

Authentication Solution for Linux

Optimized end-to-end solution for
local and remote users.



Table of Contents

Executive Summary	3
Authentication and ID Management for Linux	3
Ease of use – One-PIN-and-You’re-In	3
Access Abuse	3
Eliminate Static Passwords	3
The Only Comprehensive Authentication Solution for Linux	3
Introduction and Overview	4
CRYPTO-Shield 6 for Linux	4
Access Point Protection	5
Business Issues	7
Open Source	7
End User Experience	7
IT/Helpdesk Experience	7
CRYPTO-Shield 6 and Security/Authentication	8
Regulatory Environment – HIPPA/Sarbanes-Oxley	8
Competitive Environment	9
Value Equation	9
Business Scenarios	9
Technical Issues	11
CRYPTOCARD Technology	11
System Requirements	11
About CRYPTOCARD	13

Executive Summary

Authentication and ID Management for Linux

The need for strong, reliable network protection has never been greater due to the proliferation of deployed workforces, users requiring network access from a variety of devices, and the sheer value and volume of online ‘assets’.

By providing users with an ‘access from anywhere’ network solution, the notion of Network Authentication and ID Management becomes the cornerstone of any network security protocol – you have to know with a high degree of confidence that users are who they say they are, when requesting access to private, proprietary and sensitive information within your network.

Static passwords, by far the most widely used authentication option, have been identified by the FBI, Gartner, the RCMP, and others as one of, if not the biggest threat to network security. Even when stringent password changing protocols are maintained, static passwords are simply no match for the password cracking forces at work.

CRYPTOCard brings its industry leading end-to-end authentication solution to Linux (and hybrid) networks. There is no other comprehensive solution available to Linux networks on the market today.

Ease of use – One-PIN-and-You’re-In

When making any technology decision, one must consider the affect upon both the IT department and the end user. CRYPTOCard’s solution implements easily, integrates with a broad range of legacy systems and will

actually be significantly less hassle for end users than the static password solution you are likely using today.

Access Abuse

How big is the problem? Well, it’s estimated that billions are lost each year to network attacks committed by exploiting the weaknesses inherent in static passwords. Whether through untraceable ‘internal’ infringements (perhaps a disgruntled employee ‘wandering’ beyond his approved network access boundaries) or a coordinated external attack, the fact is that LAN, WAN, www and VPN access all provide unintended, but nonetheless real, opportunity for misuse – and all are protected by nothing more than ineffective static passwords.

Eliminate Static Passwords

It is the only answer. Until you have control over who accesses your network, the rest of your network protection measures are ineffective and give a false sense of security where none exists. Static passwords must be eliminated.

The Only Comprehensive Authentication Solution for Linux

For Linux users looking for a first rate, comprehensive authentication solution – one that is engineered to implement easily and intelligently with Linux (and hybrid) networks and that protects every access point to your electronic assets... there is only one answer – CRYPTO-Shield 6 – fully compatible with Red Hat Enterprise Linux and SUSE Linux

Introduction and Overview

CRYPTO-Shield 6 for Linux

CRYPTO-Shield 6 for Linux is the authentication solution for IT infrastructures organized around Linux Red Hat Enterprise Server or SUSE Linux Enterprise Server. Once implemented, your Linux Server becomes the centralized authentication and token management system for all users, regardless of their computing platform or location.

CRYPTOCard's strong two-factor authentication solution protects every access point to your networked assets. From LAN logon, to VPN access to Websites and Portals, CRYPTO-Shield authenticates users with a simple 'One-PIN-And-You're-In' experience – it's as easy as using an ATM to access a bank account.

Two-Factor Authentication

Like an ATM, CRYPTO-Shield 6 authenticates users by requiring two levels of proof. First, users are equipped with an authenticator or token. The token is something that proves that they are authorized to enter the network. The second factor is something they know – a secret PIN that enables the token/authenticator.

When a user tries to access the network, they will need their token (Token options are described in more detail below) and their PIN. The PIN enables the token, which generates a one-time password (the password expires after a single use, so if sniffed or stolen, it is completely useless). The one-time password is sent to the CRYPTO-Server (which is in synch with the Token) and access is granted.

Should a token be lost, it's useless without the PIN. Because the PIN is not a password, it can be easy to remember and need never be changed. And because the token is something physical that is needed to access the network, if it is ever stolen, it will be a very short time before the loss is noticed and reported – tokens are easily revoked by an administrator from anywhere in the world.

