

Carolinas HealthCare System Simplifies Authentication with SecureAuth IEP

Customer Thumbnail

- 15 hospitals in North and South Carolina
- Headquartered in Charlotte, NC
- Over 1,000 CHS physicians practice in more than 300 locations
- More than 30,000 employees
- Roughly 27,000 PCs
- **Key IT challenge: finding a strong authentication solution that is easy to administer and more cost-effective than tokens**

The Challenge: Replacing tokens with a more user-friendly form of authentication

Carolinas HealthCare System (CHS) had a problem with authentication. With 15 hospitals in North and South Carolina and more than 30,000 employees, strong authentication was becoming a pain point for IT.

CHS relied on tokens from a major security vendor, and the tokens themselves were the problem. While tokens boosted security, the additional security came at a steep cost: drastically increased IT overhead. Every time tokens expired, each time a new employee was hired and every time a token was lost or broken, someone from the IT staff had to manually provision a new token. This workflow was costly, and employees complained about the ease of use and having to keep up with their tokens.

“Tokens worked well from a security standpoint, but our health care workers didn’t like them at all. They had to keep track of them; they often lost or damaged them, and it seemed like they would go missing at the worst possible times, preventing our employees from doing their jobs,” said Todd Greene, Manager of Information Security, Carolinas HealthCare System.

Greene and his security team began looking for an alternative. They attempted to find a vendor that offered strong two-factor authentication that didn’t rely on the use of tokens.

The first two vendors they investigated, however, fell short. The first had bugs in the software that circumvented security and would be difficult to integrate and manage on a daily basis. The second was simply too expensive. Once professional services fees and licensing were factored into the overall cost, the solution was much more cost effective than tokens; however, the return on investment would take significantly longer.

Selection Criteria: Cutting costs and IT overhead without sacrificing security

Greene decided to step back and focus on what exactly CHS needed from a multifactor authentication solution. The first couple of criteria were obvious, the reasons CHS wanted to replace tokens in the first place: cost and usability.

Other selection criteria weren’t as obvious, but were every bit as important. For starters, security couldn’t be sacrificed for simplicity and cost. CHS also hoped to find an authentication system that could leverage their existing data stores – which would help ensure the integrity of the system.

Key Benefits:

- No tokens or additional software
- Auto-enrollment for end users
- No additional data stores
- Simple for IT to expire certificates
- Full X.509 bi-directional authentication

They also needed redundancy beyond a simple cold spare backup, which would require manual intervention in the event of a system failure. CHS wanted a fully redundant system that would automatically kick in when needed.

Next, ease of use is critical, but it's more complicated than simply getting rid of hardware tokens. How difficult is the new process to learn? How do new users enroll into the system? What happens when we want to expire their account?

A final criterion was a unique one. Most software authentication vendors brand their logon screens. CHS wanted to brand its own logon interface and needed to find a vendor who would accommodate this.

The Answer: SecureAuth IEP's two-factor authentication

With those criteria in mind, Greene investigated a company with a unique approach: SecureAuth Corporation. On first glance, SecureAuth's authentication solution, SecureAuth IEP, met all of Greene's criteria. It was an all-software, plug-and-play solution that offered bi-directional security.

When Greene dug deeper, he became more impressed. He was very pleased to learn that SecureAuth integrates, out-of-the-box, with Juniper's SSL VPN.

"For more than two years, we'd been beating on vendors' doors trying to get them to integrate strong authentication with Juniper's SSL VPN. No one would do it," Greene said. "With SecureAuth, in a matter of two weeks we went from initial talks to a pilot.

Each time we asked for additional features, they delivered – usually within a day or two." – **Todd Greene, Manager of Information Security, Carolinas HealthCare System**

SecureAuth's professional services team worked with CHS to customize SecureAuth IEP to meet their unique needs, helping them with everything from help desk tools to a branded logon interface. They also tweaked the enrollment process to include a knowledge-based sign-up option.

"Our CIO took part in the pilot and loved SecureAuth. His next question to me was 'how quickly can we roll this out?'" Greene said.

Handling HIPAA

For certain industries, such as health care and the financial sector, a key consideration with any security solution is meeting industry regulations. CHS is no exception, having to comply with HIPAA.

Greene noted that authentication is trickier in health care than in other regulated industries like banking. When a user logs into a bank account, it's usually a one-to-one relationship. In health care, on the other hand, a physician logs into a system and can access any number of patient records; a one-to-many relationship.

“If someone breaks into my bank account, it’s a problem, but it’s not the end of the world,” Greene said. “The bank will replace my funds and the attacker won’t learn much about me beyond how much money I had in my account and my recent activity. If the wrong person accesses my health records, though, they can learn all sorts of sensitive personal details about me.”

