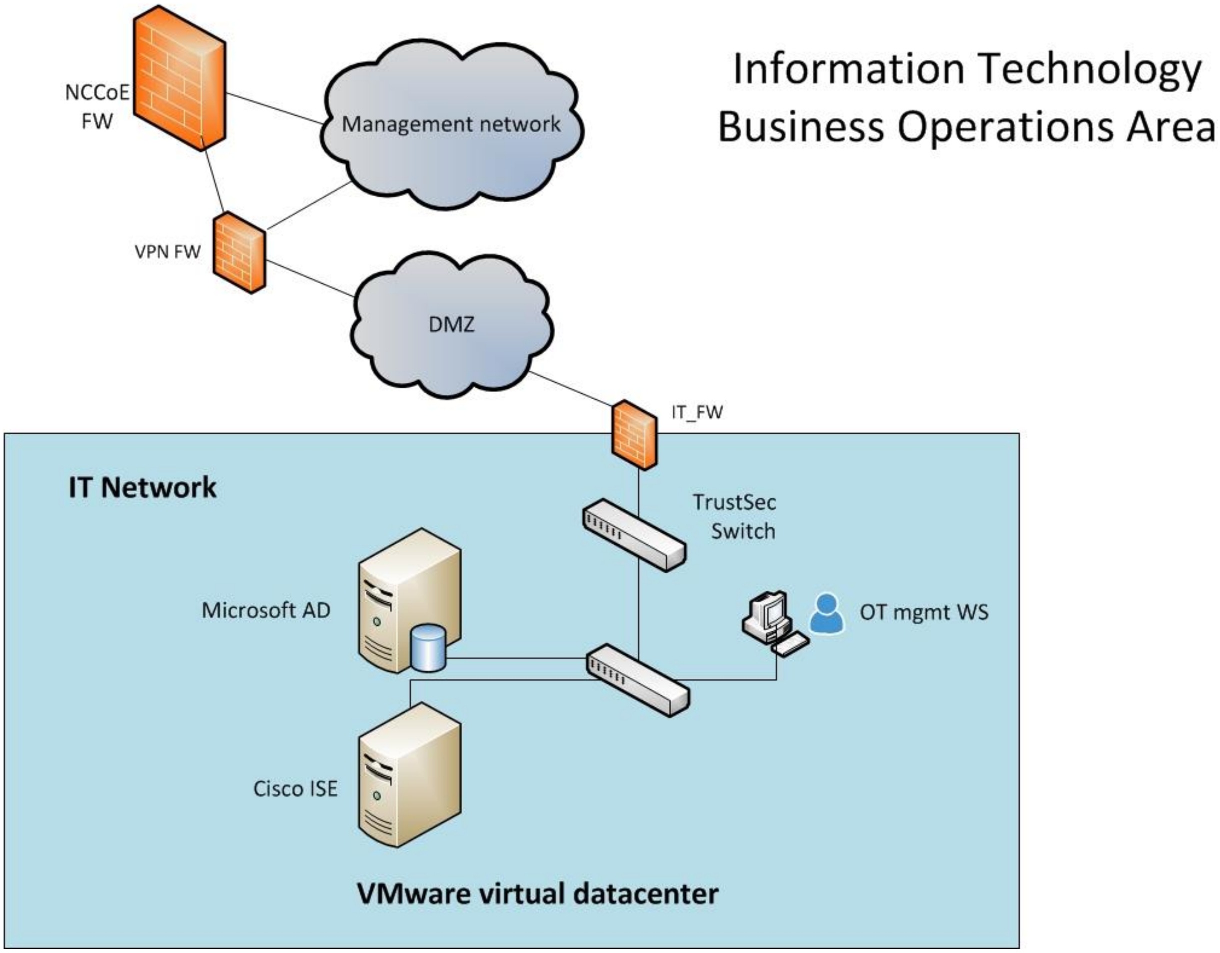
5.6.4 Information Technology Network

The builds include the following IT network components:

- AD
- Cisco ISE
- TrustSec switch
- workstation

A typical enterprise includes information-sharing systems, email, and application servers. We did not include these systems in the architecture because they are not needed to demonstrate the effectiveness of the IdAM example solution. The specific vendor products used in this network are identified in Table 5-1 (refer to Section 5.6) and Figure 5-13.

Figure 5-13 IT Network



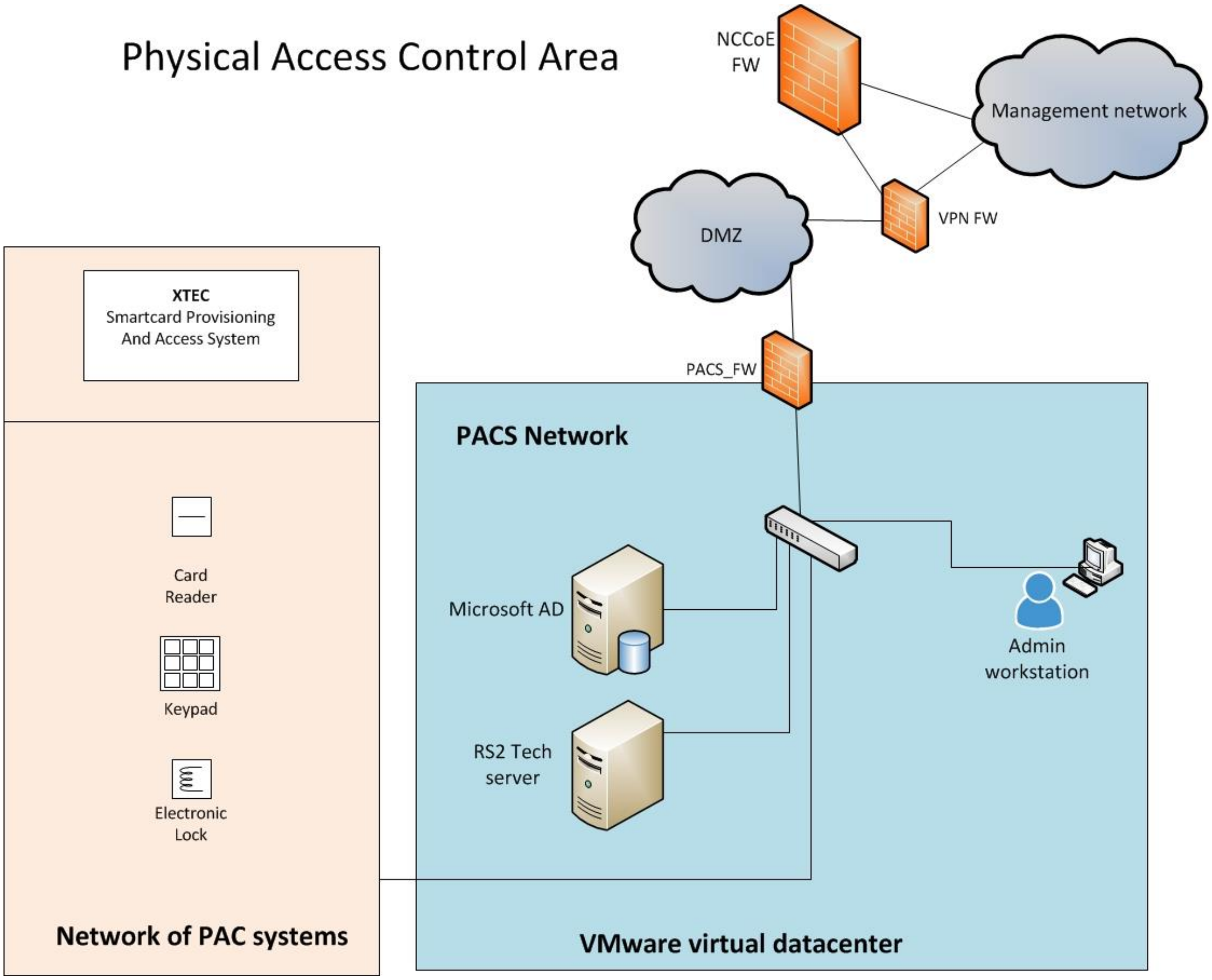
5.6.5 Physical Access and Control System Network

The builds include the following PACS network components:

- AD
- PACS control server – Access It!
- integrated access-control unit (including a card reader, keypad, and door strike) – RS2
- workstation

This network emulates a typical enterprise PACS. The specific vendor products used in this network are identified in Table 5-1 (refer to Section 5.6) and Figure 5-14.

Figure 5-14 PACS Network



Two technologies are demonstrated in the PACS network: XTec XNode and RS2 Access It!. XTec XNode is a PACS using smart-card readers, pin pads, and an internet cloud-based authorization service. The cloud service can federate (interoperate) with corporate identity and access stores or can be operated as a fully outsourced PACS IdAM solution. XNode was used as a standalone access-control capability. It was not integrated or federated with the converged IdAM system, and its ability to contribute to compliance with NERC CIP Version 5 security requirements was not addressed. The RS2 system includes card readers, pin pads, and the Access It! local management server. The local management server is integrated with the central identity and access store via the AlertEnterprise Guardian product. In Build #1, Guardian receives IdAM data directly from Identity Manager. Once the information is received, Guardian provisions the information to the PACS management server. In Build #2, Guardian monitors the PACS directory for IdAM changes. Once changes are identified, Guardian collects the information and provisions the IdAM information to the PACS management server.

5.6.6 Identity and Access Management Network

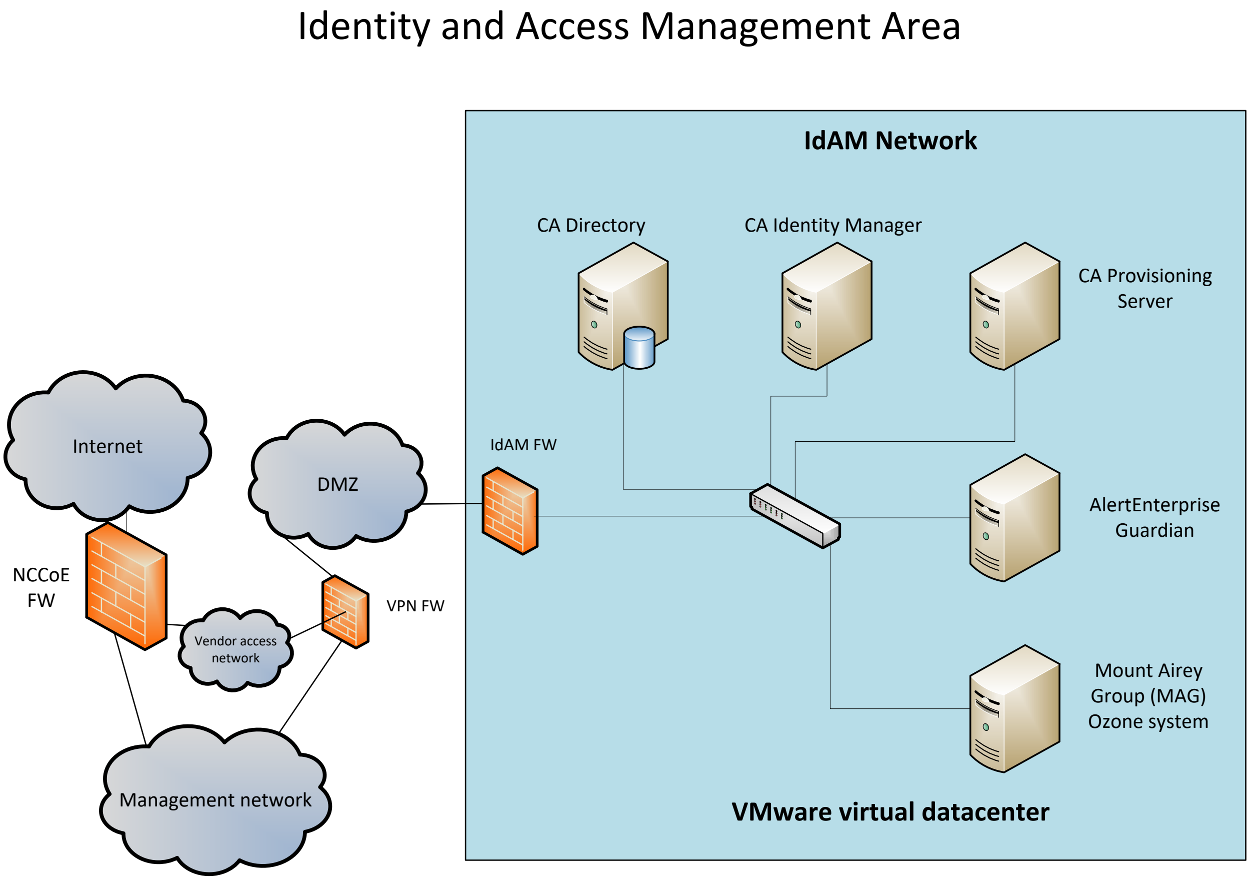
5.6.6.1 Build #1

Build #1 includes the following IdAM network components:

