

Inside Perspective

Helping you unleash the full power of MEDITECH

Wild

Electronic newsletter published every 8 weeks

Simplified Sign-On—Overview and technologies (Part 1 of 3)

Scott Blanchette, Principal Consultant

There is little disagreement that maximizing the benefits of healthcare information technology hinges on making electronic clinical systems easy to use for physicians, nurses, and other providers. Nor is there any doubt that hospitals need to vigorously protect patient information for ethical, business, and regulatory reasons. Every healthcare provider that generates, retains, or relies on electronic information is faced with the conflicting challenge: How do you make patient information instantly and widely available to those who should have access to it, while reliably and securely preventing access by everyone else?

“Simplified Sign-On” (or SSO for the purpose of this article) is a compilation of several new systems and technologies integrated with existing HCIS applications to provide secure, yet streamlined access to authorized users. SSO covers a wide range of functionality, including user provisioning and identity management, authentication, Single Sign-On, session management and context management. In addition there are a number of pure technologies such as radio frequency identification (RFID), biometric identification, smart-cards, and portal applications that can play a key role in helping to establish or confirm the identity of the user.

Today, a full complement of Simplified Sign-On applications is being delivered by a number of vendors, including Microsoft, Novell, IBM, Citrix, Forward Advantage, Sentillion, Imprivata, Encenutate, and others.

What is Simplified Sign-On?

To understand Simplified Sign-On, first we have to understand the main functional components that comprise an enterprise-wide, end-to-end solution.

Authentication

Authentication systems and technologies are designed to establish or confirm the identity of a user during login, so that appropriate access to various resources can be given. Typically, authentication is multi-factor, requiring more than one attribute which must match to establish a user's identity. To be strong, factors need to fall into at least two of the following three categories:

- Something you have (e.g., RSA Token or RFID badge)
- Something you know (e.g., password or PIN)
- Something you are (e.g., a fingerprint)

Single Sign-On (also commonly referred to as SSO)

Single Sign-On is the process that enables secure access of disparate applications by a user through a single, streamlined authentication process. Quite simply, Single Sign-On means that a user logs in only once for each session, and that any applications accessed during that session will not need to further authenticate the user. The reliance by all applications on the initial authentication drives the need for the first authentication to be secure, robust, and reliable. The mechanics of Single Sign-On are achieved through various means, depending on the vendor, but are generally based on the use of API's or scripting technologies.

Session and context management and proximity devices

Session management in Simplified Sign-On extends the ease of use of applications by providing additional functionality beyond the user login. To some degree, the technical aspects of session management can be provided through Citrix or Microsoft Terminal services. Generally, session management refers to the ability to “park” a session and then later resume that session where it was left off, either from the same device, or a different device entirely. Several of the Simplified Sign-On solutions enhance the functionality by supporting proximity devices, such as RFID, to automatically detect when a user leaves a specific workstation. Context management systems, generally based on CCOW (Clinical Context Object Workgroup), allow enabled applications to synchronize with each other, seamlessly presenting views of the same patient to the end user.

Management, auditing, and reporting tools

With all of the new functionality and integration between systems, it is important that the IT department be able to manage, maintain, audit, and report activity from all SSO applications efficiently and effectively. Several SSO systems associate information in a centralized store and serve it to applications as needed, making user information, authorizations, and access records available for reporting.

As with many enabling infrastructure projects, the success of an SSO initiative will be largely driven by the quality of the underlying applications. Conversely, the perception of the HCIS applications is influenced by first impressions, and SSO is the gateway to all other applications.

Summary

Simplified Sign-On is the umbrella phrase used to describe a series of technologies that, in conjunction with existing systems and applications, and applied through a coordinated and planned strategy, allow an organization to address both security and accessibility. In essence they are the technologies required to “close the gap” in making an Electronic Medical Record available to the clinician. Success will be measured by how well these conflicting objectives are balanced, with neither being compromised.

Scott Blanchette has over twenty-five years experience in the healthcare industry in which he spent more than ten years as a CIO, managing information system departments for a number of MEDITECH hospitals. Email him at editor@jjwild.com.

Coming Issues: SSO Part 2—MEDITECH SSO functionality
SSO Part 3—Implementation and operational considerations