NIST CYBERSECURITY PRACTICE GUIDE ENERGY

IDENTITY AND ACCESS MANAGEMENT FOR ELECTRIC UTILITIES

Approach, Architecture, and Security Characteristics

For CIOs, CISOs, and Security Managers

Jim McCarthy Don Faatz Harry Perper

Chris Peloquin John Wiltberger

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-2b
DRAFT

NIST Special Publication 1800-2b

IDENTITY AND ACCESS MANAGEMENT FOR ELECTRIC UTILITIES

Energy

Draft

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

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, 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, materials, or equipment 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, 98 pages (August 2015)
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: Energy_NCCoE@nist.gov

Public comment period: *August 25, 2015 through October 23, 2015*

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
9600 Gudelsky Drive (Mail Stop 2002), Rockville, MD 20850
Email: Energy_NCCoE@nist.gov

National Cybersecurity Center of Excellence

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

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

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. The documents in this series 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, and industrial control systems. They must authenticate authorized individuals to the devices and facilities to which they 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 dialogue 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 centralized, standards-based technical approach that unifies identity and access management (IdAM) functions across operational technology (OT) networks, physical access control systems (PACS), and information technology systems (IT). These networks often operate independently, which can result in identity and access information disparity, increased costs, inefficiencies, and loss of capacity and service delivery capability. This guide describes our collaborative efforts with technology providers and electric company stakeholders to address the security challenges energy providers face in the core function of IdAM. It offers a technical approach to meeting the challenge, and also incorporates a business value mind-set 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 sophistication. It shows energy providers how we met the challenge 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 the guide. While the reference solution was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it 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; cyber security; electricity subsector; energy sector; identity and access management; information technology

Acknowledgments

The NCCoE wishes to acknowledge the special contributions of Nadya Bartol, Senior Cybersecurity Strategist, Utilities Telecom Council; Jonathan Margulies, formerly with NCCoE and now with Qmulos; and Victoria Pillitteri of NIST, who were instrumental in the initial definition and development of the Identity and Access Management use case. Paul Timmel, formerly detailed to NCCoE from the National Security Agency, helped with these stages and also helped to get the project build started.

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

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)
Ayal Vogel	Radiflow
Dario Lobozzo	Radiflow
Steve Schmalz	RSA
Tony Kroukamp (The SCE Group)	RSA
Kala Kinyon (The SCE Group)	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
Danny Vital	XTec
Mari Devitte	XTec
David Hellbock	XTec
John Schiefer	XTec

Table of Contents

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 using commercially available products.

The NCCoE's approach provides a centralized access management system that reduces risk of disruption of service by reducing opportunities for cyberattack 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. The guide helps organizations gain efficiencies in identity and access management, while saving them research and proof of concept costs.

1.1 The Challenge

The electric power industry is upgrading older, outdated infrastructure to take advantage of emerging technologies that will create "a platform [that] efficiently [integrates] new energy resources, new technologies, and new devices into the system."[1] The ever greater numbers of technologies, devices, and systems connected to utilities' grid networks need protection from physical and cybersecurity attacks.[2]

IdAM implementations in the electricity subsector are often decentralized and controlled by numerous departments within an energy company. Several negative outcomes can result from this: an increased risk of attack and service disruption, 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.

To better protect power generation, transmission, and distribution, energy companies need to be able to control physical and logical access to their networked resources, including buildings, equipment, information technology, and industrial control systems (ICS)—all of which have unique technical and political challenges.[3] Identity and access management (IdAM) systems for these assets often exist in silos, and employees who manage access to these systems lack methods to effectively coordinate access to devices and facilities in these silos. This drives inefficiency and creates security risks, according to our electric utility stakeholders.

We considered a scenario in which a utility technician has access to several physical substations and remote terminal units connected to the company's network in those substations. Personal

[1] Thought Leaders Speak Out: The Evolving Electric Power Industry, The Edison Foundation Institute, June 2015.
[2] State of the Electric Utility 2015, Utility Dive, January 2015.
[3] Protect Critical Infrastructure, McAfee, 2012.

matters require the technician to move out of the region, so she terminates her employment at the company. Without a centralized IdAM system, managing routine events like this one can become cumbersome and time-consuming. How can energy companies be confident that access to the appropriate physical and technological resources across the enterprise is granted or revoked correctly, and in a timely fashion?

As this scenario shows, energy companies need to be able to authenticate the individuals and systems to which they are giving access rights with a high degree of certainty. In addition, energy companies need to be able to enforce access control policies (e.g., allow, deny, inquire further) consistently, uniformly and quickly across resources.

1.2 The Solution

The example solution we propose demonstrates the following capabilities:

- centrally assigns and provisions access privileges to users based on a set of programmed business rules for IT, OT, and physical resources
- creates, activates, and deactivates users for IT, OT, and physical resources
- provides a view of all user accounts within the enterprise and the access rights they have been granted
- can change an existing user's access to one or more resources

We accomplished this solution through deployment of a single centralized IdAM platform that implements:

- an IdAM workflow to manage the overall process and to require explicit approval of requests to access certain resources
- 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

These combined capabilities can greatly reduce the time to update access to IT, OT, and physical resources. They reduce opportunities for attack or error and lower the impact of identity and access incidents on energy delivery, thereby lowering overall business risk. They also improve a company's security posture by integrating all the IdAM-related audit logs into one, greatly improving visibility into authentication and authorization activities. Another benefit of this example solution is that it supports use of multiple digital identities by a single person. A current employee is likely to have several distinct digital identities because of independent management of digital identities across IT, OT, and physical resources.

The guide:

- maps security characteristics to guidance and best practices from standards organizations, including the North American Electric Reliability Corporation's (NERC)

Critical Infrastructure Protection (CIP) standards and NIST SP 800-53, Rev.4, *" Security and Privacy Controls for Federal Information Systems and Organizations "*

- provides a
  - detailed example solution and capabilities that address security controls
  - demonstrated approach using multiple products to achieve the same result
  - how-to for implementers and security engineers with instructions on how the example solution can be integrated and configured into their enterprises in a manner that achieves security goals, with minimum impact on operational efficiency and expense

Commercial, standards-based products, like the ones we used, are readily available and interoperable with existing information technology infrastructure and investments. While our simulated environment may be most similar in breadth and diversity to the widely distributed networks of large organizations, this guide is modular and provides guidance on implementation of unified IdAM capabilities to organizations of all sizes. These include, but are not limited to, corporate and regional business offices, power generation plants, and substations.

This guide lists all the necessary components and provides installation, configuration, and integration information so that an energy company can replicate what we have built. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your utility's security experts should identify the standards-based products that will best integrate with your existing tools and IT system 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 Risks

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

Operationally, a lack of a centralized 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 introduction of additional threats to the environment, such as malware and denial of service (especially oriented towards 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 centralized 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 information technology, personnel, and data. This example solution addresses imminent operational security risks and incorporates strategic risk considerations, too.

Adopting any new technology can introduce new risks to your enterprise. We understand that this example solution to mitigate the risks of decentralized IdAM may, in turn, introduce new risks. By centralizing IdAM functions, we decrease the risk that multiple IdAM platforms can be infiltrated to gain unauthorized access to networked devices. We recognize, however, that centralizing IdAM functions may provide 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 Threats, Vulnerabilities and Assumptions, and provide a comprehensive list of mitigations in Section 5.9.6, Security Recommendations.

1.4 Benefits

The example solution described in this guide has the following benefits:

- products and capabilities can be adopted on a component-by-component basis, or as a whole
- minimizes impact to the enterprise and existing infrastructure
- reduces opportunities for attack or error, and impact of identity and access incidents on energy delivery, thereby lowering overall business risk
- allows rapid provisioning and de-provisioning of access from a centralized platform, so IT personnel can spend more time on other critical tasks
- improves situational awareness: proper access and authorization can be confirmed via the use of a single, centralized solution
- improves security posture by tracking and auditing access requests and other IdAM activity across all networks

1.5 Technology Partners

The technology vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products 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:

- AlertEnterprise
- CA Technologies
- Cisco Systems, Inc.
- GlobalSign
- Mount Airey Group
- RS2 Technologies
- RSA Security, LLC
- RADiFlow

- Schneider Electric
- TDi Technologies
- XTec, Inc.

1.6 Feedback

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

- email energy_nccoe@nist.gov
- participate in our forums at http://nccoe.nist.gov/forums/energy

Or learn more by arranging a demonstration of this example solution by contacting us at energy_nccoe@nist.gov.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and provides users with the information they need to replicate this approach to identity and access management. The example solution is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST 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 electricity subsector organizations face in implementing and using IdAM systems
- example solution built at the NCCoE
- benefits of adopting a secure, centralized IdAM system, and the risks of isolated, decentralized systems

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 SP1800-2b, which describes what we did and why. The following sections will be of particular interest:

- Section 4.3, Risk Assessment and Mitigation, provides a detailed description of two types of risk analysis we performed
- Table 1, Use Case Security Characteristics Mapped to Relevant Standards and Controls, in Section 4.3, Risk Assessment and Mitigation, maps the security characteristics of this example solution to cybersecurity standards and best practices, including NERC-CIP v.3 and v.5

IT professionals who want to implement an approach this like this will find the whole practice guide useful. You can use the How-To portion of the guide, NIST Special Publication Series 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 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 in energy industry organizations. While we have used a suite of commercial products to address

this challenge, this guide does not endorse these particular products.[4] Your organization's security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. 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 operational technology systems (OT), physical access control systems (PACS), and IT systems (IT). If you use other products, we hope you will seek those that are congruent with applicable standards and best practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to energy_nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/energy.

3 INTRODUCTION

The NCCoE initiated this project because IT security leaders in the electricity subsector 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 we consulted told us that they need to control physical and logical access to their resources, including buildings, equipment, IT, and industrial control systems. They need to authenticate only designated individuals and devices to which they 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. Current IdAM implementations are often not centralized and are controlled by numerous departments within an energy company. Several negative outcomes can result from this situation: an increased risk of attack and service disruption, 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. Another key consideration is the need for companies to demonstrate compliance with industry standards and/or government regulations.

We 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

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

functionality and capability. Sections 5.3.1 and 5.3.2 detail these two example solutions. 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.[5]

4 Approach

4.1 Audience

This guide is intended for individuals responsible for implementing IT 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 of 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.

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 partners on the basis of their ability to provide these characteristics. We initially thought it would be feasible to include federation of identity management[6] services in the scope. 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 centralized 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.

[5] J. Saltzer, Protection and the control of information sharing in multics, Communication of the ACM, 17 (7), 388-402 (1974)

[6] "Federated identity management (FIM) is an arrangement 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." http://searchsecurity.techtarget.com/definition/federated-identity-management

4.2.1 Assumptions

4.2.1.1 Security

All network and system changes have the potential to increase the attack surface within an enterprise. In Section 4.3, Risk Assessment and Mitigation, we provide detailed recommendations on how to secure this reference solution.

4.2.1.2 Modularity

This example solution is made of many commercially available parts. You might swap one of the products we used for one 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 you can implement based on your needs.

4.2.1.3 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.

4.2.1.4 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 the NCCoE could implement some type of identity federation mechanism to authenticate and authorize individuals both internal and external to the organization, this capability exceeded the scope of the build.

4.2.1.5 Technical Implementation

The 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.

4.2.1.6 Limited Scalability Testing

We experienced a major constraint in terms of replicating the user base size that would be found at medium and large energy providers. We do not identify scalability thresholds in our builds, as those depend on the type and size of the implementation and are particular to the individual enterprise.

4.2.1.7 Replication of Enterprise Network

We were able to replicate the three silos: 1) physical access control systems, 2) information technology or corporate networks, and 3) the operational technology network, in a limited

manner. The goal was to demonstrate both logically and physically that provisioning functions could be performed from a centralized 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.

4.3 Risk Assessment and Mitigation

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 risk to the components introduced by adoption of the solution.

4.3.1 Assessing Risk Posture

According to NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems,[7] "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 Risk Management Framework (RMF)[8] material available to the public.

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 centralized 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 these the tactical risks:

- 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 centralized or federated controls

[7] Guide for Conducting Risk Assessments, National Institute of Standards and Technology Special Publication 800-30, Rev. 1, September 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[8] National Institute of Standards and Technology (NIST), Risk Management Framework (RMF) http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/

- 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,[9] 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. Below is a summary of the strategic risks:

- impact on service delivery
- cost of implementation
- budget expenditure as they relate 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
- 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 NIST's SP 800-53 Rev.4[10] controls where applicable, along with other applicable industry and mainstream security standards.

4.3.2 Managing IdAM Risk

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.[11] 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

[9] Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology Special Publication 800-53, Rev. 4, April 2013, http://dx.doi.org/10.6028/NIST.SP.800-53r4

[10] Managing Information Security Risk, National Institute of Standards and Technology Special Publication 800-39, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[11] J. Saltzer, Protection and the control of information sharing in multics, Communication of the ACM, 17 (7), 388-402 (1974)

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 the confidentiality of its users.[12]

To protect the build components, we implemented the following requirements in our lab environment: access control, data security, and protective technology. Section 5.9, Evaluation of Security Characteristics, 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.

4.3.3 Security Characteristics and Controls Mapping

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 1 maps the desired security characteristics and example capabilities of the use case to the Framework for Improving Critical Infrastructure Cybersecurity, relevant NIST standards, industry standards, and controls and best practices.

[12] Section 5.9.5.1.1 describes the security controls in place to mitigate this risk.

367 *Table 1. Use Case Security Characteristics Mapped to Relevant Standards and Controls*

Example Characteristic		**Cybersecurity Standards and Best Practices**						**Specific Related and Best Practices**
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS CAG20**	**NERC CIP v3/5**[13]
Authentication for OT	Authentication mechanisms	Protect	Access Control	**PR.AC-1**: Identities and credentials are managed for authorized devices and users	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	CSC 3-3, CSC 12-1, CSC 12-10,CSC 16-12	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

[13] The relationship of NERC CIP requirements to the Security Characteristics is derived from a mapping between NIST 800-53 rev4 security controls and NERC CIP requirements. It is provided for reference only. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance.

Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS CAG20**	**NERC CIP v3/5[13]**
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	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	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,
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	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	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

Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS CAG20**	**NERC CIP v3/5[13]**
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	CSC 4-2,CSC 12-1, CSC 12-10, CSC 14-2, CSC 14-3,	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
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	CSC 16-16, CSC 17-7	CIP-011-5 R1

Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS CAG20**	**NERC CIP v3/5[13]**
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	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	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

4.4 Technologies

Table 2 provides information about the products and technologies that we implemented in order to satisfy the security control requirements.[14]

Table 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
				RSA	IMG[15] 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	Mechanisms for centrally managed provisioning of		Virtual Directory		Adaptive Directory	7.1.5 R29692	Authoritative source for digital identities and authorized access to resources.