- central IdAM system
- PACS IdAM interface system
- SQL server
- MAG Ozone components

The IdAM was separated to highlight the unique IdAM components that were proposed to address the use-case requirements. The implementation is not a recommendation to separate IdAM functions on their own network. The products used in this build are identified in Table 5-1 (refer to Section 5.6) and Figure 5-15.

Figure 5-15 Central IdAM Network, Build #1



The central IdAM system is the authoritative central store for identity and access authorization data. CA Identity Manager provides a central identity and access store, as well as a workflow management capability, in Build #1 (Figure 5-15). The central IdAM system takes over the control of the directory instances in each silo. The control is implemented by providing an administrative account credential for each managed directory to the IdAM system. This is an important aspect of the implementation. When the administrative credential is issued, the organization must limit access to the managed directories of the IdAM system to a reduced number of administrative users. The security of the solution partially depends on limited access to the managed directories, as discussed in Section 5.9.6.

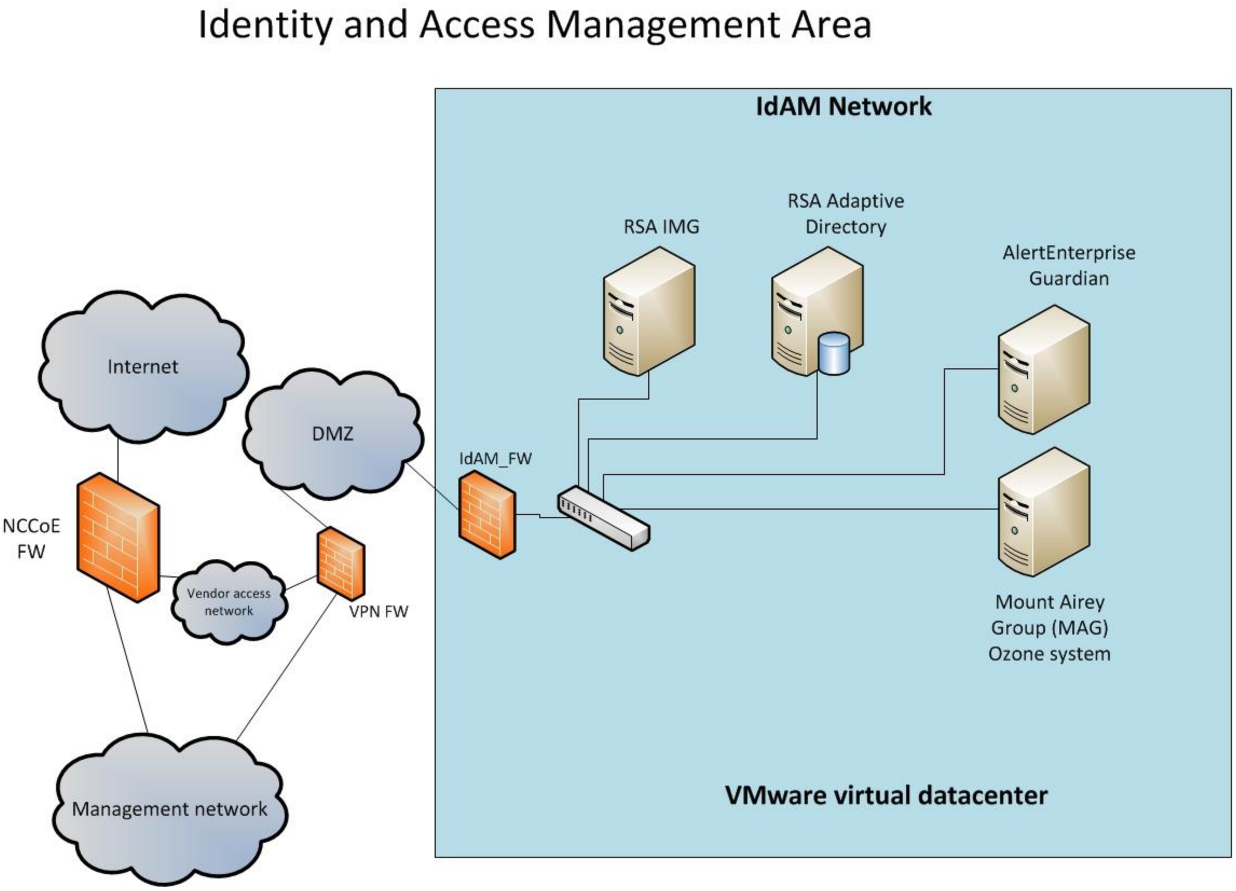
In this build, the OT, PACS, and IT directories synchronize (sync) with the central IdAM system by using Lightweight Directory Access Protocol Secure (LDAPS). This synchronization is set up to immediately sync changes from the IdAM system to each directory. In addition, an automated sync function can be implemented to check for unauthorized changes in each directory to increase the security of the implementation. Automated sync was not implemented in this build.

AlertEnterprise Guardian integrates the IdAM central store with the PACS access management system (Access It!). Guardian includes integration and translation capabilities to transfer the IdAM data to the Access It! management server database. In this build, Guardian is integrated with Identity Manager for IdAM synchronization.

5.6.6.2 Build #2

The IdAM network components include a central IdAM system, PACS IdAM interface system, and the MAG Ozone components. The IdAM network represents the proposed converged IdAM network/system. This network was separated to highlight the unique IdAM components that were proposed to address the use-case requirements. The implementation is not a recommendation to separate IdAM functions own their own network. The products used in this build are identified in Table 5-1 (refer to Section 5.6) and Figure 5-16.

Figure 5-16 Central IdAM Network, Build #2



The central IdAM systems are the authoritative central store for identity and access authorization data. RSA IdAM products and AlertEnterprise provide central identity and access stores, as well as a workflow management capability. The central IdAM system takes over the control of the directory instances in each silo. The control is implemented by providing an administrative account credential for each managed directory to the IdAM system. This is an important aspect of the implementation. When the administrative credential is issued, the organization must limit the access to the managed directories of the IdAM system to a reduced number of administrative users. The security of the solution partially depends on limited access to the managed directories, as discussed in Section 5.9.6.

In this build, the OT, PACS, and IT directories sync with the central IdAM system by using LDAPS. This synchronization is set up to immediately sync changes from the IdAM system to each directory. The IdAM system automatically syncs with each directory to check for unauthorized changes to increase the security of the implementation.

In this build, Guardian was used to integrate the IdAM system with the PACS access management system (Access It!). Guardian includes integration and translation capabilities to transfer the IdAM data to Access It!. Guardian monitors the PACS directory for IdAM updates.

The MAG Ozone product provides secure attribute distribution within the enterprise. Section 5.4 describes its use.

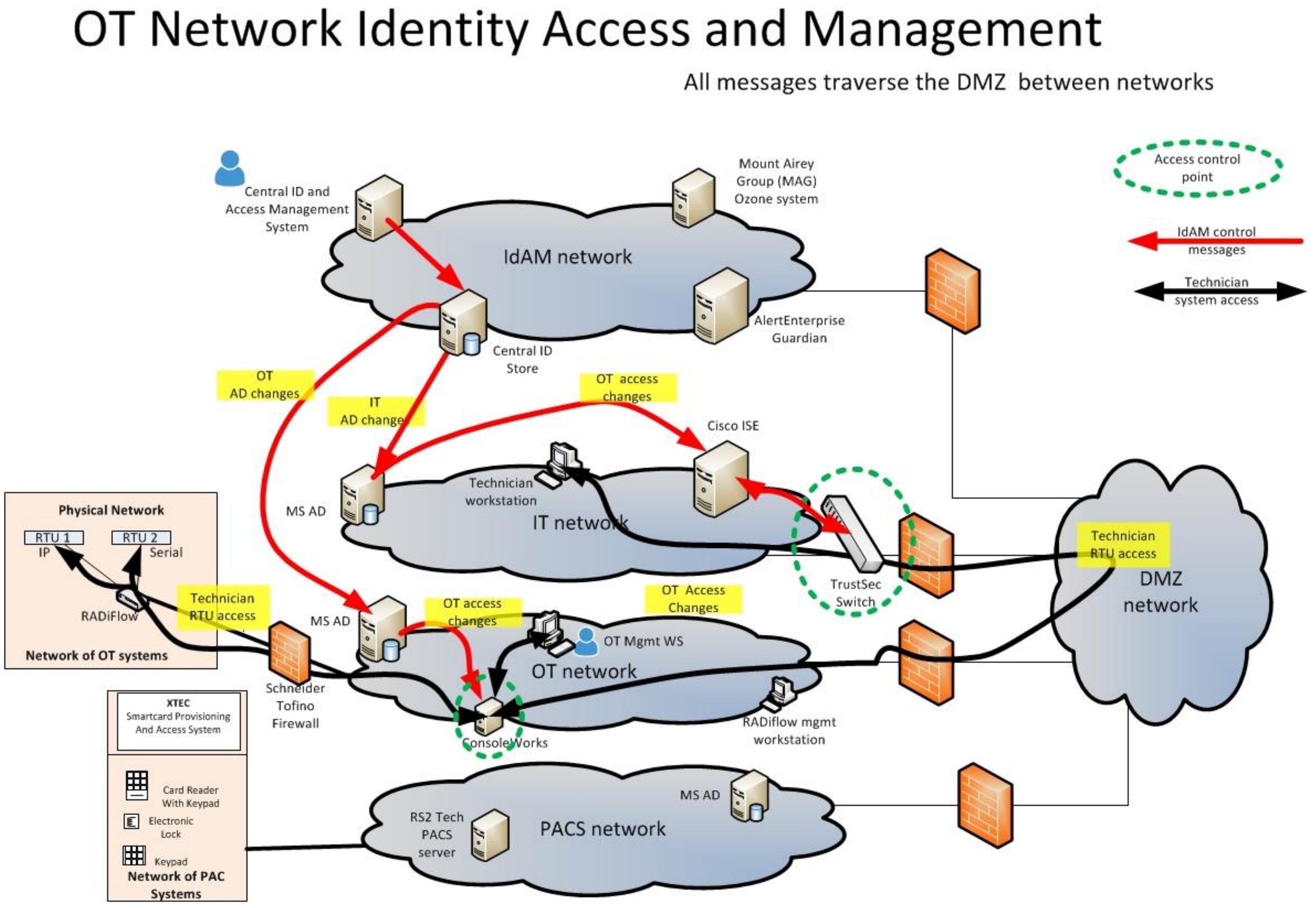
5.6.7 Access Authorization Information Flow and Control Points

The access and authorization for each user is based on the business and security rules implemented in workflows within the central IdAM system products (RSA IMG, CA Identity Manager). The workflows include management approval chains as well as approval/denial data logging. Once the central IdAM system has processed the access and authority request, the updated user access and authorization data is pushed to the central identity store. The central identity store contains the distribution mechanism for updating the various downstream (synchronized) directories with user access and authorization data. This process applies to new users, terminated users (disabled or deleted users), and any changes to a user profile. Changes include promotions, job responsibility changes, and anything else that would affect the systems that a user needs to access.