Linux and Hybrid Networks

Real-world networks are rarely simplified/ideal infrastructures. More often, there may be a mixture of Linux, Apache, Windows and Mac OS that contribute to a network's heterogeneity.

CRYPTOCard has been a leader and innovator in the authentication realm since 1989 and we support all major OS platforms. Our industry firsts include solutions for Linux based networks, Apache Web Servers and we offer the only native solution available for Mac OS X. The product is purchased to be compatible with your enterprise server, that single implementation (for example, on your Linux Server) allows all users, regardless of their 'computing platform' to authenticate to the CRYPTO-Server.

CRYPTO-Shield 6

CRYPTO-Shield 6 is the Linux-centric authentication solution for IT infrastructures organized around a Linux server. Once implemented, your Linux Server becomes the centralized authentication and token management system for all users.

In addition to the standard access point authentication for VPN's, Web Servers, Portals and wireless LANs, the Linux edition of CRYPTO-Shield 6.3 also offers these features

- Enforce CRYPTOCARD authentication for desktop access
- Protect any PAM-aware application
- Tight integration with Open LDAP
- Support for MSCHAP.V2 authentication
- Redundant failover
- Support for non-Linux computing environments
- Apache Secured by CRYPTOCARD

Access Point Protection

CRYPTO-Logon

It is distressing that some of the most costly network breaches are perpetrated from within the attacked network by a trusted user, or someone using a trusted user's credentials. CRYPTO-Logon, ensures that workstations are only accessed by authorized users and it audits their activity.

CRYPTO-VPN

Despite being an important facet of your network protection arsenal, out of the box, your VPN is protected only by weak static passwords. CRYPTO-VPN delivers strong authentication to VPN access.

CRYPTO-Web

Protect your Apache websites and web portals with two-factor authentication. CRYPTO-Web protects whole sites, or any portions thereof. Various levels of access authorization are easily assigned on a user-by-user basis. (Also compatible with IIS)

CRYPTO-Console

The command centre, where a system administrator can deploy, revoke, track and audit all CRYPTO-Server activity.

CRYPTO-Deploy

CRYPTO-Deploy is a web-based method to activate deployed hardware tokens from anywhere in the world, to anywhere in the world in just a matter of seconds.

CRYPTO-Kit

For the advanced IT organization, CRYPTO-Kit allows you to build two-factor authentication functionality into any of your own systems.

CRYPTO-Tokens

Tokens are the enablers of the CRYPTOCARD Authentication Solution – Tokens (or authenticators) are one-time password generators. CRYPTOCARD offers a wide token variety delivering greater flexibility and allowing organizations to achieve the perfect balance of security and ease of use with in their network environment.

Token Types

KT-1 – Keychain Token

The PIN protected KT-1 is our most popular token form. Key chain convenience with a rugged alloy casing and easy to read display.



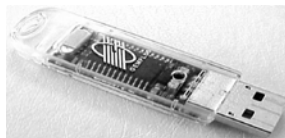
SC-1 – Smart Card Token

The 64 K chip, Magstripe and built-in door access capability make this a garage, building and network access option. (USB or PCMCIA Card Reader required and available from CRYPTOCard).



SC-3 – USB Token

This token is a software implementation of the RB-1 hardware token installed on a USB packaged smart card. Ideal for organizations that want the advantages and flexibility of hardware tokens with the convenience and integration of software tokens. The SC-3 can also store digital certificates for PKI applications.



ST-1 – Software Token

Perfect for people who use predominantly 1 workstation. The ST-1 GUI installed right on the user's desktop – One-PIN-and-You're-In! The ST-1 offer fast/easy deployability worldwide.



RB-1 – Pinpad Token

Delivering the ultimate in security, this credit card sized, calculator device is a powerful gatekeeper.



ST-1 – Software Token for BlackBerry or WinCE

With the proliferation of Handhelds accessing Networks our ST-1 token can also be installed on your BlackBerry or WinCE handheld, providing you with the convenience of a software token and the portability of a hardware token.



Business Issues

Making a case for any new technology involves careful consideration of the many business issues that support (or conflict with) the notion of adopting new systems. Everything from simple accounting to understanding how the technology cooperates with existing systems, implementation issues, the regulatory environment etc. This section provides an overview of the major considerations a corporation might want to take into account if considering an Authentication Solution to reside on their Linux server.