[14] This table describes only the product capabilities 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.
[15] RSA IMG is now known as RSA VIA Governance and RSA VIA Lifecycle

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
federated entities	access		Credential Management	GlobalSign	Enterprise PKI	N/A	Provides NAESB-compliant X.509 certificates to OT personnel.
			Credential Management / Physical Access Control	XTec	Credential Issuance Solutions	N/A	Provides PIV-I smartcard credentials and physical access control capability using the smartcard.
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 smartcard credentials and physical access control capability using the smartcard.
			Physical Access Control Enforcement	RS2 Technologies	AccessIT!	4.1.15	Controls physical access to power facilities, buildings, etc.
Authorization (provisioning) OT	Access policy management mechanisms	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Provisioning	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the IdAM workflow to Access It Universal
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access						

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
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.
				RSA	IMG[16]	6.9.74968	
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access		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.
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	Console Works	4.9-0u0	Controls access to industrial control system (ICS) devices by people (ICS engineers and technicians).

[16] RSA IMG is now known as RSA VIA Governance and RSA VIA Lifecycle

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
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	Console Works	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.
			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

5 ARCHITECTURE

5.1 Example Solution Description

IdAM is the discipline of managing the relationship between a person and the resources 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 and held accountable for their use of 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 1.

Figure 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**[17] provides life-cycle management of credentials such as employee badges or digital certificates.
3. **Access rights management** determines the resources 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**[18] allows or denies a digital identity access to a resource.
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 used infrequently. For example, verifying identity typically involves physically reviewing documents such as a driver's license or passport. Credential issuance and management is

[17] NIST SP 800-63-2, Electronic Authentication Guideline, provides additional information on credential issuance and management, as well as authentication.
[18] NIST IR 7316, Assessment of Access Control Systems, explains commonly used access control policies, models, and mechanisms.

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 a person enters a facility using a badge, or logs into a computer system. A directory, such as Microsoft Active Directory (AD), is often used in the implementation of run-time functions.

Provisioning is the "glue" that 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, all of these IdAM capabilities are frequently replicated at least three times—once for a person's access to OT, again for access to PACS, and then to access IT. Additionally, these capabilities may be independently replicated for each system within OT or IT. This replication makes it difficult to ensure that employees have access to the resources they need to perform their jobs, and only those resources. Newly hired employees may not have access to all 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 centralizing some of the administrative capabilities into a core IdAM capability used across OT, PACS, and IT, while leaving the run-time capabilities replicated and distributed. Figure 2 illustrates the example solution.

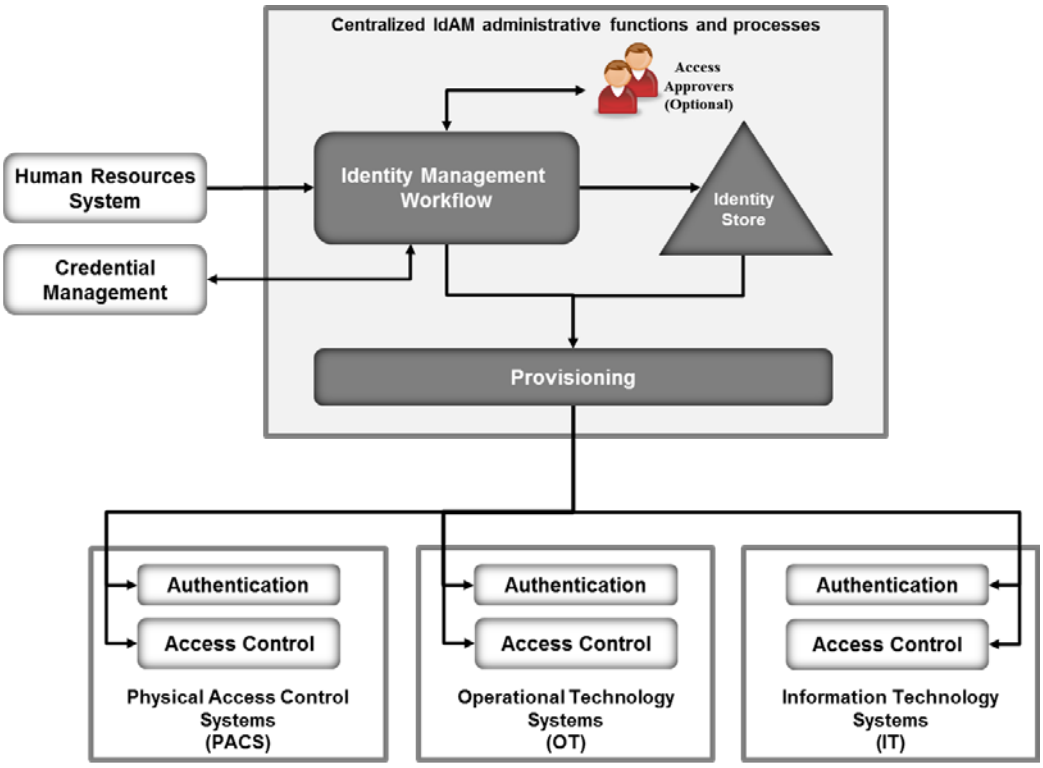


Figure 2. IdAM example solution

The centralized IdAM capability implements:

- 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 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 adoption of the example solution.

Instead, the identity store associates all of an employee's digital identifiers so all of that 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 either are needed by all employees or for an employee's job. The workflow stores information about credentials and authorized accesses in the identity store. The workflow can then invoke provisioning to populate run-time functions 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 waits for responses. When the workflow receives approvals, it stores the authorized accesses in the identity store and provisions them to the run-time functions. All information about approved, pending,[19] and provisioned physical and logical access authorizations is maintained in the identity store.

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 run-time functions. It directs that associated credentials be invalidated and destroyed. It removes information about those credentials from the identity

[19] Pending access authorizations may be either authorizations that have been approved but not yet provisioned or time-bounded authorizations to be provisioned/deprovisioned at a future time.

store and de-provisions credential information from the run-time functions.[20] It then identifies resource accesses needed for the employee's new job, authorizes them in the identity store, and provisions them to the run-time functions. The workflow identifies any new credentials that will be needed in the new job, triggers creation and issuance of those credentials, waits for them to be created, updates the identity store, and provisions new credential information to the run-time functions.

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

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 The Physical Access Control System Silo

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

Figure 3 shows the architecture of the PACS silo.

[20] Workflow actions are programmable and can be customized to meet organization-specific needs.

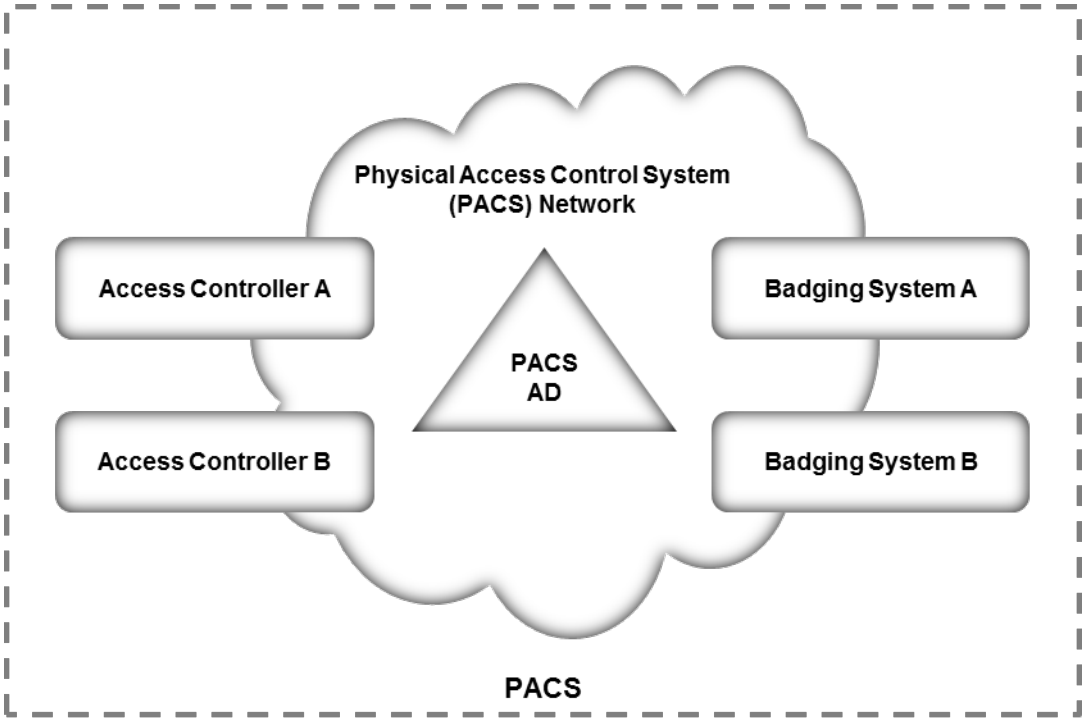


Figure 3. Notional PACS architecture

An instance of Microsoft Active Directory 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 Active Directory instance from the centralized IdAM system.

The PACS Active Directory instance may also store authorized physical access information used by the access control systems. If the access control systems are integrated with Active Directory, then the IdAM system will provision authorization information to PACS Active Directory. If the access control systems are not integrated with Active Directory, then authorization information will be provisioned directly to the access control system.[21]

5.1.2 The 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 electric energy to customers, and 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 4 shows the notional architecture of the OT silo.

[21] Build #1 provisions directly to the access control system. Build #2 provisions to the PACS AD.

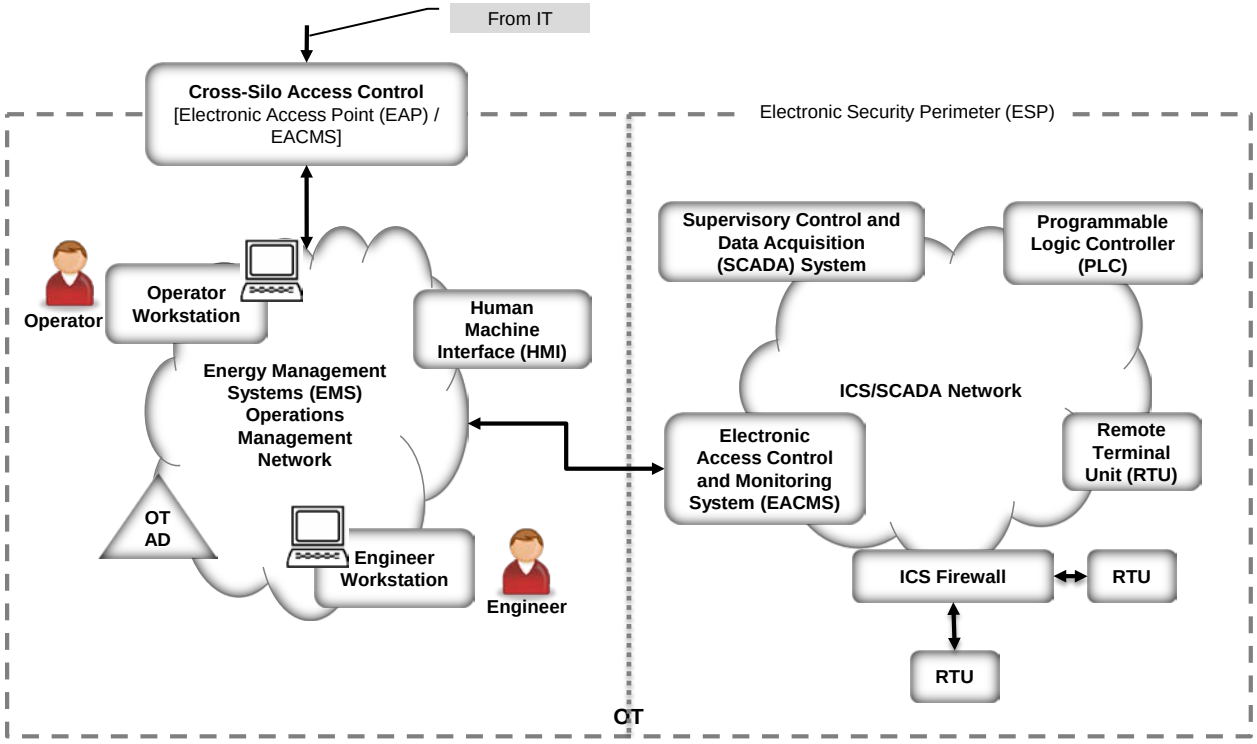


Figure 4. Notional OT silo architecture

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

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 terminal access to the programmable logic controllers (PLCs) 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 Active Directory instance or directly into the EACMS by the centralized IdAM system. The centralized 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 Active Directory instance.

An ICS/SCADA firewall controls communication among ICS/SCADA devices. The centralized IdAM system does not currently manage or provision authorizations that control device-to-device communication. 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 centralized IdAM system.

5.1.3 The 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 Active Directory instance 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 centralized IdAM system. Applications that are not integrated with Active Directory can be provisioned directly by the centralized IdAM system.

Figure 5 shows the notional architecture of the IT silo.