5.6.7.1 OT Access and Authorization Information Flow

This section describes the OT ICS/SCADA access and authorization information flow for both builds. Figure 5-17 depicts the access and authorization information flow for OT ICS/SCADA devices.

Figure 5-17 Access and Authorization Information Flow for OT ICS/SCADA Devices



The red lines in Figure 5-17 indicate the access and authorization data exchanges. The black lines depict the data paths of two OT ICS/SCADA technicians accessing RTUs in the SCADA network (one from the IT network, and one from the OT network). Note that all data routed between networks flows through the DMZ and network firewalls.

In the OT network, ConsoleWorks controls access to the OT ICS/SCADA devices. ConsoleWorks uses the OT directory to determine which users are authorized to access OT ICS/SCADA devices; it is the control point for users accessing OT network devices. ConsoleWorks stores profiles for groups and specific users. The profiles define the OT devices that each user is authorized to access. In addition, ConsoleWorks monitors and logs each user session. This feature allows an organization to monitor user activity, block undesired activities, and generate alerts for suspicious or undesired activities.

In the IT network, a Cisco TrustSec switch controls which users have access to the OT network. ISE controls the TrustSec switch. This provides an Electronic Access Point to the ICS/SCADA network, as described in NERC CIP-005. ISE uses the IT directory identity store to determine user access authority and to limit access to the ICS/SCADA network to authorized users. This capability enhances the enterprise’s ability to follow NERC CIP-005. ConsoleWorks also authorizes users to access OT devices.

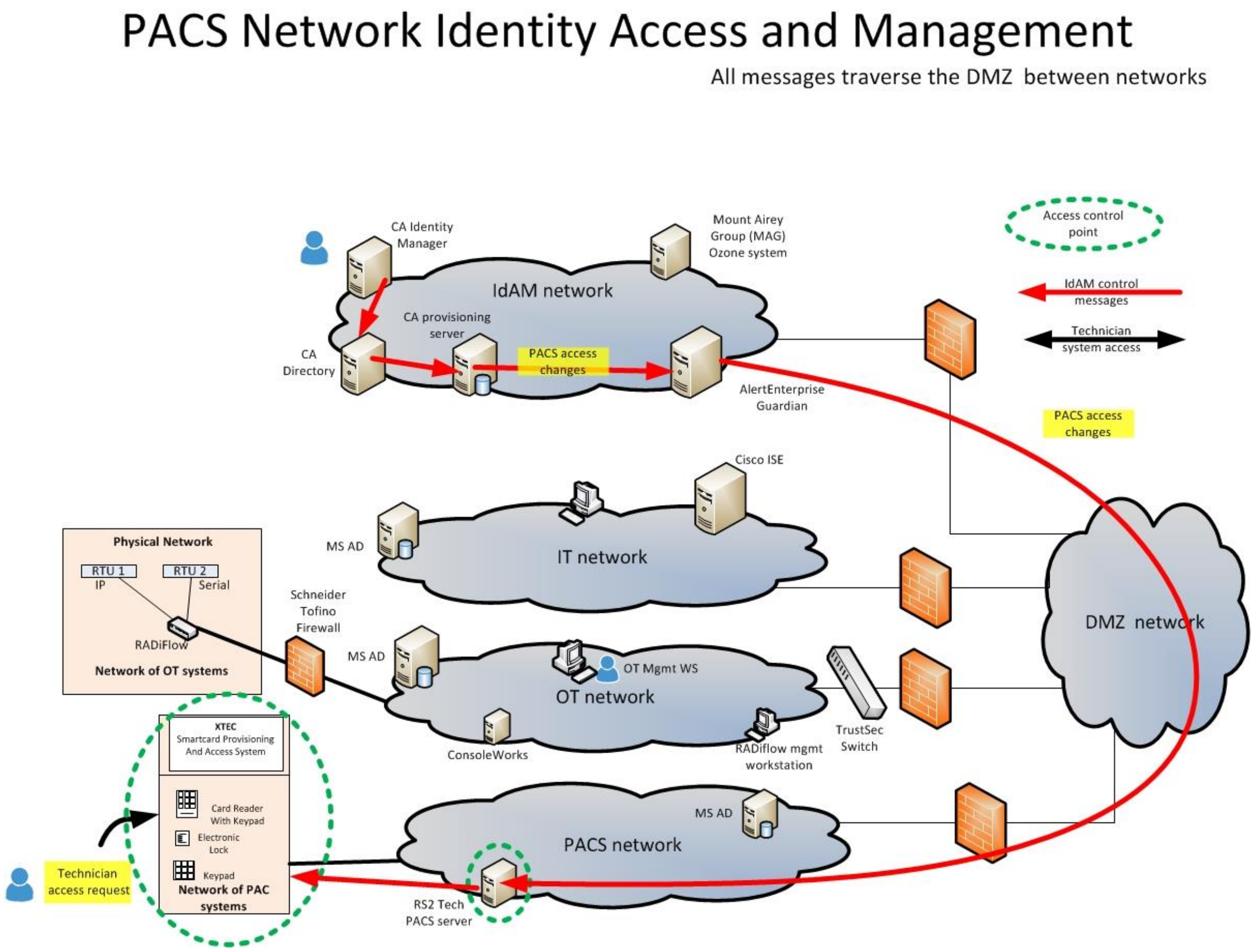
5.6.7.2 PACS Access and Authorization Information Flow

The PACS access and authorization information flows in each build are described in this section.

5.6.7.2.1 Build #1

Figure 5-18 depicts the access and authorization information flow for the PACS Network, Build #1.

Figure 5-18 Access and Authorization Information Flow for the PACS Network, Build #1



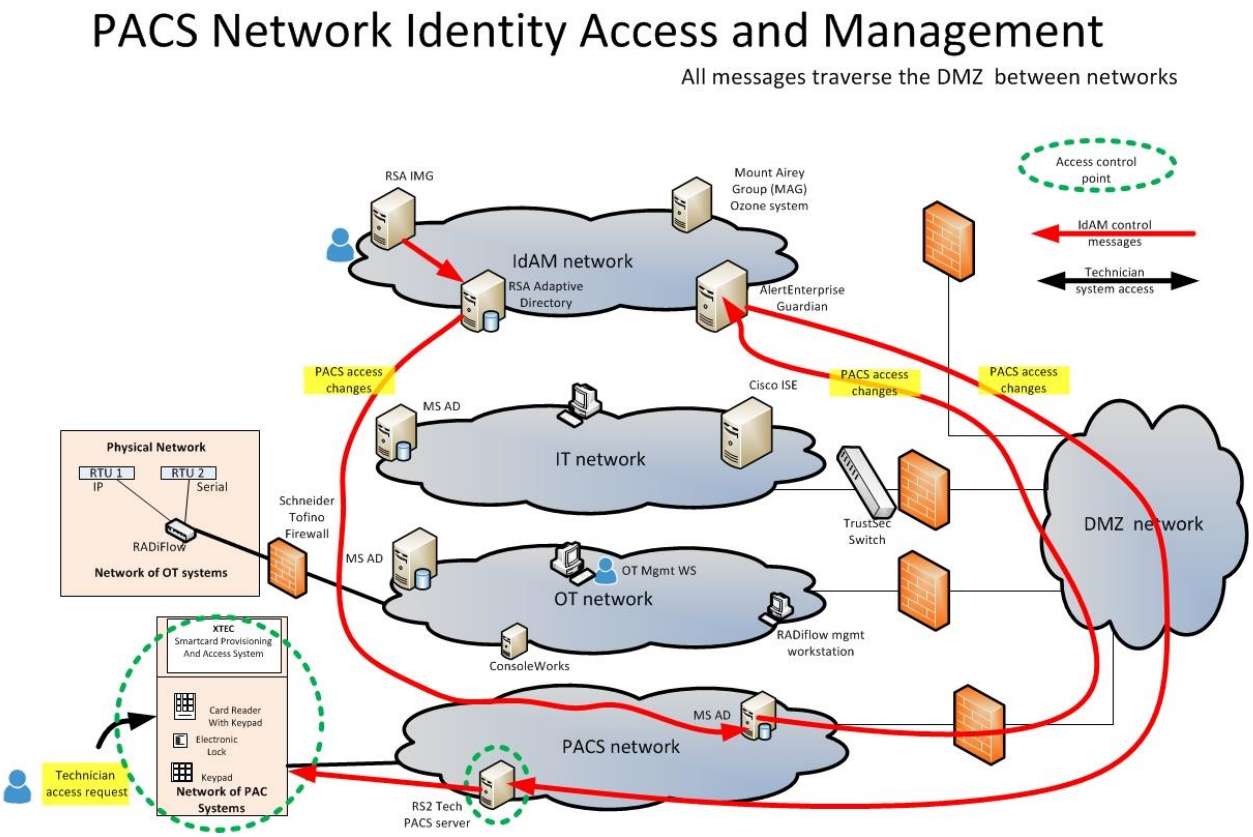
The PACS network includes devices, such as door locks and keypads. In Figure 5-18, the red lines indicate the access and authorization data exchanges. Note that all data routed between networks flows through the DMZ and network firewalls.

In the PACS network, the Access It! management server controls physical access to facilities, rooms, etc. Access It! updates the PACS devices as needed. The devices also report/log user access to this server for logging/auditing purposes. In most environments, the PACS network is segregated from other networks, typically using VLANs. Guardian collects the access and authorization data from the Identity Manager provisioning server and provides it to Access It!.

5.6.7.2.2 Build #2

Figure 5-19 depicts the access and authorization information flow for the PACS Network, Build #2.

