

Novell NHS Smart Card Login Frequently Asked Questions

Doctors and nurses find logging into multiple systems with multiple passwords time consuming and disruptive to patient care. Speeding up access by sharing or writing down passwords has serious legal and security implications, potentially putting confidential patient information at risk. Smart Card Login via the Novell Identity Assurance client, originally developed to meet the exacting demands of the US Department of Defense, helps to eliminate these problems.

The following list of questions and answers explains how Novell NHS Smart Card Login protects data and systems through workstation, network and application login.

Q: Do I need local Smart Card Login?

A: Research has highlighted the problem of multiple local application passwords as the second most important infrastructure security issue for healthcare authorities. Using NHS Smart Card Login for local authentication can simplify this issue.

Q: Will my clinical users want to use Smart Card Login?

A: Research has shown that doctors and nurses consider logging into multiple local applications and systems, each with different authentication credentials, is a major barrier to exploiting the potential benefits of IT in the day-to-day care of their patients.

Q: Will Smart Card Login reduce security risks?

A: When doctors and nurses share login information or write down passwords in order to speed up their access to information there is a real risk that confidential data could be compromised. Smart Card Login helps prevent such incidents and the potentially serious legal and security consequences.

Q: Can I login to my PC, network and applications?

A: With an NHS Smart Card you can login to your PC, local network and local applications without having to enter a username and password.

Q: What will it cost?

A: The software licences required to implement NHS Smart Card Login have been centrally funded by Connecting for Health as part of an enterprise-wide software agreement. So the software will cost you nothing.

Q: What happens when my laptop is off site or the network is unavailable?

A: You can continue to work on your laptop even when the network connection is unavailable, using your NHS Smart Card and passcode to authenticate – the added security of two factor authentication is necessary when working in the community. You must also have previously logged in at least once while the laptop was connected to the network.

Q: What happens when the workstation has no Smart Card reader or I want to use a PDA without a Smart Card reader?

A: You can retain the option to login with a user name and password in situations where a Smart Card cannot be used.

Q: What about the significant number of users who do not currently have a Smart Card, and may never get one?

A: They simply login as they did previously using their current username and password. Other centrally funded software is available to help with enforcing a stronger password policy, synchronising passwords across applications and enabling self service resetting of passwords.

Q: What do I need?

A: You need to ensure your users are recorded in a directory such as Active Directory or eDirectory. You also need to have the NHS root certificate and sub-certificate (distributed with the NHS Identity Agent software) for import into the solution. Each user needs to know the passcode and have an NHS Smart Card with a valid, non-expired certificate.

Q: Is training available?

A: Connecting for Health provides centrally funded training on products within the Enterprise Wide Agreement. Please visit <http://www.novell.com/offices/emea/uk/nhs/index.html> for details of scheduled courses or contact the NHS team at nhs@novell.com to discuss options for bespoke training.

Q: Do I need a working connection to N3 and the Spine authentication service to be available 24x7?

A: No, you are dependent only on your local network. Spine authentication is entirely unaffected by locally deployed Smart Card login technology.

Q: What about fast user switching at busy shared workstations?

A: Smart Card login is a big help as it avoids the user having to enter a local network user name and password in addition to using the Smart Card and passcode for accessing national applications. The user is asked for one set of credentials only each time user switching takes place.

Q: Does NHS Smart Card Login work with the NHS Smart Cards issued for access to national applications?

A: Yes, which means you can take advantage of the existing Registration Authority processes and the card issuing systems which are already funded and in operation. So there is no need to issue and manage your own local cards.

Q: I have read that the NHS certificates run out after 2 years. Can you prevent a user's card from suddenly ceasing to work?

A: No, strict security measures prevent an expired certificate from being used for login. However, when a user logs in they are warned if their certificate is due to expire. You can configure this notice period for each user. For example, a notification period of six weeks gives even the busiest users plenty of time to get their certificates reissued.

Q: Do I need to run my own Certificate Authority?

A: No, there is no need to mint and manage your own local certificates. The solution operates using the certificates that come with your NHS Smart Card, saving you time and money.

Q: Will NHS Smart Card Login work with my locally issued Smart Cards and certificates?

A: Yes, the solution will work with any standard X.509 certificates. Locally issued or trusted partner certificates can all be accepted alongside centrally issued NHS certificates, providing maximum flexibility.

Q: Can I add Smart Card Login to my existing local applications?

A: Generally yes, for example you can use it with applications that authenticate against your current Active Directory. By protecting patient identifiable data in existing local systems in this way, you can extend the life of these systems while reducing the risk of unauthorised disclosure of personal information.