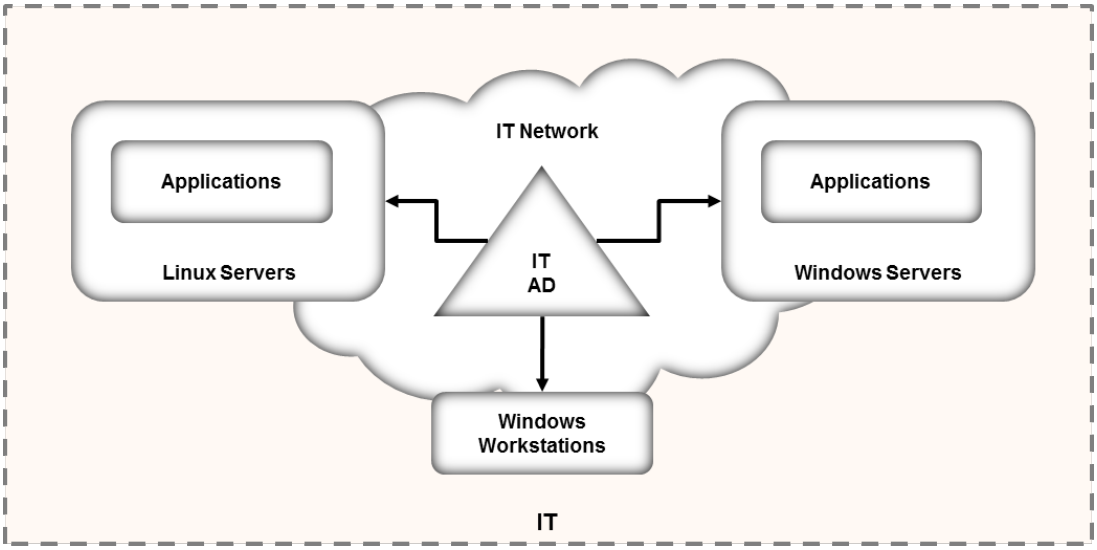


Figure 5. Notional IT silo architecture

5.2 Example Solution Relationship to Use Case

When we first defined this challenge[22] in collaboration with industry members, we wrote the following scenario:

"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

[22] http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Identity_Access_Management.pdf

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 centralized management of identities and authorizations, but assumes the decision to allow a particular technician 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 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 the technician a work order that requires access to a substation triggers actions within the IdAM workflow to authorize access to the substation and provision that authorization to the substation PACS. When the technician presents her physical access credential at the substation, the PACS uses the provisioned authorization to determine if she should be allowed 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 management of identities and authorizations but assumes that run-time functions such as authenticating a user and granting her 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 her mobile device. The EACMS authenticates the technician and controls her access to ICS/SCADA devices within the substation. Assigning the technician to this work order triggers an IdAM workflow that authorizes her 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 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 centralized IdAM capability. Both builds used the following products:

- AlertEnterprise Guardian implements provisioning to an RS2 Technologies (RS2) AccessIT! Physical Access Control System (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 Identity Management and Governance (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 6 illustrates Build #1.

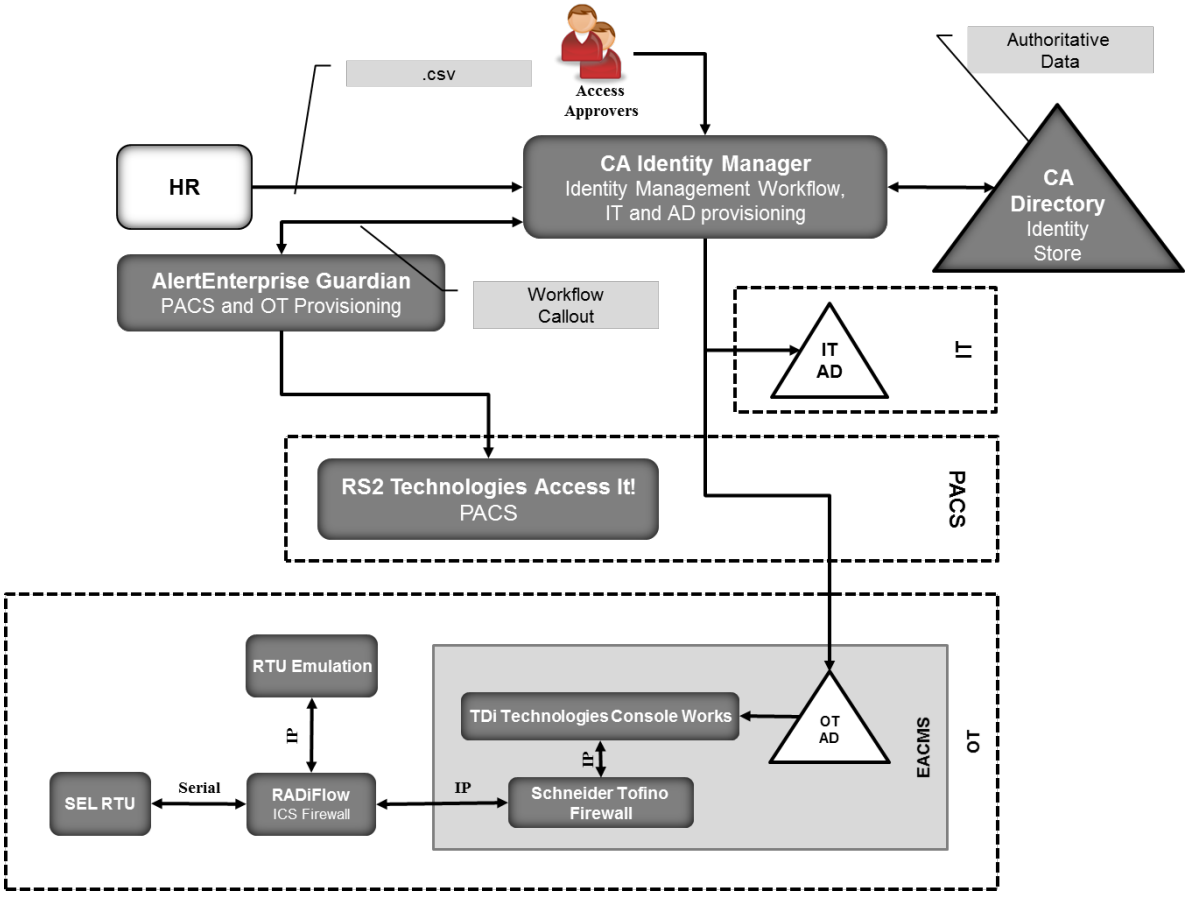


Figure 6. Build #1

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 using manually produced .csv files. Identity Manager also provisions information to Microsoft Active Directory

instances in business systems (IT), and the operational system (OT). No relationship among these Active Directory instances is assumed.

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

AlertEnterprise Guardian[23] provisions physical access authorizations into the RS2 PACS. 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 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 Active Directory instance. Identity Manager provisions ICS/SCADA access authorizations in the OT Active Directory instance. ConsoleWorks uses the access authorizations in OT Active Directory to control user access to ICS/SCADA devices. Console Works also captures an audit trail of all user access to the ICS/SCADA network.

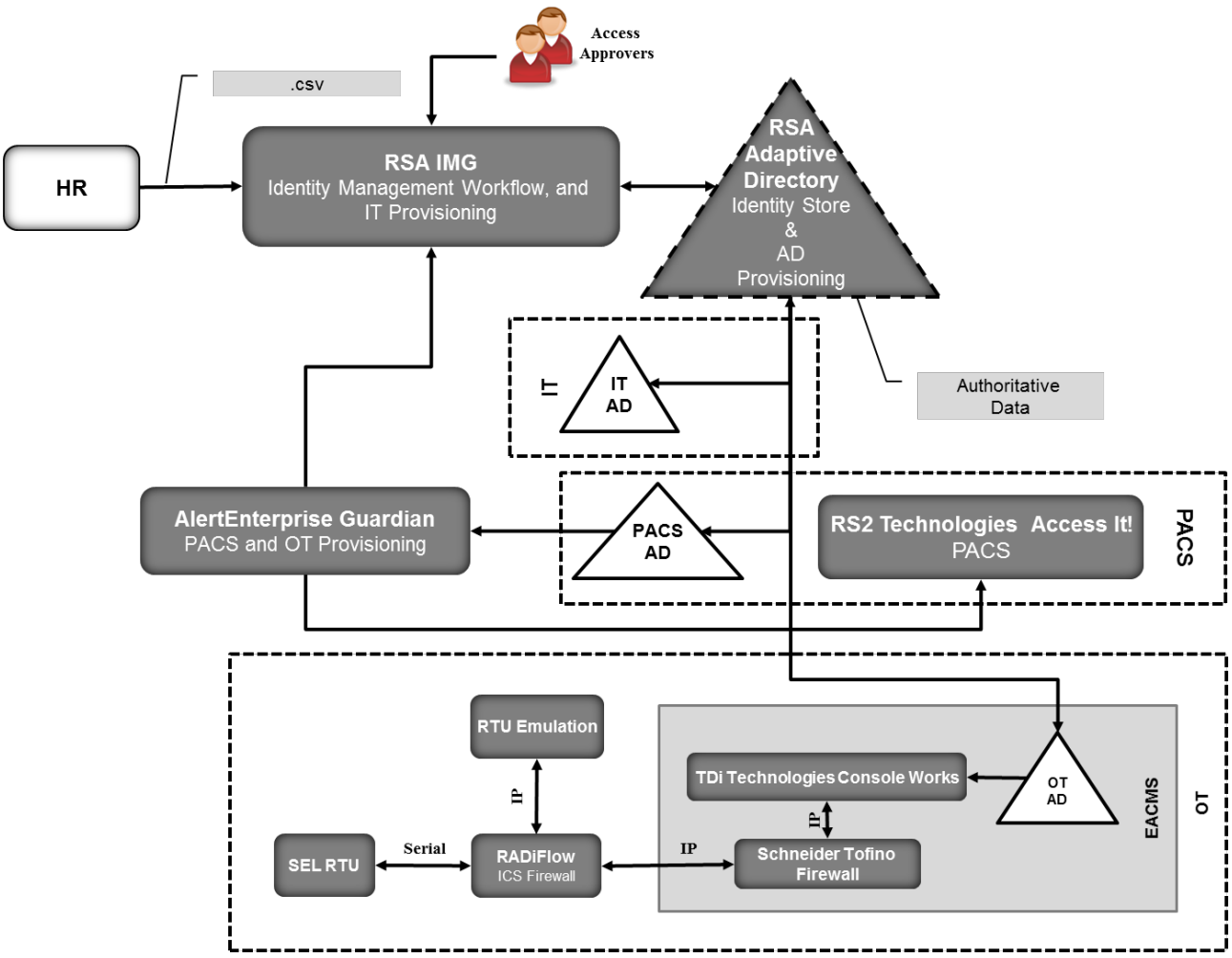
A Schneider Electric Tofino firewall is installed between Console \Works and the ICS/SCADA network. The firewall determines which IP addresses within the ICS/SCADA network are accessible through ConsoleWorks and which network protocols can be used when accessing those addresses. The combination of Console Works and the Tofino firewall implement an Electronic Access Control and Monitoring System (EACMS) between the Energy Management System / Operations Management Network and the ICS/SCADA network.

5.3.2 Build #2

Figure 7 illustrates Build #2.

[23] Guardian is also capable of implementing workflow and provisioning ICS devices. However, those capabilities were not used in this build.

637



638

639 *Figure 7. Build #2*

640 RSA IMG implements the IdAM workflow. It receives input from an HR system in the form of
641 .csv files. RSA IMG also has the capability to provision information to systems. In Build #2, RSA
642 IMG stores information in RSA Adaptive Directory, which subsequently provisions the
643 information to its associated Active Directory instances.

644 RSA Adaptive Directory implements the identity store and provisioning portions of the example
645 solution. RSA Adaptive Directory is a virtual directory that acts as a proxy in front of multiple
646 back-end directories. The build assumes that each silo—OT, PACS, and IT—hosts a Microsoft
647 Active Directory instance. No relationship among these Active Directory instances is assumed.
648 When an IMG workflow stores information in Adaptive Directory, that information is actually
649 stored in one or more of the underlying Active Directory instances. In this way, storing
650 information in Adaptive Directory provisions that information into one or more Active Directory
651 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 Active Directory instance. AlertEnterprise Guardian monitors the Active Directory PACS instance for updates such as changed physical access authorizations for an existing user, addition of a new user with physical access authorizations, or 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 is used in the OT silo to provide an EACMS between the EMS/Operations Management Network and the ICS/SCADA network. ConsoleWorks utilizes the OT Active Directory for 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 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 Active Directory instance. AlertEnterprise Guardian detects the authorization change for the technician and provisions it to RS2. When the technician arrives at the substation and scans her credentials at the door, RS2 allows her entry.

The workflow also authorizes access to ICS/SCADA devices in the substation. In Build #1, Identity Manger stores this authorization in the CA directory and provisions it to the OT Active Directory instance. In Build #2, IMG writes this authorization to Adaptive Directory, which stores it in the OT Active Directory instance. When the technician connects her mobile device to ConsoleWorks in the substation, she is authenticated, and ConsoleWorks checks the OT Active Directory instance, sees that she is authorized, and allows 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 Active Directory. ConsoleWorks detects the change in the OT Active Directory 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 Active Directory instances. AlertEnterprise Guardian detects the change in the PACS Active Directory instance and de-provisions the technician's substation physical access. ConsoleWorks detects the change in the OT Active Directory 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.[24]

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 show in Figure 8. These products implement IdAM capabilities that, while necessary to completely implement IdAM within an organization, are not an integral part of the centralized IdAM capability.

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

XTec AuthentX Identity and Credential Management System[25] provides a personal identity verification interoperable (PIV-I) smartcard credential based on NIST standards that can be used for logical and physical access. AuthentX demonstrates 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.

XTec demonstrates a cloud-based implementation of the XTec physical access control (PACS) product. 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 control credential revocation to all interoperable resources immediately.

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

[25] The description of the XTec product and its role supporting the implementation of the example solution was provided to NCCoE by XTec.

GlobalSign operates a North American Energy Standards Board (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.[26]

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

The MAG Ozone product provides a high-assurance attribute-based access control[27] (ABAC) implementation. 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, their values are managed through Ozone Console.

[26] https://www.GlobalSign.com/en/digital-certificates-for-naesb/
[27] NIST Special Publication 800-162, Guide to Attributed Based Access Control (ABAC) Definition and Considerations.