Figure 5-19 Access and Authorization Information Flow for the PACS Network, Build #2

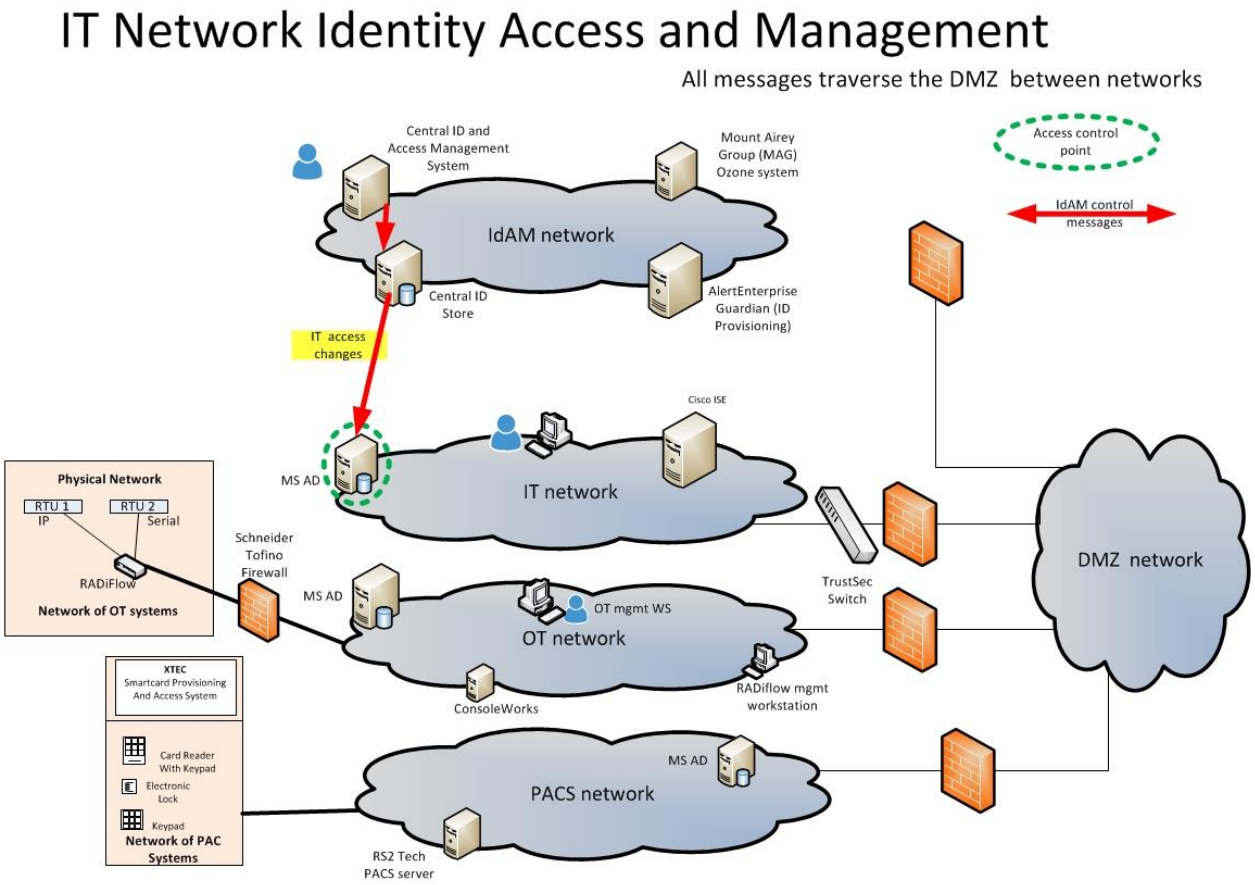


The red lines in Figure 5-19 indicate the access and authorization data exchanges or PACS access in Build #2. The red lines represent logical, not physical, information flows. PACS access changes from RSA Adaptive Directory in the IdAM network to Microsoft AD in the PACS network physically flow through the DMZ network. In this build, IMG provisions all PACS IdAM data to the PACS directory. AlertEnterprise collects the access and authorization data from the PACS directory and provides it to Access It!.

5.6.7.3 IT Access and Authorization Information Flow

Figure 5-20 depicts the access and authorization information flow for the IT Network.

Figure 5-20 Access and Authorization Information Flow for the IT Network



The red lines in Figure 5-20 indicate the access and authorization data exchanges in both builds. Note that all data is routed among the OT, PACS, IT, and IdAM networks through the DMZ. In the IT network, the hosts and other systems access the IT directory to determine which users are authorized to access devices on the IT network. AD provides the typical identity store function of storing the access permissions.

5.7 Data

The builds required a user data set to populate the central IdAM system. In both builds, the IdAM system was initially populated with user data from a synthetic data set. The data set was designed to mirror a typical HR-system data-set export file. Because the NCCoE lab does not have an HR system, it used a CSV file, which is a typical HR-system export-file type, to simulate an HR system. The preferred solution is a mutually authenticated, integrity-protected connection between an HR system and the IdAM system. The data included user names, titles, access assignments, unique identifiers, and other details required to complete valid directory entries. Once the set of user data was loaded into the IdAM system, each silo directory was provisioned with the appropriate user data. Each silo directory was pre-configured with the group and attribute fields that are needed to support the builds. For example, the OT network directory had user groups corresponding to the ConsoleWorks user groups. The details are included in the How-To guide (*NIST SP 1800-2C*).

5.8 Security Characteristics Related to NERC CIP Version 5

The example solution impacts, and is impacted by, the requirement to conform to NERC CIP Version 5 standards. The NERC CIP cybersecurity standards provide specific requirements that apply to the bulk power system and were used as a reference by the development team. The proposed solution is designed to be CIP-informed. This document attempts to capture some of the key areas where CIP standards are relevant to elements of the solution and its implementation, for reference purposes. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance.

Because the example solution may control authorizations to access critical cyber assets, it may be subject to security requirements defined in NERC CIP Version 5.

The example solution is informed by NERC CIP Version 5 requirements and may contribute to CIP-aligned implementations by providing mechanisms for efficiently and cost-effectively centralizing the logging and auditing of all IdAM activity. With this solution in place, information regarding which users have access to what components is easily available via the central identity store. Without the solution, this information would have to be gathered separately from each identity store in IT, OT, and PACS.

Table 5-2 describes how the converged IdAM solution relates to some NERC CIP Version 5 requirements.

Table 5-2 NERC CIP Version 5 Requirements

NERC CIP Requirement	IdAM Role
CIP 004-5.1 requires completions of training priori to granting electronic access and unescorted physical access to applicable cyber assets.	The IdAM workflow can be configured to check a training system before granting access to critical cyber assets.
CIP 004-5.1 has several requirements related to background investigations, criminal-history checks, and personnel risk assessments being completed before granting logical or physical access to cyber assets.	The IdAM workflow can be configured to verify that individuals have met these requirements before granting access to critical cyber assets.

NERC CIP Requirement	IdAM Role
CIP 004-5.1 requires periodic review and verification of all logical and physical access.	The identity store maintains authoritative information on all logical and physical access to resources. The IdAM workflow can be configured to support periodic access reviews.
CIP 004-5.1 requires timely revocation of logical and physical access when an employee is terminated or changes jobs.	The IdAM workflow receives information on terminations and job changes, from the HR system. It can immediately de-provision access for these employees.
CIP 004-5.1 requires a process based on need to grant logical and/or physical access to assets.	The IdAM workflow is the process for authorizing access. The workflow design and implementation document the process.
CIP-007-5 requires responsible entities to identify and inventory all known enabled default or other generic account types.	The IdAM identity store can maintain this information. The IdAM provisioning capability can ensure that identity stores in OT, IT, and PACS are consistent with the information in the IdAM identity store.

5.9 Evaluation of Security Characteristics

The NCCoE gratefully acknowledges the contribution of Sallie Edwards and Susan Symington, from The MITRE Corporation, for writing this section.

The security characteristic evaluation seeks to understand the extent to which the IdAM example solution provides a more secure, uniform, and efficient solution for managing authentication and authorization services and access control across three independent electricity subsector networks. In addition, the evaluation seeks to understand the security benefits and drawbacks of the example solution.

5.9.1 Scope

The evaluation included the analysis of the example solution, to identify weaknesses, discuss mitigations, and understand benefits and trade-offs.

We considered the following elements of the IdAM example solution:

- security functionality of the components depicted within the OT, PACS, IT, and IdAM networks in Figure 5-2, and their interactions with each other, with the exception of the XTec standalone access-control system
- analysis of the capabilities and overall workflow process for centralizing the management of authentication and authorization services on, and access control to, the IT, OT, and PACS

networks, including assumptions, threats, vulnerabilities, mitigations, benefits, drawbacks, trade-offs, and risks related to the following characteristics:

  - centralization
  - automation
  - audit (accountability and tracking)
  - authentication
  - authorization
  - access control
  - provisioning

- new “cross-silo” attacks that would not have been possible without the converged IdAM capability
- how the example solution addresses the security characteristics listed in the use-case description (https://www.nccoe.nist.gov/projects/use-cases/idam)
- security recommendations that should be addressed when deploying the IdAM design in a real-world, operational environment
- hands-on evaluation of the laboratory build, as appropriate, to support the analysis and to demonstrate value
- security-related aspects of the OT, PACS, and IT networks, as they potentially impact the solution posed by the example solution

The following elements of the example solution were not considered:

- evaluation of any specific vendor product or its implementation
- considerations regarding how to secure direct access to each of the three energy networks (OT, PACS, and IT)
- aspects of the build that are specific to the laboratory setting in which the build is implemented

5.9.2 Security Characteristics Evaluation Assumptions and Limitations

This security characteristic evaluation has the following limitations:

- The evaluation examines the security claims made by the example solution; however, it is not a comprehensive test of all security components.
- The evaluation cannot identify all weaknesses. Its purpose is to verify that the example solution meets its security claims, and to understand the trade-offs involved in doing so.

- This is not a red team exercise. The intent was to verify the security claims, not to break hardware or software involved in the example solution.
- The lab routers and firewalls were not included in the evaluation. It is assumed that they are hardened. Testing these devices would reveal only weaknesses in implementation that would not be of value to those adopting this example solution.

5.9.3 Example Solution Analysis

Table 5-3 lists the example-solution components, their functions, and the security characteristics that they provide. This analysis focuses on these security capabilities, rather than on the vendor-specific components. In theory, any number of commercially available components can provide these security capabilities. Some of these components are in Build #1 of the IdAM example solution, and other components are in Build #2. We discuss these components as generic components that provide a specific security functionality, rather than as vendor products. One vendor product could be substituted for another vendor product that provides the same security functionality, without affecting the results of the evaluation.

