NMAS provides **flexible and secure**
NDS authentication

Novell Modular Authentication Service

Novell®

TABLE OF CONTENTS

NMAS PROVIDES FLEXIBLE AND SECURE NDS AUTHENTICATION

As Novell® continues to enhance and expand the services and functionality of its leading enterprise directory, Novell Directory Services® (NDS®), the methods for authenticating to NDS are also being enhanced and expanded. Novell Modular Authentication Service (NMAS, pronounced en-mass) is a new dual offering of authentication products that let users authenticate to NDS through different and multiple authentication methods, thus providing increased flexibility and security to network directory resources.

USER AUTHENTICATION DEFINED

When a user authenticates to a private or public computer network (including the Internet), the user is simply providing some sort of confirmation that he or she is who he or she claims to be. Authentication is most commonly done through the use of login passwords. The password serves to authenticate the name or identifier (ID) of the user logging in to the system.

STANDARD NDS AUTHENTICATION

Before the introduction of NMAS, NDS used a very secure two-process mutual authentication method, known as "password challenge response" user authentication. The first process involved user login where a password and nonce (identifiers that are used only once) values generated by both the client and server were hashed twice using two different hash algorithms and later encrypted using an RSA* encryption algorithm. The second process involved background authentication to an NDS server.

EXTENSIBLE NDS AUTHENTICATION THROUGH NMAS

While Novell makes a concerted effort to make its password challenge response authentication method secure, many NDS-installed organizations have determined that password authentication is insufficient for their security needs. Such organizations have decided to expand their network authentication from requiring the network user to authenticate via "something you know" (for example, a password) to "something you have" (for example, a smart card), or "something that you are" (for example, a fingerprint).

The NMAS framework is extensible in that it allows for these and other forms of alternative authentication methods. NMAS-supported authentication methods include both authentication modules developed by Novell as well as by third-parties. A summary of each of these authentication methods follows.

SIMPLE PASSWORD/HASH AUTHENTICATION

With NMAS, Novell provides login methods common with LDAP, Internet browsers, and other directories. These include cleartext, SHA-1, and MD-5 login methods.

Cleartext

Cleartext (or plaintext) authentication is a process of sending a password over the wire in an unencrypted form. Aside from no authentication at all, from a security standpoint, this is the lowest form of user authentication. Because there is no encryption process, plaintext authentication is normally quite fast. This authentication method is included in NMAS to provide faster authentication in networks requiring less security, as well as to provide interoperability with systems that use cleartext authentication (for example, FTP/Telnet and POP3 e-mail).

SHA-1

Developed and published by the National Institute of Standards and Technology (NIST) in 1993 and 1995, the secure hash algorithm (SHA-1) is a popular hash algorithm for network authentication based on a hash algorithm. A hash (or message digest) is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. In terms of security, SHA-1/MD5 authentication is more secure than cleartext because the password is altered when it travels across the network. Authentication is relatively fast because it is easy to compute a shorter hashed value.

MD-5

Developed by Ron Rivest at MIT, this message-digest algorithm takes a message of arbitrary length and produces a 128-bit message digest (or hash) output. MD-5 was, at one time, the most widely used secure hash algorithm.

STANDARD NDS PASSWORD AUTHENTICATION

As discussed previously, this is the password challenge response authentication method that uses different hash algorithms and, beginning with the release of NMAS, the DES (Data Encryption Standard) algorithm. The multiple cyphering techniques provide a very secure password authentication method. Because of the increased security it offers, the standard NDS password authentication is slower than cleartext or SHA-1/MD5 authentication.

PHYSICAL DEVICE AUTHENTICATION

Another way that a user can authenticate is through the use of a physical object that the user carries with himself or herself and proves his or her identity (“something you have”) and is granted access accordingly. Third-party authentication developers have written authentication modules for two types of physical devices: smart cards and tokens.

A smart card is a plastic card, about the size of a credit card, that includes an embedded microchip that can store data and perform cryptographic functions. Depending on what is stored on the microchip, a smart card can be used for a variety of tasks. With NMAS, a smart card can be used to establish an identity when authenticating to NDS. The ActivCard* Gold* smart card for example, lets a user prove his or her identity by using his or her private key and associated X.509 v3 user certificate that is stored on the smart card.