CRYPTOCard's Authentication Technology is designed to solve problems – not create them. Everything from compatibility and implementation to end-user and help desk issues, support a very positive opinion of the product. Ease of use for both the end-user and IT staff is central to our development philosophy.

Open Source

Linux was built around an Open Source philosophy that allows users to modify and add to the OS code to suit their needs. CRYPTOCard respects and embraces that Open Source perspective. We support a wide choice of both Open Source and Proprietary protocols with full support for any organization that wants to maintain a completely Open Source environment. CRYPTO-Kit is our Application Program (API) Interface that allows our customers 'open' freedom to adapt our technology to their systems and solutions.

End User Experience

One thing we learned early in our history is that unwieldy authentication systems meet with too much user resistance to ever work well. We have devoted our R&D to making our systems smaller, faster, easier, automatic and integrated. The user experience with a CRYPTOCard solution has been reduced to One-PIN-and-You're-In ease. And, with no more Password changing (and remembering) concerns, end-users cheer the adoption of this technology.

IT/Helpdesk Experience

Our commitment to 'smaller, faster, easier, automatic, and integrated' reaps big benefits to the IT department as well. You will find that CRYPTOCard technology is compatible with a vast selection of top industry networking solutions. By visiting CRYPTOCard.com you can explore our many partnerships and compatibilities. CRYPTO-Shield 6 is easy to install and implement. Deployment – even globally – is nothing short of elegant. When needed, our support services are happy to help. The big bonus for System Admins is that they will never have to troubleshoot another forgotten password or hound users to adhere to password changing protocols again. FYI – It's estimated that as many as 1 in 2 helpdesk calls in an average organization are password related. Even if that's high for your business, it's more than likely that there are, nonetheless, some significant efficiencies to be found here.

CRYPTO-Server 6 and Security/Authentication

The Importance of a secure environment can not be overstated. The cost of network breaches is estimated to be in the billions of dollars each year. In an FBI survey of 538 companies 85% had detected a network breach and 2 out of 3 had suffered financial loss as a result. As the cornerstone of any security protocol user authentication is vitally important. Our broad product range delivers a flexible solution that is both manageable and affordable.

The Problem With Passwords

The problem with passwords is that they were developed when it was estimated that we might need to protect the worlds' 100 (or so) computers. Static passwords are simply old technology that is not up to the task of protecting the modern computer network.

People are part of the problem, to be sure. Mired with a proliferation of passwords to remember (on average we juggle about 12 each!) we do the human thing, we write them down, stick them under our keyboards (who would think of looking there?) and ignore password changing protocols.

But even if you could solve that problem, the fact is, cybercrime is sophisticated – there are tools that can crack any password, and it's not a question of 'if', it's just a question of 'when?'.

The Incredible Cost of Free Passwords

Even if you ignore (against the advice of the FBI, the RCMP, Gartner, The SANS Institute...) the threat of a network breach or attack, static passwords are, nonetheless a tremendous drain on IT departments. Using industry average numbers (as reported by Gartner) somewhere between 30% and 50% of Help Desk calls are for password related issues. Again, on average, about \$340 per seat per

year is spent servicing forgotten or otherwise troublesome password issues. How many users does it take before that becomes a significant number – 200 users? (= \$68,000). 2500 users? (= \$850,000).

The bottom line is, so-called free passwords are anything but free.

Secure Password Technology™

If static passwords are the problem... what's the solution? CRYPTOCARD's Secure Password Technology - an authentication solution that employs a single-use password system. A password, generated by an authenticator (or token) is used only once to permit network access. After this single login, the password is discarded and completely useless.

A user is equipped with a Token authenticator and the token generates a One-Time Password for every login attempt. On login, this one-time password must match the one-time password generated by the CRYPTO-Server (the CRYPTO-Server controls access to the Network).

To gain access to the network a user **MUST** have their token **AND** know the PIN that enables their token.

Users can choose a number, which, while secret, can be easy for them to remember. Tokens will become locked after a set number of failed PIN entries.

Secure Password Technology is an unhackable first line of defense in a secure network environment.

Regulatory Environment – HIPPA/Sarbanes-Oxley

There has been an enormous movement in the last few years to ensure that corporations, healthcare providers, publicly traded companies, etc. take responsibility for the sensitive information they are charged with.