Table 5-3 IdAM Components and Security Capability Mapping

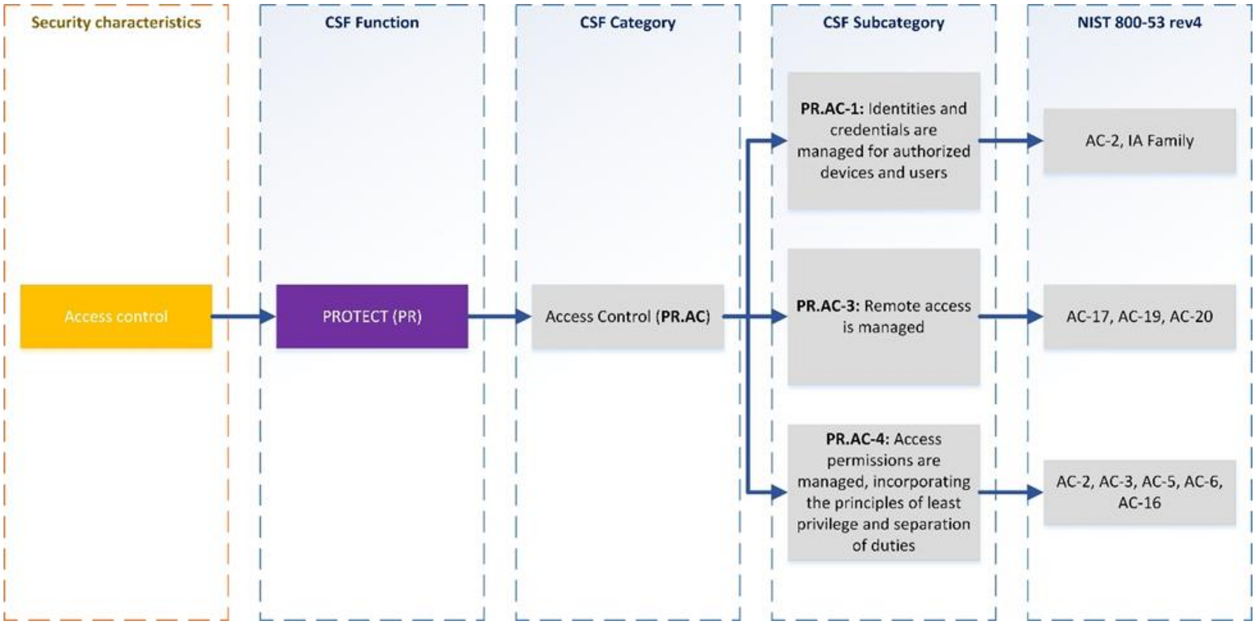
Component	Specific Product	Function	Security Characteristic
Identity, authorization, and workflow manager	RSA IMG or CA Identity Manager	IdAM workflow engine; manages identities, credentials, and authorization for all other network components in the use case; enforces workflows to ensure that access-control policies are enforced	Authentication and authorization
Identity store	RSA Adaptive Directory (identity store), which is used with RSA IMG, or Windows SQL 2012, which is used with CA Identity Manager	Database of user identities	Authentication and authorization

Component	Specific Product	Function	Security Characteristic
High-assurance attribute service	MAG Ozone system	Access control solution with ABAC architecture; provides increased assurance by signing attributes with private key infrastructure (PKI) and requiring users to authenticate with PKI	
Translator between the AD and the PACS and OT access management systems	AlertEnterprise Guardian	Translates from RSA/CA IdAM stores on the IdAM network to OT and PACS access management systems, enabling access management devices in the OT and PACS networks to be provisioned from the IdAM network	Authorization and access control
Directory service	Microsoft AD (for IT devices) or RS2 PACS server (for PACS devices)	Database of PACS or IT resource and user identifiers, and their associated security policies	Authentication and authorization
SCADA router and the remote manager of the SCADA router	Radiflow	IP-addressable industrial control system gateway that enables remote control of physical devices: management workstation enables remote management of physical SCADA router; SCADA router serves as firewall, terminal server, and IP-to-serial connectivity	Access control
Network access-control and policy-enforcement system	Cisco ISE	Allows access policies for network endpoints to be controlled centrally	Network security
Standalone smart-card provisioning and access system	XTec	Smart-card-based physical access control	Authentication, authorization, and access control

5.9.4 Security Characteristics Addressed

One aspect of our security evaluation involved assessing how well the IdAM example solution addresses the security characteristics that it was intended to support. These security characteristics are listed in a security control map published in the appendix of the IdAM use-case description [10]. Six security characteristics are listed in the security control map, each of which is further classified by the Cybersecurity Framework (CSF) categories and subcategories to which they map. The CSF subcategories further map to specific sections of each standard or best practice that are cited in the CSF in reference to that subcategory. Figure 5-21 depicts an example of the process for determining the security standards-based attributes for the example solution.

Figure 5-21 Example Process for Determining the Security Standards-Based Attributes for the Example Solution


Security characteristics
CSF Function
CSF Category
CSF Subcategory
NIST 800-53 rev4
Access control
PROTECT (PR)
Access Control (PR.AC)
PR.AC-1: Identities and credentials are managed for authorized devices and users
PR.AC-3: Remote access is managed
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
AC-2, IA Family
AC-17, AC-19, AC-20
AC-2, AC-3, AC-5, AC-6, AC-16

We used the CSF subcategories to provide structure to the security assessment by consulting the specific sections of each standard or best practice that are cited in reference to that subcategory. The cited sections provide example-solution validation points by listing specific traits that a solution that supports the desired security characteristics should exhibit. Using the CSF subcategories as a basis for organizing our analysis, and consulting the specific sections of the security standards that are cited with respect to each subcategory, allowed us to systematically consider how well the example solution supports the security characteristics identified in the use-case description.

The remainder of this subsection discusses how the example solution addresses the six desired security characteristics that are listed in the use-case description appendix [10]:

- authentication for OT
- access control for OT
- authorization (provisioning) for OT
- centrally monitor the use of accounts
- protect the exchange of identity and access information
- provision, modify, or revoke access throughout all federated entities

The remainder of this subsection also discusses how the authentication, access control, and authorization (provisioning) security characteristics are addressed for PACS, not just for OT.

5.9.4.1 Authentication, Access Control, and Authorization for OT

The implementation includes the capabilities that support these security characteristics. Section 5.6.7.1 describes the information flows for supporting authentication, access control, and authorization (provisioning) on the OT network.

5.9.4.2 Centrally Monitor Use of Accounts

The example solution supports converged accountability and tracking of user accounts, with the IdAM identity, authorization, and workflow manager acting as the locus of this capability.

On the OT network, the console access manager, which acts as the gatekeeper to all ICS/SCADA devices, monitors and logs all ICS/SCADA access requests and responses, as well as all user interactions with the ICS/SCADA OT devices. These logs should be centrally monitored along with other ICS/SCADA OT monitoring within the enterprise.

The network access-control component also logs all access requests and responses received at, and generated by, the IT network switch that controls access to the OT network from the IT network. These logs should be centrally monitored along with other ICS/SCADA OT monitoring within the enterprise.

On the PACS network, the PACS devices also report/log user access requests and responses to the PACS server. These logs should be centrally monitored along with other ICS/SCADA OT monitoring within the enterprise. In addition, the IdAM identity, authorization, and workflow manager and the translator component log the PACS access change (add, delete, or change) requests.

While these technical security controls provide capabilities to capture the information needed for accountability, they are only effective when combined with necessary procedural and managerial security controls. Implementation of these controls is outside the scope of this guide.

5.9.4.3 Protect Exchange of Identity and Access Information

All IdAM-related information exchanges between IdAM components (as shown by the red lines in Figure 5-17 through Figure 5-20) should be performed in protected mode. In other words, at the least, integrity checking mechanisms are performed on this communication so that tampering can be detected. Preferably, these communications are encrypted. In particular, the following information exchanges should be performed in protected mode:

- all information exchanges to/from the directory services in the IT, OT, and PACS networks
- all information exchanges between the console access manager (e.g., the ConsoleWorks component shown in Figure 5-17) and the OT directory service
- all information exchanges between the PACS server and the PACS translator component (e.g., the AlertEnterprise component shown in Figure 5-18 and Figure 5-19)

Because of time constraints, the laboratory builds of the example solution did not include encryption or integrity assurance for every IdAM information exchange. Nevertheless, such protection is strongly recommended when deploying the example solution.

5.9.4.4 Provision, Modify, or Revoke Access

User authorizations for the use of all IT, OT, and PACS network account assets, for ICS/SCADA devices and for physical access to rooms, facilities, etc., are provisioned, modified, and revoked by modifying user authorization information in the central IdAM identity, authorization, and workflow manager (CA Identity Manager or RSA IMG). These components, in turn, propagate the changes to all entities that are used to make local authorization and access determinations. Such information propagation ensures that all attempts to access IT, OT, and PACS network assets, SCADA devices, and rooms and facilities are uniformly handled because they are subject to the same updated access and authorization information when the silo directory, console manager, PACS server, or other IdAM device is consulted in response to the access attempt.

5.9.5 Assessment of Reference Architecture

The IdAM example solution is not intended to encompass all aspects of electricity subsector organization operations. It was designed to centralize the management of authorization and access in three disparate IdAM silos. Thus, our assessment considers the solution itself, not the broader problem of providing general security to all aspects of electricity subsector organization operations.

The example solution includes three network silos (OT, PACS, and IT), plus an IdAM network with numerous components that provide centralization, uniformity, and efficiency through the use of IdAM workflows. All threats and vulnerabilities that are present on the IT, OT, and PACS networks are also present in the example solution, so they will need to be addressed during solution deployment. This evaluation assumes that the OT, PACS, and IT networks are already protected by using physical-access-control and network-security components, such as firewalls and intrusion detection devices that are configured according to best practices.

5.9.5.1 Threats, Vulnerabilities, and Assumptions

This evaluation concerns the IdAM network itself, its components, and their interaction with IdAM components on the IT, OT, and PACS networks, which provide the benefits afforded by the example solution and introduce new attack surfaces and potential threats. For example, each of the IT, OT, and PACS networks has directory service components that must be secured. If the information in these directories is not safeguarded against tampering, the organization is at risk. These directories must be safeguarded in both the existing three-silo architecture and the example solution. The example solution, however, includes additional, related directory components that must also be protected, as described in Section 5.6.

The identity, authorization, and workflow manager and the identity store on the IdAM network must be protected from unauthorized access, and their information must be safeguarded. All of the data in the directory service components in the OT, PACS, and IT networks is accessible by the identity, authorization, and workflow manager and the identity store. The ability to propagate data from the IdAM network to the OT, PACS, and IT networks is the main strength, and the greatest vulnerability, of the example solution. If the IdAM identity store, or the identity, authorization, and workflow manager that has access to it, were compromised, this would equate to a compromise of each of the directory services in the IT, OT, and PACS networks. As a result, controlling access to the IdAM network and to each IdAM component, and securing communications among IdAM components, is essential to securing the example solution. Therefore, the analysis of the security of the IdAM network, its components, and the communications among IdAM components is central to the evaluation of the IdAM example solution.

5.9.5.1.1 Controlling Access to the Identity, Authorization, and Workflow Manager

The identity, authorization, and workflow manager on the IdAM network contains information regarding actual users and accounts for the OT, PACS, and IT networks. It manages the identities and credentials for the rest of the use case, but it does not manage them for itself. In other words, the identity, authorization, and workflow manager component itself does not control user access to the identity, authorization, and workflow manager. It has a separate set of user accounts and passwords that are specific to this component and that IdAM administrators use to log into it. This access must be strictly controlled so that only authorized IdAM administrators can log into the identity, authorization, and workflow manager. Users or authorized systems (such as an HR system or a work order management system) must log into the identity, authorization, and workflow manager to provision all electricity subsector systems (i.e., add identity information and authorization rules for new users, delete information for former users, and modify information as user authorizations change). The risks associated with access to the IdAM workflow are described in Section 4.3.2.

There is no AD running on the IdAM network. In the builds, access to the identity, authorization, and workflow manager and to all other components of the IdAM network is granted by the use of a username and credential, presented via either a web interface or each machine's OS console. An organization deploying the example solution operationally would, of course, be free to implement alternative access-control mechanisms. While both privileged and unprivileged users may access the identity, authorization, and workflow manager and other IdAM components, only highly privileged users should be permitted to create, delete, or modify accounts. Monitoring, logging, and auditing all activity that is performed directly on IdAM components, such as the identity, authorization, and workflow manager or the identity store, is essential to ensure that authorized users are not performing unauthorized activities.