With Novell’s Certificate Server 2.0 product that is shipped with NMAS, a network administrator has a powerful PKI (Public Key Infrastructure) where the administrator can issue X.509 v3 user certificates for, among other things, NDS authentication.

A token is a hand-held hardware device that generates a one-time password to authenticate its owner. Token authentication systems are based on one of two alternative schemes: challenge-response and time-synchronous authentication.

With the challenge-response approach, the user logs in to an authentication server, which then issues a prompt for a personal identification number (PIN) or a user ID. The user provides the PIN or ID to the server, which then issues a “challenge”—a random number that appears on the user's workstation. The user enters that challenge number into the token, which then encrypts the challenge with the user’s encryption key and displays a response. The user types in this response and sends it to the authentication server.

While the user is obtaining a response from the token, the authentication server calculates what the appropriate response should be based

on its database of user keys. When the server receives the user's response, it compares that response with the one it has calculated. If the two responses match, the user is authenticated to the network. If they don't match, access is denied.

Vasco Data Security* provides a module for NDS authentication using its Digipass* token.

RSA Security* uses a time-synchronous authentication scheme. RSA SecurID* is a two-factor authentication solution requiring a PIN that the user knows, and an RSA SecurID authenticator, which the user has. RSA SecurID authenticators generate a one-time passcode every sixty seconds. The combination of user PIN and current authenticator code is valid only for that particular user at that one moment in time. The RSA ACE/Server security software protecting the network takes just seconds to verify the code and grant access.

RSA Security Inc. provides a module for NDS authentication using RSA SecurID authenticators along with RSA ACE/Server* security software.

BIOMETRIC AUTHENTICATION

Another authentication technique supported by NDS is biometric authentication. Biometrics is the science and technology of measuring and statistically analyzing human body characteristics ("something you are"). Biometric authentication can be classified into two groups: static biometric authentication and dynamic biometric authentication.

Static biometric authentication captures and verifies physiological characteristics linked to the individual. Common static biometric characteristics include fingerprints, eye retinas and irises, and facial features.

Dynamic biometric authentication captures and verifies behavioral characteristics of an individual. Common dynamic biometric characteristics include voice or handwriting.

Biometric authentication requires readers or scanning devices, software that converts the scanned information into digital form, and, wherever the data is to be analyzed, a database or directory that stores the biometric data for comparison with entered biometric data. In converting the biometric input, the software identifies specific points of data as match points. The match points are processed using analgorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Identicator*, a division of Identix*, provides a module for NDS authentication using its BioLogon* 2.0 fingerprint authentication software.

SAFLINK Corp.* provides three modules for NDS authentication using licensed biometric authentication technology for facial, fingerprint, and voice authentication.

CONSOLEONE MANAGEMENT

NMAS is managed through an easy-to-install ConsoleOne™ snap-in module. ConsoleOne is the Java* authored, GUI-based, NDS management framework for managing NDS. Specific ConsoleOne property pages let the administrator manage authentication methods, the sequence of those methods, and the security grade associated with those methods. Each of these management tasks is explained further below.

MANAGING AUTHENTICATION METHODS

During the installation of the snap-in module, NMAS extends the NDS schema and creates new objects in the NDS tree's Security container.

These new objects are the Authorized Login Methods container and Login Policy objects. All authentication methods are stored and managed in the Authorized Login Methods container.

By default, NMAS installs the standard NDS password authentication method. Additional authentication methods can be installed using a wizard launched from the Authorized Login Methods container using the Create New Object option.

MANAGING AUTHENTICATION SEQUENCES

Assigning how a user authenticates using NMAS is done by defining a login sequence and then enrolling a user with a method (e.g., password, token, biometric, etc.) Sequences incorporate one or more authentication methods and are stored in the Login Policy object in the Security container. A sequence includes the methods and the order in which those methods execute during user authentication.

For example, suppose your organization implements a login policy that requires users to log in using "something they are" and "something they know." As the administrator, you decide to require each user to authenticate using the Identicator BioLogon method, along with a SHA-1 password method. You would first decide the sequence of login prompts (Identicator prompt first followed by SHA-1 password or vice versa) and then create the sequence in the Login Sequences property page.

