

One sign to rule them all



Accessing multiple systems needs to be done securely, quickly and efficiently – but how to do this without when each system has its own password? Dan Worth finds out about OneSign.



"It can provide audit trails of which systems people are accessing and when and so forth. It also means IT staff can easily remove a user's right to access a certain system, or the entire network, easily and seamlessly."

David Ting,
CTO, Imprivata.

Imprivata is a company that provides such a solution through its Single-Sign On (SSO) programme called OneSign which helps workers collate all their passwords into one simple log on. This can then be paired with a strong authentication device such as a smart card, biometric reader or proximity reader, to maintain security and also streamline workflow. The solution is already in use across the emergency services, including fire services and NHS Trusts. David Ting the CTO of Imprivata highlights that the risk of forgetting passwords, or writing them on scraps of papers that are then left next to computers is quite high. "We've even heard of staff writing passwords on walls next to computers, which clearly is far from ideal!"

The OneSign system initially works by inputting all data and passwords for each application and these details are then remembered by OneSign. The user is then only required to input one password, which grants access to all relevant applications. This can be used in conjunction with a device such as a smart card for more secure access. "If a doctor is dealing with a patient and can draw up the relevant information or application on his computer quickly he not only saves time throughout the day – which can be enough time to see another patient sometimes – but also provides a better level of service as they spend less time looking for the right password, and more time talking and helping the patient."

Herb Parker, Head of Strategic Infrastructure at Oxford Radcliffe NHS Trust, which has been using the system since March 2009, agrees. "Human nature means that relying on staff to simply remember their passwords is not a good enough way to combat the risks to security in our working environment and so the SSO OneSign system from Imprivata has helped combat this.

"Furthermore, as part of our remit to improve efficiencies and productivity, the ability for staff to log in to applications quickly and securely, helping them save time and provide a better level of service, means efficiencies and productivity are improved too. Most staff now carry a Smart Card that they use to access computer information, either by inserting it into a keyboard and entering their password or, for keyboards that conform to infection control guidelines and so can't have slots, staff can use a proximity reader that senses the card's presence, and then enter the information after that in the same way."

The benefits of SSO extend beyond users though, and through to IT staff as well, as Ting explains: "It can provide audit trails of which systems people are accessing and when and so forth. It also means IT staff can easily remove a user's right to access a certain system, or the entire network, easily and seamlessly, so that certain individuals – who have left the organisation say, or move into a role where they do not have rights to certain data – do not have access to information any longer than they should."

Parker from Oxford Radcliffe explains how the password manager system from Imprivata has helped to drastically reduce the amount of calls the IT department receives regarding forgotten passwords. "For the 15 years that I have been at Oxford Radcliffe the top call every month to the IT department has been forgotten passwords. However, in the last few months this has dropped dramatically after we gave staff the ability to reset their own passwords. It works by asking staff, when they are first given access to the system, or retrospectively for those already employed, to answer six questions from a choice of 22. Then, if they forget their password and wish to reset it, they are then asked three of these six questions before being allowed to reset the password.

"This added security means staff are able to take control of their password management and therefore remove the time constraints these previously placed on IT staff."

Implementing these systems though, is not an easy task, as Parker explains: "It's taken us a while to get staff on to the system as it involves getting them to come in, signing on to the system, being registered to a smart card and so forth – during time when they need to be working. We've had the system since December 2008 and for the OneSign system, after purchasing 3,000 licences, have so far registered 146 personnel.

"However, within the next month or two we should have a further 1,000 signed up as part of a significant drive we've been scheduling. Furthermore, as we start to ensure each new member of staff is properly provisioned when they join the Trust, we can increase the numbers of those on the OneSign SSO more efficiently. We also have 13,100 licences for the Password Manager software, and now have 9,000 staff signed up, meaning we should have enough licences left over to accommodate growth in the organisation."