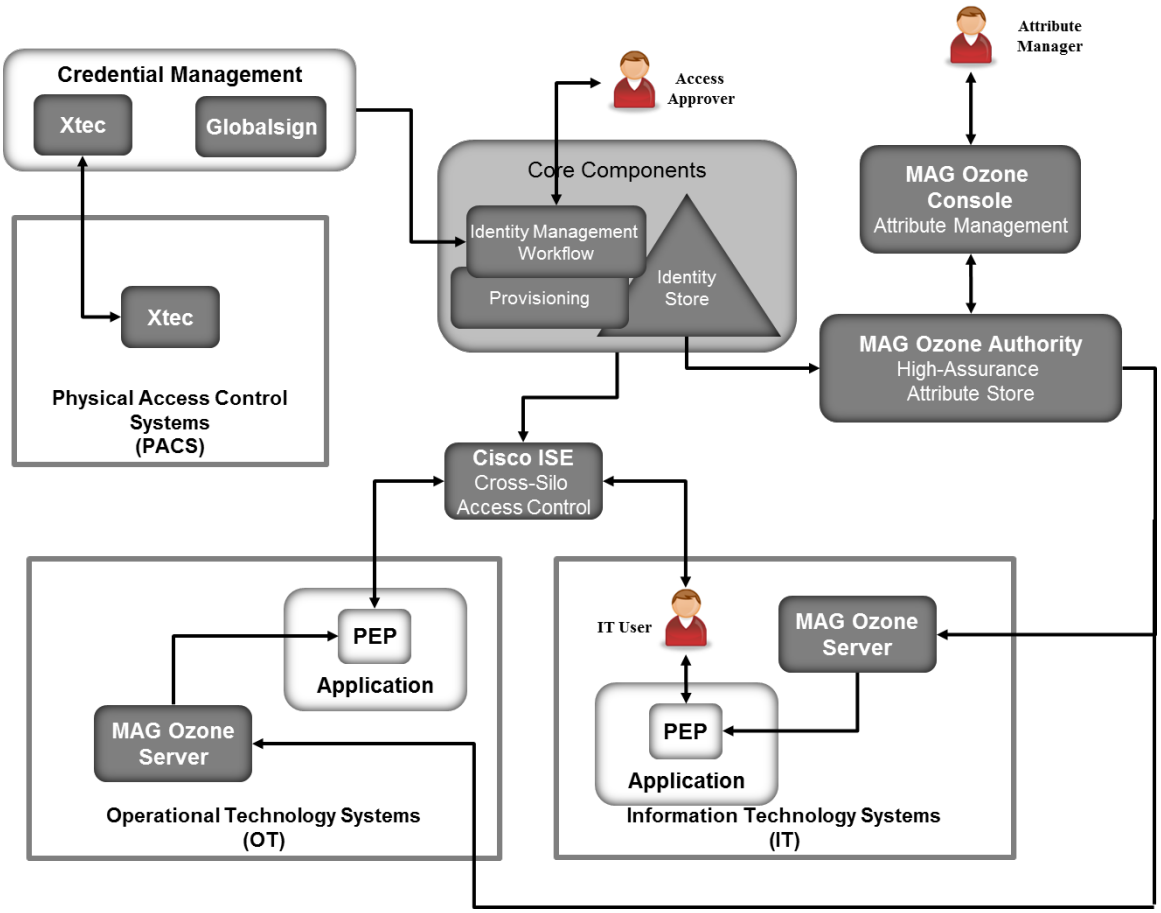


Figure 8. Supporting components

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. The application is described in Appendix C.[28]

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.

[28] 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. http://nccoe.nist.gov/content/attribute-based-access-control

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 Active Directory 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.

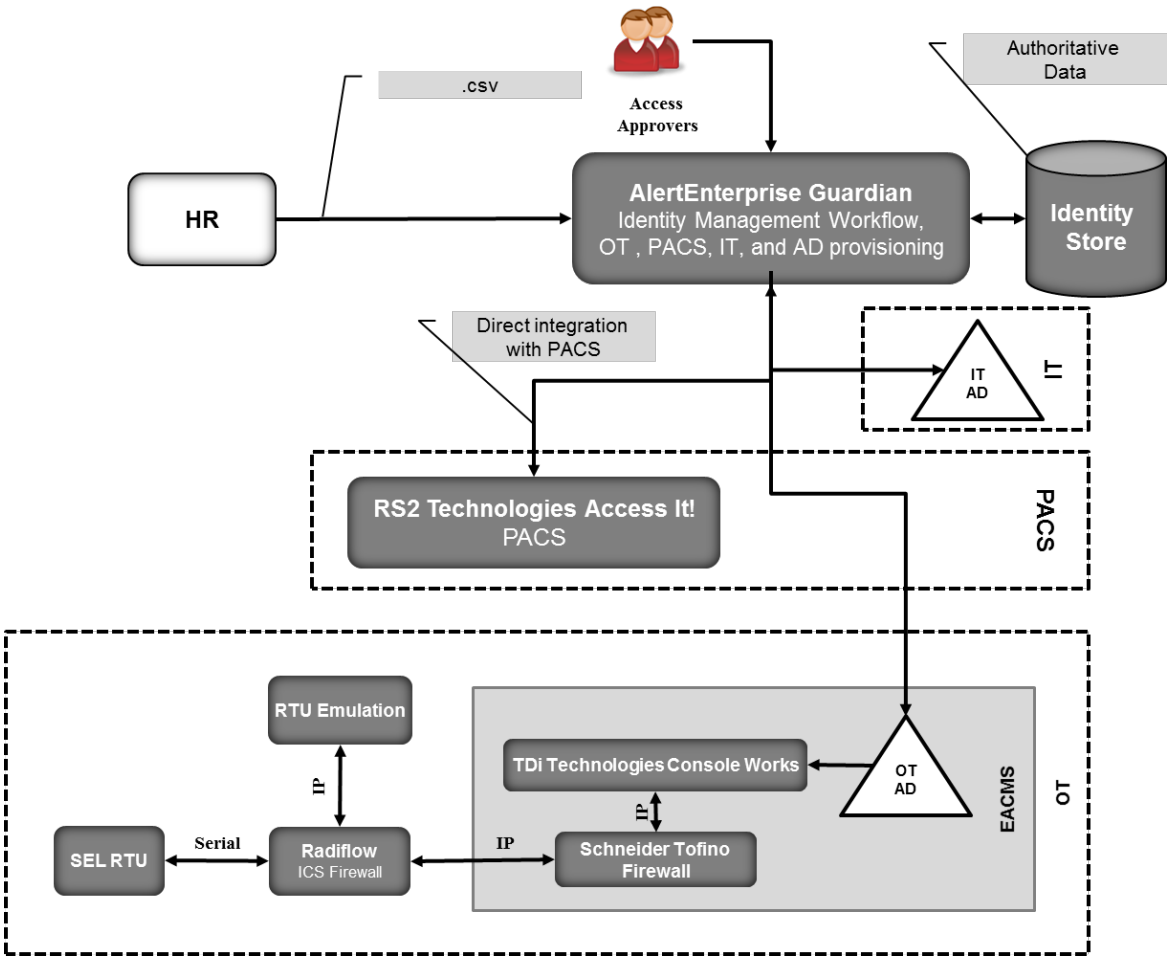


Figure 9. Build #3

AlertEnterprise Guardian 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 using manually produced .csv files. Guardian provisions information to Microsoft Active Directory instances in OT and IT. No relationship among these Active Directory instances is assumed.

IT applications are assumed to be integrated with Active Directory and use credential information and authorization information in the IT Active Directory instance. If there are IT

applications that are not integrated with Active Directory, 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 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 Active Directory instance. Guardian provisions ICS/SCADA access authorizations in the OT Active Directory instance. ConsoleWorks uses the access authorizations in OT Active Directory to control user access to ICS/SCADA devices.

Additional information about Build #3 is available from the AlertEnterprise Web site at http://www.alertenterprise.com/resources-standards-nistcoe.php .

5.6 Build Implementation Description

The infrastructure was built on Dell model PowerEdge R620 server hardware. The server operating system was VMware vSphere virtualization operating environment. In addition, we used a 6-terabyte Dell EqualLogic network attached storage (NAS) product, and 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 Technologies 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 3 lists the software and hardware components we used in the build, as well the specific function each component contributes.

795 *Table 3. Build Architecture Component List*

Product Vendor	Component Name	Function
Dell	PowerEdge R620	Physical server hardware
Dell	PowerConnect 7024	Physical network switch
Dell	EqualLogic	Network attached storage
VMware	vSphere vCenter Server version 5.5	Virtual server and workstation environment
Microsoft	Windows Server 2012 r2 Active Directory Server	Authentication and authority
Microsoft	Windows 7	Information management
Windows	Windows Server 2012 r2 DNS Server	Domain name system
Windows	SQL Server	Database
AlertEnterprise	Enterprise Guardian	Interface and translation between IdAM central store and the PACS management server
CA Technologies	Identity Manager Rel 12.6.05 Build 06109.28	Identity and access automation management application, IdAM provisioning
Cisco	ISE Network Server 3415	Network access controller
Cisco	Catalyst Model 3650	TrustSec-enabled physical network switch
GlobalSign	Digital Certificates	Cloud certificate authority
Mount Airey Group	Ozone Authority	Central attribute management system
Mount Airey Group	Ozone Console	Ozone administrative management console

Product Vendor	Component Name	Function
Mount Airey Group	Ozone Envoy	Enterprise identity store interface
Mount Airey Group	Ozone Server	Ozone centralized attribute based authorization server
RADiFlow	(iSIM) Industrial Service Management Tool	Supervisory control and data acquisition (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 Technologies	AccessIT! Universal Release 4.1.15 Physical access control components	Configures and monitors the PACS devices (e.g., card readers, keypads, etc.)
Schweitzer Electronics Laboratory	SEL-2411	Programmable automation controller
Schneider Electric	Tofino Firewall model number TCSEFEA23F3F20	Industrial Ethernet firewall
XTEC	XNode	Remote access control and management

796

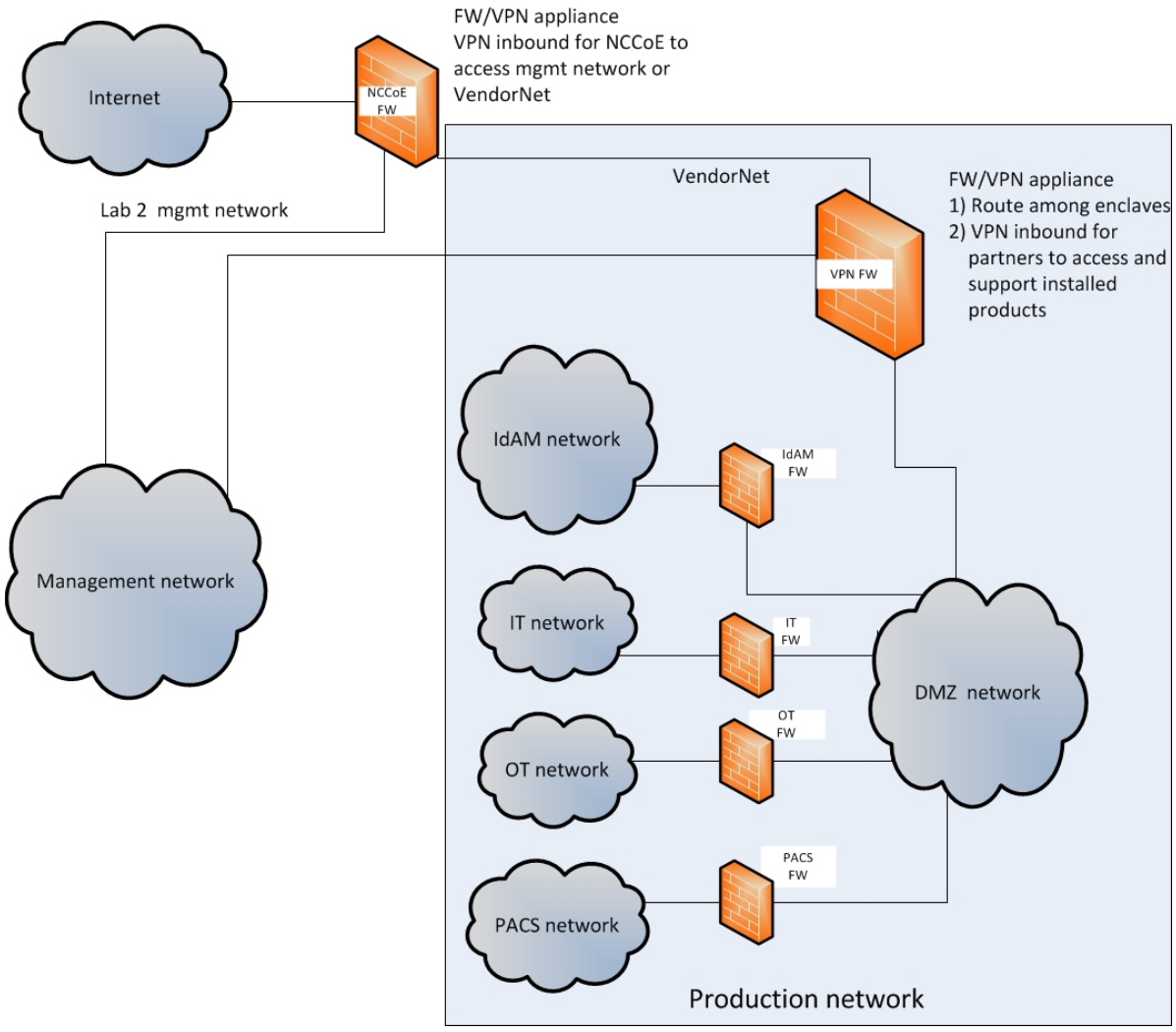
797 5.6.1 Build Architecture Components Overview

798 The build architecture consists of multiple networks that mirror the infrastructure of a typical
799 energy industry corporation. The networks are a management network and a production

network (Figure 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 11 consists of:

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

These networks were implemented separately to match a typical electricity subsector enterprise infrastructure. 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 OT, PACS, and IT networks.



