

Market Leading Innovation

The CRYPTOCARD tokens used by CRYPTO-MAS are the most robust available and are supported by industry leading warranties. CRYPTOCARD offers a full selection of tokens, each offering different user benefits.

An organization can select the token most appropriate for their users and security policies – token types can even be mixed within a network offering unrivalled flexibility. CRYPTO-MAS offers the following token types: – Hardware, Software and Mobile tokens.

Hardware tokens are physical devices that, with the simple push of a button, generate a one-time password. CRYPTOCARD tokens offer advanced configurable options, deliver the highest degree of security and have the most durable steel casing on the market – enhancing CRYPTOCARD's reputation for quality.

Software tokens reside on a user's computer - whether laptop, or hand-held. Laptop based tokens are cost effective for anyone who only needs access from one computer; whilst 'portable' software tokens are available for mobile equipment like our Software Token for Blackberry.

Mobile tokens provide a token code via an SMS message received by your mobile phone. The Mobile Token works on all ordinary mobile phones.

CRYPTOCARD Tokens



- Authentication Modes
 - Event synchronous
 - Challenge/Response
- Encryption Algorithms
 - DES, 3DES, AES 128-bit, 192-bit, 256-bit
- Passcode Complexity
 - Up to 8 characters
 - Numeric and Hexadecimal (0-9, A-F)
 - Up to Base 64 (0-9, Aa-Zz, Shift + 0-9)
- PIN Management
 - Token-based PIN, Server-side PIN
 - Disallow trivial PINs (1234, 1111, ABCD)

CRYPTO-MAS

CRYPTOCARD's Managed Authentication Service

Your Token on Your Mobile Phone

Securing Your Network
and Remote Access
has never been easier!



E-mail: info@cryptocard.com
www.cryptocard.com

CRYPTOCARD Europe

Eden Park, Ham Green
Bristol
BS20 0EB UK
Tel: +44 870 7077 700
Fax: +44 870 7077 711

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

Secure Your World...

Changes in the way we work and the increased reliance on access to IT systems and data mean that businesses are increasingly exposing themselves to Hackers, ID Thieves and Fraudsters due to the continued use of static passwords. Two-Factor Authentication is a proven solution to this problem and CRYPTO-MAS now makes this available and affordable for a wider audience by removing cost and technology barriers.

CRYPTOCARD
Secure Your World.

“We have been using the CRYPTOCard Managed Service for the past 12 months. Our users have total confidence in the system and find it easier than having to decide on, and regularly change, the traditional static password system we were previously using.”

Colin Campbell, Stroud and Swindon Building Society, UK

“When we looked at the total cost of ownership of buying servers and doing it ourselves, versus putting password protection through the CRYPTO-MAS systems, the difference was well worth it. There was no upfront investment, no upfront setup and we were on the system over lunchtime. It literally took 45 minutes.”

Ware Adams, Managing Director, DC Energy

Choose CRYPTO-MAS if you want authentication with:

- 99.99% availability using global infrastructure
- Zero up-front investment in servers or infrastructure
- Simple quarterly payments
- Simple low cost integration and deployment
- Compatibility with all leading VPN & Firewalls devices
- Secures websites, portals and web applications
- A broad range of tokens
- Scalability from 10 to 100,000+ users

“In Butler Group’s opinion CRYPTOCard’s service suits any organisation looking to implement security without the overheads of implementation, support, and management normally associated with traditional in-house systems.”

Butler Group. Sept 2008

Is your data secure?

Businesses are increasingly relying on providing data and information access to improve the effectiveness of their business. So, they are turning to VPN and remote access to benefit from flexible working practices for employees, and are deploying web based collaboration tools to improve business processes and workflows with partners, suppliers and internal resources. This increased access to data heightens vulnerability to theft, fraud and hacking.

Two-Factor Authentication provides a solution to this problem by validating who is accessing the network. The process itself is simple and provides the same solution in the networked world as your ATM card and PIN does for your bank; the ‘something only you have’ is a token which provides a unique One Time Password (OTP), the ‘something only you know’ is your secret PIN. However, traditional solutions require the integration of expensive and complex servers and add to a company’s support burden.

CRYPTO-MAS delivers hassle free two-factor authentication (2FA) services without the need for complex integration, up-front investment or on-going support.

