

IdAM Portfolio

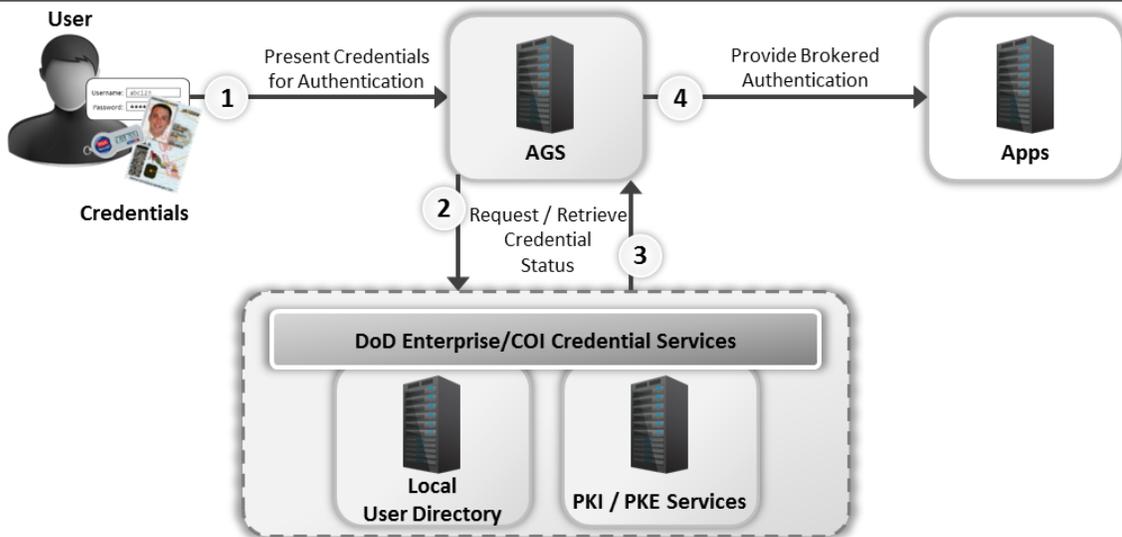
The DoD IdAM Portfolio provides digital identity, authentication, and authorization services for the DoD Enterprise. These services provide components with tools to help manage users and safeguard IT resources.

Background

The Authentication Gateway Services (AGS) is a Government deployed Commercial Off-the-Shelf (COTS) authentication middleware that provides a centralized endpoint for user authentication and propagates that authentication to applications it protects.

Why AGS?

AGS provides brokered authentication for DoD applications that do not natively support PKI authentication, allowing for compliance with USCYBERCOM Communication Task Order (CTO) 07-15 which mandates direct PK-enablement. The service also provides brokered authentication for DoD applications that require username/password authentication for non-DoD users.



To Order the Service

- Contact your DISA ESD CME team to define your requirements and become an early adopter of AGS

Rates

- Fee-for-service tailored to implementation and usage

Implementation Options

- Currently available on NIPRNet only
- Deployed at DECCs as a DISA-managed service and DoD Data Centers
- AGS will be installed in the same logical security boundary as the applications it protects

Standard Features

- The Enterprise Service will offer:
 - Identity Translation – provide a method to map the user's presented identity (CAC or username/password¹) to a format or identity suitable for the application
 - Header Injection - provide a way for a proxy to represent a consumer sending a Web request and to authenticate the consumer to an application
 - Resource request with SAML – allow a proxy to represent a consumer sending a Web request via a SAML Assertion (e.g., allowing SAML-enabled COTS solutions to act as an application)

¹ Application owners must maintain own database