5.9.5.1.2 Logging Activity on IdAM Components

Logging all activity that is performed on IdAM components is crucial for securing the example solution. Ideally, access to all components on the IdAM network should be logged for the purpose of auditing and accountability. The example solution is designed to allow the logging of all user activity on IdAM systems (e.g., identity, access, and authorization changes). The example solution should also log all activity that is performed by administrators so that no activity is exempt from monitoring, logging, and auditing. This section provides a closer look at the following three different types of IdAM system users (in terms of the amount of privilege that they have) and whether or not their activity should be logged:

- unprivileged users
- administrators
- super-administrators

Unprivileged users, by definition, are not authorized to interact with any IdAM system. They cannot create an account on the identity, authorization, and workflow manager, or modify the privileges of a user who already has an account. A user who works for HR, for example, who needs to add a user identity or modify a user's authorizations, would have an account on the identity, authorization, and workflow manager (that was set up by a privileged user) that allows him/her to add to or modify the information in the identity, authorization, and workflow manager component via a web interface. Such a user would never be able to access the identity, authorization, and workflow manager via its machine's OS console. Console access would enable the user to manage the OS on which the component is running. All that the unprivileged user needs is the ability to use his/her own, unprivileged, user-level account on the identity, authorization, and workflow manager's machine. Because the example solution is designed to monitor and log all activity that occurs over a web interface, it will log all unprivileged user activity.

Administrators, by definition, can access OS consoles and create user accounts on IdAM machines, such as the identity, authorization, and workflow manager. However, they are not authorized to change the access-control policies within the console access manager. As a result, when administrators access the consoles of an IdAM system OS, they must do so via the console access manager. The console access manager will log and monitor all administrator activity at any OS console.

Super-administrators, by definition, can not only access machine consoles and create user accounts on IdAM machine OSs, but they can change the access-control policies within the console access manager. Therefore, the example solution cannot force them to use the console access manager when accessing the consoles of IdAM system machine OSs. If super-administrators do access the consoles of IdAM system machine OSs, and do so not via the console manager, then their activity will not be logged or monitored. So, while super-administrators should be strongly encouraged by policy to use the console access manager, IdAM does not provide a technical mechanism to ensure that they will use the console access manager.

Access to the identity store on the IdAM network also must be strictly controlled, and the identity store should be configured so that it will only perform addition, modification, and deletion requests that are received from the identity, authorization, and workflow manager. If the identity store were to accept updates or edits from another entity, the result could be catastrophic. Any updates made by an administrator would have to be made via the machine console, so, at least, these updates would be logged. Updates made by a super-administrator could escape detection if the super-administrator were to defy organization policy and access the identity store console without going through the console access manager. We acknowledge insider threats, but feel that mitigating the risk of insider threats presently relies more on organizational policy decisions than on technology. Therefore, addressing insider threat is outside the scope of this project.

5.9.5.1.3 Unauthorized Modification of Access and Authorization Information

User identity and credential information is added into the identity, authorization, and workflow manager, and then propagated to other IdAM components. If this information were deleted, modified, or falsified while in transit between components or while stored in a component, the result could be catastrophic. It is essential to protect access to each IdAM component so that adversaries cannot modify IdAM information stored in the components, and so that IdAM information has, at least, its integrity and, ideally, its confidentiality protected when in transit between IdAM components.

5.9.5.2 Mitigations: Essentials for Securing the IdAM Example Solution

Based on the information flows for supporting OT authentication, OT access control, and OT authorization described in Section 5.6.7, securing the part of the IdAM example solution that supports OT access control requires the following actions:

- securing access to the following components:
  - identity, authorization, and workflow manager; identity store; and network access-control components on the IdAM network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)

    - directory service and console access manager components on the OT network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)
    - IT network access-control switch that serves as a gateway to the OT network from the IT network
- protecting the integrity of the information exchanges between the following components:
    - identity manager and the identity stores
    - identity store and the directory service on the OT network
    - directory service and the console access manager components on the OT network, as well as the network access-control and policy-enforcement system within the IT network
    - network access-control and component identity stores
    - network access-control component on the IT network and the IT network access-control switch that serves as a gateway to the OT network

Based on the information flows for supporting PACS authentication, PACS access control, and PACS authorization described in Section 5.6.7, securing the part of the IdAM example solution that supports PACS access control requires the following actions:

- securing access to the following components:
    - identity, authorization, and workflow manager; identity store; and IdAM translator components on the IdAM network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)
    - IdAM identity store and PACS directory service components on the PACS network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)
- protecting the integrity of the information exchanges between the components:
    - identity manager and identity stores
    - identity store on the IdAM network and the PACS directory service on the PACS network
    - IdAM translator component on the IdAM network and the IdAM directory service on the PACS network
    - IdAM translator component on the IdAM network and the PACS management server on the PACS network

5.9.5.3 Trade-offs

As mentioned earlier, the very characteristics that are the main objectives of the example solution, namely centralization and uniformity of the management of authorization and access, are also its main vulnerabilities. A successful attack on the IdAM network or its components could result in a compromise of one or all of the OT, PACS, and IT networks. Organizations that implement the example solution may incur additional costs to secure the IdAM network and its components.

5.9.5.3.1 Benefits

The benefits of the IdAM example solution include consolidated management of identity and access audit data; documented and repeatable business and security access decision processes (workflows); approval/denial data logging; rapid provisioning and de-provisioning using consistent, efficient, and automated processes; and better situational awareness through the ability to track and audit all access requests and other IdAM activity across all four networks (IT, OT, PACS, and IdAM). Other important benefits include greatly reduced time to implement access-control changes, and highly automated identity synchronization across silos. For example, an OT, PACS, and/or IT access change request can be implemented within minutes. These benefits directly reduce the cost of the regulatory audit requirements imposed on the energy industry. They also enable IdAM processes to be handled efficiently, and with more granular, prompt, and cost-effective control.

5.9.6 Security Recommendations

While the example solution provides a converged IdAM security solution, the solution itself provides a single attack vector that, if compromised, could have devastating consequences. Therefore, an organization that implements the example solution must take great care to secure the IdAM example solution itself. When deploying their own implementations, organizations should adhere to the following security recommendations:

- Conduct their own evaluations of their example-solution implementation.
- Deploy all components on securely configured OSs that use multifactor authentication and are configured according to best practices, based on Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) [15] and example secure configuration guidelines found in the Center for Internet Security (CIS) Security Benchmarks [16].
- Ensure that all OSs on which example-solution implementation components are running are hardened, maintained, and kept up-to-date in terms of patching, version control, and virus and malware detection.
- Put into place a security infrastructure that will protect the example solution itself, and will secure the communications among the components on the IdAM network and between these components and the IdAM components on the other three networks, as described in Section 5.9.5.2. Many of the remaining recommendations relate to providing such a security infrastructure.

- Design the authorization and workflow policies that are enforced by the identity, authorization, and workflow manager component, to enforce the principles of least privilege and separation of duties.
- Design the authorization and access-control policies that govern user access to the IdAM components themselves, to enforce the principles of least privilege and separation of duties.
- Segregate IdAM components onto their own network, either physically or by using private VLANs and port-based authentication, or similar mechanisms (e.g., in IEEE 802.1X, a standard for port-based network access control [17] that provides an authentication mechanism to devices that are to be attached to a local area network).
- Deploy a security infrastructure to secure the IdAM network and the IdAM platforms themselves. This infrastructure must consist of a holistic set of components that work together to prevent the IdAM network, components, and workflow from being used as an attack vector.
- Protect the IdAM network by using security components, such as firewalls and intrusion detection devices that are configured according to best practices (e.g., in NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy [18]).
- Protect each of the OT, PACS, and IT networks by using security components, such as firewalls and intrusion detection devices that are configured according to best practices.
- Strictly control physical access to the OT, PACS, IT, and IdAM networks.
- Configure firewalls to limit connections between the IdAM network and the production (IT, OT, and PACS) networks, except for the connections needed to support required internetwork communications to specific IP address and port combinations in certain directions.
- Perform, in protected mode, all IdAM-related information exchanges between IdAM components (as shown by the red lines in Figure 5-17 through Figure 5-20)—meaning that, at the least, integrity-checking mechanisms are performed on this communication so that tampering can be detected. Preferably, these communications should be encrypted. In particular, the following information exchanges should be performed in protected mode:
    - all information exchanges to/from the directory services in each of the OT, PACS, and IT networks
    - all information exchanges between the console access manager (i.e., the ConsoleWorks component in Figure 5-17) and the OT directory service
    - all information exchanges between the network access-control manager (i.e., the Cisco ISE component in Figure 5-17) and the switch in the IT network that controls access to the OT network
    - all information exchanges between the PACS server and the PACS translator component (e.g., the AlertEnterprise component in Figure 5-18 and Figure 5-19)

In the case of IdAM exchanges with the silo directories, protected mode is defined as the use of Start Transport Layer Security (TLS) [19], rather than LDAPS, which uses Secure Socket Layer and has been deprecated in favor of Start TLS.

- Install, configure, and use each component of the example solution (e.g., the identity, authorization, and workflow manager or the PAC server) according to the security guidance provided by the component vendor.
- Configure all IdAM components on the IdAM network so that it is impossible to remotely access them.
- Log all IdAM activity (e.g., direct access to IdAM components on the IdAM network, all messages exchanged between IdAM components). Limit the number of users who are able to control whether or not a performed activity is logged.
- Require super-administrators (i.e., users who are authorized to change the access-control policies within the console access manager) to use a console access manager when accessing the console of all devices on the IdAM network, and never to directly access any console. Use of a console access manger ensures that all activity that is performed via the console is logged.
- Configure the console access manager to have an always-on connection to all devices on the IdAM network so that it can monitor each device’s console port. This configuration ensures that all activity that is performed over the console port will be logged. Configure the console access manager to generate an alert if the always-on connection to any device is disconnected. This configuration ensures that security auditors can be aware of any times during which the console port of a device may have been accessed without the activity being logged or monitored.
- Configure all devices on the IdAM network so that they have only one console port (the port to which the console access manager has an always-on connection). Alternatively, where applicable, configure the devices on the IdAM network to allow only one console connection or login at a time. This will ensure that the console access manager will log all activity that is performed via the console of any of these devices.

5.9.7 Security Characteristics Evaluation Summary

Overall, the example solution and the workflow processes that it enforces succeed in centralizing IdAM functions across the OT, PACS, and IT networks, to provide an efficient, uniform, and secure solution for authenticating and authorizing access across all systems and facilities. The solution enables access-control policies across all three networks to be enforced consistently, quickly, and with a high degree of granularity, so that users are granted only enough privilege necessary to complete their work, and for only the necessary amount of time. It also enables a converged, simplified audit capability for accountability and tracking. This requires all access to the IdAM network, its components, and the information exchanged between these components and the OT, PACS, and IT networks, to be secured and monitored.

Organizations adopting this example solution must also have policies, procedures, and processes in place that effectively use the solutions capabilities to maximize benefits. Further, the organizations must consider and address the security risks associated with their deployment. Section 5.9.6 describes basic security considerations for the example solution.

6 Functional Evaluation

We conducted a functional evaluation of the IdAM example solution to verify that several common key provisioning functions of the example solution, as implemented in our laboratory build, worked as expected. The IdAM workflow capability demonstrated the ability to perform the following actions centrally:

- assign and provision access privileges to users, based on a set of programmed business rules in the OT, PACS, and IT networks and systems
- create, activate, and deactivate users in the OT, PACS, and IT networks and systems
- change an existing user’s access to the various networks and systems

Section 6.1 explains the functional test plan in more detail, and lists the procedures used for each of the functional tests.