The NMAS framework lets administrators easily chain both Novell and third-party authentication methods as part of a login sequence. No collaborative engineering work between different companies is needed. The NMAS framework does the collaboration. This makes it possible to create a sequence using, for example, the Identicator fingerprint reader, a Vasco token, and a standard NDS password.

GRADED AUTHENTICATION

This powerful feature lets administrators determine a scale or grade of the authentication methods supported and grant access rights accordingly. For example, the organization's security policy might specify that a biometric is a stronger form of authentication than a password, and a smart card is a stronger form of authentication than a biometric (this point is certainly debatable, and Novell makes no claims as to the superiority of one authentication method over another). As a result, a user successfully authenticated with a biometric might receive a very wide set of access rights because the administrator has greater confidence in that form of authentication and is more assured that the user is not an intruder. Conversely, a user authenticating to the network with a password might be granted a limited set of access rights. This allows the administration of network access rights to be more finely controlled through authentication by requiring stronger forms of authentication from those users who need access to highly sensitive information and/or wider access.

NDS PARTITION AND VOLUME LABELS

Graded authentication lets network administrators assign security labels to NDS partitions and volumes based on the number and type of login factors deemed necessary to enable access to these partitions and volumes. For example, an administrator might assign a Biometric & Token label to a NetWare® volume and subsequently create a login sequence that would include both a biometric and token authentication method.

NMAS lets administrators assign any one of the following labels to NDS volumes and partitions:

- BIOMETRIC & PASSWORD & TOKEN
- BIOMETRIC & PASSWORD
- BIOMETRIC & TOKEN
- PASSWORD & TOKEN
- BIOMETRIC
- PASSWORD
- TOKEN
- LOGGED IN

The access requirements associated with each of these labels are self-evident, except perhaps with the access requirements of the Logged In label, which enables access without requiring the use of a specific NMAS login method. All users who have authenticated to NDS have at a minimum, read-only rights to any partition and volume labeled Logged In. All NDS partitions and volumes have the Logged In label by default, so an administrator must label only those partitions and volumes requiring restricted access.

CLEARANCE LEVEL ASSIGNMENTS

Enforcing user access to labeled NDS volumes and partitions is done through assigning clearance levels to users. At the discretion of the network administrator, an NDS User object can be assigned one or many clearance levels. A user's access is dependent on both the label of the NDS volume or partition and the clearance the user has when logging in.

No matter what method a user uses to log in, he or she cannot access volumes and partitions with similar-method security labels unless he or she has been granted clearance that allows such access.

The clearance level names are identical to the security label names. That is, an administrator can assign User objects clearance levels such as Biometric & Password & Token, Biometric & Password, Biometric & Token, and so on down the list shown above. In addition, administrators can assign a Multilevel Administration clearance. Multilevel Administration clearance provides read-write access to all areas on the network—a clearance that should be assigned to only a select few.

ENFORCED RESTRICTIONS

Users are prohibited from accessing NDS partitions and volumes that require login factors that are not included in their clearance level. For example, a user with Biometric & Token clearance does not gain access to volumes and partitions labeled Biometric & Password & Token, nor could that user access volumes and partitions labeled Password. This ensures that users cannot access areas with security labels that are higher than or entirely different from their clearance level.

Users are granted read-only access to partitions and volumes with labels that require fewer but at least one of the factors stated in their clearance level. For example, if a user is granted Biometric & Token clearance and requests that clearance at login, that user gains read-only access to partitions and volumes labeled Biometric and those labeled Token.

In the example above, even though the user's clearance level may appear to be sufficient to be granted read-write access to partitions and volumes labeled Biometric and those labeled Token, the user is intentionally denied read-write access. This is a security measure to ensure that confidential information remains on the volume or partition where it resides without that information being accidentally or maliciously copied to an area where it should not be stored.

DUAL PRODUCT OFFERINGS

NMAS is available in two product offerings, namely the Novell Modular Authentication Service Starter Pack and the Novell Modular Authentication Service Enterprise Edition. Each are described in detail below.

STARTER PACK

Available as a free Web download and bundled with certain Novell products, the Novell Modular Authentication Service Starter Pack lets network administrators create single-method login sequences using any of the available methods. This way, administrators can set up departments and even individual user access to NDS partitions and volumes according to perceived security needs.

