# Bronze

## Audience

The audience for this document is IT management of an IdPO.

## What is Bronze?

Identity Assurance is a collection of identity and authentication-related technologies, polices and practices that we implement to achieve a certain security objective, thus protecting a service or resource. The primary difference with what you do now and the InCommon Profiles is that someone has done the thinking for you: if you have a specific risk profile that you would like to address, use this published identity assurance profile.

The inCommon Bronze Identity Assurance Profile supports sequential identity, which means that over time the same person is returning with the same credential. It's most useful for things like group membership, where identity is not as important as being a part of a project or class or having an entitlement. The classic library use case of  verified user of a campus license agreement applies here.

## Why Bronze Certification?

For campus identity providers, Bronze provides a generally-accepted good practice for passwords and credentials.

Bronze certification:

- provides visible proof of your good practice through publication in the InCommon metadata, on the **InCommon website**, and on the US Government **FICAM website.**
- provides a community and federally approved practice statement. What other sources do you have that are as comprehensive?
- gives you a good baseline of credential practices you can use to address your security needs. Using the profiles can help you shine a light on things that you should be protecting better.
- gets you up and running with Assurance with a simpler profile. Provides a stepping stone to Silver certification.There is no audit required, and it's free to get certified.
- normalizes practices across the Federation as implementation spreads.

Over time, Bronze may replace the Participant Operating Practices as the baseline requirement for participating in the Federation. This in turn will help drive service provider adoption as their risk decreases.

## Why InCommon's Program/Profile?

InCommon is the only federation serving Education that provides the standards,  related trust certification program, and the metdata infrastructure that helps make it all go. And it's all approved for use by the US Government with their agencies.

**Background**

The National Institutes of Standards and Technologies, the XXXX for the Federal Government, developed NIST 800-63 Electronic Authentication Guidelines in XXX for use by Federal Agencies. The Federal CIOs established the Identity, Credential and Access Management subcommittee to develop programs to enable third-party credentials (like those from InCommon Participants) to be used with agency apps.

In response to the FICAM program, InCommon assembled a team of leading identity architects from the HE community to develop the community profiles for HE adopters. Understanding that campuses are not federal agencies and have different ways of doing things, the writers baked in diversity of deployment (alternative means), adoptability (removal of audit for Bronze, acceptance of common risk practice), and flexibility (intent of requirement, not specific technology). As a result, the profiles are written by Higher Ed for Higher Ed, but are comparable to the corresponding Levels of Assurance in 800-63.