815

816 *Figure 10. Management and production networks*

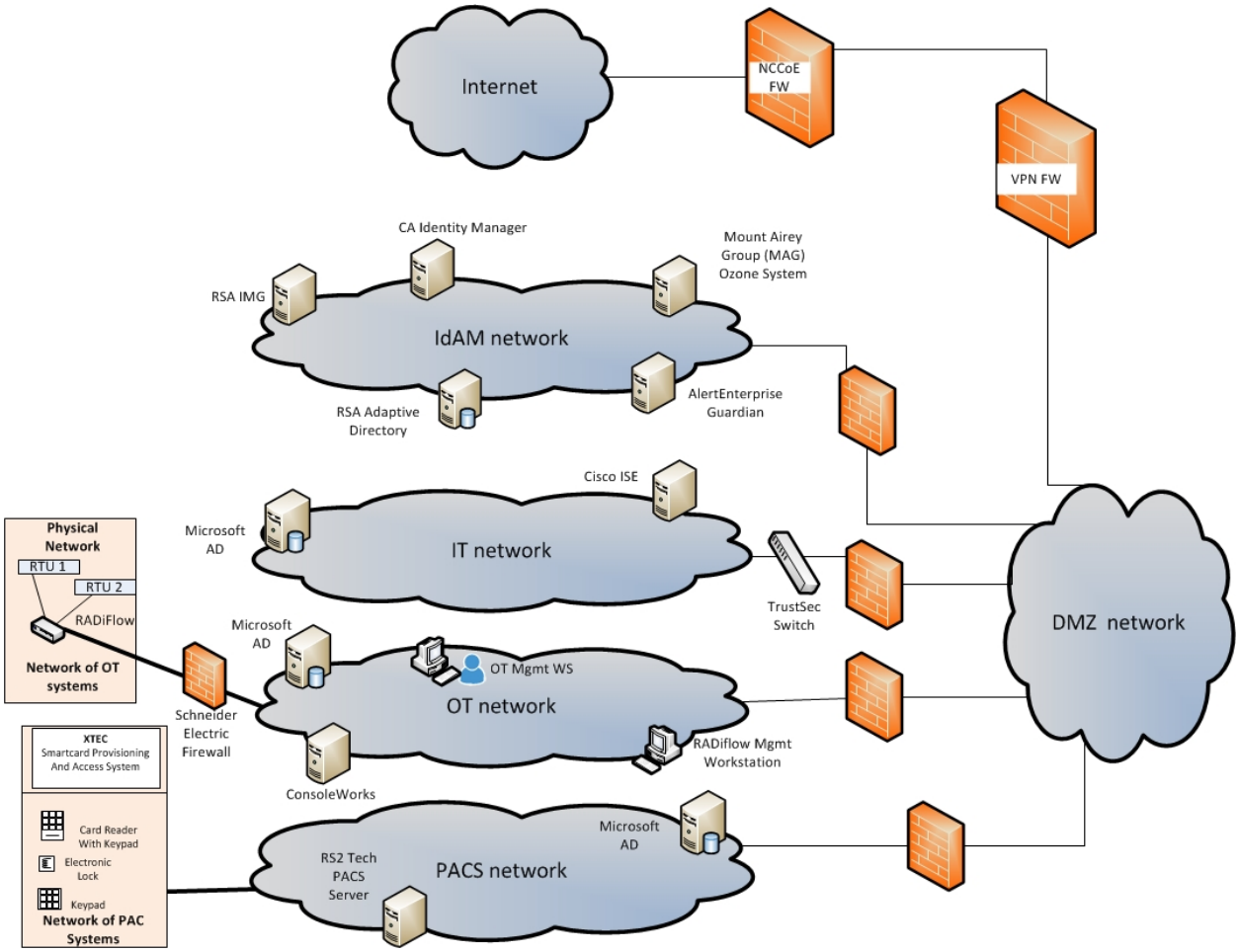


Figure 11. IdAM build architecture production network

The IdAM network represents the proposed centralized/converged IdAM network/system. This network was separated into OT, PACS, and IT to highlight the unique IdAM components 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 used to support the EMSs and ICS/SCADA systems. Typically, this network is either not connected to the enterprise IT network or is connected with a data diode (a one-way communication device from the OT network to the IT network). Two-way traffic is allowed per NERC-CIP and is enabled via the OT firewall only for specific ports and protocols between specific systems identified by IP address.

The PACS network represents the network that supports the physical access control systems across the enterprise. Typically, this network uses the enterprise IT network and is segmented from the user networks by virtual local area networks (VLANs). 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

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

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).

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 Figures 9 and 10. VLAN switching functions are handled by physical Dell switches and the virtual environment. Routing was accomplished using the firewall.

Demilitarized Zone – 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.

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 3 and Figure 12. OT network.

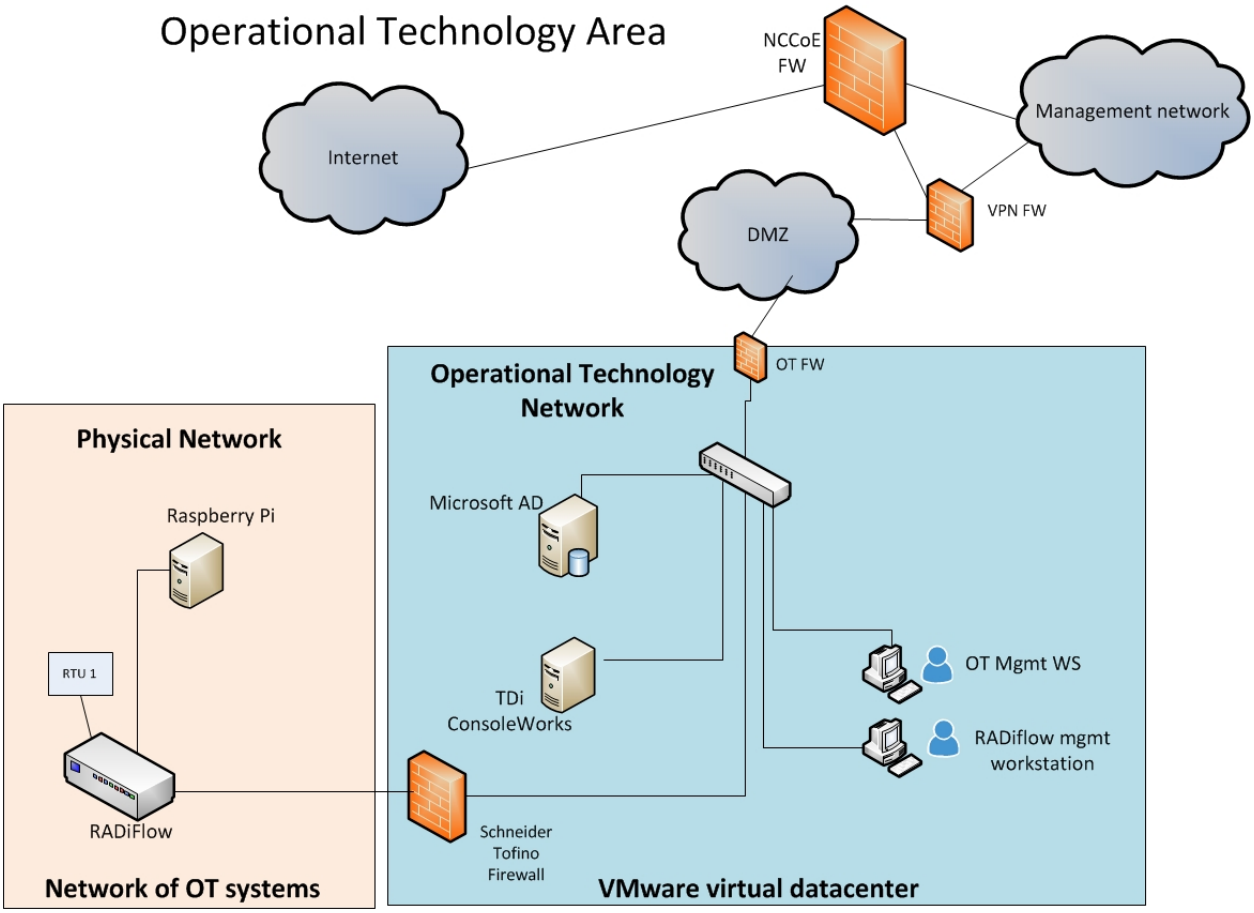


Figure 12. OT network

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 as well as issue real-time function commands (e.g., open/close relays). The access control/gateway uses the OT directory to obtain access authority for each user requesting access to an RTU.

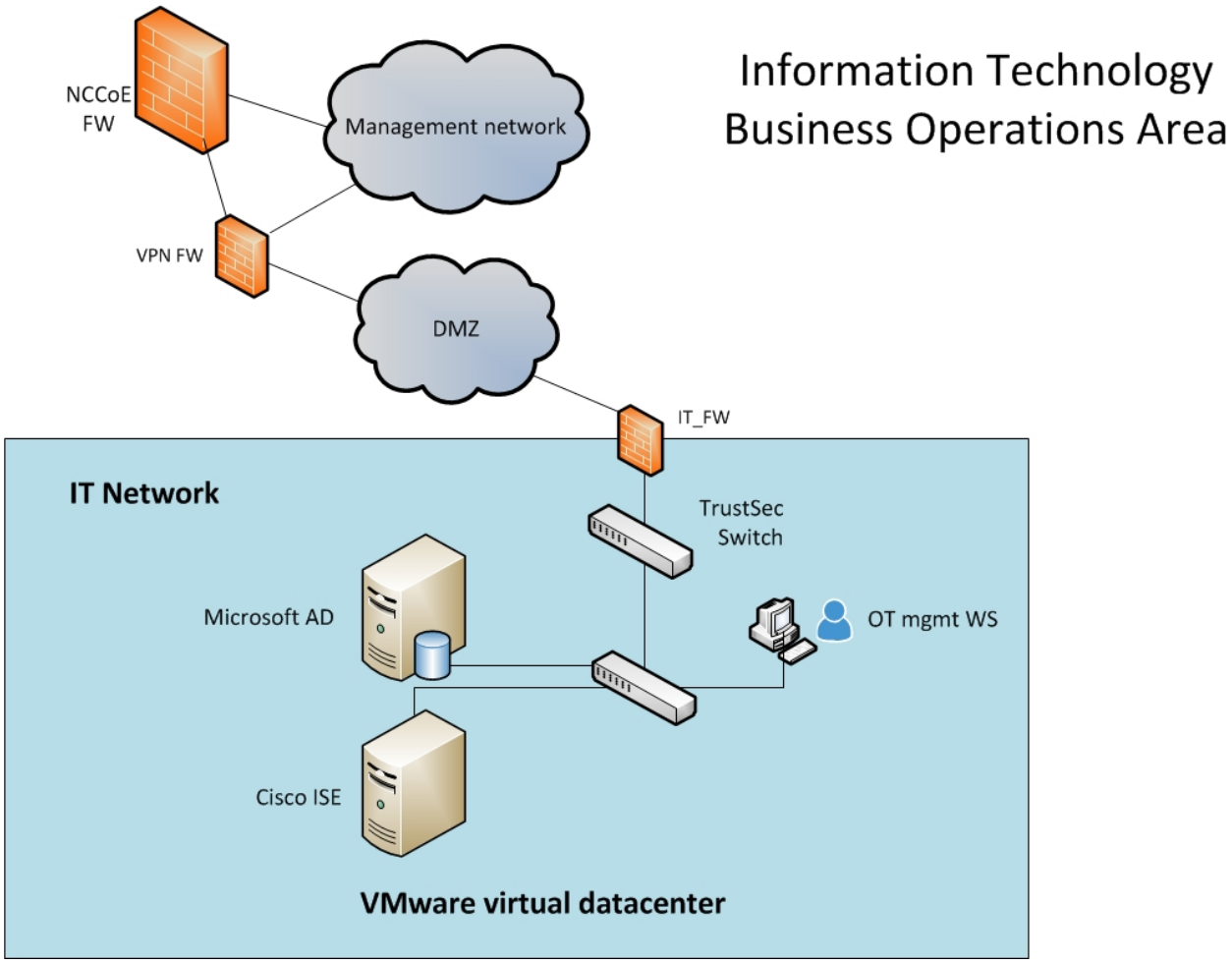
5.6.4 Information Technology Network

The builds include the following IT network components:

- Active Directory
- 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

879 the effectiveness of the IdAM example solution. The specific vendor products used in this
880 network are identified in Table 3 and Figure 13.



881

882 *Figure 13. IT network*

883 5.6.5 Physical Access and Control System Network

884 The builds include the following PACS network components:

885 • Active Directory
886 • PACS control server – Access IT!
887 • integrated access control unit (including a card reader, keypad, and door strike)—RS2
888 Technologies
889 • workstation

890 This network emulates a typical enterprise PACS. The specific vendor products used in this
891 network are identified in Table 3 and Figure 14.

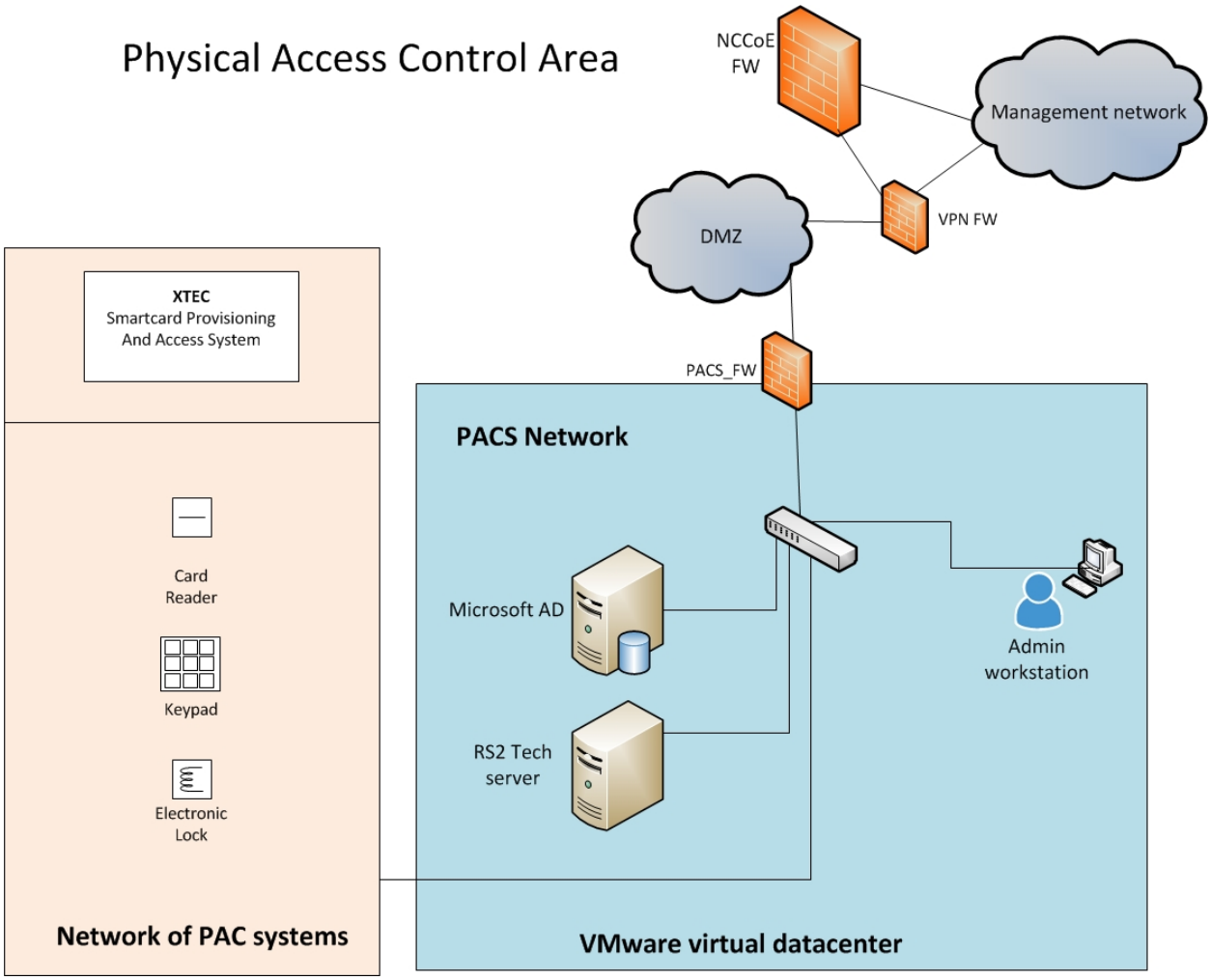


Figure 14. PACS network

Two technologies are demonstrated in the PACS network: XTEC XNode and RS2 Technologies AccessIT!. XTEC XNode is a physical access system 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. The RS2 Technologies system includes card readers, pin pads, and the AccessIT! 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
- Structured Query Language (SQL) server
- MAG Ozone components

The IdAM was separated to highlight the unique IdAM components 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 3 and Figure 15. Central IdAM network.

