



Authentication Case Study

OneHealthPort™

Company Background

OneHealthPort (OHP) was founded by a consortium of health plans and health care providers in the Pacific Northwest. The OneHealthPort security service provides a single point of connection to major hospitals and health plans.

Project Drivers

OneHealthPort was founded to provide a single point of access for physicians and other healthcare providers to access information at hospitals and health insurance companies. The consortium recognized the need for a shared security solution to provide secure access for a large number of providers, while allowing health plans and hospitals to continue using legacy systems. The project could only be a success if it brought productivity benefits to both sides, so the security technology could not be a barrier to adoption.

Scope

The scope of the project is to cover healthcare providers, health insurance plans, hospitals and other service providers (such as labs) in the Pacific Northwest.

IT Environment

The health insurance companies' web sites accessed through the service run on a wide variety of technologies, including Cold Fusion, ASPs, Weblogic, J2EE, and Websphere. The directory information was held in a variety of platforms including Netegrity, SunOne, Oracle, Microsoft Active Directory, and SQL server. OHP needed to develop a service that could interoperate with all of these technologies, and that would work with the wide variety of client platforms used by providers. The service, including the authentication solution is hosted by CyberTrust.

Why OHP Chose the TriCipher Armored Credential System™ (TACS)

OHP first tried to implement a traditional PKI system but found it too difficult and too expensive for their purposes. Their partner, CyberTrust, discovered the TriCipher Armored Credential System and proposed it to OHP.

The set of requirements filled by TACS includes:

- **zero footprint** on user desktop to make it easy for providers to adopt
- **cryptographic control** of data in transport
- **strong authentication** behind the scenes
- adept **security credential and key management**
- application **identity mapping** processes
- **standards-based** support for a variety of infrastructure components, including Web servers, Web browsers, SSL accelerators, routers, application servers, databases and 2nd factors
- a specialized **identity management appliance** that acts as a central controller for user authentication and user data profiles.
- **ability to federate** with other authentication services
- **flexible multi-factor infrastructure** that supports easy migration of groups of users to 2-factor authentication over time
- **ability to use memorable passwords**

Benefits

OHP does a user survey to determine what benefits the provider community is seeing from using the service. Over 80% say the service saves them time, and 85% report that it saves them phone calls and faxing to the insurance companies. About 30% cite a decrease in the number of claims rejected and faster payments. An astonishing 48% report that using the service increases their job satisfaction.

Deployment

The first implementation, with Premera Blue Cross, took three to four months, but subsequent implementations with insurance providers have taken about 100 person-hours over 5 weeks or so. The five weeks includes the minimal time needed for training, as well as creation of a media and promotion strategy to drive usage.

Adoption by doctors' offices and other providers is straightforward. They sign up for a credential online through the service, their identity is confirmed, and the credential is issued. They sign one HIPAA agreement to work with all the health plans and service providers and only need to sign on once to access all member web sites.

Reliability

The TACS Appliance has never had an outage since OHP went live in March, 2003.

Future

The OHP service continues to grow and now serves 6,900 organizations and over 15,000 individual providers. OHP plans to add the ability for participants to perform digital signatures and to send secure email. OHP is also exploring other forms of second factor authentication, including mobile options such as PDAs or cell phones and using the computer or other login device as a second factor.



Tricipher, Inc.
1900 Alameda de las Pulgas
Suite 112
San Mateo, CA 94403
Tel: +1.650.372.1300
Fax: +1.650.372.1301
www.tricipher.com