ENTERPRISE EDITION

Available as a for-purchase product, the Novell Modular Authentication Service Enterprise Edition allows for multi-factor authentication by allowing methods to be chained together in a desired sequence order. In addition, the graded authentication feature is enabled to allow NDS tree partition and volume access rights according to the methods used at login.

NOVELL CLIENT SUPPORT

Novell has updated its Windows* 95/98 and Windows NT* clients to efficiently support the NMAS login methods. With NMAS, NDS users can indicate the login sequence that they will use to log in to NDS and, if needed, the clearance they need. The login sequence and clearance may be selected in a new tabbed page in the Novell Client™ login dialog.

CERTIFIED MODULES

Novell assures the compatibility of the methods available for Web download or included in either product, by insuring that each pass the "Yes—Tested and Approved" and "NDS Enabled" certification tests.

To maintain the assurance that the modules remain unaltered, NMAS will only allow Novell digitally signed modules to be installed.

As Novell works with more partners to develop authentication modules, Novell will continue to test and certify new modules. Upon certification, these digitally signed modules may be made available to NMAS users through Web download.

REQUIREMENTS

SERVER:	NetWare 5 SP3 with NDS 8 (version 10.6 or above) and NICI 1.5
CLIENT PLATFORM:	Windows NT 4 SP3 or higher, Windows 95 OSR2B, or Windows 98 SP1
NOVELL CLIENT:	Novell Client for Windows 95/98 version 3.2 or higher Novell Client for Windows NT/2000 version 4.7 or higher
PROCESSOR:	486/33 or higher
MEMORY:	64 MB minimum on server; 40 MB on client
HARD DISK SPACE:	100 MB of available disk space on the NetWare 5 server. **NOTE**: If PKIS 2.0 and ConsoleOne are already installed, only 10 MB is required.
RIGHTS:	Administrator rights to the NetWare 5 server to install NMAS from a client; NT administrator rights to install client software on Windows NT

CONCLUSION

As organizations look to provide enhanced security to their networks, choosing to implement different and multiple login methods is a logical approach. NMAS makes implementing an advanced authentication system in your NDS tree easy and painless.

Novell continues to partner with some of the world's most popular authentication developers in providing a framework that allows many different forms of authentication to work together and provide enhanced security in NDS managed networks.

Graded authentication provides the ability to grant access rights according to the authentication method used. This allows network access rights to be finely controlled through authentication.

NMAS is one more solution that delivers on the long-standing Novell commitment to providing innovative enterprise network security that creates immediate value to Novell customers. Fully directory-enabled and designed with administrators and end-users in mind, NMAS provides the flexibility and security that organizations need today to manage their secure network.

Novell Corporate Headquarters
122 East 1700 South
Provo, UT 84606
USA
Tel: (801) 861 7000
Toll-free: (800) 453 1267

AMERICAS REGION

Novell Canada
3100 Steeles Avenue East
Suite 500
Markham, Ontario L3R 8T3
Canada
Tel: (905) 940 2670
Fax: (905) 940 2688

Novell de Argentina S.A.
Ing. Butty 240, piso 6
Edificio Laminar
1001 Capital Federal
Argentina
Tel: (54) 11 4 312 2626
Fax: (54) 11 4 312 8025

Novell do Brasil Software Limitada
Avenida das Nações
Unidas, 12.995
8º Andar
04578-000 São Paulo - SP
Brazil
Tel: (55) 11 5505 4040
Fax: (55) 11 5505 4041

Novell de Chile
Av. Nueva Tajamar 555
Of. 901
Las Condes - Santiago
Chile
Tel: (56) 2 3397 070
Fax: (56) 2 3397 071

Novell de Colombia
Teleport Business Park
Calle 114 No. 9 - 45
Torre B - Of. 709
Santafé de Bogotá
Colombia
Tel: (57) 1 629-2969
Fax: (57) 1 629-3509

Novell de México
Blvd. Manuel Avila
Camacho #138-1
Col. Lomas de Chapultepec
Mexico D.F., C.P. 11000
Tel: (52) 5 284 2700
Fax: (52) 5 284 2799

Novell North Region Latin América
One East Broward Blvd.
Suite 700
Ft. Lauderdale, FL 33301
USA
Tel: (954) 713 2869
Fax: (954) 356 0409