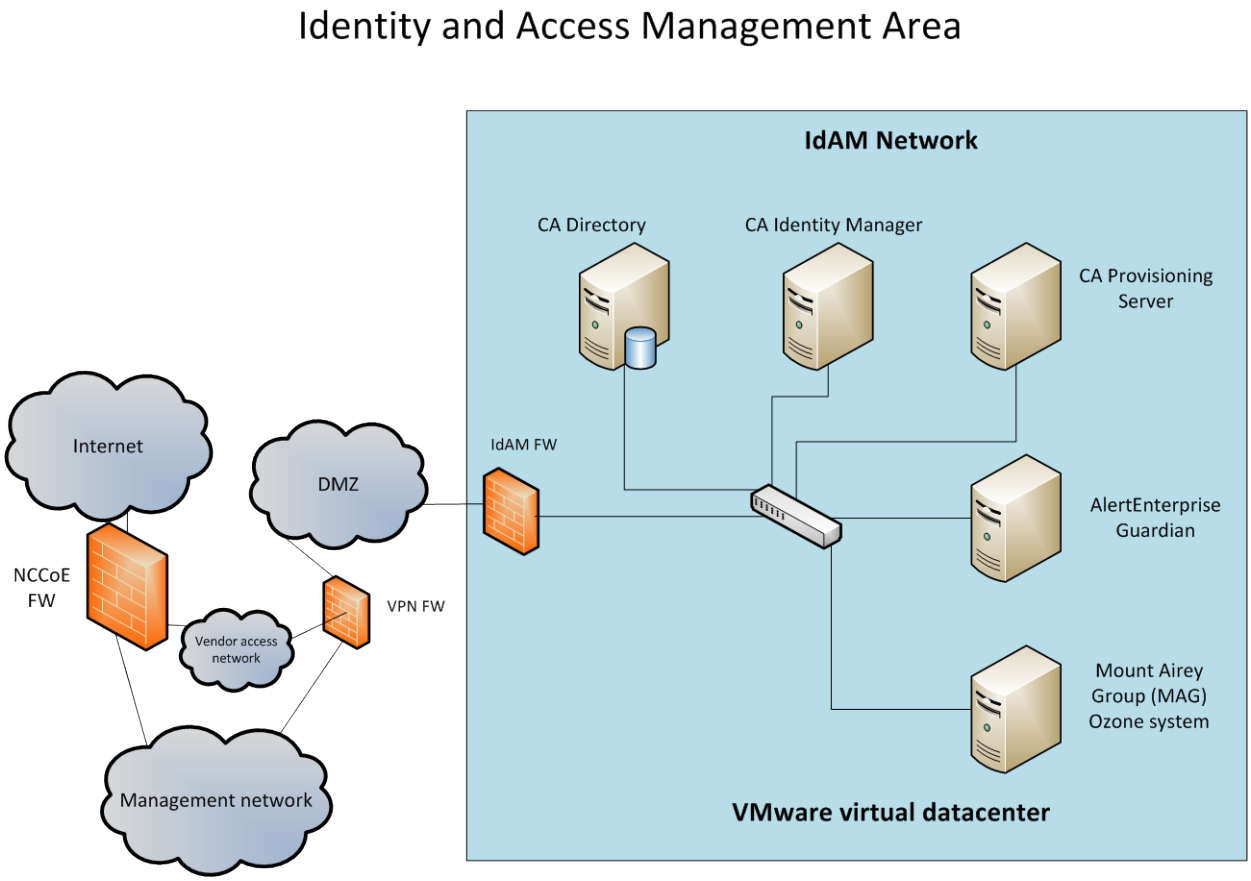


Figure 15. Central IdAM network, Build #1

The central IdAM system is the authoritative central store for identity and access authorization data. CA Identity Manager provides central identity and access store as well as workflow management capability in Build #1 (see Figure 15). The central IdAM system takes over 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

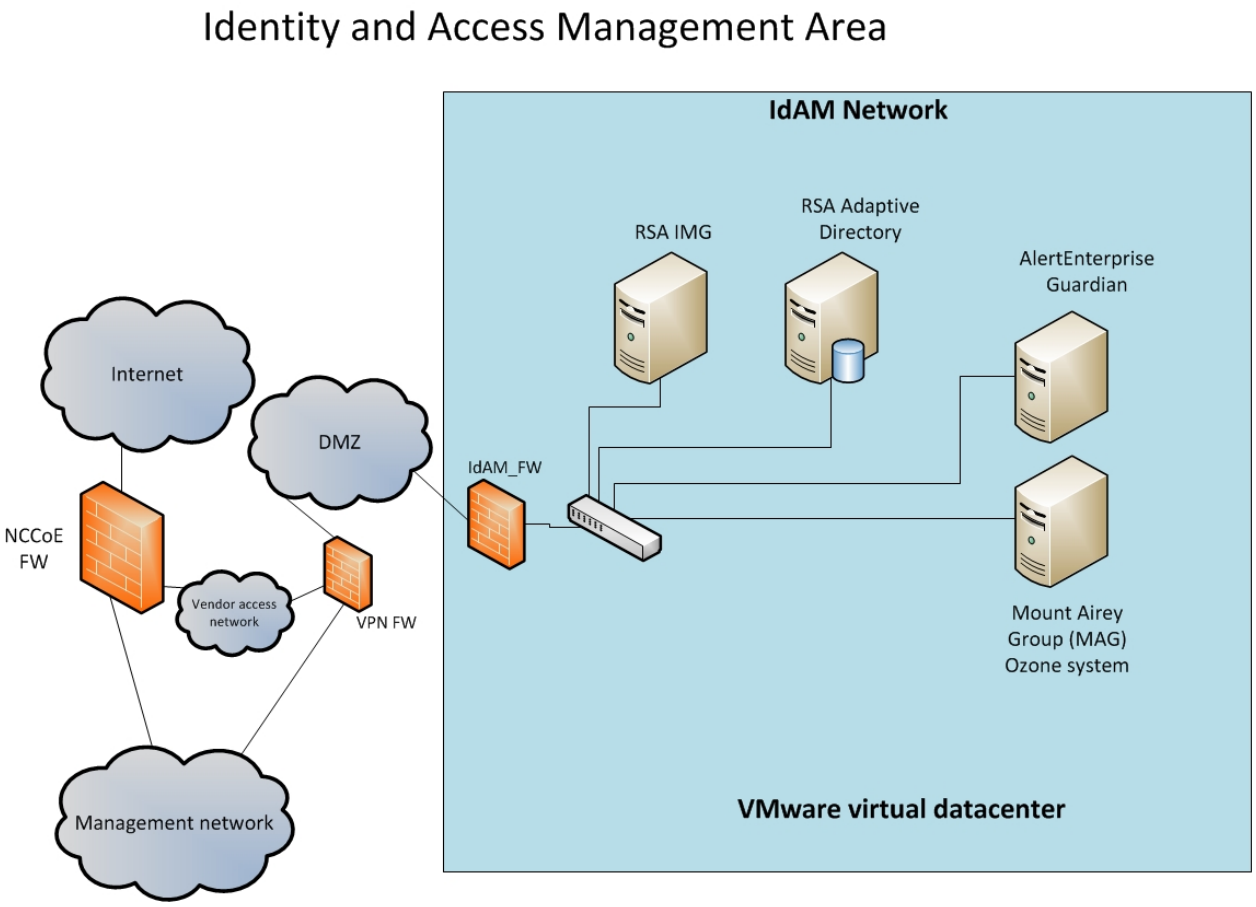
number of administrative users. The security of the solution partially depends on limited access to the managed directories, as discussed in Section 5.9.6, Security Recommendations.

In this build, the OT, PACS, and IT directories synchronize (sync) with the central IdAM system using Lightweight Directory Access Protocol Secure (LDAPS). This synchronization is set up to sync changes immediately 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 (AccessIT!). Guardian includes integration and translation capabilities to transfer the IdAM data to the AccessIT! 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 centralized/converged identity and access management network/system. This network was separated to highlight the unique IdAM components 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 3 and Figure 16. Central IdAM network, Build #2.



946

947 *Figure 16. Central IdAM network, Build #2*

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

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

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

964 The MAG Ozone product provides secure attribute distribution within the enterprise. Section
965 5.4 describes its use.

966 ### 5.6.7 Access Authorization Information Flow and Control Points

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

977 #### *5.6.7.1 OT Access and Authorization Information Flow*

978 This section describes the OT ICS/SCADA access and authorization information flow for both
979 builds.

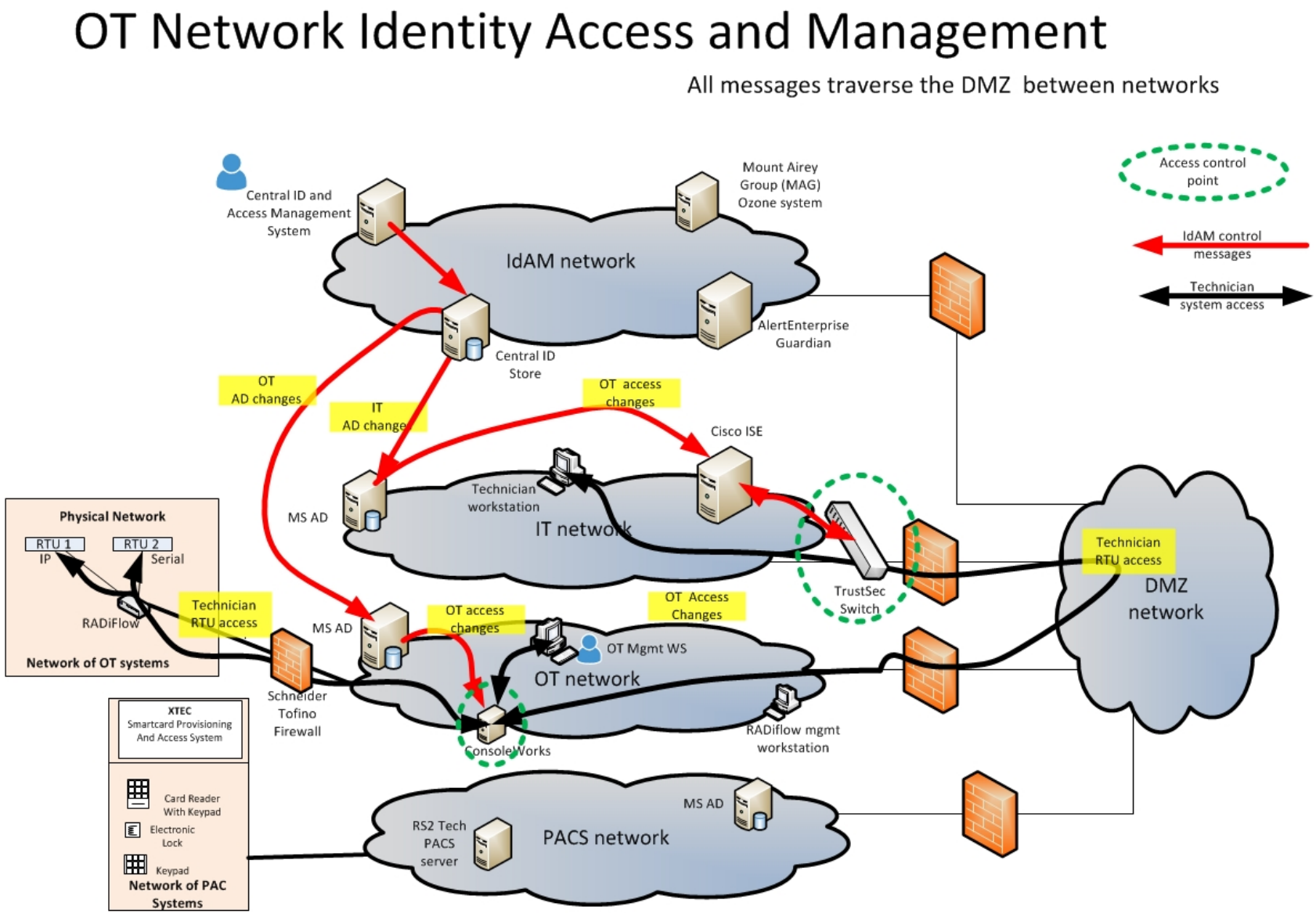


Figure 17. Access and authorization information flow for OT ICS/SCADA devices

Figure 17 depicts the access and authorization information flow for OT ICS/SCADA devices. The red lines 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 which OT devices 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 TrustSec switch controls which users have access to the OT network. ISE controls the TrustSec switch. This meets the NERC CIP-005 requirement to maintain an electronic security perimeter between the ICS/SCADA network and the rest of the corporate networks. ISE uses the IT directory identity store to determine user access authority and 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 below.

