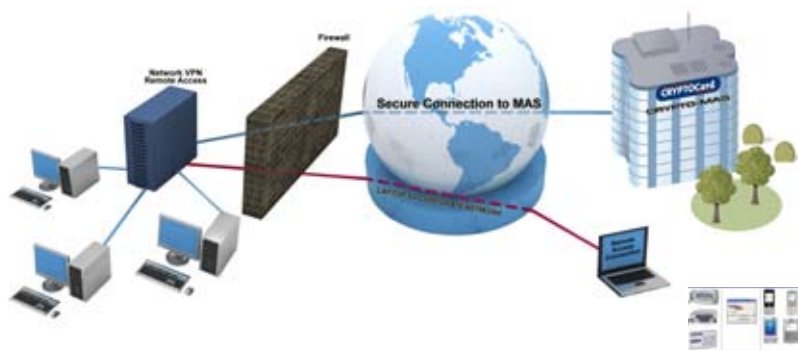


# CRYPTO-MAS

## Service Architecture

CRYPTO-MAS delivers market leading two-factor authentication without the need for a company to invest up-front or to worry about allocating resources to managing the solution. It delivers authentication 24/7. All this is made possible by the well designed architecture of the service, which includes multi-national datacentres and a totally scalable infrastructure that can support businesses with thousands of users just as easily as it copes with businesses who only need to secure ten users.



### Simple integration

Getting the service up and running is incredibly simple and requires no investment in infrastructure or changes to business processes. Log-on requests are now authenticated using CRYPTO-MAS rather than the access device or server. When they are logging on, users simply replace their passwords with a token generated code. The CRYPTO-MAS infrastructure ensures that everything is in place to provide a hassle free access security mechanism that locks the door to unwanted intruders.

### Secure 24/7 Authentication

The CRYPTO-MAS architecture is built upon multiple datacentres around the globe, each of which is housed in a secure, well managed and totally resilient building. Each building is regularly audited by an independent consultant. Data that is held in these centres is backed up onto multiple servers with built-in redundancy and back-up capability. All of the datacentres are interlinked with a robust network infrastructure with links provided by multiple service providers.

There are few components within the CRYPTO-MAS architecture that are as important as the

Authentications Points-of-Presence (A-PoP's). These provide the interface between the CRYPTO-MAS service itself and the remote access or web sites that it is protecting.

### Supports any RADIUS device

A company may have multiple devices that connect to the A-PoP's – these elements are called Authentication Nodes (or Authnodes for short). Each Authnode will be a RADIUS based device – CRYPTO-MAS has been proven and tested with a wide range of Authnodes from leading vendors such as Cisco, SonicWALL, WatchGuard, Juniper and many others.

Each Authnode that uses MAS will be connected to up to two A-PoP's to ensure resilience – so that if one fails then authentication requests will automatically be routed through to the other.

The link from the Authnode to the A-PoP is secured and the information that is sent over the link is also encrypted to ensure maximum security throughout.

### CRYPTO-MAS Key Features:

- Compatible with leading access devices (VPN, Firewall)
- Secures web sites and portals
- Simple integration with existing infrastructures
- 99.99% availability using global infrastructure
- High levels of security
- Flexible support options
- User self-service portal

