

Transforming security for healthcare providers

||||| Integrated identity and access management systems



FINANCIAL SERVICES & RETAIL

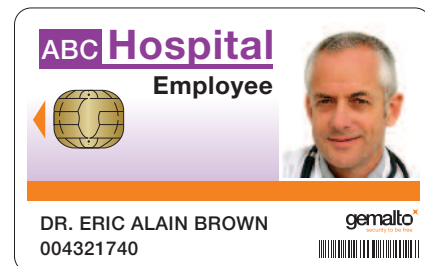
ENTERPRISE > SOLUTION BRIEF

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

TELECOMMUNICATIONS

TRANSPORT



gemalto
security to be free

Transforming security for healthcare providers

IIIIII Integrated identity and access management systems

Healthcare IT Systems: the imperative to evolve

Like other businesses, healthcare institutions are facing the pressure to control operational costs, upgrade and manage information systems and enhance the productivity of employees who provide patient services. Protecting the privacy of patient records is an important concern and the standard practice of user name – password authentication is no longer considered to be secure. These factors are creating the momentum for a fundamental shift in the way computer systems are used to deliver patient care and manage the growing volume of medical data.

Two oncoming forces are likely to accelerate this momentum and make the imperative to evolve and expand information systems even more urgent:

- Economic incentives to use new technologies that improve patient care
- Adoption of electronic health records

Government-funded economic incentives for new technologies will lower the investment cost for infrastructure needed to integrate disparate patient care and diagnostic systems and to deploy applications that help clinicians work more productively. Medical records and patient data will increasingly be stored electronically for use throughout the service delivery process.

Requirements for next generation solutions

Securing network access and sensitive information is required by law. It also fosters an environment in which highly mobile doctors and healthcare workers can communicate and collaborate openly and with confidence that patient information is not being compromised. In addition, the Drug Enforcement Administration has proposed regulations that require doctors to use two factor authentication when issuing electronic prescriptions for controlled substances.



Advantages of smart card security

Smart card-based solutions are frequently deployed for healthcare-related applications and have been used for authentication, payment authorization and secure storage of electronic health records for several years. Using a smart card solution for patient applications enables healthcare providers to streamline the patient intake process and reduce errors, duplicate records, and the number of rejected claims. The use of smart cards increases the overall safety of patient information while ensuring both cost-effective and efficient records management.

Smart card technology also offers several advantages for healthcare provider identity and access management systems. Because they function as a single, portable identity token for a wide range of personalized security services, smart card devices eliminate the need for employees to carry multiple identity tokens and remember login names with complex, frequently changing passwords. Using smart cards for logon reduces password-related support costs and the amount of time doctors and care providers spend during the workday to log on to their desktop, network and applications.

Gemalto, the world leader in digital security

Gemalto offers a comprehensive family of compatible smart cards, smart card readers, authentication and secure memory tokens, software and services which are based on current industry standards and specifications. These products incorporate proven smart card technology and enable component optimization and integration with existing hardware infrastructures. Gemalto's strong authentication portfolio supports both Java and .NET environments and multiple authentication methods such as single key, one-time password, digital certificate (PKI) and biometrics.

Integrated solution from Gemalto and partners

Gemalto, Microsoft®, and Citrix®, have worked together to develop identity and access management solutions that are tailored to the specific needs of healthcare organizations. Gemalto smart card technology, Microsoft operating systems and identity management products, and Citrix application infrastructure can be easily integrated within a thin client environment to provide a secure identity and access management solution. This solution can be deployed for a wide array of security and productivity applications that include:

- Desktop, network and application logon
- Single sign-on and instant access to care applications
- Remote network access
- Data encryption (email messages, documents and disk drives)
- Digital signature of email and documents
- Secure transactions and payments
- Visual identification
- Physical access control

Optimize security and productivity for doctors and employees

> Secure Logon with Single Sign-On

In a typical deployment, doctors and clinicians use their Gemalto .NET smart card to enter the facility and securely log on to workstations, laptops and mobile devices running the Windows®, operating systems or to thin client systems running Citrix ICA®, protocol. Then they are automatically connected to patient care applications without a separate logon. Two-factor authentication makes the network more secure and users can only access pre-authorized workstations and applications.

