APTA STANDARDS PROGRAM
RECOMMENDED PRACTICE

APTA SS-ECS-RP-005-25
First Published: May 27, 2025

Enterprise Cyber Security Working Group

Approaching Access Management

Abstract: This recommended practice suggests the essential techniques and uses of identity and access management. It also suggests good practices when designing and administering access management systems.

Keywords: access, authentication, cybersecurity, information security, passwords, risk management

Summary: In the computing environments needed by today's transportation-related organizations, there is increasing complexity that requires several approaches to authenticate and authorize individuals, devices and services to perform functions and activities. This document defines sufficient practices for the various business cases that transit agencies, suppliers and partners must address. This may be an identity access management approach—although role-based access and other access and authentication methods may be involved in the discussion.

Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document and its continued maintenance, which is detailed in the manual for the APTA Standards Program. This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the Enterprise Cyber Security Working Group as directed by the Security and Emergency Management Standards Policy and Planning Committee.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

This is a new document.

Table of Contents

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Enterprise Cyber Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Dr. Julius Smith, Chair, *Dallas Area Rapid Transit*
Ahmed Idrees, Vice Chair, *Sound Transit*

Lee Allen, *Transportation Security Administration*
Peter Anderson, *GCRTA*
Muneer Baig, *SYSUSA*
Michael Bosche Sr., *OCTA*
Alesia Cain, *Clever Devices Ltd.*
Timothy Coogan, *Regional Transportation District*
Rachel Deen, *Transit Safety & Security Solutions*
Terry Follmer, *CapMetro*
Donald Luey, *Foothill Transit*
Clare Mueting, *TSA*
Sean Ryan, *MTA Metro-North Railroad*
John Sherman, *Hampton Roads Transit*
Dan Sullivan, *Regional Transportation District*
Anthony Tisdale, *FTA*
William Tsuei, *Access Services*
Jeff Van Wingerden, *Sound Transit*
Leigh Weber, *Cybersecurity Analysis Ltd.*

Project team
Polly Hanson, *American Public Transportation Association*
Michael Echols, *Max Cybersecurity LLC, ECSWG facilitator*
Brian Heanue, *American Public Transportation Association*

Introduction

This introduction is not part of APTA SS-ECS-RP-005-25, "Approaching Access Management."

This document is intended primarily for cybersecurity, information security and risk management practitioners or other individuals with information security responsibilities at small to medium-sized transit agencies. It is also intended to recommend considerations when developing an authentication and access management plan.

Scope and purpose

This document provides suggestions to aid transit agencies with identity and access management. Its purpose is to help initiate basic thought processes on designing user access management for sensitive systems or roles.

Approaching Access Management

1. Possible discussion considerations

Here are some categories of networked/communication devices that may require secure authentication measures:

- desktop/laptop computers
- servers/virtualized host environments
- network devices (switches, routers, etc.)
- telephones: VoIP (desktops), mobile phones (company-issued and personal devices)
- printers/fax devices (shared and personal)
- building access/energy management/security:
    - turnstiles/door access
    - lighting systems (motion detectors, time-of-day/day-of-week operation)
    - HVAC (smart management including time-of-day/day-of-week/motion detectors)
    - fire alarm systems
    - people-movers (escalators, elevators, linear people-mover)
    - parking garage systems (available spots by floor/sector, garage door operation)
    - security cameras
    - campus access to roads (gates, visitor access credentials)

User credentials, mobile phone numbers and service accounts can be considered as authentication factors to authenticate a user or service. In contrast, Wi-Fi networks can be considered computing environments that authentication must protect. Here are some areas of security controls for identity validation, authentication, authorization and access control:

- human centered credentials (username, password)
- system-level accounts that need automatic authentication (often used by applications to access the underlying operating system or to reach a database system)
- guest access to the Wi-Fi networks
- enterprise access to the internal Wi-Fi networks
- use of mobile phones and their apps while connecting over public networks (LTE, 5G)

2. Possible question considerations

- How do “traditional” computing devices (e.g., desktop or laptop computers) authenticate into a network?
- How do “nontraditional” devices such as VoIP phones, cameras, printers and network devices authenticate when entering the Enterprise or Guest networks?
- How do building management systems authenticate when entering their part of the network?
- What is the proper use of password vaults?
- What is the appropriate use of multifactor authentication (MFA)?

- How do servers, virtual server environments, database systems, security stack devices and IT services (internet services, gateways, web servers, email services, directory services) get authenticated?
- How are trust and identity managed between on-premises and cloud environments?
- How are trust and identity managed among multiple cloud environments?

3. Recommendations

There are several excellent resources available to guide transit agencies through the process of developing, updating or migrating an account and authentication management system. NIST 800-63B (see References) covers authentication and life cycle management and is a good starting place.

Also, when developing an access management plan, agencies should consider the following:

- **Location-based security:** Include a user's physical location information in identity and access management decisions. A user's location may be obtained by IP address geolocation data, Wi-Fi network attributes, GPS data from mobile phones, and enterprise vs. home-office network attributes. These location-based attributes can be used to enhance authentication controls by requesting MFA from a remote location or blocking foreign IPs, for example.
- **Password hardening:** Require that users set up stronger and stronger passwords based on preestablished strength criteria. Additionally, maintain a prohibited keyword list that cannot be used in passwords, such as company name or user's name. Then scan for and remove weak passwords.
- **Enforce password change:** Have systems administrators set up rules based on making people change their passwords on a predefined basis.
- **Multifactor authentication:** This allows for an additional security layer to be activated during the login process, such as sending a push notification or text message to an employee's phone to verify their identity before logging into an application. Moreover, organizations should look to implement adaptive MFA, which leverages machine learning to determine whether MFA is necessary based on risk calculations at the time of login.
- **Password managers:** Deploy an enterprise password manager tool for users to store their work-related application credentials securely. Additionally, this enables the users to create strong, unique passwords for their various applications.
- **Privileged access management:** Deploy a PAM solution to protect highly privileged user and application accounts that have elevated access to critical systems.
- **Single sign-on:** Where possible, enable applications to use a single authentication source such as Active Directory or SAML to eliminate local accounts on each platform. This enables the centralized onboarding and offboarding of users linked to the human resources processes.
- **SCADA/ICS and OT systems:** Maintain separate access control systems for SCADA/ICS and OT systems.
- **Actively monitor for suspicious activity:** Establish processes to routinely monitor and respond to suspicious activity on identity and access control systems.

References

Auth0, "How To Have a Successful IDM Project," October 2018. https://auth0.com/blog/how-to-have-a-successful-idm-project/

Institute of Electrical and Electronics Engineers, "Design Best Practices for an Authentication System," June 2016. https://cybersecurity.ieee.org/blog/2016/06/02/design-best-practices-for-an-authentication-system/

National Institute of Standards and Technology, NIST 800-63B, "Digital Identity Guidelines." pages.nist.gov/800-63-3/

U.S. Department of Defense, "Identity and Access Management Recommended Best Practices for Administrators," March 2023. https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF

Microsoft, "Azure Identity Management and access control security best practices," September 2024. https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

Abbreviations and acronyms

5G	fifth-generation wireless
GPS	Global Positioning System
HVAC	heating, ventilation and air conditioning
ICS	industrial control system
IP	Internet Protocol
IT	information technology
LTE	Long-Term Evolution
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
OT	operational technology
PAM	privileged access management
SCADA	Supervisory Control and Data Acquisition
TSA	Transportation Security Administration
VoIP	Voice over Internet Protocol

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	Oct. 4, 2024	March 3, 2025	March 27, 2025	Apr. 25, 2025	May 27, 2025