Novell de Panamá
Calle 53 Marbella,
World Trade Center
Piso 2, Oficina 10
Cuidad de Panama
Panama
Tel: (507) 206-8714
Fax: (507) 206-8777

Novell del Perú
Martir Olaya 129 Office 1701
Centro Empresarial Pardo
Miraflores
Lima, Peru
Tel: (511) 214 1340
Fax: (511) 214 1087

Novell de Puerto Rico
255 Ponce de León
Royal Bank Center,
Suite 202
Hato Rey, Puerto Rico 00918
Tel: (787) 771-3816
Fax: (787) 771-3811

Novell de Uruguay
Cerrito 534, piso 4
11000 Montevideo, Uruguay
Tel: (598 2) 915-5032
Tel: (598 2) 915-5026
Fax: (598 2) 915-4932

Novell de Venezuela
Plaza La Castellana
Torre BanCaracas
Piso 10, Ofic.10-04
La Castellana
Código Postal 1060
Caracas, Venezuela
Tel: (58) 2 264 2534
Fax: (58) 2 264 2171

EUROPE, MIDDLE EAST, AFRICA REGION

Novell Austria
Heiligenstädter Lände 27c
1190 Vienna
Austria
Tel: (43) 1 36 77 444
Fax: (43) 1 36 77 444 20

Novell Belgium NV
Koninging Astridplein 5,
(3rd floor)
2018 Antwerpen
Belgium
Tel: (32) 3 206 1793
Fax: (32) 3 206 1799

Novell Praha s.r.o.
Praha City Center
Klimentska 46
110 02 Praha 1
Czech Republic
Tel: (420) 2 2185 6611
Fax: (420) 2 2185 6622

Novell Danmark
Slotsmarken 12
DK 2970 Hørsholm
Denmark
Tel: (+45) 45 16 00 20
Fax: (+45) 45 16 00 40

Novell Finland
Sinimäentie 10 C
02630 Espoo
Finland
Tel: (358) 9 502 951
Fax: (358) 9 5029 5300

Novell France
Tour Framatome
1 Place de la Coupole
92084 Paris La Défense
Cedex
France
Tel: (33) 1 47 96 60 60
Fax: (33) 1 47 78 94 72

Novell Germany
Monschauer Strasse 12
40549 Düsseldorf, Germany
Tel: (49) 211 5631 0
Fax: (49) 211 5631 250

Novell Hungary
East-West Business Center
1088 Budapest
Rákóczi út 1-3
Hungary
Tel: (36) 1 235 7656
Fax: (36) 1 266 6360

Novell Israel
Ackerstein Building
Medinat Hayehudim St 103
Herzliyya 46776
Israel
Tel: (972) 99 51 44 55
Fax: (972) 99 51 44 66

Novell Italia
Piazza Don Mapelli 75
20099 Sesto San Giovanni
Milan, Italy
Tel: (39) 02 2626 3262
Fax: (39) 02 2626 3195

Novell Middle East
17th Floor
Dubai World Trade Center
P.O. Box 9313
Dubai, United Arab Emirates
Tel: +971 4331 6444
Fax: +971 4331 9248

Novell Netherlands
Barbizonlaan 25
2908 MB Capelle a/d Ijssel
PO Box 85024
3009 MA Rotterdam
The Netherlands
Tel: (31) 10 286 4722
Fax: (31) 10 286 4010

Novell Norge
Østensjøveien 34
Po. box: 6555, Etterstad
0606 Oslo
Norway
Tel: +47 23 37 77 70
Fax: +47 23 37 77 71

Novell Polska
ul. Sienna 64
00-825 Warszawa, Poland
Tel: (48) 22 620 39 79
Fax: (48) 22 620 31 03

Novell Portugal
Centro Empresarial Torres
de Lisboa
Rua Tomas da Fonseca,
Torre G
1600 Lisboa
Portugal
Tel: +351 21 723 06 30
Fax: +351 21 722 35 33

Novell Russia and CIS
Suite 524
Radisson-Slavyanskaya Hotel
2 Berezhkovskaya Nab.
Moscow 121059
Russia
Tel: (7) 095 941 8075/73
Fax: (7) 095 941 8066

Novell South Africa
Morning View Office Park
214 Rivonia Road,
Morningside
P.O. Box 1840
Rivonia 2128
Gauteng
Republic of South Africa
Tel: (27) 11 322 8300
Fax: (27) 11 322 8400

