

Two Factor Authentication for your smartphone

Signify helps organisations to secure their computer networks. We provide a secure alternative to passwords that safely enables remote access to systems and information by delivering two-factor authentication as an on-demand, hosted service.



Signify Software Tokens deliver market leading RSA two factor authentication by turning a smartphone (BlackBerry or Windows Mobile) into a strong authentication token. Our service makes it easy to securely identify users 24 x 7 by confirming they have their smartphone with them. As a fully hosted service we ensure that the service works securely and reliably.

Signify Software Tokens are ideal for users who need secure remote access from any computer, but don't want to carry a token in addition to their other mobile devices.

What are Signify Software Tokens?

Signify Software Tokens allow a user's smartphone to be used just like a strong authentication token, which they need to have with them when they wish to remotely access networks, files and applications. Signify delivers RSA software tokens which work just like RSA's market leading SecurID keyfob tokens. You get RSA security and reliability with the convenience of using your own smartphone, delivered by Signify's proven hosted service.

When a user wishes to access their corporate data remotely using a PC or laptop, they simply enter their secret PIN into their smartphone token application. The smartphone then generates a one time passcode which the user then enters into the password field on their PC or laptop. By demonstrating that they have these two 'factors' – a secret PIN and their smartphone – the user is securely identified.

Signify Software Tokens provide a better user experience because they enable users to use their preferred mobile device to authenticate themselves. Users usually tend to look after their smartphones more carefully than a keyfob token and are therefore less likely to lose them. When lost, they are more likely to report that fact, enabling the token to be disabled, ensuring that your corporate security is maintained.

Key benefits

Guaranteed Reliability:

- Works without mobile phone network coverage
- Distributed and resilient infrastructure
- SLA backed service

Proven Security:

- Market leading RSA software token
- Infrastructure designed and managed with security in mind
- Secure web portal administration

Flexible to your requirements:

- Mix our token and tokenless services
- Utilises your user's existing smartphone device
- Variety of contract lengths

Quick to deploy:

- Compatible with all leading VPNs, firewalls and web servers
- No training required
- No physical token to deploy
- Efficient software token provisioning process

A Complete Managed Service

The successful deployment of two-factor authentication takes more than just technology; you also need to implement a framework of policies, procedures, logistics and user support. These are automated through key features of our service:

Authentication Infrastructure: Security and reliability is designed in and implemented across multiple data centres, to deliver and validate one time passcodes every time. 99.999% service availability over the last 5 years.

The Identity Management Centre (IMC): Manage all aspects of your service through our easy-to-use web portal. This portal gives you more control and visibility of the service than if you ran the servers yourself.

End User Web Helpdesk: Our 24 x 7 self-service web helpdesk lets your users resolve their common problems such as forgotten PINs. This reduces your costs and improves the end user experience.

Software Token Provisioning Process: The software token and seed record is simply pushed to a user's smartphone upon request, ensuring that provisioning is quick and easy for the user. We achieve this by streamlining the set up procedure for each user, to ensure they can start working first time, every time, without adding load to your already busy IT team.

You may not want a software token for all your users? Signify's range of services make it easy for you to give each user the most appropriate form of authentication to match their working pattern and security privileges. You can mix and match *Signify Software Tokens* with our *RSA SecurID from Signify* and *Signify Passcode OnDemand* services.

Included Features	
Authentication Device	Uses the existing smartphone each user already carries Software token is installed as an additional application
Authentication Service	Annual service fee per user Unlimited authentications per user
Organisation Base Pack	IMC web portal for administration Telephone/e-mail support for administrators from our dedicated support team End user web helpdesk for automated resolution of end user issues
Optional Features	Discounts for multi-year contracts Software token life to suit how long you keep your smartphones

Authorised partner:



The Secure Authentication Service

info@signify.net www.signify.net

+44 (0)1223 472572