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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

IDENTITY AND ACCESS MANAGEMENT

Securing Networked Infrastructure for the Energy Sector

The National Cybersecurity Center of Excellence (NCCoE), in collaboration with energy sector stakeholders and cybersecurity vendors, has developed an example identity and access management (IdAM) solution. The solution provides a demonstration of commercially available technologies that support a converged IdAM platform. This platform follows both standards and best practices, and is informed by NERC CIP version 5 rules. If you would like to utilize the design or view a demonstration, please contact us at energy_nccoe@nist.gov.

CHALLENGE

As the electric power industry upgrades infrastructure to take advantage of emerging technologies, utilities are also moving towards greater information technology (IT) and operational technology (OT) convergence. This allows technologies, devices, and systems to connect to the grid to provide access to data normally held in silos, and enhance productivity. One such area that touches both IT and OT departments is identity and access management (IdAM), which manages access to networked resources, including buildings, equipment, technology, and industrial control systems.

Many utilities run decentralized IdAM systems managed by separate departments whose employees often lack time and methods to coordinate access to devices and facilities across IT and OT silos. According to our electric sector stakeholders, this inefficiency can result in security risks for utilities. Additionally, a decentralized IdAM platform spread across separate silos in a utility can lead to an increased risk of attack and service disruption, an inability to identify potential sources of a problem or attack, and a lack of overall traceability and accountability regarding who has access to both critical and noncritical assets.

SOLUTION

A converged IdAM platform can provide a comprehensive view of all users and their access rights across the enterprise. The NCCoE developed an example converged IdAM solution that utilities can use to increase security and efficiency in managing access to their networked devices and facilities.

The development of this example solution is documented in NIST Cybersecurity Practice Guide, Special Publication 1800-2: “Identity and Access Management for Electric Utilities.” Utilities can use some or all of the guide to implement a converged IdAM system using NIST and industry standards, including the North American Electric Reliability Corporation’s (NERC) Critical Infrastructure Protection (CIP) standards. Commercial, standards-based products, like the ones the NCCoE used, are easily available and interoperable with commonly used infrastructure.

BENEFITS

The example implementation:

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

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCoE
Visit http://nccoe.nist.gov

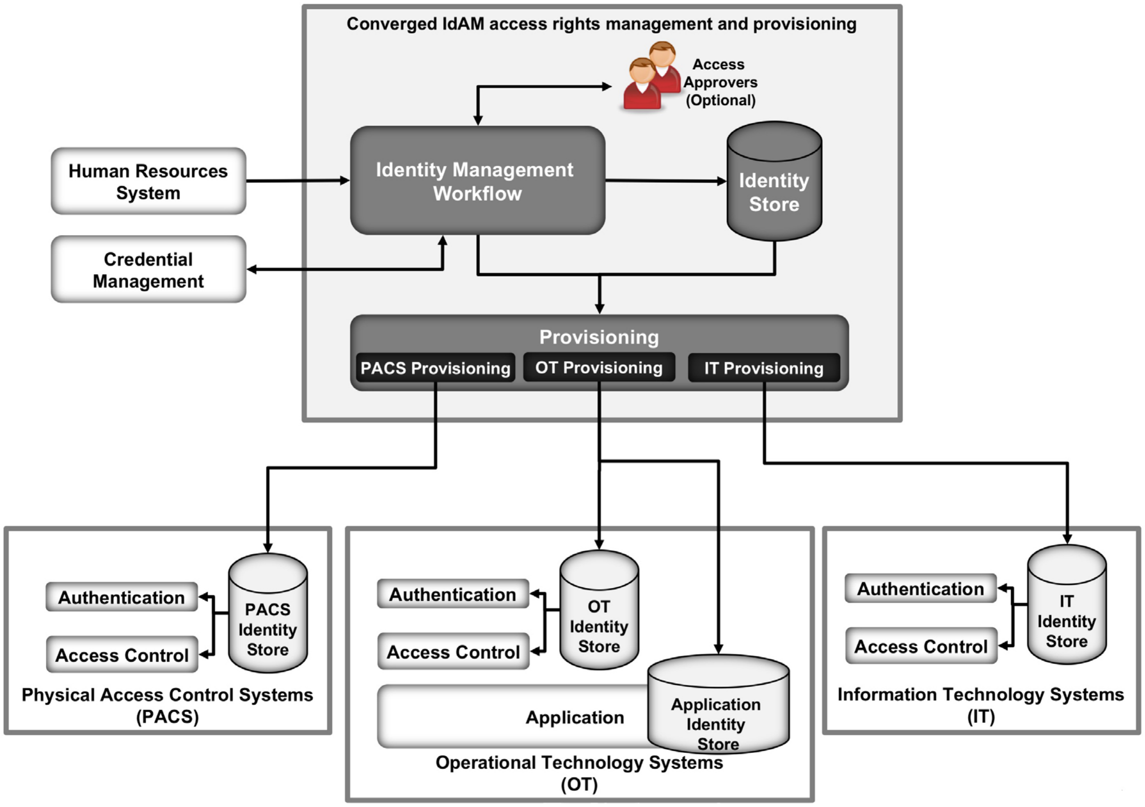
CONTACT US
nccoe@nist.gov
301-975-0200

IMPLEMENTATION OVERVIEW

Our example implementation includes components such as:

- services for authenticating and authorizing users based on identity and role
- services for authenticating and authorizing devices
- an identity and access governance capability that translates human-readable access needs into machine-readable authorizations
- industrial control systems equipment, such as remote terminal units, programmable logic controllers, and relays, along with associated software and communications equipment (e.g., routers and firewalls)
- physical access control devices that use standard communication interfaces
- "bump-in-the-wire" devices for augmenting operational technology with authentication, authorization, access control, encrypted communication, and logging capabilities

HIGH-LEVEL ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

AlertEnterprise! ca technologies CISCO GlobalSign. GMO INTERNET GROUP radiflow Secure your Assets 2KS Technologies RSA Schneider Electric tdi technologies XTEC

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

DOWNLOAD THE PRACTICE GUIDE

For more information on this project, visit:
https://nccoe.nist.gov/projects/use_cases/idam

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please emai energy_nccoe@nist.gov.