

Kier Group plc Kicks the Password Habit



Identity Management Security outsourced using the Signify Managed Authentication Service

As a leading international building and civil engineering contractor, Kier Group plc employs 7000 people worldwide and has an annual turnover in excess of £1.4bn. Kier Group's growth has been achieved organically and by acquisition. This has led to the existence of many autonomous companies, all with their own systems and security.

"The decision to choose the Signify managed service was pretty simple when we compared an in-house solution to their solution that offered all the features we needed at far less than the real cost."

Group IT Director
Terry Walker

The business case?

Critical to Kier's success is the secure access it provides staff who are working remotely, often with limited IT infrastructure, to project information held on central servers. Kier recognised that their old system of a basic managed dial service from BT, with user authentication based on standard passwords, was becoming increasingly vulnerable, difficult to manage and would no longer scale-up to the challenge.

The solution?

RSA SecurID was the preferred solution and Kier evaluated the costs and overheads of managing an in-house RSA SecurID system against a fully managed service. The unanimous decision was taken to choose Signify's managed service.

Implemented for more than 1,000 executives, engineers and site workers, Signify now supports remote access from the UK and worldwide. Users have secure sign-on to a wide variety of systems and services including web based email, IPSEC VPN and Kier specialist industry applications.

Terry Walker, Kier Group IT Director said "The decision to choose the Signify managed service was pretty simple. Their focus in this area offered all the features that we needed and delivered a 24 x 7 service for far less than the real in-house cost".

Benefits

- Secure collaboration between subsidiaries regionally and nationally
- Consistent remote access for site and office based staff
- Centrally maintained security policy
- Delegated administration of users
- IT staff focus on core business applications
- Smooth integration with existing systems including:
 - BT RAS
 - IPSEC VPN
 - Microsoft Outlook Web Access
 - Citrix Secure Access to specialist applications
- Multi-site access defined per user
- Single, secure log-in
- Full usage stats and audit trail





Flexibility, control and cost – key decision drivers

One of the key drivers in considering Signify for secure authentication was to separate out the provision of remote access from the authentication process. Kier regularly review suppliers and it was important to ensure that they retained the option of changing access suppliers without the overhead of also changing the authentication method as well.

Walker explained, “With an in-house authentication service we realised we would need to train our already over-stretched IT team on new technology, and we’d have the logistical burden of rolling out security devices to a widespread user base and also the need to provide those users with ongoing 24x7 support. It would have been a challenge for us to offer this when we should be concentrating on ‘our day job.’”

“It’s ideal because users can be granted access to one or several of our remote access services, and they use their single, secure Signify ID to log in at all points. It reduces their stress because they don’t have to remember different passwords to access different systems, and it vastly improves our position from an auditing and security standpoint.” explained Walker.

Centralised policy, delegated administration

With Kier centrally maintaining its security policy but delegating user management to its subsidiaries, it became apparent

that the solution they chose had to offer fully integrated management of the entire token lifecycle.

“The Identity Management Centre (IMC) is superb. It gives us all the central security policy control we need from HQ while allowing us to delegate the day-to-day user management to local administrators at each site who know who should be allowed access and who should be switched off.” commented Walker.

Measuring ROI...

The benefits to Kier have been numerous. The Signify IMC has enabled Kier to centralise the distribution of tokens and lets their administrators quickly switch user accounts on and off should the need arise. The IMC gives them secure web browser access to a full audit trail showing who has access to the systems and when they have been connected. None of this was possible with their original dial-up, password based system.

Password Security an issue for remote users

Some of the issues Kier faced with its old system were that users did not change their passwords often enough and shared accounts left the system open to abuse. Kier’s helpdesk was finding it difficult to maintain control over access and know the number of users accessing the network at any one time.

In Summary

Outsourcing authentication and identity management to Signify means Kier have found they have not had to recruit people with skills in this area. This not only keeps costs down but their existing IT staff are able to focus on the applications that are core to their business without the burden and headache of rolling out security devices to a widespread and remote user base.

“Signify has provided us with a complete identity management service rather than just another authentication product”, said Walker.

“Their Identity Management Centre (IMC) is superb. It gives us all the central security policy control while allowing us to delegate user management to local site administrators.”

“Signify provide us with a complete identity management service rather than just another authentication product”

info@signify.net

www.signify.net

+44 (0)1223 472572

RSA and RSA SecurID
are trademarks of
RSA Security Inc