United States Environmental Protection Agency

Office of Information Collection:

The Exchange Network E-Authentication Pilot

In December 2005, EPA completed a one-year pilot demonstrating how they could provide credential validation services to participating state and federal partners by leveraging an interface between the Environmental Information Exchange Network (EN) web services and the federal e-Authentication architecture. E-Authentication is the process of confirming the identity of individuals who use credentials to sign-on to computer systems or create electronic signatures. Credentials include PINS, passwords, and public key infrastructure (PKI) certificates.

Purpose

EPA's EN can provide a medium for web-services-based secure data exchange with and among our partners. Through the EN e-Authentication Pilot, EPA showed that the EN web services can be combined with the federal e-Authentication architecture to offer credential validation services to any partner that can access the EN. For example, by linking EN PKI functionality with the Federal Bridge, the pilot demonstrated that participating applications can accept and rely on PKI certificates that are validated by the EN. The pilot showed that:

Two Federal e-Authentication Strategies:

- For PKI credentials: use of the Federal Bridge to accredit credential providers and to link relying systems to those providers for credential validation.
- For non-PKI credentials (e.g., PINS and Passwords): establish "trust circles" between credential providers and relying systems and use SAML assertion-based authentication.

- The EN can support partners with Network nodes who want to accept PKI certificates to authenticate application users but can't afford the full cost of issuing, managing, and authenticating PKI certificates;
- The EN can support partners with Network nodes who want to accept non-PKI credentials that they do not issue or manage by establishing "trust relationships" with non-PKI credential providers and supporting assertion-based authentication, using Security Assertion Mark-up Language (SAML); and
- The e-Authentication vision of interoperable credentials can include any state, tribe, or territory with an operational node on the EN.

Background

The federal e-Authentication initiative supports the re-use of credentials across computer systems. The goal is to minimize or eliminate the need to register for and use multiple credentials, reducing the burden on federal employees, businesses, ordinary citizens, and state and local government officials who access federal systems. If credentials can be re-used, then individuals need not acquire and keep track of separate credentials for each computer system they access. In principle, a single credential could be used across all systems.

To enable credential re-use, the General Services Administration (GSA) is developing a government-wide e-Authentication architecture, specifically designed to allow computer systems to accept credentials that they did not issue. In the EN e-Authentication pilot, EPA partnered with GSA to demonstrate e-Authentication architecture's strategy for both PKI and non-PKI credentials.

For PKI credentials, the strategy is to make credentials issued for different systems, by different credential authorities, interoperable. Prior to the EN e-Authentication pilot, EPA and Illinois had already completed a pilot testing the interoperability of their PKI certificates. Working with GSA, both EPA and Illinois were able to successfully accept and validate each other's certificates. Specifically, Illinois certificates were accepted and validated by EPA's Central Data Exchange (CDX), and EPA certificates were accepted and validated by the Illinois electronic Discharge Monitoring Report (eDMR) system using GSA's e-Authentication architecture. The pilot provided the first demonstration of credential interoperability between state and federal governments.

For non-PKI credentials, the strategy is to promote a "federated" approach to credential issuance and validation. The federated approach limits the use of a credential to interactions between the credential holder and the system that issued it, to minimize the risk of compromising the secret – the PIN, password, personal knowledge, etc. – that the credential may include. Under the approach, a particular end-user presents his/her credential to the issuing system, which validates it and then sends an authentication "assertion" to any other system in the "federation" that the credential holder wishes to access. These "assertions" are sent in a standardized format provided by SAML.

Current Status

EPA is now developing a production version of the PKI component of the EN e-Authentication pilot, with the objective of using the CDX EN Network Node (CDX-0Node) to provide the PKI certificate validation services to Indiana's Emission Inventory Tracking System, which receives air emissions reports from facilities regulated under Indiana's air program. The project is a partnership between EPA, GSA, and Indiana. With productions scheduled to begin March 31, 2007, the project will fulfill EPA's commitment to OMB: to implement e-Authentication for CDX-Node by the end of the second quarter 2007.

More Information

David Schwarz
Information Exchange Partnership Branch
Office of Environmental Information, OEI
(202) 566-1704
schwarz.david@epa.gov

January 2007