

Identity Management for Network Environments

Protecting sensitive data inside of networks with OpenLDAP



Described Version: OpenLDAP 2.3.34

Also applicable for: OpenLDAP 2.3.32

Target platforms: Windows Vista/XP/2000, Linux

MARX hardware: CrypToken M2048 / MX2048 JCOP



Secure Network Resource Management!

The main benefit of using LDAP is that information for an entire organization can be consolidated into a central repository. For example, rather than managing user lists for each group within an organization, LDAP can be used as a central directory accessible from anywhere on the network.

Because LDAP supports Secure Sockets Layer (SSL) and Transport Layer Security (TLS), sensitive data can be protected from prying eyes. Due to a well-defined client Application Programming Interface (API) supported for LDAP, the number of LDAP-enabled applications is numerous, continuously increasing in quantity and quality.

- **Mobile and secure certificate storage**
- **Enhanced security with two-factor authentication**
- **Authentication with X.509 certificates**
- **Safe against phishing and password theft**

Table of Contents

- 1. Identity and Access Management with LDAP directories.....2
- 2. CrypToken: cryptographic hardware for LDAP-based security solutions.....3

1. Identity and Access Management with LDAP directories

The **Lightweight Directory Access Protocol** (LDAP) is a set of open protocols used to access centrally stored information over a network. Its current version is LDAPv3 which is specified in a series of IETF Standard Track RFCs as detailed in RFC 4510 (<http://tools.ietf.org/html/rfc4510>).

LDAP is based on the X.500 standard for directory sharing, but is less complicated and resource-intensive. Like X.500, LDAP organizes information in a hierarchical manner using directories. These directories can store a variety of information and are often used for storing authentication related data like user lists, groups, certificates, security policies and privileges in various Identity Management and Access solutions.

The main benefit of using LDAP is that information for an entire organization can be consolidated into a central repository. For example, rather than managing user lists for each group within an organization, LDAP can be used as a central directory accessible from anywhere on the network. And because LDAP supports Secure Sockets Layer (SSL) and Transport Layer Security (TLS), sensitive data can be protected from prying eyes. Due to a well-defined client Application Programming Interface (API) supported for LDAP, the number of LDAP-enabled applications is numerous, continuously increasing in quantity and quality.

LDAP directories commonly form the basis of Identity Management and Access solutions and are tightly integrated with them. Out of the several directory service providers, two market leaders are:

Novell **eDirectory**

<http://www.novell.com/products/edirectory/overview.html>

Microsoft **Active Directory**

<http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx>

Both Active Directory and eDirectory support a range of authentication options, from simple password submission (including SHA-1 and MD-5 password hashing) up to PKI based, involving biometrics, smart cards, tokens, etc.

Active Directory relies on Microsoft CryptoAPI for smart card-based strong authentication. Smart card or USB token vendors provide Cryptographic Service Providers (CSP) for their hardware to be used in the Microsoft Crypto environment. Microsoft certifies and digitally signs those CSPs (CSPs do not work in Windows Server 2000/2003 unless they have been digitally signed by Microsoft). Smart cards and USB tokens can be directly used for Active Directory strong authentication after that.

See “**Active Directory service and MARX CryptToken**” for more details on using CryptTokens for Active Directory based security solutions.

On the other hand Novell eDirectory is more flexible and provides support for both PC/SC (CSPs on Windows platforms) and PKCS#11 interfaces to be used for smart card-based authentication. Other prominent vendors including Oracle, Sun, and IBM also provide their LDAP Directory Services for centralized identity, access and authentication management. Strong authentication in their solutions is based on RSA Labs’ Public Key Cryptographic Standards (PKCS#11) and Microsoft CryptoAPI (CSPs), the two most widely adopted cryptographic interfaces.

2. CrypToken: cryptographic hardware for LDAP-based security solutions

MARX® CryptoTech LP provides a comprehensive support for Microsoft Windows Cryptographic Services and RSA Labs' Public Key Cryptographic Standards with its CrypToken product series. Signed by Microsoft Cryptographic Service Providers allow direct use of CrypTokens for X.509 certificates secure storage and manipulation, strong authentication, digital signatures and data encryption in Microsoft Active Directory (within Microsoft Identity & Access platform) or any third party LDAP-based identity management solutions for Windows platform.

Comprehensive support of PKCS#11 makes MARX CrypTokens straightforwardly usable in LDAP Directory Services of other vendors such as: Novell, Oracle, Sun, IBM, and many others.

MARX offers two models of CrypToken: CrypToken M2048 (with MULTOS operating system) and CrypToken MX2048 (for JavaCard) 2000. Due to Microsoft CryptoAPI comprehensive support both of them can be straightforwardly used in Active Directory-based security solutions.

The CrypToken is equipped with SafeSign middleware. SafeSign is a powerful and cost effective Public Key middleware solution for USB Tokens and Smart Cards.

It's our business to protect yours

The CrypToken is ideal for...

- Online Banking: Secure Internet banking and financial transactions.
- VPN: Virtual Private Network control from remote locations.
- eGovernment: Access control to confidential information.
- Email: Encryption and digital signature of confidential emails.
- eCommerce: Secure B2B/B2C authentication.
- RAS and network logon: Access for authorized users only.
- WebSecurity: Secure web portal and internet and intranet identification.
- DataSecurity: Encryption of sensitive information.



Get your CrypToken Evaluation Kit:

www.cryptoken.com/eval
+49(0)8403 9295-14

Comparison table CrypToken M2048 and CrypToken MX2048

Features	M2048	MX2048
Token operating system	MULTOS	JavaCard
Operation	Driverless, if CCID OS used	
Certification smart card chip	EAL 5+ EMV, ISO7816	EAL 4+, EMV, ISO7816, JavaCard 2.3.1, GlobalPlatform 2.1.1
Controller chip certification	WHQL (Microsoft), HBCI (Home Banking Computer Interface), EMV, ISO7816	
Smart card chip	Infineon SLE66xx series	SmartMX/JCOP21
Cryptographic standards supported	PKCS#11v2.01, MS-CAPI	
Operating systems supported	Windows Vista/XP/2000, Linux, MacOS X	Windows Vista/XP/2000, Linux, MacOS X
Memory (total)	64 KByte	72 KByte
Casing & LED	Metal Designer Case, LED (duo color green/red, for „stand by/activity“), eye for key ring/lanyard	
Electrical certifications	FCC, CE, RWTUEV	FCC, CE, RWTUEV
Dimensions	0.51" x 0.32" x 1.38" (13 x 8 x 35 mm)	0.51" x 0.32" x 1.38" (13 x 8 x 35 mm)
Weight	0.326 oz (9,25g)	0.326 oz (9,25g)

CrypToken certifications



All trademarks used in this document are property of their respective owners.

MARX CryptoTech Germany

Vohburger Strasse 68
D-85104 Wackerstein
Phone: +49 (0) 8403 9295-14
Fax: +49 (0) 8403 929529
contact@cryptoken.com

MARX CryptoTech LP

4485 Tench Road #310
Suwanee, GA 30024 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 770 904 3893
info@cryptotech.com

www.cryptoken.com