

## E-Authentication

*Making trust possible*



### **E-Authentication Delivers Technical Architecture**

*Another major element of the Authentication Service Component of the Federal Enterprise Architecture is now in place.*

The E-Authentication Initiative ([www.cio.gov/eauthentication](http://www.cio.gov/eauthentication)) is pleased to announce that its technical architecture has been ratified by the E-Authentication Executive Steering Committee (ESC). The ESC, comprised of 22 Federal agencies, approved the Initiative's technical approach without opposition.

E-Authentication is the cross-cutting initiative of the E-Gov component of the President's Management Agenda. The program's mission is to provide online identity verification services to the U.S. Government, particularly to the other 24 E-Government Initiatives.

The Initiative's [technical architecture](#) is a major element of E-Authentication, and its delivery means Federal agencies will soon be able to implement the Authentication Service Component of the Federal Enterprise Architecture.

The E-Authentication technical architecture features an open standards-based, federated approach. This approach allows E-Authentication to meet the diverse authentication needs of its many customers with one service offering based on a single set of policies, but supported by multiple technologies and interoperable products. This gives E-Authentication the ability to deliver a uniform approach to authentication government-wide, and it gives agencies value by providing a choice of technologies and interoperable products to achieve their authentication needs.

The open standard that the E-Authentication architecture currently supports is the Security Assertion Markup Language (SAML) 1.0 artifact profile. A government IT system that wishes to implement the Authentication Service Component would do so by purchasing and integrating an authentication product from the E-Authentication [Approved Technology Provider List](#). The list is made up of products that support the SAML 1.0 protocol and have demonstrated basic interoperability in the E-Authentication Interoperability Lab.

Interoperability is a key tenet of the E-Authentication technical approach because it means that all government IT systems and all identity credential service providers can work within the E-Authentication environment without all having to purchase the same product or suite of products. The ability to choose from among a number of interoperable products saves E-Authentication's federal customer agencies money, and gives them the ability to find the product that best integrates with their back-end systems.

The field of authentication is growing rapidly, particularly the area of federated identity. As industry makes rapid progress in this area, protocols in addition to SAML 1.0 artifact profile will mature and gain traction in the marketplace. The E-Authentication technical architecture has been developed to account for this evolution, and it will expand to include these protocols as they become viable. The E-Authentication Initiative is closely tracking – and in fact, working with the groups that are driving – the development of next-generation authentication schemes like the Liberty Alliance, SAML 1.1, Shibboleth and the Microsoft WS Federation.

Through the E-Authentication Bulletin, we will keep you informed of our progress, as well as the advent of new authentication protocols and technologies.

In the meantime, if you have an application that is planning to implement E-Authentication in the near future, or if you want more information on E-Authentication, contact the E-Authentication Program Management Office at [e-authentication@gsa.gov](mailto:e-authentication@gsa.gov), or visit our Web site at [www.cio.gov/eauthentication](http://www.cio.gov/eauthentication).