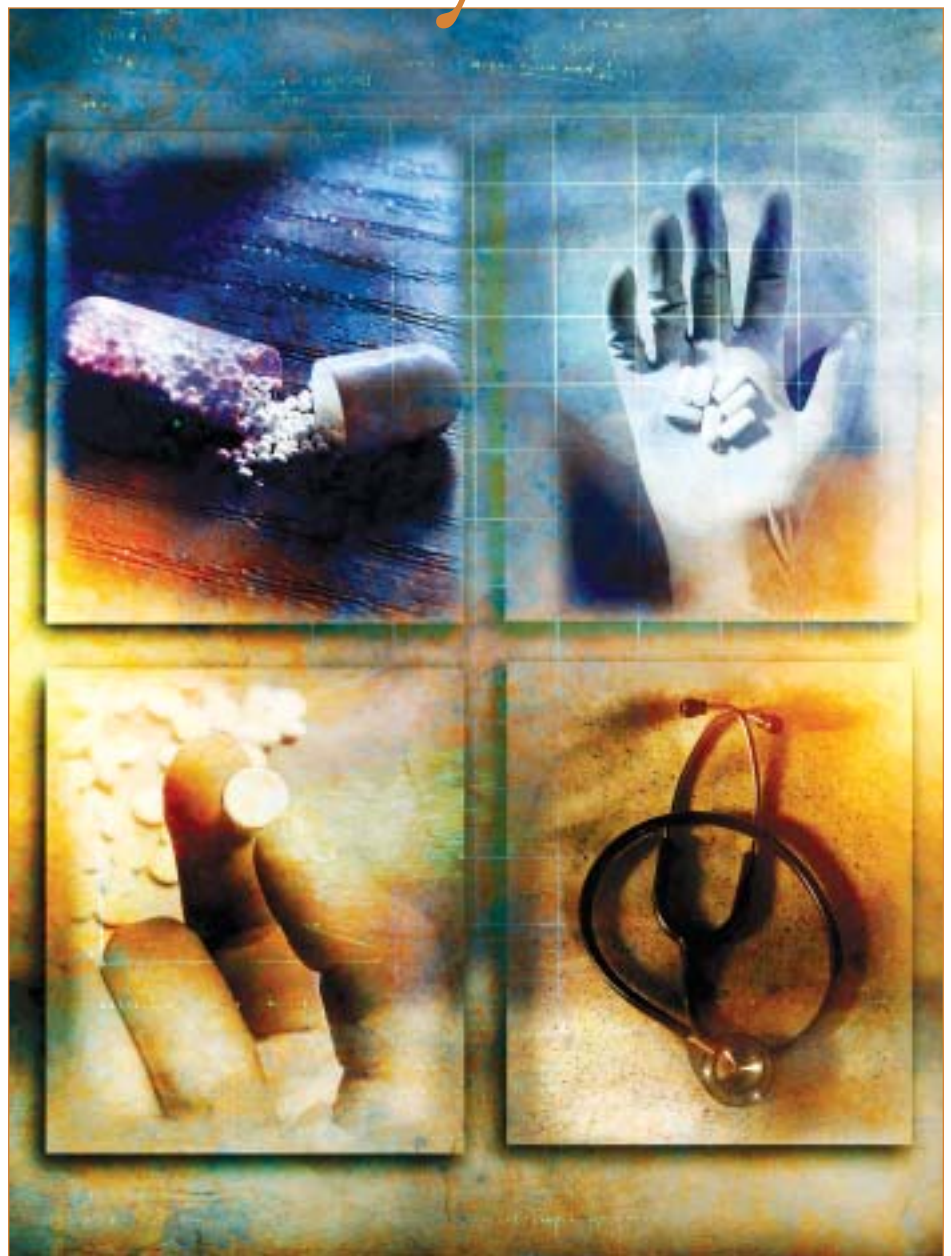


SSHA Deploys Managed Identity Service

In March 2002, following a five year study, Ontario legislated the formation of the Smart Systems for Health Agency (SSHA) with mandates to form a common IT infrastructure and private network to connect more than 150,000 health care providers physicians, community and continuing care providers, hospital and laboratory personnel, pharmacists, and public health professionals across 24,000 sites throughout the province of Ontario. A foundational service of this infrastructure, enabling security and privacy compliance, is its identity management, provisioning, and user registration service.

