White Paper

Contents

HP MFP Smartcard Authenication Solution

Abstract:

The HP Common Access Card Solution provides authentication for Department of Defense (DOD) Common Access Cards (CAC) employing a Smart Card reader at the HP MFP device. The solution is Homeland Security Presidential Directive 12 (HSPD-12) compliant, using Public Key Infrastructure (PKI) encryption and Kerberos authentication to provide authenticated E-mail and Scan to Folder sessions.

.

Notice:

Neither HP, nor any of its subsidiaries, shall be liable for technical or editorial errors or omissions contained herein. The information in this publication is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

1 Introduction

The Common Access Card (CAC) is a United States Department of Defense (DoD) smartcard issued as standard identification for military personnel and contractor personnel. The CAC is used as a general identification card as well as for authentication to enable access to DoD computers and networks. The HP Common Access Card Solution extends the CAC to the HP MFP devices. Users are able to authenticate at the MFP by inserting their CAC into an attached card reader and entering their PIN. After their card is accepted, the user can send E-mail or Scan documents to folders. The user ends their session by removing their CAC card from the device's card reader.

Figure 1 – Example DoD Common Access Card

2 Methodology

The CAC session begins when the user inserts their 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on the card is checked for a valid expiration date, then against the Certificate Authority server that it has not been revoked.
- The CAC certificate is used for Private Key-Public key authentication to establish and decrypt a Kerberos session key.
- The 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.

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

3 Topology

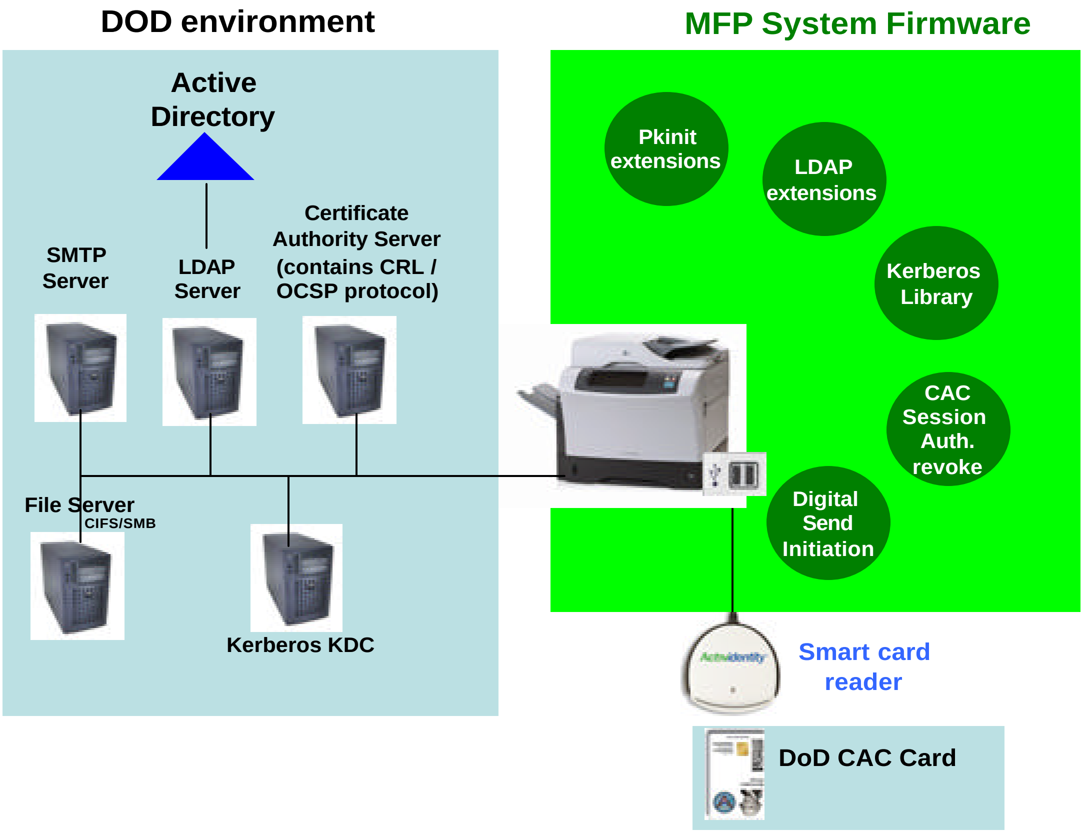

Figure 2 – Network Topology

4 Session Sequence

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

- User selects feature using "DoD CAC" Authentication Agent at the HP MFP
- User is prompted to insert CAC
- User inserts CAC into attached card reader
- CAC is validated – accomplished by the following steps
  - User is prompted to enter PIN
  - PIN is validated
  - Certificate is read from CAC
  - Verify that certificate is not revoked by checking CRL/OCSP
- Call Kerberos Pkinit with certificate
- Kerberos Pkinit returns encrypted tickets
- Kerberos Pkinit decrypts tickets with private key from CAC
- Kerberos Session Ticket used to call LDAP Active Directory lookup
- Active Directory user information returned
- User selects Send to e-mail or Scan to network folder
- Active Directory user information applied to Send to e-mail or Scan to network folder
- User takes CAC out of reader, ending the session
- Certificate temporarily stored on device is securely erased