

Common Access Card Authentication

Overview

Kemp LoadMaster offers support for all US Federal certificate-based Identity Smart Cards including the DOD CAC (Common Access Card), PIV (Personal Identity Verification) and the TSA TWIC (Transportation Worker Identification Credential). Kemp LoadMaster integrates with the back-end PKI infrastructure and Windows Active Directory to present an integrated authentication environment for personnel accessing services using CAC.

How it works

The Edge Security Pack (ESP) feature of the Kemp LoadMaster supports integration with DoD environments leveraging CAC authentication and Active Directory application infrastructures. The LoadMaster acts on behalf of clients presenting X.509 certificates via CAC and becomes the authenticated Kerberos client for services hosted on the internal application servers.

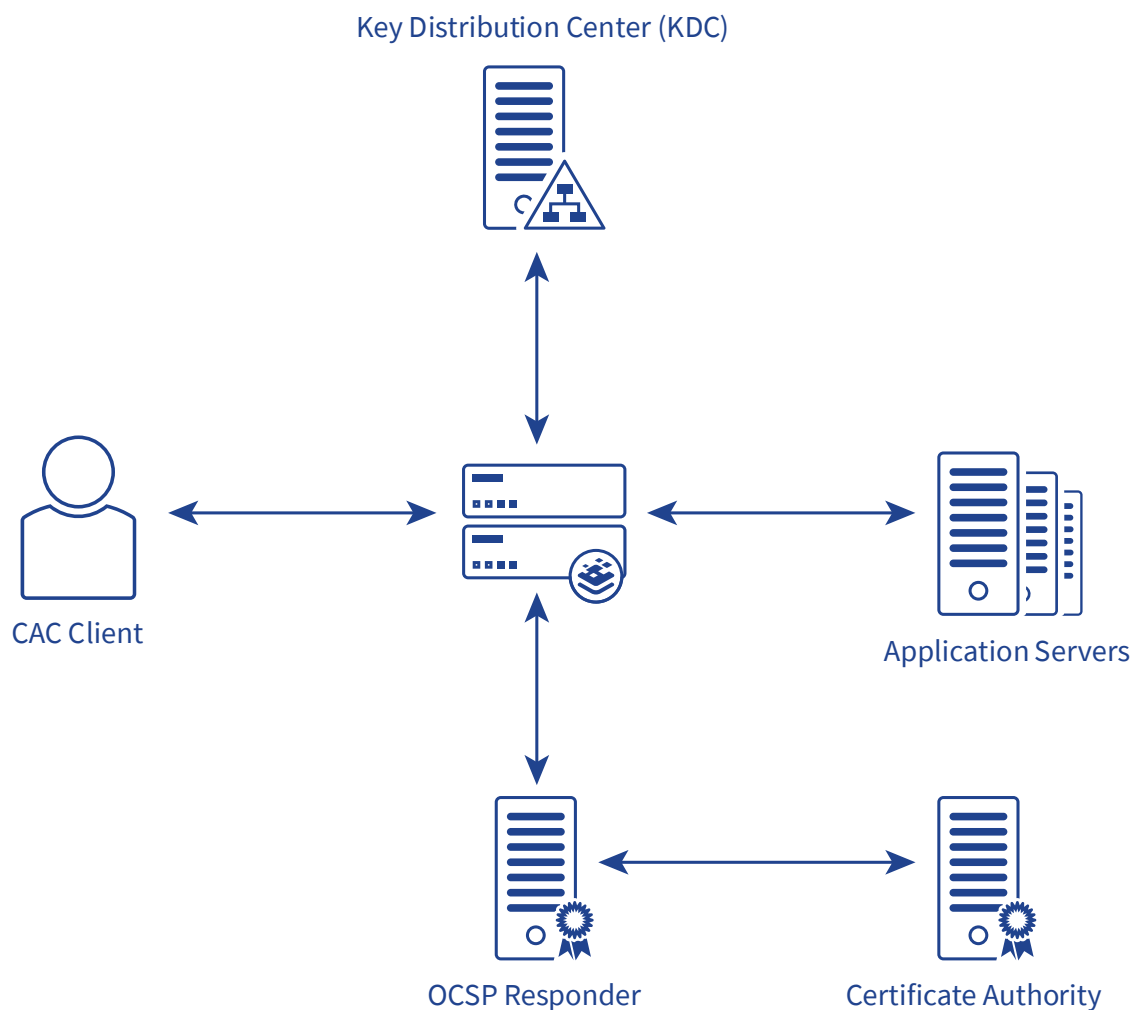


Figure 1 CAC Authentication Topology

The request for and presentation of the client certificate happens during initial SSL session establishment. There are two stages to the process of a user gaining access to an application with CAC:

- **Authentication** – occurs during SSL session establishment and entails:
 - o Verifying the certificate date
 - o Verifying revocation status via Online Certificate Status Protocol (OCSP)
 - o Verifying the full chain to the Certificate Authority (CA)

- **Authorization** – occurs after SSL session establishment and the matching of the certificate Subject Alternative Name (SAN) against the User Principal Name (UPN) of the appropriate principal in Active Directory.

Features

- Certificate based administrative account access to LoadMaster
- Certificate based authentication for load balanced applications
- LoadMaster can join a Kerberos Active Directory domain
- LoadMaster acts as a Kerberos service principal
- Support for Kerberos Constrained Delegation (KCD)
- Mapping of x.509v3 certificate Subject Alternative Name (SAN) to Active Directory account
- Full integration with OCSP for certificate validation
- NTPv3 (Network Time Protocol) security and authentication
- SNMPv3 security and authentication
- FIPS 140-2 validated cryptography

About Kemp LoadMaster

Kemp LoadMaster is used across defense, intelligence, and federal civilian agencies to ensure application availability, security and performance. LoadMaster is available on a range of platforms including physical appliance, virtual appliance, bare-metal appliances and public/private cloud services. LoadMaster appliances include application and global load balancing, authentication proxy, application proxy, application single sign in, and web application firewall services. Kemp LoadMaster is listed on the Department of Defense Information Network Approved Products List (DoDIN APL).

About Kemp Technologies

With over 25,000 worldwide clients and a broad customer base within the US Department of Defense, the Federal Civilian Agencies and the US Intelligence Community, Kemp Technologies is the leader in price/performance value for load balancers and application delivery controllers in the government industry.