xage GOVERNMENT

Remote Smart Card-based Authentication

CAC Passthrough for DoW Environments

Common access cards (CACs), YubiKeys, and other X.509-based smart cards are a type of smart card that are frequently used by the U.S. Department of War (DoW) to access highly sensitive applications. Traditionally, use of smart cards requires operators to be physically onsite to be able to present the smart card to the target system in order to access the private applications that require smart card-based authentication. This process presents significant logistical challenges and, in some cases, may significantly delay the access to critical information. Organizations need a highly secure and streamlined approach that enables operators to remotely access secured applications using their smart cards without needing to be onsite.

A Unique and Unmatched Authentication Solution

Seamless Remote Access with Smart Cards—No Onsite Presence Required

Operators can securely access mission-critical applications from a remote, private Windows workstation using their smart card—all from their local laptop—without needing to be physically onsite.

Zero Trust, Agentless, RDP-free

With Xage's Zero Trust architecture, operators can securely access private applications via a web browser using their smart card, eliminating the need for the vulnerable RDP protocol. Additionally, administrators can implement break-and-inspect capabilities for enhanced security and monitoring.

Unrivaled Industry Leadership

Xage is the only vendor providing this advanced authentication capability—offering a secure, resilient, and seamless solution that works in multicloud and hybrid environments to protect classified and unclassified Defense applications.

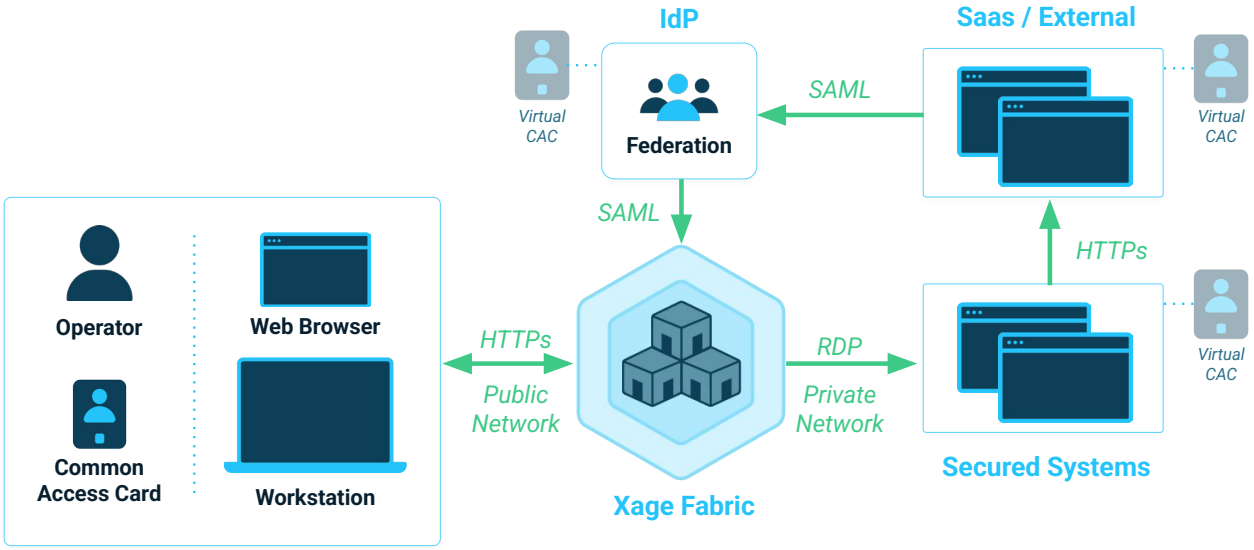
 © Xage Security | All Rights Reserved

xage GOVERNMENT

Xage Capabilities

The Xage Fabric Platform is a highly available and resilient cybersecurity mesh that enables secure access, enforces privilege control, and manages microsegmentation to protect cloud, IT, and OT environments—all without disrupting existing systems. Additionally, Xage is the industry-leading solution for operating in Denied, Degraded, Intermittent, and Limited (DDIL) environments.

Remote Smart Card-based Authentication Workflow



1. **Access Xage Fabric UI:** Authorized operators access the Xage Fabric UI from their device, laptop, or workstation.
2. **Authenticate with Xage Fabric:** Operators authenticate to Xage Fabric using valid credentials (such as a CAC or YubiKey) federated via SAML.
3. **View Available Workstations:** After successful authentication, the operator is presented with a centrally managed list of workstations they have access to, based on Zero Trust access policies implemented on the Xage Fabric.
4. **Connect to a Workstation**: The operator securely connects to one of the listed workstations through the browser-based Xage Fabric UI.
5. **Open a Browser on the Remote Workstation:** Once connected, the operator opens a browser on the remote workstation.
6. **Access Mission-Critical Applications:** The operator accesses any mission-critical web application that requires smart card authentication.
7. **Remote CAC Authentication:** Xage Fabric enables seamless authentication by securely relaying the challenge/response process from the remote workstation to the local operator's machine where the smart card is inserted. Once the PIN verification is provided locally, the authentication challenge on the remote workstation is securely completed.

xage GOVERNMENT