Assured Identity

DISA driving anonymity out of its networks

Assured Identity is the concept of establishing and continuously validating a digital identity, then assigning attributes to that identity and strongly associating it with an individual or trusted device. DISA is addressing this initiative by prototyping hardware attestation on mobile devices and two separate prototypes of continuous multi-factor authentication (CMFA).

Assured Identity fundamental capabilities:

- Leverage native sensors on mobile devices to collect and exercise biometric and contextual factors for continuous multi-factor authentication.
- Issue and protect the Purebred derived credentials and associated private keys with hardware-based secure elements equivalent to the credential strength on Common Access Cards (CAC).
- Observe user behaviors to establish patterns and associations with network authorizations.

DISA is pursuing the development of assured identity to advance how federal agencies identify and authenticate people and devices to provide a more secure computing environment in these key areas:

Hardware Attestation	Protection of the derived credential from theft • Leaning on commercially available hardware-based secure elements to protect credential/associated private key on mobile devices similar to how DISA uses the Common Access Control (CAC) card.
Mobile CMFA	Mobile devices host a plethora of sensors and resources to collect, process, analyze and react to data of the surrounding environment. • Prototyping reliability and usability of biometric and contextual factors to continuously access, supplement, and strengthen the authentication process. Some factors being considered are: fingerprint, iris, face, voice, trusted location, proximity of other devices, and connected Wi-Fi networks.
Desktop CMFA	Common office environment relies on possessing the CAC to represent an individual's identity and has proven reliable and more secure than traditional username/password. • DISA is piloting a solution than can prevent, detect and respond to misuse of user's credentials. Pattern-based building of user profiles with machine learning through a software agent installed will capture user interaction such as keyboard use, dwell time and mouse track movement and speed.

On the Horizon

DOD replacement of the CAC - multifactor authentication along with behavior analysis and biometrics to verify identity.