Smart Systems for Health Agency (SSHA) was created to provide a secure, integrated province-wide networked IT infrastructure to support a series of eHealth initiatives. The goal of these initiatives is to



Through this registration service, a person's identity is verified and validated through a variety of methods that result in a basic, medium, or high level of identity clearance.

integrate health information across Ontario's health system to support health service providers in decision making. The effort was separated in this fashion to allow separate, but inter-dependent delivery of infrastructure components and applications. The shared infrastructure deployed by SSHA was to provide a framework that facilitated the integration of eHealth applications while also assuring the privacy and protection of personal health information.

In response to its mandates, SSHA has built an managed private network that links healthcare providers and SSHA data centers to securely store information. This infrastructure also provides services that allow applications to meet their security and privacy requirements, including common identity services that the applications can leverage. The infrastructure was deployed in 2003 and the first applications began to deploy on it in 2004.

SSHA offers two types of services to its healthcare clients – infrastructure services and information management services. The SSHA network is independent from government and public networks, and access is restricted to approved users. The SSHA infrastructure provides the security to assure protection of personal health information, such as data scrambling capabilities, firewalls in data centers, and registration of authorized clients, subscribers, and applications.

Identity Proofing and Management

It is the registration service that forms the heart of the identity capabilities from which the ability to authorize and

track access derive. Through this registration service, a person's identity is verified and validated through a variety of methods that result in a basic, medium, or high level of identity clearance. These levels of trust relate to the level of information a registered subscriber needs to access. Registration can be linked to a PKI so that registered healthcare providers can encrypt and digitally sign emails and verify the sender of any message. In addition, registered users can be provisioned to the specific application access their needs require and their registration trust level allows.

The SSHA will ultimately provide support infrastructure for seven eHealth applications. These are the Ontario Family Health Network/ePhysician Project (OFHN/ePP), Community Care Connects! (C3), Integrated Services for Children Information Systems (ISCIS), Health Network System (HNS), Ontario Laboratories Information Systems (OLIS), HIV Information Infrastructure Project (HIIP), and Public Health Information Systems.

Mike Pettersen, Manager, Architecture, SSHA, said, "SSHA is mandated to connect all of the public health sector in Toronto, and the health care providers in province. We do that through our infrastructure technologies. On those infrastructure technologies, with the way physicians and the like are going to be communicating, there is a high need for security and having a well identified audit of who is doing what, when. So that automatically led to the need for having a form of identity management that allows us to track all of that."

SSHA chose Oblix COREid for their identity management component.

"We have a very extensive IT infrastructure that consists of multiple data centers," said Pettersen. "One of our big service offerings is around the network space – LAN, ELAN, managed private networks, etc. That's a significant one for getting all the different locations in the province connected within our world. Within that we also have a set of services for communications called our secure messaging infrastructure, which is an email offering that uses our PKI implementation. The majority of our infrastructure is a Microsoft based one – though we have Sun systems in place and do host many different other players."

PKI as an Attribute of Identity

Walter Dan, VP of Integrated Technology Solutions at Allstream, a key implementer on the project, said "The PKI is there to be able to provide security, confidentiality and data integrity to secure email and other services that SSHA will host or support in the future. The identity management solution was brought in to provide a greater level of security from the standpoint of being able to register, enroll, and provision users into many systems, not just PKI. So PKI becomes a managed endpoint to the identity solution."

