



Web Secure

Our clients are increasingly reliant on Web based applications and data, making these available to their staff, their partners and the public.

The demand for location independent access is similarly increasing, whether via Internet enabled access or connections to local networks.

As both these trends continue so does the risk that the increasingly sensitive data, whether personal data protected under European law or commercially sensitive data, may be accessed by unauthorised individuals. For many of these scenarios the weak point is the login itself – a single factor password is often not sufficient protection. In other cases there are underlying weaknesses in your code that allow hackers to use exploits, such as passing SQL commands within the login parameters to access your systems

We help organisations ensure that people have access to only the information they are entitled to, introducing stronger security measures where needed and providing a full security support service. Our customers can be confident that they have managed the risks appropriately and that this will be maintained, whatever line-of-business or day-to-day challenges they are faced with.

What is Web Secure?

Web Secure is a group of services designed to increase your confidence that your security needs associated with your online presence and Web accessible applications are met, while minimising the effort associated with security management and administration.

We provide a comprehensive technical and operational service releasing you to concentrate on your line of business, while we take care of managing the systems, processes and people that your security relies on.

Web Secure Authentication

This is our core service for clients wishing to improve the security of their application login process.

At the heart of this approach to Web security is our partnership with RSA, the leading providers of authentication services and products. We provide a fully managed, resilient RSA SecurID solution, running on our servers in our hardened hosting environment.

Users wishing to access your systems are authenticated via a multifactor (UserID, password or hard-token) login before being allowed access to your systems.

It includes:

- RSA SecurID token management for two-factor authentication.
- Dedicated or shared-server Ace Servers with integration to your applications.
- User management, including allocation and replacement of hard tokens, helpdesk support and user updates.

The shared server option provides reliable and resilient authentication with no single point of failure through the use of multiple servers etc. The service is fully managed, so you don't have to invest your staff's time in getting to grips with the technology or its support.

We are able to substantially reduce the usual running costs of this type of service, offering savings of around 40% or greater compared with dedicated solutions.

Furthermore our support services team takes care of all aspects of user management, relieving your internal team of the need to issue, maintain and troubleshoot UserID's, passwords and tokens.

Web Secure Authentication provides the quick, reliable and low-effort path to improving your logon security.

Key Benefits

Web Secure Authentication

Hardware tokens are available in several **convenient form factors**: key fob, card and PINpad formats to match your preferences.

RSA SecurID authenticators are **as simple to use as entering a password**, but much more secure, ensuring they don't require additional training or generate increased support calls.

Each user has access to a unique symmetric key which is combined with a powerful algorithm to generate a time-based code which only the RSA ACE/Server can validate, so no one else can enter the system, even if they know the password, giving you **extra-strong security**.

Most common hardware/software support RSA SecureID two-factor authentication right out of the box, so you can be confident that it will be **compatible with your infrastructure**.

Our fully managed service **minimises your deployment time, deployment cost and administrative burden**, so you can apply your desired level of security now and know it will be maintained, irrespective of other challenges and changes in your organisation.

Web Secure Security Services

A suite of general security services, providing: Secure Network Connectivity, Identity Management Services and Security Management and Operations.

Head Office
Innovation Close
York Science Park
York
YO10 5ZD
UK

London Office
17c Curzon Street
London
W1J 5HR
UK

t: +44 (0) 1904 438 000
f: +44 (0) 1904 435 450

e: info@ioko365.com

Web Secure Security Services

We can offer a suite of additional security services including:

Secure Network Connectivity

- VPN management, PPTP/IPSEC
- Roaming mobile user single sign-on through iPass

Identity Management Services

- ADS design, deployment and management (plus traditional NT domain migration, LDAP etc)
- Single sign-on systems using RSA Clear Trust and Netegrity Siteminder

Security Management and Operations

- Platform design, build and hardening
- Ongoing platform management (including patch checking, deployment and remediation technologies)
- Penetration testing of MS platforms (including .Net)
- Security vulnerability alert feed management
- Firewall management

RSA Technology

RSA SecurID® two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator) - providing a much more reliable level of user authentication than reusable passwords.

RSA Security offers enterprises a wide range of user authentication options to help positively identify users before they interact with mission-critical data and applications through:

- VPNs
- Wireless communications
- E-mail
- Intranets
- Extranets

- Web servers
- Other network resources

They are designed to fit seamlessly into the existing e-business infrastructures of our customers worldwide. RSA Security's authentication solutions remain an industry standard for organisations looking to protect their key business data assets.

The Gold Standard in Two-Factor User Authentication

The RSA SecurID® solution is the world's leading two-factor user authentication system, relied on by thousands of organisations worldwide to protect valuable network resources.



RSA SecurID SD600 Fob

Used in conjunction with RSA ACE/Server® software and RSA ACE/Agent®, an RSA SecurID authenticator functions like an ATM card. Network users must identify themselves with two unique factors before they are granted access. More than 15 million people around the world confidently use RSA SecurID authenticators to securely access VPN and remote access applications, web servers & applications, network operating systems and more:

- Authenticate users at network, system and application levels
- Secure internal and remote network access
- Available in hardware and software tokens
- Compatible with leading remote access servers, wireless access points, web servers, firewalls and VPNs
- Easy-to-use, industry-proven technology

- Designed with industry-standard technology

Carelink Services and Solutions

Web Secure works seamlessly with many of our other solutions and offerings, such as:

- Content Management Internet solutions
- Regional CMS
- ioko Detect 2004
- SharePoint Portal Server solutions

or anywhere that external access to your organisations information tools is needed.

What Next?

If you would like any further information on Web Secure or our other services and solutions, please contact us:

Web: www.carelink.co.uk

You can contact us directly by email, telephone or mail at the address above:

Email: info@carelink.com

Tel: 01904 438000

and ask for Carelink Sales

