HOWARD™
TECHNOLOGY SOLUTIONS

For more information visit www.Howard.com or call us at 888.912.3151

Security & Identity Solutions

IDENTIPHI ADVANCED AUTHENTICATION

Positively identify users accessing your systems.

Benefits

Strong Proof of Identity
Ensures the validity of users who wish to access your network and supports multifactor authentication.

Protect Access to Data
Replace static passwords with strong configurable multifactor authentication using smart cards, biometrics and/or tokens.

Faster and Easier Logins
Users are no longer required to use and remember passwords for network access.

Enhance Users' Productivity
Reduce the time users spend managing credentials and logging into corporate systems.

Reduce Help Desk Costs
Eliminate support calls related to password resets to significantly reduce support center costs.

Government Compliance
Meet new regulations and legislative requirements while protecting data from unauthorized access.

Extensive auditing
SNMP and SMTP statistics provide real time, comprehensive reports for effective security management.

Take Password Management Out of the User's Hands

IdentiPHI Advanced Authentication significantly increases network security by enforcing stronger identity management policies. Users must prove their identity at the computer or network login using stronger authentication methods. IdentiPHI Advanced Authentication replaces standard password authentication with multifactor techniques including smart cards, hardware tokens, biometric devices, one time passwords and pass phrases.

Detect and prevent unauthorized access

Network security is a two step process. You must first identify users and validate that they are who they claim to be; then you must confirm that they are authorized to access your network. Most importantly, you need the ability to easily and accurately enforce a security policy that restricts access only to authorized users. IdentiPHI AA carries out identification and authorization using a wide range of logical access methods. IdentiPHI AA can authenticate users with one or more of the identity authentication methods described below.

Smart Cards

- An embedded chip stores credentials and certificates.
- Accessible through reader devices attached to a user's workstation.
- Protected by a password or PIN
- IdentiPHI AA has built-in support for a wide-range of smartcards
- IdentiPHI AA allows administrators to define policies

SMART CARDS

Biometric Devices

- Validate a user's identity based on unique biological characteristics using fingerprints.
- Identiphi AA has built-in support for most fingerprint sensor devices.
- Users cannot "lose" their credentials or share them with others.
- Biometric authentication can be combined with other identity management methods such as smart cards.


BIOMETRICS

Tokens

One-time Password (OTP) Tokens

- OPT Tokens generate temporary access codes
- The code requires the user to authenticate within a few minutes before the code expires.
- Identiphi AA provides server side PIN protection

USB Smartkey Tokens

- USB Smartkey tokens are similar to smartcards, but eliminate the reader.
- Smartkey tokens connect directly to a workstation through a USB port.
- Identiphi AA supports Smartkey tokens that are protected by a PIN
- Allows the administrator to define policies when a token is removed.

TOKENS

www.howard.com
888.912.3151 general 888.323.3151 technical support 601.399.5060 fax

HOWARD™
TECHNOLOGY SOLUTIONS

For more information visit www.Howard.com or call us at 888.912.3151

IdentiPHI Advanced Authentication

IDENTIPHI™

Technical Features

Security
- Special security administration group controls functionality, Supported devices, audit configuration, workstation and server defaults.
- Workstation and server configurations inherited from the directory at connection.
- Encrypted Secure Socket Layers (SSL) communication between client and server.
- Advanced Encryption Standard (AES256) encrypted data store.
- AA Verify plug-in provides integration of Advanced Authentication into Single Sign-On enabled applications.
- Workstations can be configured with stronger authentication using more than one device.

Configuration and Management
- Comprehensive directory-based policy inheritance model based on corporate hierarchy.
- Ability to scope functionality of the system to the Domain, organizational unit, container, machine and user level.
- Administration performed via Microsoft Management Console plug-ins.
- Auto detection and configuration on workstations allow rapid deployment and support of smartcard environment.

Authentication and Enrollment
- Replace static password validation with strong configurable authentication (biometrics, smartcards, TPM, OTP tokens and multifactor).
- Self-enrollment policies reduce administrative overhead.
- Q&A Passphrase substitution policies allow user access to the network when device authentication is unavailable without help desk calls.
- Configurable systray icon functionality provides easy to use interface for users.

Auditing and Reporting
- Windows Event logs record all Advanced Authentication activity. SNMP traps generated for configurable events.
- SMTP statistics are gathered and distributed based on configuration policy settings.
- Detailed information recorded in the event logs enable auditors to determine “out of character” authentications.

System Requirements
Supported server operating:
- Microsoft Windows 2000
- Microsoft Windows 2003
- Citrix Metaframe

Supported directories:
- Microsoft Active Directory
- Upcoming support for eDirectory and other LDAP compliant directories

Supported workstation operating systems:
- Microsoft Windows 2000
- Microsoft Windows XP

Supported Smart Cards
Multos:
- Keycorp

Java:
- Oberthur
- IBM JCOP
- MartSoft
- Aspects
- Gemplus
- Schlumberger / Axalto
- G&D Sm@rtCafe

Proprietary:
- G&D Starcos

Supported Hardware Tokens
- Rainbow iKey
- Aladdin eToken
- G&D Starkey
- Vasco DigiPass

Supported Biometric Devices
Sensor Manufacturers:
- Authentec
- Upek
- Fujitsu
- Tacoma
- Testech
- Cross Match
- Security First Corp.
- Fingertech

Reader Device Manufacturers Supported:
- Upek
- APC
- IBM
- Fujitsu
- Cross Match
- Zvetco
- Silex
- Startech
- Targus
- Key Source International
- Cherry
- RiTech
- Animation Technology
- MPC
- SecuGen
- Fingertech

For more information on IdentiPHI Advanced Authentication please contact:

Howard Technology Solutions
888.912.3151
601.399.5077 (fax)
www.Howard.com