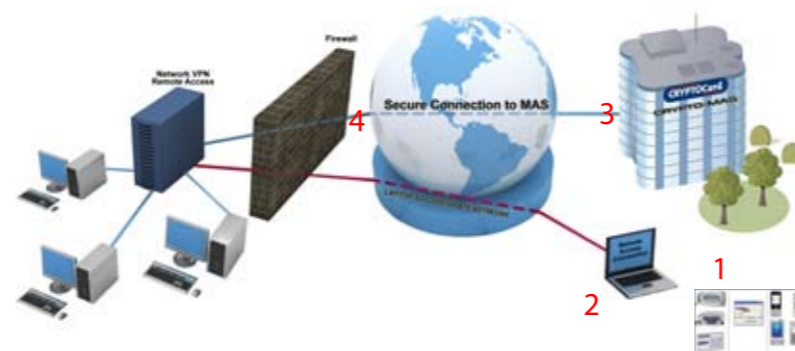
Authentication made simple

CRYPTO-MAS is simplicity itself: When trying to connect to the corporate network or web server, users are asked to identify themselves using their unique OTP and PIN, this request is then sent to the MAS service, the user is then authorised by the MAS service and given access to the enterprise network.

CRYPTO-MAS is located in secure data centres and provides a simple network interface between the web application being secured or the remote access routers or firewalls and the service itself. CRYPTO-MAS has a simple to use portal which provides all of the functionality needed to allow a service provider or an end user customer to set the system up, allocate and deploy tokens, manage the process of adds, moves and changes and produce activity reports.

The CRYPTO-MAS Service

The service can best be summarised in the diagram, where we can see three core elements shown.



1. You are allocated a token and your details entered into the system
2. You connect to the network and are prompted for User name and PIN+OTP
3. You are then authenticated by MAS
4. You are granted access to the network

Users

Each user of the service is provided with a token which delivers the One Time Password, which when combined with the unique PIN that they have, identifies them to the MAS service – which then authorises their connection to the network.

Tokens are available in a wide range of formats and styles to provide the utmost in convenience, portability, durability, interoperability and multi-role functionality.

An organization can select the token type or token types that are most appropriate for their user base and security policies - ensuring successful implementation and acceptance by matching tokens to working practices and lifestyle.

Enterprise Network

There is very little work required within the enterprise network in order for a company to make use of the MAS service.

Upon signing up for the service, the Firewall, Switch, Web application or gateway that provides access to the network (commonly called an AuthNode) is re-configured to pass all authentication requests to the MAS service via something called an Authentication Point-of-Presence (A-PoP).

The service is proven to work with a whole range of web based applications and also devices from Cisco, Juniper, Watchguard, SonicWALL ... in fact any RADIUS based device or application is compatible.

Log-on requests from users are sent to the MAS service from the AuthNode over a secure encrypted link, where they are authenticated against the user database that is held in the MAS service centre.

CRYPTO-MAS Service

CRYPTOCard’s secured data-centres and global infrastructure contain the heart of the MAS service. The main server is the authentication component of the whole service and which responds to the authentication requests from firewalls, VPN devices, etc, via the A-PoP.

The whole service is administered and managed by the MAS-Portal (MAP) which can be accessed from any standard

web browser and which in itself is secured using two-factor authentication.

The service provides authentication for users stored in the internal database – these details are simply entered either manually or by importing a CSV file via MAP. MAP provides workflow automation tools which aid in the deployment and management of all tokens and so substantially minimises administrative overheads.

MAP also provides comprehensive reporting tools which aid support and management of the system.

Flexible and available

CRYPTO-MAS provides unrivalled scalability, from a few as ten users to as many as tens of thousands within a single company. The servers have been designed to work in a multi-company environment and can therefore also handle many thousands of individual companies and their individual AuthNodes at any one time.

The service is backed by SLA’s guaranteeing 99.99% availability by leveraging its fully redundant infrastructure (covering Servers, Databases, LAN, Communications links etc) across multiple data centres.

CRYPTOCard delivers support that spans from a normal 8x5 level right through to a 24x7x365 follow the sun service.

Fast to install and simple to use!

CRYPTO-MAS requires little technical knowledge to set-up and manage. Administration is limited to using MAP to effect Adds, Moves and Changes and any reporting that may be required. Most CRYPTO-MAS installations can be carried out within an hour or even less - for example, if software or SMS tokens are being used this can be reduced to a matter of minutes.

Affordable

CRYPTO-MAS can be purchased as a complete OPEX based service, where a simple quarterly payment covers the delivery of the service and the chosen tokens. There are no hidden costs and no major up-front investments are required.