Build #1

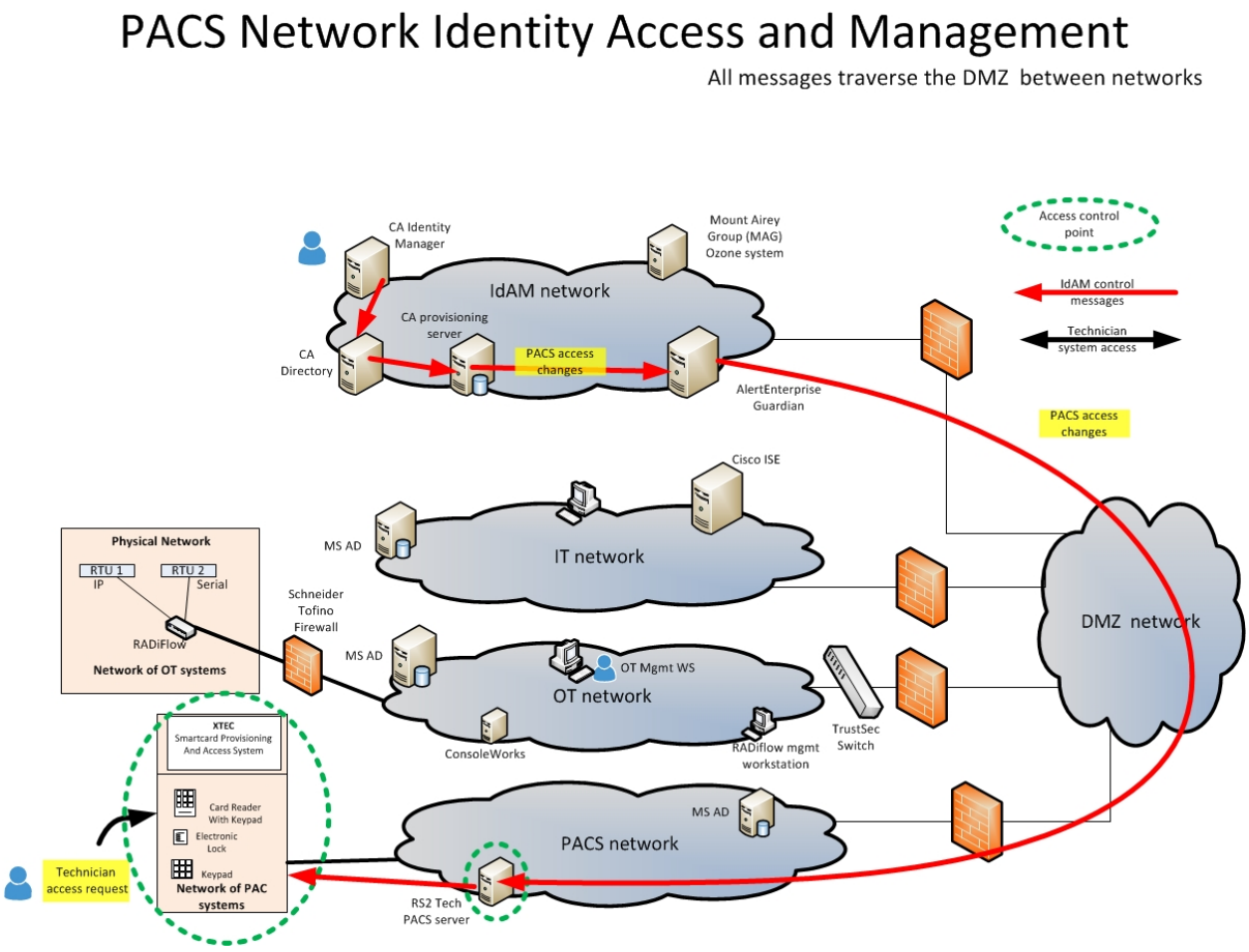


Figure 18. Access and authorization information flow for the PACS network, Build #1

The PACS network includes devices such as door locks and keypads. In Figure 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 AccessIT! management server controls physical access to facilities, rooms, and the like. AccessIT! updates the PACS devices as needed. The devices also report/log user accesses to this server for logging/auditing purposes. In most environments, the PACS network is segregated from other networks, typically using VLANs. Guardian provides the access and authorization data that it collects from the Identity Manager provisioning server to AccessIT!.

Build #2

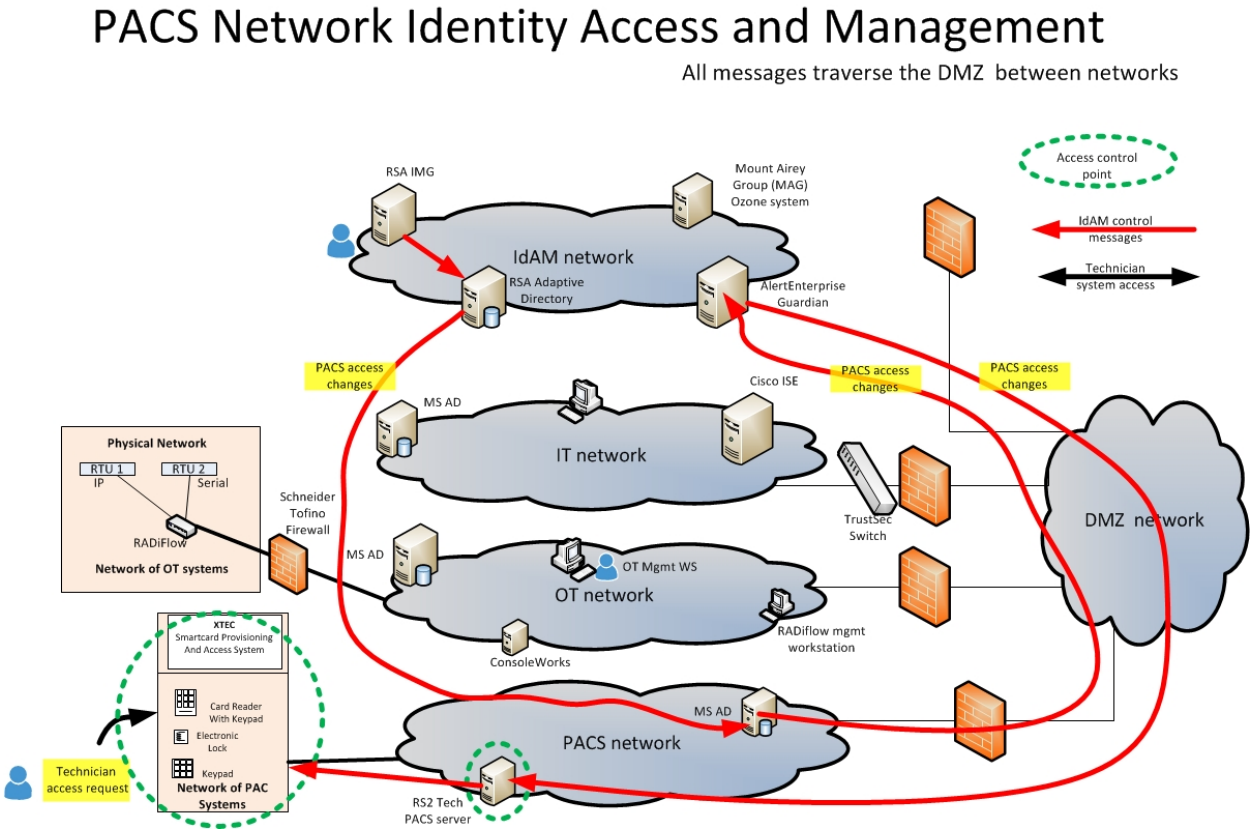


Figure 19. Access and authorization information flow for the PACS network, Build #2

The red lines in Figure 19 indicate the access and authorization data exchanges or PACS access in Build #2. In this build, IMG provisions all PACS IdAM data to the PACS directory. AlertEnterprise provides the access and authorization data that it collects from the PACS directory to AccessIT!.

5.6.7.3 *IT Access and Authorization Information Flow*

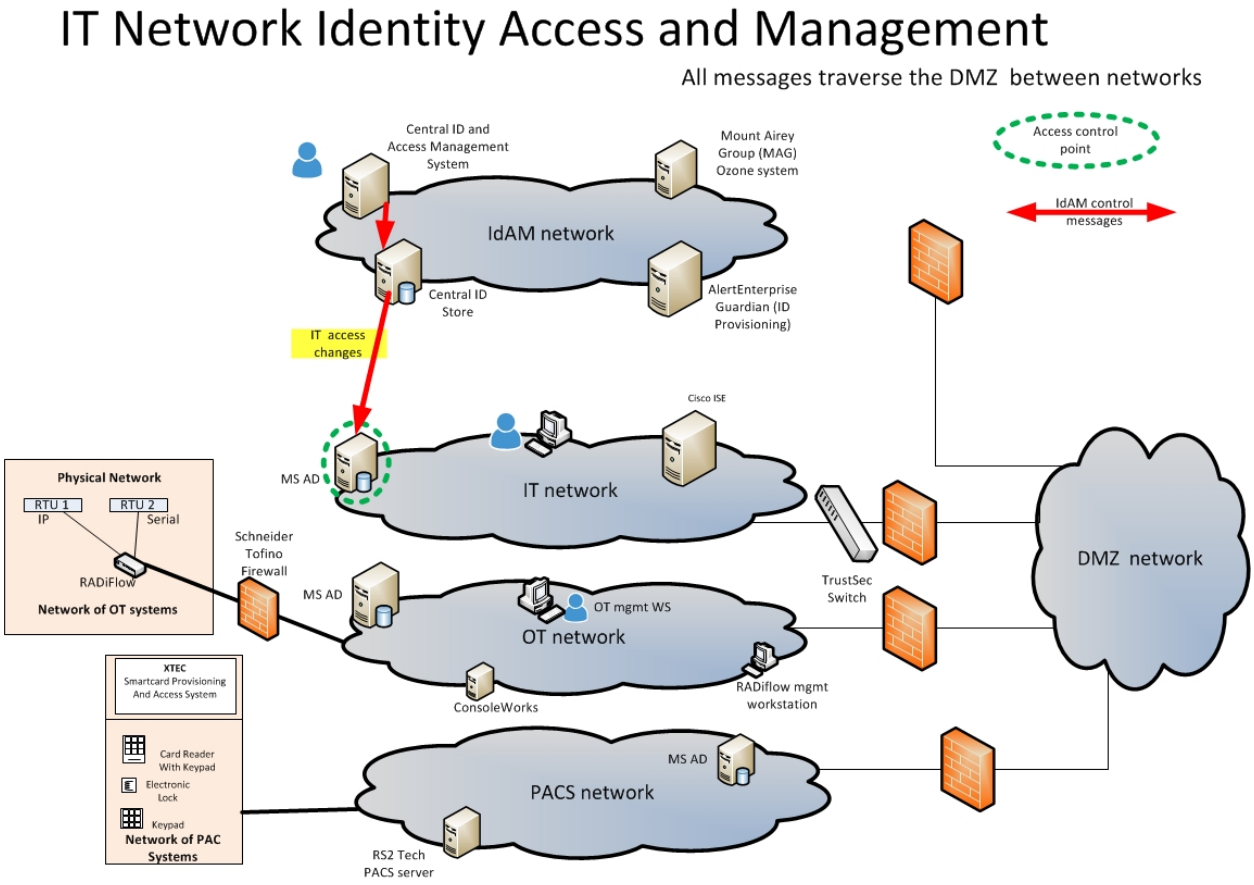


Figure 20. Access and authorization information flow for the IT network

The red lines in Figure 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. Active Directory provides the typical identity store function of storing the access permissions.

5.7 Data

The builds required a user dataset to populate the central IdAM system. In both builds, the IdAM system was initially populated with user data from a synthetic dataset. The dataset was designed to mirror a typical HR system dataset export file. A .csv file was used, which is a typical HR system export file type. 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 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.

5.8 Security Characteristics Related to NERC-CIP

The example solution both impacts and is impacted by the requirement to conform to NERC-CIP standards.[29]

Because the example solution uses routed protocols, by definition, it falls within the security perimeter of the adopting electricity subsector organization.[30] According to NERC-CIP, there must be a well-defined process for controlling access to all components within the organization's security perimeter.[31] So, access to the IdAM network must be controlled.

The example solution is informed by NERC-CIP requirements and may contribute to CIP-aligned implementations by providing mechanisms for centralizing logging and auditing of all IdAM activity efficiently and cost-effectively.[32] 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 of the IT, OT, and PACS network access control/directory components.

Table 4 describes how the centralized IdAM solution relates to NERC-CIP requirements.

Table 4. NERC-CIP Requirements

NERC-CIP Requirement	IdAM Role
CIP 004-3a Maintain a list of individuals with logical or unescorted physical access to Critical Cyber Assets.	IdAM maintains, in the identity store, a record of all logical and physical access to resources. If critical cyber assets are identified as such, IdAM inherently maintains such a list.
CIP 004-3a Conduct a cybersecurity training program for individuals with logical or unescorted physical access to Critical Cyber Assets.	The IdAM workflow can be configured to check a training system before granting access to critical cyber assets.
CIP 004-3a Conduct personnel risk	The IdAM workflow can be configured to

[29] The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (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.

[30] NERC Standard CIP-002-3 Cyber Security – Critical Cyber Asset Identification, Requirements section R3.

[31] NERC Standard CIP-005-3a Cyber Security – Electronic Security Perimeter(s), Requirements section R2.

[32] NERC Standard CIP-007-3a Cyber Security – Systems Security Management, Requirements section R6.

NERC-CIP Requirement	IdAM Role
assessment. Individuals must have an acceptable risk assessment before being granted access to Critical Cyber Assets.	verify that individuals have an acceptable risk assessment before granting access to critical cyber assets.
CIP 004-3a A list of all personnel with logical or unescorted physical access to Critical Cyber Assets must be maintained.	The identity store maintains authoritative information on all logical and physical access to resources. The identity store is a list of all personnel with logical or unescorted physical access to critical cyber assets.
CIP 004-3a Personnel with logical of physical access to Critical Cyber Assets must have that access removed within 24 hours if terminated for cause and within 7 days otherwise.	The IdAM workflow receives information from the HR system on terminations and can immediately de-provision access for terminated employees. Information from the HR system will need to be provided to the IdAM workflow at least daily to meet the 24-hour constraint.
CIP 005-3 requires documentation of the process for authorizing access in accordance with NERC CIP 004-3.	The IdAM workflow is the process for authorizing access. The workflow design and implementation documents the process.

NERC CIP 005-3 requires cyber assets used in access control and/or monitoring of an electronic security perimeter to be protected per CIP requirements. In both builds, the IdAM workflow, the identity store, and the provisioning capability control the information used to make access control decisions. They are considered inside the electronic security perimeter and must be protected according to NERC-CIP requirements. Connections from the IdAM components to IT, OT, and PACS must be considered access points to the electronic security perimeter.

5.9 Evaluation of Security Characteristics

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

5.9.1 Scope

The evaluation included 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 components depicted within the OT, PACS, IT, and IdAM networks in Figure 2, and their interactions with each other, with the exception of the XTEC stand-alone 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 centralized IdAM capability
- how the example solution addresses the security characteristics listed in the use case description https://nccoe.nist.gov/content/energy
- 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 analysis and 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 lists the example solution components, their functions, and the security characteristics 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 others are in Build #2. We discuss them as generic components providing a specific security functionality rather than as vendor products. One vendor product could be substituted for another that provides the same security functionality without affecting the results of the evaluation.