Care providers often continue the work started by a colleague with the same workstation and application that was previously in use. Using a smart card-based solution with Citrix Password Manager™, applications can be locked but not closed to enable fast and secure access at a later time. For example, if a nurse updates patient information and locks the workstation or logs off, the application securely locks. Later, a doctor who needs immediate access to that patient's record logs on with a smart card device and the application unlocks without reloading to provide immediate access.

> Secure Remote Access

On-demand remote access with mobile devices is a necessity in today's environment. Healthcare employees not only access patient records and care applications in hospitals and clinics but also from home, wherever patients are, and en route between locations. With the Gemalto .NET Smart Card, healthcare personnel can securely logon to the network with a VPN client and PKI certificate. In addition to strengthening network security, this practice also increases productivity by enabling healthcare employees to work from anywhere at any time, thus increasing their ability to respond to patients as needed.

> Message Encryption and Digital Signature

Most care providers communicate and exchange patient information via email despite the security risks. The integrated IAM solution provides encryption technology to protect message content so only the sender and the intended recipients can read it. Messages are encrypted using the public key of the recipient's encryption certificate. When the messages are received, they are then deciphered

using the private key from the recipient's encryption certificate which is stored on the smart card device. Email messages and files also can be similarly protected with a digital signature to ensure the authenticity of communications and documents exchanged.

Benefits throughout the organization

The integrated solution from Gemalto, Microsoft and Citrix is easily adaptable to existing computing and network infrastructure and can be expanded to meet future security requirements using Public Key Infrastructure (PKI) certificates. It offers healthcare providers several benefits that include:

- Increased employee productivity with fast secure access and services such as digital signature, single sign-on to workstations and applications, and secure VPN authentication
- Favorable and rapid ROI due to interoperability with existing Microsoft infrastructure and Citrix thin client architecture
- Reduced password support cost and costs associated with data breach
- Enhanced security for logon, remote access, and sensitive patient information. Identity credentials stored on the smart card device are more portable and secure than those stored on a PC
- Optimized IT resource utilization with integrated identity management services, reduced password support requirements, and streamlined integration
- An efficient and streamlined process for regulatory compliance through auditing of shared workstation access events

Solution architecture and components

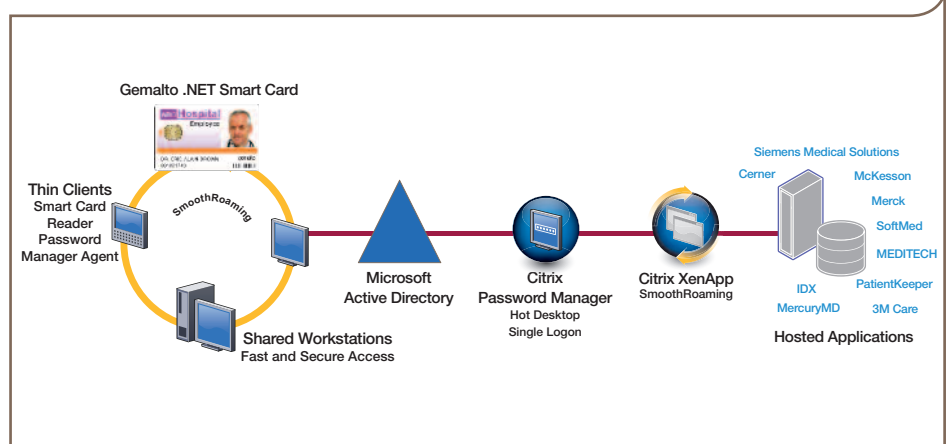
Thin client networks offer several advantages for many organizations, especially in service industries such as healthcare. They deliver access to applications and information with virtually any device over any network connection and users are able to access the same familiar desktop, regardless of location. In addition, desktop sessions can be transferred from one thin client device to another without having to restart applications

Cost savings can be substantial because thin client hardware costs less than desktop PCs and laptops, and the licensing fees for server-based operating systems and applications are lower. Additional savings are attributable to lower costs for management, maintenance and support. And with Gemalto .NET strong authentication, application and role segmentation can be easily implemented for individual users.

