IA.L2-3.5.1

Identification & Authentication

Identification [CUI Data]

"Identify system users, processes acting on behalf of users, and devices."

Objectives

[a]
System users are identified.

[b]
Processes acting on behalf of users are identified.

[c]
Devices accessing the system are identified.

Key Discussion Points

Three Things to ID:
Users, processes, and devices — all three must be uniquely identified. Missing any one is a gap.

Unique Identifiers:
Every user gets a unique username. Every device gets a unique identifier — MAC, IP, or asset tag. No shared identities.

Processes Count Too:
Service accounts, scripts, scheduled tasks, and scan agents are processes acting on behalf of users — they must be identified too.

Foundation for 3.5.2:
You cannot authenticate what you have not identified. 3.5.1 creates the identity; 3.5.2 verifies it. Both are required.

Assessment Methods

EXAMINE

Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings; system audit logs; list of system accounts.

INTERVIEW

Personnel with system operations responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities; system developers.

TEST

Organizational processes for uniquely identifying and authenticating users; mechanisms supporting or implementing identification and authentication capability.

IA.L2-3.5.1

IDENTIFICATION & AUTHENTICATION — Identification [CUI Data]

Plain English

What this control is really saying:

Before you can control access to anything, you need to know who or what is asking for access. This control requires that every user has a unique identity, every process acting on the system is identified, and every device is identifiable. It sounds basic — and it is — but it's the foundation everything else in the IA domain is built on.

How it is used:

- Every employee has a unique Active Directory account — no shared user logins exist on any CUI system.
- All devices in the CUI environment are assigned a unique asset identifier documented in the system inventory.
- Service accounts for backup, scanning, and monitoring are uniquely named, documented in the SSP, and reviewed annually.
- MAC addresses and IP assignments are tracked in the network documentation — every device accessing CUI systems is on the list.

Real World Example

The Scenario

Acme Defense has five employees all using individual Windows accounts. However, the CNC machine controller runs under a built-in 'Administrator' account shared by the operator and the IT admin. Two network switches have never been assigned asset identifiers.

What the assessor finds

The CNC controller account is shared — actions on it cannot be attributed to either the operator or the IT admin. The two switches do not appear in the asset inventory. One backup service account is named 'svc' with no documentation of its purpose or owner.

SPRS Score Impact

3.5.1 carries a point value of 1. Though low-weighted, identification is the prerequisite for every other IA control — without unique identities for users, processes, and devices, authentication and access control are meaningless.

What Good Looks Like

Unique individual accounts for all users, no shared logins, all devices inventoried with unique identifiers, service accounts documented and reviewed, guest accounts disabled, SSP reflects the full identity landscape.

Common Gaps

What assessors actually find in the field:

✗ **Shared accounts in use**

Multiple users share a single login — individual actions cannot be traced to a specific person.

✗ **Devices not inventoried**

No device inventory exists — systems connecting to the CUI environment are unknown and untracked.

✗ **Service accounts undocumented**

Backup and scan agents run under generic service accounts that are not documented or reviewed.

✗ **No username standards**

Some users have individual accounts; others share department logins — identification is inconsistent.

✗ **Guest accounts active**

Built-in Guest accounts are enabled on workstations — anyone can access the system without a unique identity.