



ADmitMac[®] for PIV v2.0

A Secure Integration of FIPS 201 PIV Cards for the Apple Macintosh

ADmitMac for PIV (ADPIV) securely integrates U.S. Government FIPS 201 Personal Identity Verification (PIV) with Apple Macintosh computers. ADPIV provides a single sign-on environment, verifying a PIV card against a centralized network authority. ADPIV obtains Kerberos tickets using PIV certificates, makes these tickets available to “Kerberized” applications, locks the computer upon removal of a PIV card, and protects the computer from unauthorized use when it wakes from sleep.

This version enables E-mail user access to Exchange using Entourage 2004 or OWA without needing passwords. ADPIV takes care of authentication to Exchange servers. Entourage 2008 users can authenticate using a PIV card.

Security goes far beyond a simple verification of the PIN against the PIV card. With ADPIV, the card itself is challenged to ensure that neither the card nor the privileges granted the user have been revoked.

When a PIV card is inserted into a Macintosh, ADPIV changes the normal login screen and challenges the user to enter their PIV PIN authorization. Upon verification of the user’s PIN, ADPIV then obtains the proper network credentials from the Active Directory. ADPIV includes its own PKINIT (Public Key Cryptography for Initial Authentication in Kerberos) that enables this secure integration.

ADmitMac for PIV Advantages:

- + No passwords needed - single sign-on environment using Kerberos PKINIT. Never requires the use of passwords to login or to mount network volumes
- + Adds Exchange/Entourage support for users that don’t have passwords
- + Never requires the use of passwords to login or to mount network volumes
- + Automatically locks the computer upon removal of the PIV, and when waking from sleep
- + Screen-saver integrated with PIV card security
- + Conforms to FIPS 201, Meets Department of Defense Public Key Infrastructure (PKI) requirements
- + Works with custom OCSP Responder configurations

Standard Features:

- + Administrators can easily manage Macintosh computers in their Microsoft Windows domain
- + Enhanced security including NTLMv2 and SMB Signing
- + Provides bidirectional file and printer sharing
- + Full support of Dfs – Distributed File System
- + Integrates with Microsoft’s NTFS file system for storage of both file forks in single file (avoids ._ files)
- + Integrates with Apple’s Workgroup Manager to fully support Managed Desktop (MCX) settings with no schema changes



Advanced Features:

- ✦ Exchange Gateway to support Entourage users without using passwords.
- ✦ Allows for user login with home directories located on the Macintosh client's local hard disk or on the network
- ✦ Automatically configures Macintosh for use with Kerberos
- ✦ Fully signed and sealed (encrypted) LDAP connections prevent disclosure of user's personal information and prevent man-in-the-middle attacks
- ✦ Support for bidirectional SMB-signed connections, NTLM SSP, and NTLMv2
- ✦ Expired and reset passwords are handled correctly when users log in to the Macintosh desktop
- ✦ Caches user credentials for mobile user access when not connected to the network
- ✦ Supports browsing for published shares
- ✦ Provides access to shared printers by browsing the list of printers published in a domain, or manually
- ✦ Kerberos credentials are set up automatically when a user logs in.
- ✦ Support for cross-realm trusts with MIT Kerberos. Support for multiple domains within a forest
- ✦ Administrators can choose domain search paths for users, groups, published printers and shares to limit searches to specific organizational units
- ✦ Administrators can give local administrative privileges to domain members based on username or domain group
- ✦ Administrators can give administrative privileges to the user specified as the Macintosh's manager in the domain computer records
- ✦ Supports Mac OS X Server service principal names
- ✦ Home directories may be located in a path where the user does not have access to the parent folders
- ✦ Administrators can utilize Apple's Workgroup Manager MCX settings
- ✦ ADmitMac Deployment utility creates custom ADmitMac install packages for multi-computer installations
- ✦ Dynamic DNS registration support: IP addresses registered with DNS using computer account name
- ✦ AD Commander allows administrators to edit Active Directory users and groups from Macintosh
- ✦ Logs all security related events related to PIV authentication.

Conforms with Microsoft SMB/CIFS standards, including use of TCP port 445, NetBIOS-less communication and to the following specifications:

RFC 4556 Public Key Cryptography for Initial Authentication in Kerberos (PKINIT); RFC 4120 The Kerberos Network Authentication Service (V5); RFC 1777 Lightweight Directory Access Protocol (LDAP); RFC 2743 Generic Security Service Application Program Interface Version 2; RFC 1964 The Kerberos Version 5 GSS-API Mechanism; RFC 2222 Simple Authentication and Security Layer; RFC 3244 Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols; RFC 1001,1002 Protocol standard for a NetBIOS service on a TCP/UDP transport; Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements, Version 1.0, 13 July 2000; Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Interface Specification, Version 1.2 10 August 2000

ADmitMac is a registered trademark of Thursby Software Systems, Inc.
Apple and Macintosh are registered trademarks of Apple Computer, Inc.
All other trademarks are the property of their respective owners.

Thursby Software Systems, Inc.

5840 W. Interstate 20
Arlington, Texas 76017 U.S.A.

www.thursby.com
e-mail: sales@thursby.com
Telephone: 817-478-5070