> Gemalto .NET Smart Cards

provide a personalized employee identification credential that is used for secure logical and physical access, both within the facility and remotely. By combining something you know—your personal identification number (PIN)—with something you have: a smart card-based security device, the Gemalto .NET Smart Card protects access to facilities and information systems with strong two factor authentication. It can even be personalized with a picture and other imprinting to prevent forgery.

Gemalto also offers Device Administration Service and Instant Badge Issuance.



> **Device Administration Service** is a hosted service for issuing and supporting Gemalto .NET end-user devices. It enables IT administrators to perform routine deployment and device management services through a browser interface and features an end-user portal to support routine tasks such as PIN changing and unblocking.

> **Instant Badge Issuance** consists of a smart card badge printer and a smart card provisioning and personalization system. It works directly with Microsoft Active Directory® and Identity Lifecycle Manager to produce smart identity credentials quickly and conveniently.

> **Microsoft's Windows platform** offers an unsurpassed level of support for smart card devices and certificate services using PKI. Gemalto .NET smart card technology is integrated in Microsoft Base Smart Card Cryptographic Service Provider (CSP). It is natively supported in Windows Vista® and Windows Server® 2008 and is available via Windows Update for earlier versions. This integration enables the devices to work seamlessly with Microsoft's Terminal Services, Active Directory, Active Directory Federation Services and smart card login, making it easy to deploy and manage strong authentication and PKI systems without additional software or middleware.

> **Microsoft Identity Lifecycle Manager (ILM)** provides meta-directory and certificate management capabilities for users' identity credentials. It supports a single view of their identities throughout the organization and maintains the consistency of this view across all connected systems and applications. The certificate management functionality in ILM significantly reduces the cost of deploying and

managing digital certificates and smart cards. It also provides a solution for provisioning and de-provisioning users – IT administrators can provision a user's accounts, synchronize passwords, and manage certificates through the same process.

> **Citrix XenApp Application Delivery Infrastructure and ICA thin client technology** enable fast and secure access to the same set of patient data and applications with different thin client systems throughout the facility. Citrix XenApp™ includes Citrix Password Manager for single sign-on (SSO) to the network and applications. Password Manager supports Hot Desktop, a feature that enables users to log on and log off in seconds, instead of using the more time-consuming user name/password-based procedure. The solution also includes Citrix SmoothRoaming™, a key feature of Citrix XenApp, which further improves employee productivity by allowing users' sessions to move with them from one workstation to the next.

> **Password Manager** is launched and a Hot Desktop session starts when a user authenticates. Session startup scripts can automate application launching, and Password Manager's single sign-on functionality automatically logs on to the user's Windows, Web and host-based applications. It also handles policy enforcement and password changes—making connecting to applications easier and faster as well as more secure. Running in the Citrix XenApp environment, Password Manager performs single sign-on to remotely launched applications.

> **Hot Desktop** securely locks a user session after a workstation is idle for a configured length of time and users can also lock their sessions. But unlike a standard Windows computer lock where only the same user or an administrator can unlock the

workstation—denying potentially critical access to any other healthcare worker—Hot Desktop enables any user to unlock the thin client simply by authenticating with a Gemalto .NET Smart Card badge.

> **SmoothRoaming** enables published applications to roam with the user: simply by inserting their Gemalto .NET Smart Card badge, a doctor or nurse moving from one thin client workstation to another can seamlessly resume reviewing a medical file or recording patient data.

■ Results that impact the bottom line

The integrated IAM solution for healthcare from Gemalto, Microsoft and Citrix has been deployed by numerous hospitals and other healthcare providers. These organizations have experienced several benefits that include direct costs savings, increased employee productivity, enhanced security of patient data, more efficient compliance with industry regulations and guidelines, and an improved level of patient satisfaction and reduced frustration.

In one deployment at a regional hospital, workstation logon and application access time was reduced from 90 seconds to 15-20 seconds for the initial logon (including sign-on to applications), and to less than 10 seconds for each subsequent access. This reduction equates to an approximate 22% improvement in the productivity of its doctors and care providers. Because of this productivity increase, the hospital can potentially generate additional revenue without increasing its labor costs and can redeploy existing resources as needed.

Find out more about Gemalto's integrated healthcare IT solutions by visiting: www.gemalto.com/enterprise

||||| The world leader in digital security

www.gemalto.com

gemalto
security to be free