



Background

CTS has deployed a new service for Active Directory Federation Services (ADFS) to provide the ability for state employees in the Enterprise Active Directory (EAD) to authenticate to SaaS applications using their EAD credentials. CTS has made the service available and is currently working with Apptio, the first SaaS application to connect with the ADFS Service.

Agencies have also been asked to notify CTS about upcoming SaaS plans where authentication is needed for EAD users. This will provide awareness of upcoming agency plans as well as initiate the discussion about requirements to be included by the agencies in their procurements and negotiations regarding ADFS and SaaS applications.

Business Driver

The OCIO inquired about using a cloud-based tool as an alternative to ADFS. This paper calls this Identity as a Service (IDaaS). The driver for consideration would include speed to deploy applications for SaaS authentication (SaaS providers would already have connectors with cloud IDM vendors), account management by the agency, and low cost.

Overview and Potential Benefits of IDaaS

- The inquiry assumes that the speed to make a SaaS application ready for use with a cloud provider will be faster than that of connecting to the CTS ADFS service. Vendors provide lists of SaaS providers with whom they have an existing connector.
- The inquiry assumes that account management will be performed by the agency and speed provisioning and de-provisioning applications and users
- Auditing provided by cloud-based vendor

Questions and Answers Relating to IDaaS and ADFS Offering

- a) When an EAD agency has a requirement to have CTS connect to a SaaS provider, what happens?

CTS will work with the vendor to create a trust between ADFS and the vendor Secure Token service and create claim rules to pass the vendors required claims/assertions.

- b) What does it take for CTS to “connect” to a new application, what are the steps?

The basic steps include creating a “Relying Party Trust” between the EAD ADFS and the vendors Secure Token service. This is a relatively straight forward process that requires exchanging a MetaData file or creating a Trust manually based on the vendors



January 4, 2013

requirements. Claim rules also need to be created based on the claims required by the vendors secure token server and application(s). This is also a relatively straightforward process depending on how well the vendor has their requirements documented. This is being tested now with Apptio.

c) What roles are delegated to agencies in support of ADFS SaaS applications?

In a typical scenario CTC would be able to grant or restrict access to agencies based on membership in domain security groups. Agencies then would have the ability to grant or restrict access to staff by maintaining the membership of the domain security group. Vendor RBAC models may require centralization of some management functions within the SaaS environment depending on the shared nature of the application and the vendors ability to delegate roles within the application. Roles will also vary from vendor to vendor and from application to application.

d) How does c) compare and contrast to what IDaaS vendors provide?

In the case of one vendor, it appears that the granting or restricting of access would simply be moved from management via domain security groups to management via the vendors interface. The ability to delegate this function in the vendor tool management interface is currently unknown. Additional research would be required.

e) What about account management and provisioning and de-provisioning access to the SaaS application?

CTS assumes this would be controlled by the agencies maintenance of the security group memberships the same as in c).

f) When an agency has an employee who leaves, what is the de-provisioning activity in EAD and ADFS?

This varies by agency and in most scenarios would be the agency responsibility, the same as removing access to domain resources by removing the account from domain security groups.

g) What auditing will we be able to provide an agency regarding use in their agency

This is currently under review in the ADFS infrastructure. Currently unknown what individual SaaS vendors may be able to provide. Additional research would be required.

h) How will CTS provide a list of which agencies are using which SaaS solutions



January 4, 2013

CTS would provide this based on which domain security groups are allowed to use the ADFS Trust with each SaaS vendor and the membership of those security groups.

Additional Notes:

A follow on consultation conference call is scheduled with Gartner on 1/23/13 to the session conducted in October 2012. This will provide an opportunity to review items noted above requiring additional research.

Estimated Cost for IDaaS:

Service Cost:

Based upon a preliminary consultation with Gartner on October 12, 2012 the 'center of gravity' for pricing is between \$2 - \$3 per user/per month for basic federation functionality. Per Gartner, this pricing would likely decrease with higher volumes of users. There are other costs as well (such as creating new federations) that vary from vendor to vendor.