Novell Spain, S.A. (Madrid)
Paseo de la Castellana, 95
27th Floor
Torre Europa
28046 Madrid
Spain
Tel: (34) 1 555 65 67
Fax: (34) 1 555 29 15

Novell Spain, S.A. (Barcelona)
Avda. Diagonal 611.6º A
08028 Barcelona
Spain
Tel: (34) 3 430 47 10
Fax: (34) 3 322 28 90

Novell Sweden
Kronborgsgränd 1
164 87 Kista
Sweden
Tel: +46 8 477 4100
Toll-free: 020 35 3030
Fax: +46 8 477 4101

Novell Schweiz AG
Leutschenbachstrasse 41
8050 Zürich
Switzerland
Tel: (41) 1 308 47 47
Fax: (41) 1 302 04 01

Novell Turkey
Beybi Giz Plaza
Ayazaga Mah. Meydan Sk.
No:28, 27th Floor
80670 Maslak
Istanbul / Turkey
Tel: +90 212 335 25 45
Fax: +90 212 335 25 46

Novell United Kingdom Ltd.
Novell House
1 Arlington Square
Downshire Way
Bracknell
Berkshire, RG12 1WA
United Kingdom
Tel: +44 1344 724000
Fax: +44 1344 724001

ASIA PACIFIC REGION

Novell Pty Ltd
Level 18, 201 Miller Street
North Sydney NSW 2060
Australia
Tel: +61 2 9925 3000
Fax: +61 2 9922 2113

Novell New Zealand Limited
L12, 44 - 52 Wellesley Street
Auckland 1
New Zealand
Tel: +64 9 308 1400
Fax: +64 9 308 1409

Novell China
Floor 11 Canway Building
No. 66 Nan Li Shi Road
Beijing 100045, China
Tel: (86) 10 68028855
Fax: (86) 10 68028720

Novell Hong Kong
Room 4601-5
China Resources Building
26 Harbour Road
Wanchai
Hong Kong, China
Tel: (852) 2 588 5288
Fax: (852) 2 827 6555

Onward Novell Software (I) Ltd.
62 MIDC, 13th Street
Andheri (East)
Mumbai 400 093
India
Tel: +91 (022) 8342244
Fax: +91 (022) 8342223

Novell Japan Ltd.
Toei Mishuku Bldg.
1-13-1 Mishuku
Setagaya-Ku
Tokyo 154-8561
Japan
Tel: (81) 3 5481 1294
Fax: (81) 3 5481 1934

Novell Korea
Will-Bes Building 11 Floor
942-1, Daechi-dong
Kangnam-ku
Seoul, Korea
135-280
Tel: (82) 2 528 1400
Fax: (82) 2 528 1414

Novell Corporation (Malaysia) Sdn Bhd
Unit 501, Level 5, Uptown 1
1 Jalan SS21/58
Damansara Uptown
47400 Petaling jaya
Selangor Darul Ehsan
Malaysia
Tel: (60) 3 712 6100
Fax: (60) 3 712 6155

Novell Singapore Pte Ltd
8 Temasek Boulevard
#32-01/02 Suntec Tower Three
Singapore 038988
Tel: (65) 395 6888
Fax: (65) 395 6777

Novell Inc., Taiwan Branch Office
Rm. E, 5F.,
No. 168 Tun-Hwa N. Road
Taipei 105, Taiwan, R.O.C.
Tel: 886-2-2718 9733
Fax: 886-2-2514 9806

Novell, Inc. Thailand Representative Office
16th Flr., TISCO Tower
48 North Sathorn Rd.
Silom, Bangrak,
Bangkok 10500
Thailand
Tel: (662) 638 0310
Fax: (662) 638 0311

Printed on recycled paper. Please recycle.

Novell Product Training and Support Services
For more information about Novell's worldwide product training, certification programs, consulting and technical support services, please visit:
http://services.novell.com

For More Information
Contact your local Novell Authorized Reseller, or visit the Novell Web site at:
http://www.novell.com

US/Canada: 1 888 321 4272
Worldwide: 1 801 228 4272
Facsimile: 1 801 228 5376

Novell, Inc.
122 East 1700 South
Provo, UT 84606

Novell.

462-001061-001