Table 5. 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
High Assurance Attribute Service (AAS)	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	

Component	Specific Product	Function	Security Characteristic
Translator between Active Directory and PACS and OT Access Management Systems (AMS)	AlertEnterprise Guardian	Translates from RSA/CA IdAM stores on 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, access control
Directory Service	MS Active Directory (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 Remote Manager (RM) of 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, IP-to-serial connectivity	Access control
Network Access Control (AC) and Policy Enforcement System (PES)	Cisco ISE	Allows access policies for network endpoints to be controlled centrally	Network security
Stand-alone Smartcard Provisioning (SP) and Access System (AS)	XTEC	Smartcard-based physical access control	Authentication, authorization, 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 (http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Identity_Access_Management.pdf). Six security characteristics are listed, 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 and best practice cited in the CSF in reference to that subcategory. Figure 21 depicts an example of the process.

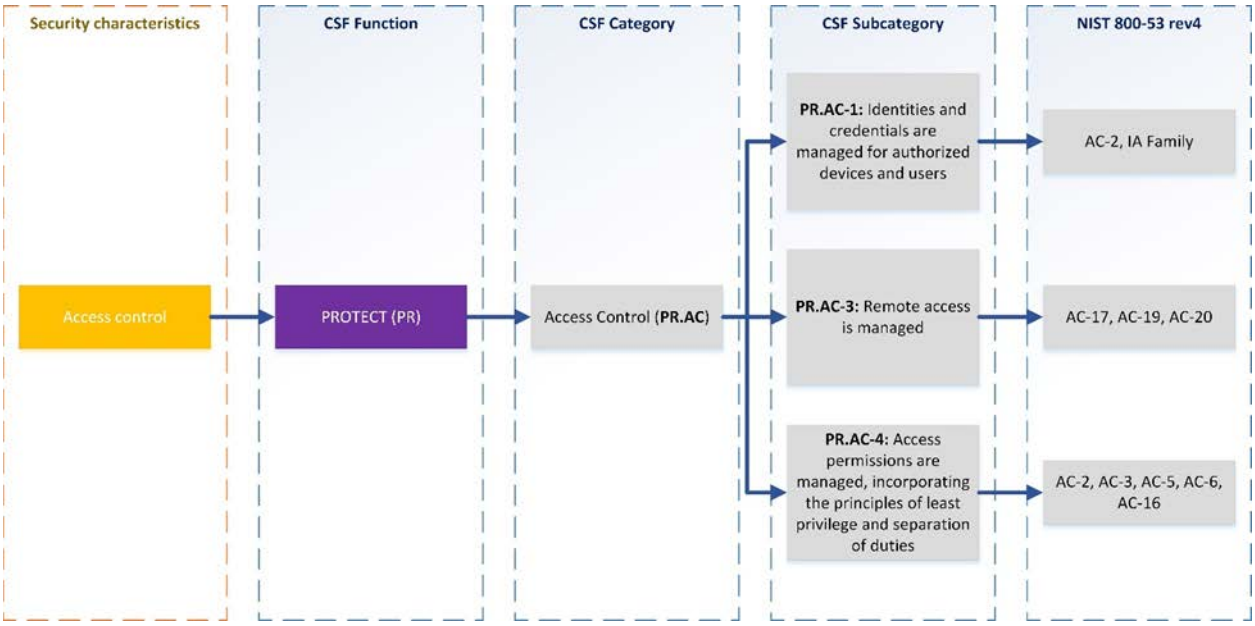


Figure 21. Example process for determining the security standards-based attributes for the example solution

We used the CSF subcategories to provide structure to the security assessment by consulting the specific sections of each standard 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:[33]

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

This section also discusses how the authentication, access control, and authorization (provisioning) security characteristics are addressed for PACS.

[33] http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Identity_Access_Management.pdf

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 centralized 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.

5.9.4.3 Protect Exchange of Identity and Access Information

All IdAM-related information exchange between IdAM components (as shown by the red lines in Figures 17 – 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 should be in protected mode:

- all information exchange 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 in Figure 17) and the OT directory service
- all information exchange between the PACS server and the PACS translator component (e.g., the AlertEnterprise component in Figures 18 and 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 use of all IT, OT, and PACS network account assets, for ICS/SCADA devices, and for physical access to rooms, facilities, and the like 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 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 handled uniformly 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 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 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 both 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 services 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.[34]

The identity, authorization, and workflow manager and the identity store on the IdAM network must be protected from unauthorized access and their information safeguarded. All of the data

[34] Section 5.6 describes the components and products in each build of the reference solution.

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 as well as 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, controlling access to each IdAM component, and securing communications among IdAM components is essential to securing the example solution. Therefore, 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[35]

The identity, authorization, and workflow manager on the IdAM network contains information regarding actual users and accounts for the OT, PACS, and IT. 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 HR 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).

There is no Active Directory 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 username and credential, presented either via Web interface or via each machine's operating system (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 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.

[35] Section 4.3.2 describes the risks associated with access to the IdAM workflow.

5.9.5.1.2. Logging Activity on IdAM Components

Logging all activity 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 logging of all user activity on IdAM systems (e.g., identity, access, and authorization changes). The example solution should also log all activity performed by administrators so that no activity is exempt from monitoring, logging, and audit. Here is a closer look at three different types of IdAM system users (in terms of the amount of privilege they have) and whether or not their activity should be logged.

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 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 operating system on which the component is running. All 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 operating system, 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 operating systems; 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 operating systems. If super-administrators do access the consoles of IdAM system's OS without doing so via the console manager, 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.

Access to the identity store on the IdAM network must also be strictly controlled, and the identity store should be configured so that it will only perform addition, modification, and deletion requests 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 machine

console, so at least these 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 rather than 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 input 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 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:

- securing access to the
  - 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 exchanged between the
  - 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 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:

- securing access to the
  - 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 exchanged between the
  - 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. 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 in minutes. These benefits directly reduce the cost of the regulatory audit requirements imposed on the energy industry. They 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 centralized 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 operating systems that use multifactor authentication and are configured according to best practices.[36]
- Ensure that all operating systems 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 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 principle 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 principle of least privilege and separation of duties.
- Segregate IdAM components onto their own network, either physically or using private VLANs and port-based authentication or similar mechanisms.[37]
- 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 using security components such as firewalls and intrusion detection devices that are configured according to best practices.

[36] The laboratory instantiation of the example solution builds did not implement every rule or guide in the STIGs upon which the builds installations were based. Exceptions were made to allow for only the needed operation of the solution. See the How-To section for details.

[37] IEEE 802.1X is a standard for Port-based Network Access Control that provides an authentication mechanism to devices that are to be attached to a local area network.

- Protect each of the OT, PACS, and IT, networks 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 connections needed to support required internetwork communications to specific IP address and port combinations in certain directions. The primary required, authorized internetwork communications are user authorization updates from the identity, authorization, and workflow manager component to the directory services on the production networks, the OT console access manager, and the PACS server, and logging information in the reverse direction. Firewalls should block all incoming connections from the Internet and to limit outgoing connections to the Internet, if any, to specific systems and required ports.
- Perform all IdAM-related information exchanged between IdAM components (as shown by the red lines in Figures 17 - 20) in protected mode, 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:
    - Perform all information exchange to/from the directory services in each of the OT, PACS, and IT, networks in protected mode.
    - Perform all information exchange between the console access manager (i.e., the ConsoleWorks component in Figure 17) and the OT directory service in protected mode.
    - Perform all information exchange between the network access control manager (i.e., the Cisco ISE component in Figure 17) and the switch in the IT network that controls access to the OT network in protected mode.
    - Perform all information exchange between the PACS server and the PACS translator component (e.g., the AlertEnterprise component in Figure 18 and 19 in protected mode.

  In the case of IdAM exchanges with the silo directories, protected mode is defined as the use of Start Transport Layer Security (TLS) (RFC 2830) 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 access them remotely.
- Log all IdAM activity, for example direct access to IdAM components on the IdAM network and all messages exchanged between IdAM components. Limit the number of users able to control whether or not activity performed 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 access any console directly. Use of a console access manger ensures that all activity 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 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 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 for only the necessary amount of time. It also enables a centralized, simplified audit capability for accountability and tracking. Such benefits come with a cost. This cost is the requirement to secure and log all access to the IdAM network, its components, and the information exchanged between these components and IdAM components on the OT, PACS, and IT, networks.

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 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 provides a template of a test case, including a description of each field in the test case.

Table 6. 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. Specifies the capability to be evaluated.
Associated Security Controls	The NIST SP 800-53 rev 4 controls addressed by the test case.
Description	Describes the objective of the test case.
Associated test cases	In some instances a test case may be based on the outcome of another 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	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
Procedure	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 ES IdAM functional evaluation requirements that are addressed using this test plan. Table 7 lists those requirements and associated test cases.

Table 7. IdAM Functional Requirements

Capability Requirement (CR) ID	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
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		
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

1516

1517

6.3 Test Case: IdAM-1

Table 8. Test Case ID: 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 as well as in the PACS network and system, including allowing and denying access.
Associated test cases	
Associated Security Controls	AC-2, AC-3, IA-2, PE-2, PE-3
Preconditions	1. HR representative .csv file is available. 2. IdAM example solution is implemented and operational in the lab environment 3. Standard and privileged user sets are known to the testers. 4. A PACS system with a card reader and simulated door access demonstration system is operational in the lab. 5. A simulated OT network with an RTU and RTU emulator (Raspberry Pi) is implemented in the lab.
Procedure	1. Activate IdAM workflow engine and run 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 Schweitzer Engineering Laboratories (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 not have access allowed.
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 as well as 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 as well as the SEL RTU and RTU emulator. Users who are denied access PACS network are unable to log into a workstation on the PACS network. Users without access are not authorized and not allowed access by the PACS

	card reader and door access demonstration system.
Actual results	This test functioned appropriately and provided the expected results. User that were denied access were unable to login to the OT and IT networks, and denied access to PACS. Users granted access to each system were able to access the OT and IT networks and granted access via PACS.
Overall result	Pass

1520

1521

6.4 Test Case IdAM-2

Table 9. Test Case ID: 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: (OT, PACS, IT,) (CR 3) The IdAM system shall include an IdAM workflow capability that can de-activate users in the following networks and systems: (IT, OT, 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.
Procedure	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 procedure 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, 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 that 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 approved. The users were no longer able to access the OT, PACS, or IT.
Overall result	Pass

6.5 Test Case IdAM-3

Table 10. Test Case ID: IdAM-3

Parent requirement	(CR 4) The IdAM system shall include a workflow capability that can change an existing user's access to the various 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 IdAM system in the state after IdAM-2 is completed.
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 chosen in 1 above. 3. Use the IdAM workflow to allow access for the set of users without access chosen in 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 demo 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 demo 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

1526

1527

APPENDIX A: ACRONYMS

Acronym	Literal Translation
ABAC	Attribute-Based Access Control
AD	Active Directory
CA	CA Technologies
CIP	Critical Infrastructure Protection
CR	Capability Requirement
CSF	Cybersecurity Framework
.csv	Comma-Separated Value
DMZ	Demilitarized Zone
EACMS	Electronic Access Control and Monitoring System
EAP	Electronic Access Point
EMS	Energy Management System
ESP	Electronic Security Perimeter
HR	Human Resources
ICS	Industrial Control System
ID	Identity
IdAM	Identity and Access Management
IDS	Intrusion Detection System
IMG	Identity Management and Governance
IP	Internet Protocol
ISE	Identity Services Engine
LDAPS	Lightweight Directory Access Protocol Secure
MAG	Mount Airey Group

Acronym	Literal Translation
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
OS	Operating System
OT	Operational Technology
PACS	Physical Access Control System
PIV-I	Personal Identity Verification Interoperable
PKI	Private Key Infrastructure
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guideline
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

APPENDIX B: REFERENCES

[1] Cybersecurity Framework, National Institute of Standards and Technology [Web site], http://www.nist.gov/cyberframework/ [accessed 2/25/14].

[2] Designation of Public Trust Positions and Investigative Requirements, 5 C.F.R. § 731.106 (2013). http://www.gpo.gov/fdsys/granule/CFR-2012-title5-vol2/CFR-2012-title5-vol2-sec731-106/content-detail.html.

[3] Office of Management and Budget (OMB), E-Authentication Guidance for Federal Agencies, OMB Memorandum 04-04, December 16, 2003. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf [accessed 2/20/14].

[4] E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[5] "Establishment of NIST Smart Grid Advisory Committee and Solicitation of Nominations for Members," 75 Federal Register 7 (January 12, 2010), pp. 1595-1596. https://federalregister.gov/a/2010-344.

[6] Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat 2946. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[7] J. Boyar, M. Find, and R. Peralta, "Four Measures of Nonlinearity," Eighth International Conference on Algorithms and Complexity (CIAC 2013), Barcelona, Spain, May 22-24, 2013, Lecture Notes in Computer Science 7878, pp. 61-72. http://dx.doi.org/10.1007/978-3-642-38233-8_6.

[8] NISTIR 7298 Revision 2, Glossary of Key Information Security Terms, Richard Kissel, Editor.

[9] V. C. Hu and K. Scarfone, Guidelines for Access Control System Evaluation Metrics, NISTIR 7874, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 48pp. http://dx.doi.org/10.6028/NIST.IR.7874.

[10] M. Souppaya and K. Scarfone, Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication (SP) 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013, 29pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [accessed 2/25/14].

[11] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[12] International Organization for Standardization/International Electrotechnical Commission, Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011, 2011. http://www.iso.org/iso/catalogue_detail?csnumber=56742 [accessed 2/25/14].

[13] Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 5280, May 2008 http://www.ietf.org/rfc/rfc5280.txt [accessed

2/20/14].

[14] Internet Security Threat Report 2013, Volume 18, Symantec Corporation, Mountain View, CA, 2013, 58pp. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf [accessed 2/25/14].

[15] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile,

[16] U.S. Department of Commerce. Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standards (FIPS) Publication 201-2, August 2013, 87pp. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf [accessed 2/25/14].

APPENDIX C: MOUNT AIREY GROUP, INC. PERSONAL PROFILE APPLICATIONS DEMONSTRATION APPLICATION

The Personal Profile Application (PPA) was developed by Mount Airey Group, Inc. in order to demonstrate the functionality of the 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; as well as 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; and is meant to protect an organizations most sensitive or highest risk resources. If an application relies on PKI-based smart cards and/or biometrics for authentication, then that system should implement the congruent security for the authorization of users for access to that resource as is provided by Ozone®.

In support of the National Cybersecurity Center of Excellence (NCCoE) Electricity Subsector Identity & 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 application.

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.

In order 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 to search for 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:

- 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.

Sample First Page Table:

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

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

Sample Search Results Page Table:

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