HIPPA and Sarbanes-Oxley put the onus on Directors and IT officers to ensure records, information and electronic assets are appropriately protected from unauthorized access. How different industries are affected varies, but the underlying trend toward creating secure networks is no longer just good business, it's the law.

With CRYPTOCARD's authentication solution, an organization can cost-effectively meet the standards set by these Acts.

For HIPPA, the basis of the act is to protect access to sensitive patient information. The cornerstone of any attempt to meet this standard, is an authentication solution that will a) give you a high degree of confidence that only authorized users are accessing this information and b) an audit or reporting capability to track activity. CRYPTOCARD's Secure Password solution meets this stringent HIPPA demand.

Sarbanes-Oxley, while never stating a requirement for authentication standards, go on to put responsibility for any misuse of electronic information/assets squarely on the shoulders of senior management. As a strong defensive measure that would meet the standards of the S-O act, CRYPTOCARD Secure Password Technology is a very effective gatekeeper.

Competitive Environment

There are a number of authentication solutions available on the market, but no other that offers a comprehensive, end-to-end authentication option for Linux. We invite comparison shoppers – most of our customers considered other solutions at some point in their purchase process. Also, head-to-head, our product proves to be more flexible, easier to use, easier to implement, more secure and anywhere from 1/2 to 1/3 the price of competing solutions.

Our philosophy of constantly pushing for a smaller, faster, easier, automatic and integrated solution has armed us with a product we confidently put alongside any product in the industry.

How secure is secure enough? With CRYPTOCARD, you hold the keys. The cryptographic keys that are the 'secret code' at the heart of any authentication system and obviously something to guard. Other vendors' tokens are purchased pre-initialized – with the secret key already installed. These vendors maintain a record of these so-called secret keys.

CRYPTOCARD tokens can be purchased uninitialized, the Security officer can then easily initialize the tokens before distributing to users with an easy-to-use CRYPTOCARD token initializer. What this means is that no one else has a copy or a record of your secret information – and isn't that what secret means?

Value Equation

Switch from Static Passwords to CRYPTOCARD's One-time Passwords ...The ROI is high but the pay back period is short:

Typical 2500 User Organization				
Help Desk Budget	Cost per User per Year	Password-related Portion	CRYPTO-Server Cost/User	Payback Period
\$850,000/year (Gartner Group)	\$340.00	\$105.00 (30% - Giga Group)	\$80.00	9 months

Most organizations recoup the capital expenditure associated with adopting CRYPTOCARD Technology in as little as 6 months – in password related helpdesk savings ALONE.

Business Scenarios

Futures Exchange:

A trading group whose success depends totally on the number of transactions they can complete in a day (hour... minute... second....) has chosen a Linux Enterprise Server to be the hub of its network. In an environment where millions of dollars can move in a minute, network security – and hence, authentication – are mission critical. With One-Pin-and-You're-In ease, CRYPTOCARD's authentication solution delivers the speed required to meet the needs of the busy and fast paced exchange. Fluctuating and seasonal markets mean unpredictable workforce and access requirements; CRYPTO-Shield 6's scalability along with CRYPTO-Console and CRYPTO-Deploy, make user and token management a simple task that can be administered from one or multiple locations, locally or from anywhere in the world.

Law Firm:

A large law firm whose Linux Server network supports a hybrid network that serves 600 lawyers, plus IT, admin staff, accounting and HR, needs a two-factor, one time password solution to meet regulatory standards. The firm's user base is an assortment of 20 % Linux, 10% Mac OSX and 70% Windows XP work stations. CRYPTO-Shield 6 is the only O/S 'agnostic' solution that can deliver its industry leading authentication solution to the firm.

Manufacturing Migration:

A manufacturing/distribution firm with a user base of 11,300 computer-equipped employees begins a 2-year migration strategy from RSA SecurID to CRYPTO-Tokens operating in SecurID mode. As the SecurID tokens expire (typically every 3 years), they are replaced with CRYPTO-Tokens that never expire (equipped with user-changeable batteries). Savings on a per unit basis alone are considerable, but

the real savings begin to add up as 3, 6, 9... years later, NO token replacement budget is required. Users appreciate the virtually unbreakable, rugged metal alloy CRYPTO-Token and are pleased by a login experience that is completely unchanged. Over a 5-year period, savings to the firm surpass \$750,000.

Technical Issues

When considering the adoption of any technology, one must assess the new systems' compatibility with legacy systems, implementation issues, and hardware/software considerations.

