



---

*Secure Authentication  
Managed Service Portfolio*

---

**THE END  
OF THE  
PASSWORD  
IS ~~NIGH!~~  
NOW!**

*Combating Corporate Identity Theft*

# Signify Managed Authentication Services

Signify offers a complete range of Secure Authentication and Identity Management services which allow you to positively identify your staff, customers, suppliers and other people who need authorised access to your sensitive information and systems.

## A secure replacement for passwords

Passwords are no longer secure enough to protect your sensitive on-line systems against the threat of identity theft, because they are so easily

snooped or guessed and can be re-used by anyone at any time.

Signify makes it easy to replace static passwords with strong, two-factor authentication, so you can be sure that your users' digital identities are secure and can be trusted at all times.

## A flexible range of authentication methods

By offering a range of services, Signify lets you give each of your users the appropriate form of authentication to match their working patterns and security access privileges.



RSA SecurID from Signify delivers the market leading strong authentication system as a fully managed service. Signify makes it quick, easy and affordable to roll out tokens to all your users and achieve compliance with the most rigorous industry regulations.

The standard RSA SecurID token, which displays a new one-time passcode (OTP) every 60 seconds, is ideal for regular users who need simple, secure access from any device, anywhere.

The new RSA SecurID 'Combo' token (available summer 2005) delivers all the 'anywhere access' flexibility of OTPs plus the potential for PKI-based authentication and digital signing along with the secure storage of passwords.



RSA SecurID  
'Classic' OTP Token



RSA SecurID  
New style OTP Token



RSA SecurID  
Combo OTP + USB Token

## Eliminate the Windows® password

RSA SecurID is no longer just for remote access: now you can use it to fully secure the desktop login process and enforce two factor security at all your access points.

Users with standard tokens simply enter their PIN plus their tokencode instead of the Windows password every time they log in: whether they are in the office, at home or on the road.

Users with the Combo token just plug their token into their laptop and enter their PIN for seamless certificate authentication.

With full support for offline, network, web and thin client access modes, your users can now have a simple, consistent and secure login process every time they connect to your systems, wherever they are. Your users will love it as they never have to remember or change their Windows password again!



Passcode OnDemand delivers simple, quick and cost effective 'two factor' authentication without having to carry a new device. It is ideal for anyone who needs occasional secure access to your SSL VPN, Extranet or Web Portal.

During the login process the user clicks a link to request a secure one-time passcode (OTP). Signify validates the user's PIN, generates a unique OTP and sends it to their registered mobile phone, PDA or email box by SMS or email.

The user logs in with this OTP, proving they both know their PIN and have access to their registered device.

Passcode OnDemand is perfect for:

- Office staff checking web email from home
- Contractors and part-time staff
- Clients and partners accessing an Extranet
- On-line banking, betting and retailing consumers

## Flexible service options

To suit different user needs and security policies:

- In 'PreSend' mode, a new OTP is automatically sent when the previous passcode has been used or expired, so your user always has a valid OTP to hand, even if out of service coverage.
- Users can choose to have several OTPs sent in one message, and can select where they want them sent.
- You can define the strength of Security Policy that is enforced on your users.



SMS Mobile Phone



Wireless PDA



Blackberry®



Email Account

# Signify Service Options

Choose the best way to roll out credentials to your users and to provide them with access to Signify's 24x7 Helpdesk service.

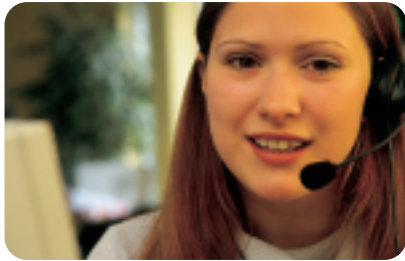
## Credential Provisioning

You can handle token delivery in-house or let Signify do it for you:

### Local provisioning:

administrators at each of your offices manage a pool of tokens and follow the IMC's simple procedures to allocate them to their local users, or

**Signify provisioning:** your administrators request new users via the IMC and Signify delivers their tokens by post or courier: ideal for your extranet users.



## Self-Service Helpdesk

Signify's fully automated helpdesk lets your users self-solve all their common problems such as lost or stolen token, forgotten PIN and undelivered OTPs.

The Signify Helpdesk can be accessed 24x7 by your users via:

**Web:** self-service over the web is part of the standard Signify service, and/or

**Telephone:** the fully automated interactive telephone helpdesk is available as a service option, and/or

**Your support team:** who can use Helpdesk Operator scripts to step the user to a solution.

Your security policy is enforced at every step, ensuring that the user is properly identified before support requests are actioned.