6.1 IdAM Functional Test Plan

This test plan includes the test cases necessary to conduct the functional evaluation of the IdAM use case. The IdAM implementation is currently deployed in a lab at the NCCoE. Section 5 describes the test environment.

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 6-1 provides a template of a test case, including a description of each field in the test case.

Table 6-1 Test-Case Fields

Test-Case Field	Description
Parent requirement	Identifies the top-level requirement, or the series of top-level requirements, leading to the testable requirement
Testable requirement	Drives the definition of the remainder of the test-case fields, and specifies the capability to be evaluated.
Associated security controls	The NIST SP 800-53 Revision 4 controls addressed by the test case
Description	Describes the objective of the test case

Test-Case Field	Description
Associated test cases	In some instances, a test case may be based on the outcome of another/other test case(s). For example, analysis-based test cases produce a result that is verifiable through various means, such as log entries, reports, and alerts.
Preconditions	Indicates the starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content
Procedures	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure
Expected results	The specific expected results for each variation in the test procedure
Actual results	The actual observed results, in comparison with the documented expected results
Overall result	The overall result of the test as pass/fail. In some test case instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.

6.2 IdAM Use-Case Requirements

This section identifies the example-solution IdAM functional-evaluation requirements that are addressed using this test plan. Table 6-2 lists those requirements and the associated test cases.

Table 6-2 IdAM Functional Requirements

Capability Requirement (CR) Identification Number	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 1	The IdAM system shall include an IdAM workflow capability that assigns and provisions access privileges to users, based on a set of programmed business rules in the following networks:			
CR 1.a		IT		
CR 1.a.1			Allow access	IdAM-1
CR 1.a.2			Deny access	IdAM-1

Capability Requirement (CR) Identification Number	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 1.b		OT		
CR 1.b.1			Allow access	IdAM-1
CR 1.b.2			Deny access	IdAM-1
CR 1.c		PACS		
CR 1.c.1			Allow access	IdAM-1
CR 1.c.2			Deny access	IdAM-1
CR 2	The IdAM system shall include an IdAM workflow capability that can create and activate new users in the following networks and systems:			
CR 2.a		IT		IdAM-2
CR 2.b		OT		IdAM-2
CR 2.c		PACS		IdAM-2
CR 3	The IdAM system shall include an IdAM workflow capability that can de-activate users in the following networks and systems:			
CR 3.a		IT		IdAM-2
CR 3.b		OT		IdAM-2
CR 3.c		PACS		IdAM-2
CR 4	The IdAM system shall include a workflow capability that can change an existing user access to the various networks and systems.			
CR 4.a		IT		
CR 4.a.1			Allow to deny	IdAM-3
CR 4.a.2			Deny to allow	IdAM-3
CR 4.b		OT		

Capability Requirement (CR) Identification Number	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 4.b.1			Allow to deny	IdAM-3
CR 4.b.2			Deny to allow	IdAM-3
CR 4.c		PACS		
CR 4.c.1			Allow to deny	IdAM-3
CR 4.c.2			Deny to allow	IdAM-3

6.3 Test Case IdAM-1

Table 6-3 lists the functional requirements for the IdAM-1 test case.

Table 6-3 Test Case IdAM-1

Parent requirement	(CR 1) The IdAM system shall include an IdAM workflow capability that assigns and provisions access privileges to users, based on a set of programmed business rules in the following networks and systems: (CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS
Testable requirement	(CR 1.a.1-2) IT, (CR 1.b.1-2) OT, (CR 1.c.1-2) PACS
Description	Show that the IdAM solution can assign and provision access in the OT and IT networks and in the PACS network and system, including allowing and denying access.
Associated test cases	Not applicable
Associated security controls	AC-2, AC-3, IA-2, PE-2, PE-3
Preconditions	▪ HR representative CSV file is available. ▪ IdAM example solution is implemented and operational in the lab environment. ▪ Standard and privileged user sets are known to the testers. ▪ A PACS with a card reader and a simulated door access demonstration system is operational in the lab. ▪ A simulated OT network with an SEL RTU and an RTU emulator (Raspberry Pi) is implemented in the lab.

Procedures	1. Activate the IdAM workflow engine, and run a command to ingest the HR CSV file. 2. At a workstation on the IT network, attempt to log in as a user known to have access in the IT network. 3. At a workstation on the IT network, attempt to log in as a user known to be denied in the IT network. 4. At a workstation on the OT network, attempt to log in as a user known to have access in the OT network. 5. At a workstation on the IT network, attempt to access the SEL RTU administrative interface as a user known to have access to the SEL RTU. 6. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user known to have access to the RTU emulator. 7. At a workstation on the IT network, attempt to access the SEL RTU administrative interface as a user known to be denied access to the SEL RTU. 8. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user known to be denied access to the RTU emulator. 9. At a workstation on the OT network, attempt to log in as a user known to be denied access in the OT network. 10. At the demonstration PACS card reader, attempt an “access” with a card for a user known to have access allowed. 11. At the demonstration PACS card reader, attempt an “access” with a card for a user known to have access denied.

Expected results (pass)	Network access allowed: - Users with allowed access are able to log into a workstation on the IT network. - Users with allowed access are able to log into a workstation on the OT network and on the SEL RTU and RTU emulator. - Users with allowed access are able to log into a workstation on the PACS network. - Users with allowed access are authorized and allowed access by the PACS card reader and door access demonstration system. Network access denied: - Users who are denied access to the IT network are unable to log into a workstation on the IT network. - Users who are denied access to the OT network are unable to log into a workstation on the OT network or on the SEL RTU and RTU emulator. - Users who are denied access to the PACS network are unable to log into a workstation on the PACS network. - Users who are denied access are not authorized and are not allowed access by the PACS card reader and door access demonstration system.
Actual results	This test functioned appropriately and provided the expected results. Users that were denied access were unable to log into the OT and IT networks, and were denied access to the PACS network. Users who were granted access to each system were able to access the OT and IT networks and were granted access via PACS.
Overall result	Pass

6.4 Test Case IdAM-2

Table 6-6-4 lists the functional requirements for the IdAM-2 test case.

Table 6-6-4 Test Case IdAM-2

Parent requirement	(CR 2) The IdAM system shall include an IdAM workflow capability that can create and activate new users in the following networks and systems: (CR 2.a) IT, (CR 2.b) OT, (CR 2.c) PACS (CR 3) The IdAM system shall include an IdAM workflow capability that can de-activate users in the following networks and systems: (CR 3.a) IT, (CR 3.b) OT, (CR 3.c) PACS
Testable requirement	(CR 2.a) IT, (CR 2.b) OT, (CR 2.c) PACS (CR 3.a) IT, (CR 3.b) OT, (CR 3.c) PACS
Description	Show that the IdAM solution can create new users, assign access based on business rules, and provision those users to the appropriate network and system access-control systems. New users are users without entries in the authoritative identity store.
Associated test cases	CR 1
Associated security controls	AC-2, AC-3, AC-5, AC-16, AU-12, IA-2, IA-4, IA-5, IA-6, PE-2, PE-3, PE-6
Preconditions	New HR CSV file created with new users included

Procedures	1. Demonstrate that the new users in the HR CSV file do not have access in the OT, PACS, or IT networks or systems using Test Case IdAM-1. 2. Perform Step 1 of CR 1, with the new HR CSV file. 3. At a workstation on the IT network, attempt to log in as a new user known to have access in the IT network. 4. At a workstation on the OT network, attempt to log in as a new user known to have access in the OT network. 5. At a workstation on the IT network, attempt to access the SEL RTU administrative interface as a new user known to have access to the SEL RTU. 6. At a workstation on the IT network, attempt to access the Radiflow router administrative interface as a new user known to have access to the Radiflow router administrative interface. 7. At a workstation on the PACS network and system, attempt to log in as a new user known to have access in the PACS network and demonstration system. 8. At a PACS card reader, attempt an “access” with a card for a new user known to have access allowed. 9. Using the IdAM system, deactivate access for one or more users with access to the OT, PACS, and IT networks and systems. If one user has access to all three networks, deactivating that user is sufficient. 10. At a workstation on the IT network, attempt to log in as a recently deactivated user known to *previously* have access in the IT network. 11. At a workstation on the OT network, attempt to log in as a recently deactivated user known to *previously* have access in the OT network. 12. At a workstation on the IT network, attempt to access the SEL RTU administrative interface as a user known to *previously* have access to the SEL RTU. 13. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user known to *previously* have access to the RTU emulator.

Expected results (pass)	(CR 2) Create and activate a new user. New users are created, and access to the three networks and systems is confirmed. (CR 2.a) IT (CR 2.b) OT network, SEL RTU and RTU emulator (CR 2.c) PACS network and demonstration card reader access system (CR 3) Deactivate a user. User is deactivated, and access is denied to the network(s) and systems to which the user previously had allowed access. (CR 3.a) IT (CR 3.b) OT network, SEL TRU, and RTU emulator (CR 3.c) PACS network and demonstration card reader access system
Actual results	This test was conducted with the expected results received. A CSV file with users was successfully uploaded. Upon approval of the user access stated in the file, the user accounts successfully logged into OT, PACS, and IT. User access was deactivated, and the deactivation was approved. The users were no longer able to access the OT, PACS, or IT.
Overall result	Pass

6.5 Test Case IdAM-3

Table 6-5 lists the functional requirements for the IdAM-3 test case.

Table 6-5 Test Case IdAM-3

Parent requirement	(CR 4) The IdAM system shall include a workflow capability that can change an existing user's access to the following networks and systems. (CR 4.a) IT, (CR 4.b) OT, (CR 4.c) PACS
Testable requirement	(CR 4.a.1, CR 4.b.1, CR 4.c.1) Allow to deny (CR 4.a.2, CR 4.b.2, CR 4.c.2) Deny to allow
Description	Show that the IdAM solution can change user access for any network or system.
Associated test cases	CR 2
Associated security controls	AC-2, AC-3, AC-5, AC-6, AC-16, AU-12, CM-7, IA-2, IA-4, IA-5, IA-6, PE-2, PE-3, PE-6
Preconditions	Reuse the IdAM system in its

Procedure	1. Choose a set of users with known access, and a set of users without access, for each of the OT, PACS, and IT networks and systems. 2. Use the IdAM workflow to deny access for the set of users with known access who were chosen in Step 1 above. 3. Use the IdAM workflow to allow access for the set of users without access who were chosen in Step 1 above. 4. At a workstation on the IT network, attempt to log in as a user whose access had been changed from allowed to denied. 5. At a workstation on the IT network, attempt to log in as a user whose access had been changed from denied to allowed. 6. At a workstation on the OT network, attempt to log in as a user whose access had been changed from allowed to denied. 7. At a workstation on the OT network, attempt to log in as a user whose access had been changed from denied to allowed. 8. At a workstation on the PACS network, attempt to log in as a user whose access had been changed from allowed to denied. 9. At a workstation on the PACS network, attempt to log in as a user whose access had been changed from denied to allowed. 10. At a PACS card reader, attempt an “access” with a card for a user whose access had been changed from allowed to denied (card access denied in the demonstration system). 11. At a PACS card reader, attempt an “access” with a card for a user whose access had been changed from denied to allowed (card access allowed in the demonstration system). 12. At a workstation on the IT network, attempt to access the Radiflow router administrative interface as a user whose access had been changed from allowed to denied. 13. At a workstation on the IT network, attempt to access the Radiflow router administrative interface as a user whose access had been changed from denied to allowed. 14. At a workstation on the OT network, attempt to access the SEL RTU administrative interface as a user whose access had been changed from allowed to denied. 15. At a workstation on the OT network, attempt to access the SEL RTU administrative interface as a user whose access had been changed from denied to allowed. 16. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user whose access had been changed from allowed to denied.

