

Software Product Description

ADmitMac® PKI v3.1

Macintosh Public Key Infrastructure Client for Microsoft Active Directory



OVERVIEW

ADmitMac PKI (Public Key Infrastructure) v3.1 combines the features of ADmitMac for CAC and ADmitMac for PIV. It allows enterprises that rely on PKI and smart card technology to incorporate Macintosh clients running Mac OS X 10.5 Leopard or Mac OS X 10.6 Snow Leopard. The Macintosh clients can take advantage of all the directory services provided by Active Directory, Group Policy and Apple's Workgroup Manager. As a result, administrators manage their domain users in a consistent way without regard for what kind of computer they use. ADmitMac PKI lets users log into a Macintosh with their smart card based domain credentials and then have access to files in their home directories wherever those directories might physically be. True single sign-on is accomplished using Kerberos PKINIT.

ADmitMac PKI is tailored for multi-user, multi-computer scenarios with administrator-defined network security. Kerberos is used to provide secure directory access, thus reducing the risk of unwanted disclosure, spoofing, and man-in-the-middle attacks. ADmitMac PKI works with domains configured using Microsoft's Highly Secure (HISEC) security templates, automatically configures the Macintosh to use Kerberos, obtains the necessary security keys from the domain and performs mutual authentication requiring the server to prove its identity. ADmitMac PKI will cache successful user login information for later use. This allows notebook or mobile users to continue using their domain account to log in when their Macintosh is not connected to the domain.

In addition to Workgroup Manager support and the AD Commander application, ADmitMac PKI 3.1 includes the ability to use Windows Group Policy to manage Macintosh computers from Active Directory. The Workgroup Manager plug-in allows administrators to implement Apple's Mac OS X desktop management (MCX) settings on the Active Directory domain, while AD Commander allows administrators to manage Active Directory users and groups from a Macintosh. With Group Policy and ADmitMac PKI's new ADM plugins, Windows administrators can manage Macintosh operating system components and applications in Active Directory using the Group Policy Management console.

BASIC ADmitMac PKI FEATURES

- Single sign-on environment using smart cards and Kerberos PKINIT. Never requires the use of passwords to login or to mount network volumes.
- Automatically locks the computer upon removal of a smart card, and when waking from sleep.
- Screen-saver integrated with smart card security.
- Supports U.S. PIV and CAC. Meets Department of Defense Public Key Infrastructure (PKI) requirements.
- Works with custom OCSP Responder configurations.
- Administrators can easily manage Macintosh computers in their Microsoft Windows domain without special training.
- Installs on the Macintosh with no Active Directory schema changes required.
- Provides bidirectional file and printer sharing.
- Supports Windows login security restrictions. Allows users to easily change passwords.
- Support for Distributed File Sharing (Dfs) - home directories can be mounted using Dfs. Shares on the Mac support Dfs as well.
- Supports NTFS file format - does not create "dot-underscore" files. Supports Windows access control lists.
- Supports long share names compatible with Windows 2003 and 2008 Server.
- Preserves users' custom desktop and documents no matter which computer they log on to.
- Offers complete interoperability with Services for Macintosh.
- Users can mount shared folders to which they are allowed access via the ADmitMac Browser.
- Requires an Active Directory network based on Microsoft Server 2003 or 2008.

ADVANCED FEATURES



- † Allows for user login with home directories located on the Macintosh client's local hard disk.
 - † Automatically configures Macintosh for use with Kerberos. Kerberos configuration files are generated automatically.
 - † 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.
 - † Print client can access shared printers. Printers may be configured by browsing the list of printers published in a domain, or entered manually.
 - † Kerberos credentials are set up automatically when a user logs in. No changes to `/etc/authorization` are required.
 - † 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 choose to give local administrative privileges to domain members based on their username or domain group membership.
 - † 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. MCX settings are now replicated to each Macintosh so they are always available even when the Macintosh is disconnected from the network.
- † ADmitMac Deployment utility creates custom ADmitMac install packages for multi-computer installations. Custom install packages support automatic installation mode where Macintosh clients are fully configured and joined to a domain without requiring human interaction.
 - † Dynamic DNS registration support: the Mac will register its IP addresses with DNS using its computer account name.
 - † Supports extended attributes.
 - † AD Commander tool allows administrators to edit Active Directory users and groups as if you were using AD Administrator Tools.
 - † Windows administrators can manage Mac operating system components and applications in Active Directory using Group Policy.
 - † Conforms with Microsoft SMB/CIFS
 - † RFCs:
 - 1001,1002 Protocol standard for a NetBIOS service on a TCP/UDP transport
 - 4556 Public Key Cryptography for Initial Authentication in Kerberos (PKINIT);
 - 4120 The Kerberos Network Authentication Service (V5);
 - 1777 Lightweight Directory Access Protocol (LDAP)
 - 2743 Generic Security Service Application Program Interface Version 2
 - 1964 The Kerberos Version 5 GSS-API Mechanism
 - 2222 Simple Authentication and Security Layer
 - 3244 Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols
 - † U.S. Government:
 - 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

Thursby Software Systems, Inc.
5840 W. Interstate 20 - Suite 160
Arlington, TX 76017-1069 U.S.A.

www.thursby.com
e-mail: sales@thursby.com
Telephone: +1 (817) 478-5070

ADmitMac PKI, ADmitMac and DAVE are registered trademarks of Thursby Software Systems, Inc.
Apple and Macintosh are registered trademarks and Mac is a trademark of Apple, Inc.
Microsoft, Windows, Windows 2000, Windows XP, Windows Vista, Windows 7, Server 2003, Server 2008 and Active Directory are registered trademarks of Microsoft Corporation.
All other trademarks are the property of their respective owners.