Q: Does that mean the system will provide single sign-on for all my applications?

A: No, it will only provide single sign-on for local applications that meet specific technical criteria – although in some cases this will mean the majority of local applications within a trust. To implement single sign-on for other applications, such as legacy green screen systems, you will usually need to buy a single sign-on product, such as Novell Secure Login.

Q: What happens when users have more than one user account?

A: The same Smart Card can be associated with more than one user account when logging in. The user simply selects the appropriate login from a displayed list, so they no longer need to remember multiple passwords for different user accounts.

Q: I have a number of generic or shared accounts – what happens to them?

A: Not a problem. You can associate a list of Smart Cards with a particular shared account. The system links the login event to a particular Smart Card making audit possible against the card owner and not just the shared account. For example, you can restrict access to a special purpose PC to the group of staff who are entitled to use it, rather than anyone reading the post-it note in the drawer below.

Q: What happens if I need to grant access to visitors from other parts of the NHS?

A: A guest account can be made available to any user with a valid NHS Smart Card, so you can easily grant access to visiting NHS employees, for example enabling them to use a workstation and your network for NHSmail or other national applications. Activities can be audited back to a particular card holder, thereby avoiding the risks involved in running workstations with kiosk-style public access. User self service also eliminates the cost of help desk staff managing temporary accounts for visitors, especially when required out of regular office hours.

Q: What if I have already deployed my own cards or other hardware tokens?

A: You can mix and match cards, enabling you to migrate users gradually or accept smart cards issued by a partner organisation. The solution supports X.509 certificates on most smart cards, the leading popular hardware tokens, and a range of legacy hardware tokens.

Q: How do I associate a Smart Card with the local user account?

A: The NHS Smart Card can be associated with a local user account either by the user, as part of the provisioning process, or by an administrator. Administration rights can be delegated for groups of users. It is recommended that the association is carried out as part of the registration authority process when the card is first issued to the user.

Q: How do I manage all of this for my thousands of users?

A: Management is simplified because the interfaces are browser based and may well already be familiar to you. Through Delegated Administration roll out becomes largely a matter of telling users about the option to use a Smart Card. Importantly, the administration tools allow you to assign administrative rights for groups of users, so day-to-day administration can be delegated.

Q: Will this system replace the Spine Authentication?

A: No, this is not a replacement for the Spine Authentication.

Q: What happens when a user leaves?

A: User access can be revoked either by the administrator or through an automated provisioning process that disables account access.

Q: Where can I get advice on deployment?

A: NHS-specific implementation documentation is available to complement the standard product documentation. This is funded by Connecting for Health to assist those implementing the solution within the NHS.

Q: Is there any limit on the number of licences I can have?

A: Connecting for Health has centrally funded a quantity of software licences, which will be distributed on a first come first served basis.

Q: How do I get the software and licences?

A: Register your interest now by visiting <http://www.novell.com/offices/emea/uk/nhs/> or calling **01344 326144**.

Q: How does NHS Smart Card Login work?

A: The user inserts their Smart Card into a reader. The digital certificate stored in the chip on the Smart Card is checked for validity, including a check on the valid from and until dates. The certificate is verified as having been issued by the NHS certificate authority. The software sends a challenge to the chip in the Smart Card. The challenge is signed (digitally encrypted) using a private key stored in the chip. The private key, which never leaves the security of the chip, can only be used if the user has entered the correct passcode when prompted.

This passcode should only be known by the valid card holder. The signed response is validated using the public key found in the validated digital certificate taken from the card.

The solution is based on Novell Identity Assurance client software, also known as Novell Enhanced Smart Card Method (NESCM), which was originally developed to meet the requirements of the US Department of Defence for smart card authentication.

Q: How can I get more technical details?

A: The Novell NHS team is waiting to help you. Please contact us if you have questions about AES, CRL, OCSP, PKI, API, ACL, PKCS11, NESCM and more. Product documentation, best practice guides and specialist technical advice are all available, so please email nhs@novell.com or give us a call on **01344 326144** with your questions.

More questions

Simply drop us an email at nhs@novell.com or call us on **01344 326124** and we will be happy to help.

Simplify and secure local access with Novell NHS Smart Card Login

**NHS Smart Card
Login Solution**

www.novell.com



Contact your local Novell
Solutions Provider,
or call Novell at:

Novell NHS Team
Novell
1 Arlington Square
Downshire Way
Bracknell
Berkshire
RG12 1WA

Tel: 01344 326144
Fax : 01344 724103.

www.novell.com