What follows is a brief explanation of the CRYPTOCARD technology.

CRYPTOCARD Technology

Included with CRYPTO-Shield are all the necessary modules and agents to lock-down an entire network including:

Linux Networks:

- Red Hat Enterprise Linux or SUSE Linux Enterprise Server
- Administrative access to routers, firewalls, VPN gateways
- Remote network access through firewalls, NAS and VPN
- Apache 1.3/ 2.0 Web Server
- Unix network / service logon (telnet, ftp, su etc. – Any PAM-enabled application)
- Kerberos (MIT)
- Protect local logon on Linux workstations (also protects Windows and Mac OS workstations)
- Fully integrated with gnome and KDE

CRYPTO-Shield 6 has been designed to accommodate virtually any network topology. Specifically, in a Linux environment, CRYPTOCARD will work 'out of the box' with any PAM aware access granting application (eg, Mail Server, Telnet Access, Open SSH Demon and many others)

For Software or Smart Card-based tokens, the CRYPTOCARD Software Tools software must be installed on each end-user system running Linux, Windows or Mac OS X. The CRYPTOCARD Software Tools software is not required when using hardware tokens

CRYPTO-Shield is also available to authenticate on:

- Mac OS X 10.3.5 Panther Server running J-Boss 3.2.2
- Exchange 2000/2003 Servers (OWA)
- Windows 2000/2003 domain logon (LAN) and local machine
- Citrix Server (ICA and RDP clients/Web Interface - NFuse/CSG)
- IIS 6.0 Web Server

System Requirements

Server

- Red Hat Enterprise Linux 3 or 4, or SLES 9
- Pentium 4 – 2.8 Ghz or better
- 2 GB of Free Disk Space
- 1 GB RAM
- Network Adapter
- CD ROM or DVD Drive
- Internet Connection

Software Requirements

CRYPTO-Shield 6 installed on Red Hat Enterprise Linux 3 or 4 or SUSE Linux Enterprise Server 9 OR Windows 2000 SP4 / 2003 Server, Mac OSX 10.3.5 Panther Server running JBoss 3.2.2.

CRYPTO-Web 6 can be installed on Apache 1.3 or 2.0 (Linux, Mac, or Windows) or MS IIS 5.0 /

IIS 6.0 (Windows only).

For Software or Smart Card-based tokens, the CRYPTOCARD EUS software installed on each end-user system running Red Hat RHEL 3 or 4, or SLES 9, Windows 2000 SP4 or XP SP2 or Mac OS X 10.3+. The CRYPTOCARD EUS software is not required when using hardware tokens.

About CRYPTOCard

Established in 1989, CRYPTOCard provides cost-effective Secure Password Technology™ to leading enterprises worldwide in the government, technology, aerospace, financial, telecommunications, and healthcare sectors. Winner of the Best of Show, award at Macworld 2004, and SC Magazine's Best Buy Award for 2005, CRYPTOCard positively authenticates a user's identity by coupling something in the user's possession (a Smart Card, hardware token, or software token), with something the user knows (their PIN), and provides centralized authentication for all physical and network access regardless of network infrastructure or user location. CRYPTOCard's partners include Citrix (Nasdaq: CTXS), Apple (Nasdaq: AAPL), Cisco (Nasdaq: CSCO), Check Point (Nasdaq: CHKP), Entrust (Nasdaq: ENTU), Oracle (Nasdaq: ORCL), Sun Microsystems (Nasdaq: SUNW), and Macromedia (Nasdaq: MACR). For additional information on CRYPTOCard, please visit www.cryptocard.com.

CRYPTOCard North America

340 March Road
Suite 600
Ottawa, Ontario
K2K 2E4 Canada

Toll Free: 800-307-7042
Tel: +1-613-599-2441
Fax: +1-613-599-2442
E-mail: info@cryptocard.com

www.cryptocard.com

CRYPTOCard Europe

Eden Park, Ham Green
Bristol BS20 0EB,
United Kingdom

Tel: +44 870 7077 700
Fax: +44 870 7077 711
E-mail: info@cryptocard.com

www.cryptocard.co.uk

CRYPTOCard and CRYPTO-Server are registered trademarks or trademarks of CRYPTOCard Inc. in Canada, the U.S.A. and/or other countries. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.
© 2006 CRYPTOCard Inc.
All rights reserved.

20070626