	17. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user whose access had been changed from denied to allowed.
Expected results (pass)	(CR 4.) Change user access. (CR 4.a) IT (CR 4.a.1) Allow-to-deny changes are successfully provisioned. (CR 4.a.2) Deny-to-allow changes are successfully provisioned. (CR 4.b) OT (CR 4.b.1) Allow-to-deny changes are successfully provisioned. (CR 4.b.2) Deny-to-allow changes are successfully provisioned. (CR 4.c) PACS (CR 4.c.1) Allow-to-deny changes are successfully provisioned. (CR 4.c.2) Deny-to-allow changes are successfully provisioned.
Actual results	The test provided the expected results, with the impact of changes to user access (allow to deny, deny to allow) and privilege levels (privileged to non-privileged, non-privileged to privileged) verified.
Overall result	Pass

Appendix A Mount Airey Group, Inc. Personal Profile Applications Demonstration Application

The Personal Profile Application (PPA) was developed by Mount Airey Group (MAG) to demonstrate the functionality of the MAG Ozone® suite of products.

Ozone implements atomic authorization for the protection of critical resources by cryptographically binding credentials to specific authorizations, access rights, and/or explicit privileges. Ozone provides a privacy protecting mechanism that allows these authorizations to be distributed across the enterprise—as close to the protected resource as necessary—without concern for tampering, data mining, or compromise. Ozone is meant to protect an organization's most-sensitive or highest-risk resources. If an application relies on private key infrastructure (PKI)–based smart cards and/or biometrics for authentication, then that system should implement the congruent security (as is provided by Ozone) for the authorization of users for access to that resource.

In support of the National Cybersecurity Center of Excellence (NCCoE) Electricity Subsector Identity and Access Management (IdAM) Use Case, the PPA was configured to incorporate digital certificates that were generated by GlobalSign, Inc., to be compliant with the North American Energy Standards Board (NAESB) certificate profile. Each certificate was provisioned within Ozone to have specific authorizations related to the PPA demonstration.

This application has three main information groups for which actions can be authorized: Personal Information, Credit Reports, and Criminal History. Based on the authorizations associated with a credential, results pages are dynamically populated.

To bring up the demonstration application, the user must present a digital certificate to the application. Upon inspection of the authorizations provisioned within Ozone for the selected certificate, the application dynamically populates the table at the bottom of the first screen with the results of the authorization queries. If the certificate has been authorized for a specific action, then the results table will display "true" for that specific action. The information identifying the certificate that was selected is also displayed above the table.

At that point, the user may either enter a name in the search box on the right, or simply hit the search button to display the Search Results page of the application. The search will return a list of names, as well as links to additional information about the people listed. The links listed will vary depending upon the authorizations for which the user was authorized at logon to the PPA. The available authorizations are as follows:

- View Personal Information – view the personal information of the selected person
- Edit Personal Information – add or edit the personal information of people in the application
- View Criminal History – view the criminal history of the selected person

- Edit Criminal History – add or edit the criminal history of people in the application
- View Credit Report – view the credit report of the selected person
- Request a New Credit Report – request an updated credit report for the selected person

A sample of the table shown on the first page is provided below:

Authorizations for: C=US, O=Blue Corp, OU=People, CN=Criminal History Editor

Table 6-6 Sample Attributes

PPA Proof	Authorized
Edit Criminal History	true
Edit Personal Information	false
Request Credit Report	false
View Credit Report	false
View Criminal History	true
View Personal Information	false

A sample of the table on the Search Results page is provided below:

Search Results

Table 6-7 Search Results

Name	View CH	Add CH	View CR	Request CR
Hicks, Chick	View	Add	View	Request
McQueen, Lightning	View	Add	View	Request
Sullivan, James P	View	Add	View	Request
Waternoose, Henry J	View	Add	View	Request
Add a new entry...editPI.jsp				

For the NCCoE Electricity Subsector IdAM Use Case, the following authorizations have been configured for the NAESB certificates:

- Jim McCarthy

  Email Address = james.mccarthy@nist.gov, CN = James McCarthy, OU = GSUS, OU = NCCoE NIST Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

    - View Personal Information
    - Edit Personal Information
    - View Criminal History
    - Edit Criminal History
    - View Credit Report
    - Request Credit Report

- Donald Faatz

  Email Address = donald.faatz@nist.gov, CN = Donald Faatz, OU = GSUS, OU = NCCoE NIST Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

    - View Criminal History
    - Edit Criminal History

- Harry Perper

  Email Address = harry.perper@nist.gov, CN = Harry Perper, OU = GSUS, OU = NCCoE NIST Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

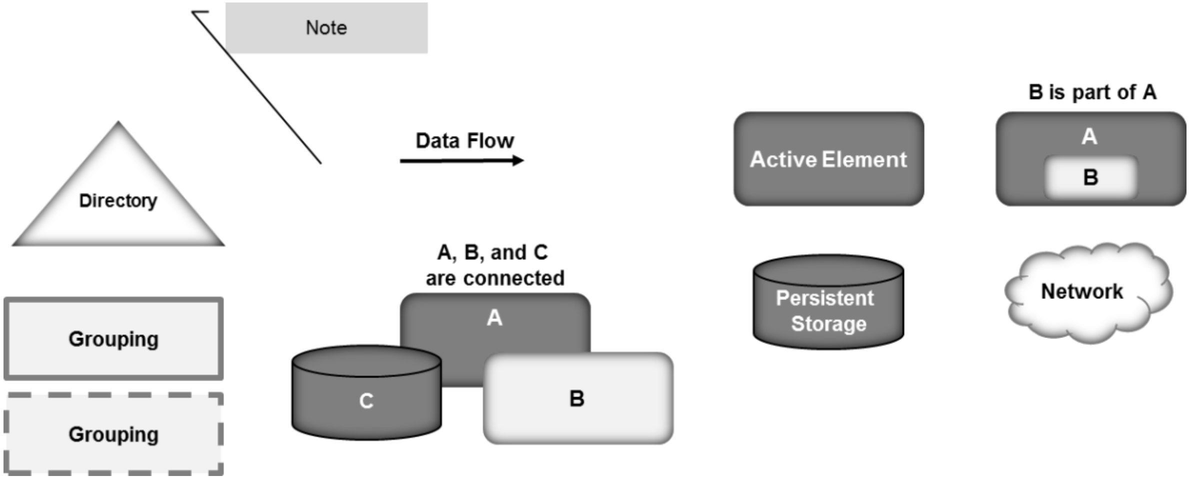
    - View Personal Information
    - Edit Personal Information
    - View Criminal History
    - View Credit Report

- John Wiltberger

  Email Address = jwiltberger@mitre.org, CN=Johnathan Wiltberger, OU = GSUS, OU = NCCoE NIST Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

    - View Personal Information
    - View Criminal History
    - View Credit Report
    - Request Credit Report

Appendix B Legend for Diagrams



Appendix C List of Acronyms

ABAC	Attribute-Based Access Control
AD	Active Directory
CA	CA Technologies
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CR	Capability Requirement
CRADA	Cooperative Research and Development Agreement
CSF	Cybersecurity Framework
CSV	Comma-Separated Value
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
EACMS	Electronic Access Control and Monitoring System
EMS	Energy Management System
HR	Human Resources
ICS	Industrial Control System
IdAM	Identity and Access Management
IDMS/CMS	Identity and Credential Management System
IMG	Identity Management and Governance
IP	Internet Protocol
ISE	Identity Services Engine
IT	Information Technology
LDAPS	Lightweight Directory Access Protocol Secure
MAG	Mount Airey Group
NAESB	North American Energy Standards Board

NAS	Network Attached Storage
NCCoE	National Cybersecurity Center of Excellence
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency/Internal Report
OASIS	Open Access Same-Time Information Systems
OS	Operating System
OT	Operational Technology
PACS	Physical Access Control System
PIV-I	Personal Identity Verification Interoperable
PKI	Private Key Infrastructure
PPA	Personal Profile Application
RMF	Risk Management Framework
RS2	RS2 Technologies
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SEL	Schweitzer Engineering Laboratories
SP	Special Publication
SQL	Structured Query Language
STIG	Security Technical Implementation Guideline
TLS	Transport Layer Security
UTC	Utilities Telecom Council
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Appendix D References

[1] *Cybersecurity Framework*, National Institute of Standards and Technology [Web Site], http://www.nist.gov/cyberframework/ [accessed 6/19/17].

[2] J. H. Saltzer, “Protection and the Control of Information Sharing in Multics,” *Communication of the ACM*, vol. 17, no. 7, pp. 388-402, July 1974.

[3] *Federated Identity Management (FIM)*, TechTarget [Web site], http://searchsecurity.techtarget.com/definition/federated-identity-management [accessed 6/19/17].

[4] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST Special Publication (SP) 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf [accessed 2/25/14].

[5] *Risk Management Framework: Quick Start Guides*, National Institute of Standards and Technology [Web site], http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/ [accessed 6/19/17].

[6] Joint Task Force Transformation Initiative, *Managing Information Security Risk*, NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf [accessed 2/25/14].

[7] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [accessed 2/25/14].

[8] W. E. Burr, D. F. Dodson, E. M. Newton, et al., *Electronic Authentication Guideline*, NIST Special Publication (SP) 800-63-2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf [accessed 2/25/14].

[9] V. C. Hu, D. Ferraiolo, and R. Kuhn, *Assessment of Access Control Systems*, NISTIR 7316, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2006. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf.

[10] *Identity and Access Management*, Use Case Version 2, National Institute of Standards and Technology, November 2013, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/es-idam-project-description-final.pdf [accessed 6/22/17].

[11] *NAESB Compliant Digital Certificate*s, GlobalSign [Web site], https://www.GlobalSign.com/en/digital-certificates-for-naesb/ [accessed 6/22/17].

[12] V. C. Hu, D. Ferraiolo, R. Kuhn, et al., *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication (SP) 800-162, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2014, http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf [accessed 6/19/17].

[13] *Attribute Based Access Control*, National Cybersecurity Center of Excellence [Web site], https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control [accessed 6/19/17].

[14] *Standards: NIST NCCoE*, AlertEnterprise [Web site], http://www.alertenterprise.com/resources-standards-nistcoe.php [accessed 6/22/17].

[15] *Operating Systems*, Information Assurance Support Environment (IASE) [Web site], https://iase.disa.mil/stigs/os/Pages/index.aspx [accessed 6/19/17].

[16] *CIS Benchmarks*, Center for Internet Security (CIS) [Web site], https://benchmarks.cisecurity.org/downloads/benchmarks/ [accessed 6/19/17].

[17] M. Seaman, Editor, *Port Based Network Access Control*, IEEE 802.1X, Draft 2.0, Institute of Electrical and Electronics Engineers, February 2008.

[18] K. Scarfone and P. Hoffman, *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication (SP) 800-41 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2009, https://www.nist.gov/publications/guidelines-firewalls-and-firewall-policy [accessed 6/19/17].

[19] J Hodges, R. Morgan, and M. Wahl, *Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2830, May 2000 https://tools.ietf.org/rfc/rfc2830.txt [accessed 6/19/17].