In health care organizations, strong, trusted authentication is a must. Anything less could put confidential data at risk.

Other Key Benefits:

- **Evaluation, proof of concept, and deployment completed in less than 30 days**
- **No APIs required**
- **Full protection from man-in-the-middle replay attacks**
- **Protection against phishing**
- **Price point and end-user ease of use comparable to that of user name and password**

The benefits of all-software authentication

SecureAuth IEP is a tokenless, non-phishable, two-factor identity and authentication solution that also includes integrated SSO and IdM services for cloud, on-premise web, VPN and mobile resources. For CHS, SecureAuth provided a true plug-n-play authentication mechanism that provides strong authentication into the network.

SecureAuth IEP’s unique technology transparently provisions clients with an x509 digital certificate (credential). SecureAuth then validates the credential as a second factor in the authentication process. Because the first factor is the actual username and password, the enterprise administrator retains 100% control over access to enterprise resources.

SecureAuth IEP works by authenticating both the client and the server for each session via a non-exportable cryptographic credential. When authorized users logs into the network for the first time or log in with a new device, they’re immediately redirected to the SecureAuth registration system, which contacts them through email, text message or phone to finish the enrollment process.

The SecureAuth registration process is customizable and allows for additional factors, such as knowledge-based questions, to positively identify users. Once the user finishes the enrollment process, SecureAuth installs the certificate on the user’s client device. From that point on, whenever that person logs onto the corporate network, they’re instantly authorized. End users are minimally impacted, never denied access, and never required to make a help desk call.

“SecureAuth IEP makes life much easier for our IT staff,” Greene said. “One of the things we had trouble with in the past was expiring hardware-based tokens. With tokens, it’s a big headache. With SecureAuth, it’s easy. If you choose, you can have all your tokenless certificates expire in 90 days.” Greene said.

About SecureAuth IEP

A true plug-n-play authentication mechanism, SecureAuth provides strong authentication into the network as well as providing SSO and IdM Services for cloud, on-premise web, VPN and mobile resources.

SecureAuth IEP works by authenticating both the user and the client for each session via a non-exportable cryptographic credential. When an authorized user logs into the network for the first time or logs in from a new device, that person is immediately redirected to the SecureAuth registration system, which contacts them through email, text message or phone to finish the enrollment process.

Once the user finishes the enrollment process, SecureAuth IEP installs the certificate on the user's client device. From that point on, whenever that person logs onto the corporate network, they're instantly authorized.

For end users, SecureAuth IEP is as easy to use as user names and passwords alone. For IT, it is much easier to deploy and administer than any other type of authentication. Relying on existing enterprise data stores, SecureAuth integrates with Juniper SSL VPNs, Cisco SSL VPNs, Cisco IPsec, Microsoft ASP .NET applications, Google Apps, [Salesforce.com](https://www.salesforce.com) and more.

About SecureAuth Corporation

SecureAuth delivers identity enforcement for cloud, web, and VPN and mobile resources. SecureAuth's all-in-one Identity Enforcement Platform delivers integrated 2-Factor Authentication, SSO, and IdM services that are 100% configurable for less than the cost of tokens.



Please visit www.gosecureauth.com

SecureAuth and SecureAuth IEP are registered trademarks of SecureAuth Corporation.

Once the tokenless certificate expires, the only thing a user will notice is an additional step in the authentication process, a kind of mini re-enrollment. They input their personal information and then SecureAuth authorizes them back into the system. Users could receive a PIN via text message or email, or they could simply answer their knowledge-based questions. It's a simple process – one requiring no IT intervention – that strengthens the integrity of the authentication process.

Adding redundancy and ensuring five nines

During the SecureAuth IEP deployment process, Greene realized that he needed to find a way to include failover capabilities. "We need five nines across the board," Greene said. Greene and the SecureAuth professional services team worked to develop a redundant, highly available backup system.

Accomplishing this request was easy. CHS ordered a second SecureAuth IEP Appliance and linked it to load balancers. It wasn't the standard way SecureAuth deploys the solution, but SecureAuth had come up with a redundant solution in a short time to meet their needs.

ROI and ongoing cost savings

Greene estimates that cost savings over the next four years at their current growth rate will be approximately \$782,000. This includes costs related to their growth, hardware replacement, software maintenance, and labor to distribute hard tokens manually.

"I should note that other vendors charge a lot of money for professional services," Greene said. "With SecureAuth it's just part of the package. They added features and customized the SecureAuth product for us, all while keeping our overall costs low. It would probably cost us more, when you factor in help desk calls, to rely on old-fashioned user names and passwords. Compared to traditional hardware-based tokens, SecureAuth IEP paid for itself almost immediately."