## Key Benefits of the Signify Service

- **Market-proven security:** strong authentication without the hassle
- **Affordable:** for all sizes of organisation
- **Scalable:** security for 5 to 50,000+ users
- **Fast deployment:** roll out in days
- **No new kit:** to buy or manage
- **Easy management:** via IMC web portal
- **Complete service:** fully automated logistics & 24x7 self-service helpdesk
- **Secure procedures:** the IMC enforces your security policy
- **Choice:** of services to suit each user's needs
- **Reliable service:** proven performance since 2000
- **Quality of service:** guaranteed by contractual Service Level Agreement

# A Complete Managed Service

Signify's complete service makes it quick, simple and affordable to provide secure authentication whatever the size of your user community.

At the heart of the Signify service is the Identity Management Centre (IMC) which provides policy-based management of the entire user lifecycle.

## Key features of the IMC are:

- **Security policy:** the IMC enforces compliance with the policy defined by your Security Officer
- **Role-based management:** the IMC defines clear roles and duties for each administrator
- **Devolved administration:** routine tasks can be handled by a local administrator who can only 'see' those users and systems that are within their scope of authority
- **End user self-service:** via their personal 'My IMC' interface and automated Helpdesk
- **Organisational modelling:** the IMC models the complex relationships between all your in-house, client and supplier organisations
- **Temporary User Access Control:** contractors and other 3rd parties can have identities which allow access only for a defined period of time
- **Own-label branding:** the IMC, tokens and all other aspects of the Signify service can be customised with your branding

## Why are OTPs the right choice?

You want to move from passwords to stronger authentication, but need to understand why one-time passcode (OTP) authentication is the best choice.

Quite simply most organisations choose OTPs because they:

- Are easy for users to understand and use in the real world
- Do not require a reader: users can log in from anywhere, using any device
- Can be delivered to users in many ways: on a token, by SMS or email
- Are supported as standard by all access systems, applications and web servers
- Are reliable and simple to support
- Are so cost effective

**OTPs deliver security that is simple, flexible, affordable, reliable and proven**

# Using Signify in your Enterprise

## Typical uses of Signify service

The Signify service is used by our clients to secure the following projects:

- **Flexible working:** Home-based staff accessing office network over VPN broadband
- **Mobile access:** Sales & other travelling staff checking email while 'on the road'
- **Client extranet:** Access via web portal to sensitive business apps
- **Supplier support:** Temporary access by remote support engineer to fix server problems
- **eGovernment:** Secure communications between local authorities, central government and health services
- **eLearning:** Teachers & careers advisors accessing sensitive student records from insecure school networks
- **24x7 IT support:** IT staff providing out of hours network support from home
- **Wireless roaming:** 'Anywhere access' for wireless users throughout corporate offices and from public WiFi hotspots

## How Signify plugs into your systems

The Signify service communicates with the key systems or 'Authentication Nodes' in your network where you challenge users to authenticate. Any system which supports either the open standard RADIUS and 802.1x protocols or the RSA ACE/Agent can become a Signify Authentication Node including:

- **VPN:** all firewalls, IPSEC & SSL VPNs
- **Wireless:** WiFi access points & hotspots
- **RAS:** all remote access servers
- **Roaming access:** ISP's & Global Roaming services
- **Web servers:** all popular web servers & proxies:
- **Web-enabled email:** OWA, iNotes, GroupWise etc
- **Web services & apps:** Java, PHP, PERL, ASP, .Net etc
- **Thin client:** Citrix, Terminal Services etc
- **Remote control:** KVM switches, PC Anywhere etc



***"Signify provides a flexible range of secure authentication options to suit all the different types of people who need access to my network"*** David Ripper, Head of IT, Sue Ryder Care



*Signify delivers secure, simple sign-on to your desktop, network, applications and on-line services.*



*The Secure Authentication Service*

[www.signify.net](http://www.signify.net)

[info@signify.net](mailto:info@signify.net)

+44 (0)1223 472572

Signify and the Signify logo are registered trademarks of Signify Solutions Limited.

RSA SecurID and the RSA logo are registered trademarks of RSA Security Inc.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

The Blackberry brand and image are the exclusive properties and trademarks or registered trademarks of Research In Motion Limited.

All other logos and trademarks are properties of their respective owners.