SSHA has built a comprehensive registration service for their identities. "We separate out the concept of registration – positively identifying our users to whatever level of assurance is required by the applications supported," said Dan. "Registration goes through a process to identify that warm body at the end of



The identity management solution was brought in to provide a greater level of security from the standpoint of being able to register, enroll, and provision users into many systems.

the tunnel. And then the enrollment is actually taking that registration event and committing the individual account into a back end system that requires authentication and authorization. So we've broken identity out into the two concepts."

Provisioning and Rollout

Once users are registered and entered into the identity management system, they can then be provisioned to the various applications. "The infrastructure is there to support the concept of all of these different health care organizations," said Dan. "To date we're around 3,500 to 4,000 users in, done on an application by application basis. The infrastructure is

there, [and] we're ramping up fairly quickly. Within the last couple of weeks we've added a couple of thousand users to support a couple of specific applications and their need for identity management, authentication and authorization."

The SSHA deployment began in late 2002. "It was a significant implementation," said Dan. "This wasn't just on the PKI/subscriber registration, this was everything from the ground up." Requirements analysis and award was completed by early 2003. "The requirements analysis and requirements reviews took three or four

months," said Dan. "And then we went into another six months on the build cycle. That encompassed the building of a PKI solution, identity solution, policy infrastructure build out, two data centers and all of that. In September of 2003 part of the infrastructure went live and has been live since then. More of the applications started to be rolled in during 2004. We are there now today to support applications as they roll out. [For each application] we'll roll out a smaller pilot, prove the concepts, understand what it is that we need to support a given user group. Once we get through that pilot phase and validation phase, then we'll roll it out a little bit deeper."

"An application can deploy much quicker because SSHA has already built all of the plumbing," said Dan. "SSHA provides the ability to take our identity solution and abstract registration from enrollment. Provisioning gives the concept of managing the user's registration event once, and then allowing them to enroll multiple times in multiple organizations against multiple applications. They've already got the data centers, they've already got the identity system, they've already got the PKI system if needed, and basically now the application owner potentially just has to bring an application to the table and everything else, authentication, authorization, user provisioning and user management will be handled by the SSHA infrastructure."

PIPEDA and Privacy Compliance

"One of our key goals within the SSHA infrastructure is to assure privacy and security," said Pettersen. "Our departments are very familiar with all of the policies that have come out. We're constantly revisiting it, and as applications come in we go through a privacy impact assessment and threat

One of our key goals within the SHHA infrastructure is to assure privacy and security. It's really paramount to us that we meet those goals.

and risk assessment each time we introduce something new into the infrastructure. It's really paramount to us that we meet those goals."

"The identity system does not negate the fact that you need to go through those processes each time," said Dan. "Each application that comes on board is introducing different data elements, and each has different privacy and security impacts. But through services and facilities, and through our policy frameworks we help a lot by supporting these people in determining what those privacy levels are, and what they should be doing to negate any risks."

"In Canada we have PIPEDA (The Personal Information Protection and

Electronic Documents Act.) The infrastructure components go through privacy impact assessments, and a lot of the policy and process for registration was vetted through the privacy and security group to come up with those mechanisms. But when [an application] comes on they still have to go through their due diligence to make sure they're using those tools in such a way that privacy is protected and applications are secured."

The SSHA identity framework assists in compliance as well. "We get comprehensive auditing and reporting capabilities in the back end," said Pettersen. "We know the credentials of the various communications traversing our networks and their ingress points

through our systems. These abilities help maintain and enforce our strict security posture."

Summary

Smart Systems for Health Agency is empowered by the Ontario Ministry of Health and Long Term Care with providing the infrastructure needed to improve the flow of patient information within Ontario's health system. Its challenge is to provide its stakeholders with a viable alternative to paper-based record keeping, within a demanding regulatory framework. Its managed infrastructure coupled with a well thought out set of identity management, registration and provisioning services, is well on its way to accomplishing those goals. ■