HP Common Access Card Solution

White paper

The HP Common Access Card solution helps government agencies optimize their IT infrastructure by supporting capture and output of digital content with advanced security features.

Abstract:

The HP Common Access Card Solution provides authentication employing a smart card reader at the HP MFP device. The solution was developed in response to increased security requirements. The solution uses public key infrastructure (PKI) encryption and Kerberos authentication to provide authenticated, digitally signed e-mail and scan-to-folder sessions.

1 Introduction

The Common Access Card (CAC) is a smart card issued as standard identification for U.S. DoD personnel and contractors. The CAC is used as a general access and identification card as well as for authentication to enable access to computers and networks. The HP Common Access Card Solution extends the CAC to HP multifunction product (MFP) devices. Users are able to authenticate at the MFP by inserting their CAC into an attached card reader and entering a PIN, which is followed by certificate validation, Kerberos authentication to the network, and Active Directory data retrieval. After their card is accepted, the user can send digitally signed e-mail or scan documents to folders. Users end their session by removing their CAC card from the device card reader.

2 Methodology

Using the CAC on LaserJet MFPs must be configured by an administrator. This can be accomplished in five steps:

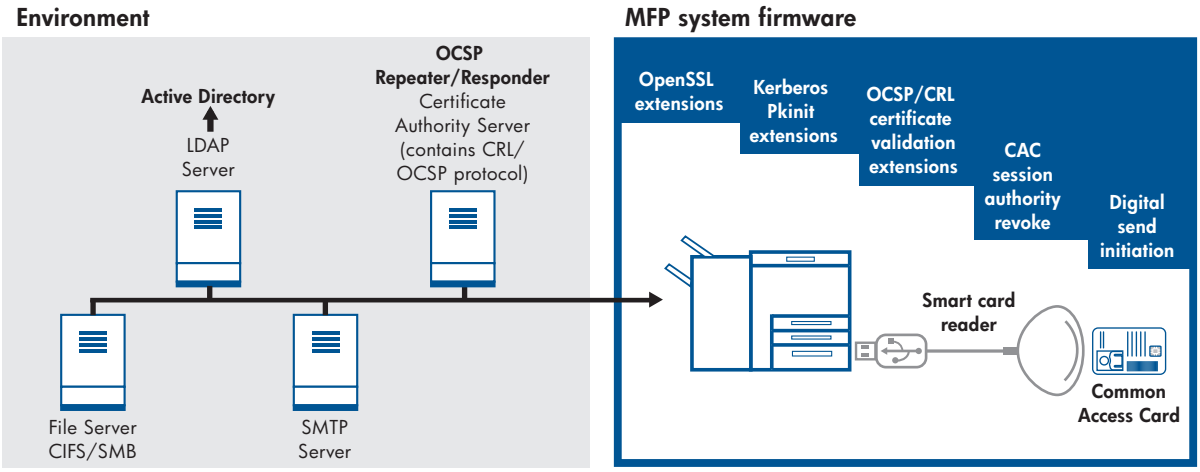
- Setup CAC authentication as an authentication agent in Authentication Manager
- Configure DNS appropriately for the network
- Load the correct certificates
- Specify the OCSP/CRL location(s)
- Choose whether or not to digitally sign the e-mails sent

The CAC session begins when the user inserts his CAC card into the HP MFP card reader.

- The card is validated against the PIN entered by the user.
- The certificate stored on the card is checked for a valid expiration date, then against the certificate authority server to verify that it has not been revoked.
  - Using OCSP or CRL
- The CAC certificate is used for public key infrastructure Kerberos authentication to obtain and use a Kerberos ticket and session key.
- The Kerberos session key is used to obtain a client/server ticket to access Active Directory using LDAP to obtain the user's e-mail attributes and folder permissions.
- If configured properly, the CAC certificate is used to digitally sign outgoing e-mail.
- For send-to-folder, the Kerberos ticket is used to authenticate to CIFS.

The session ends when the user removes the CAC from the card reader.

Figure 2. Network topology



3 Topology

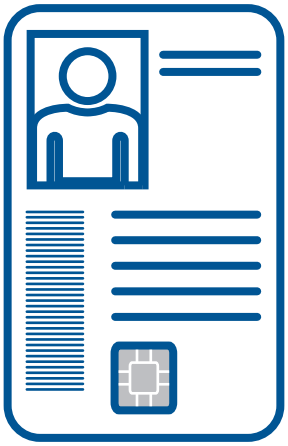
See Figure 2.

4 Session sequence

The following represents the sequence of events for a user's CAC session:

- User selects CAC Authentication Agent at the HP MFP.
- User is prompted to insert CAC.
- User inserts CAC into attached card reader.
- CAC is validated by the following steps:
  - User is prompted to enter PIN.
  - PIN is validated.
  - Certificate is read from CAC.
  - Verification that the certificate is not revoked is checked via CRL/OCSP.
- Kerberos Pkinit is called with certificate.
- Kerberos Pkinit returns encrypted ticket and session key.
- CAC private key—which never leaves the card—decrypts the Kerberos session key and ticket.
- Kerberos session ticket is used to call LDAP Active Directory lookup.
- Active Directory user information is returned.
- User selects send to e-mail or scan to network folder.
- Active Directory user information is applied to send to e-mail or scan to network folder.
- User takes the CAC out of the reader, ending the session.

Figure 1. Example Common Access Card



To learn more, visit www.hp.com

4AA1-1800ENUC Rev. 1, July 2007