**Service Providers, Identity Providers & Security Tokens**

**Service Providers (SP)**

A Service Provider (SP) is an entity that provides Web Services. Examples of Service Providers include Application Service Providers (ASP), Storage Service Providers (SSP), and Internet Service Providers (ISP).

A Service Provider relies on a trusted Identity Provider (IdP) or Security Token Service (STS) for authentication and authorization. In the WS-Federation model a Service Provider is called a “Relying Party” (RP). In SAML, the XML-standard for exchanging data, the security domains that information is passed between are a Service Provider (SP) and an Identity Provider (IdP). SAML’s Service Provider (SP) depends on receiving assertions from a SAML authority or asserting party, a SAML Identity Provider (IdP). Other Service Provider technologies important to Identity Management include Software-as-a-Service (Saas), software offered using an Application Service Provider (ASP) model; and Cloud computing providers.

**Identity Providers (IdP)**

An Identity Provider (IdP), sometimes called an Identity Service Provider or Identity Assertion Provider, is an online service or website that authenticates users on the Internet by means of security tokens, one of which is SAML 2.0. In the WS-Federation Model an Identity Provider is a Security Token Service (STS). Service Providers depend on an Identity Provider or Security Token Service to do the user authentication. OAuth is an important protocol for IdP services as most major web services are also identity providers, mainly through the use of OAuth. These include Google, Facebook, Yahoo, AOL, Microsoft, PayPal, MySpace, and Flickr among many more. Furthermore, all major email providers offer OAuth IDP (Identity Provider) services.

**Service Provider vs. Identity Provider**

“Provider” is a generic way of referring to both IdP’s and SP’s. There are overlaps when it comes to defining Identity providers vs. Service Providers. According to the OASIS organization that created SAML, an Identity provider is defined as “A kind of provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.”

A Service Provider is “A role donned by a system entity where the system entity provides services to principals or other system entities” and a Federation is “An association comprising any number of service providers and identity providers.”

In simple terms and as they relate to Identity Management, an Identity Provider can be described as a Service Provider for storing identity profiles and offering incentives to other SP’s with the aim of federating user identities. It should be noted however that Identity Providers can also provide services beyond those related to the storage of identity profiles.

**Security Token Service (STS)**

Security Tokens, sometimes called Identity Tokens, Authentication Tokens or even Software Tokens, play a major role in Identity Management as they are the device of choice for authenticating and authorizing a user’s identity or “digital identity.”

A Security Token Service (STS), sometimes mistakenly referred to as a Secure Token Service, is the web service that issues Security Tokens. An STS is inextricably linked to WS-Security as a Security Token Service (STS) issues security tokens as they are defined in the WS-Security specification. In essence, an STS is a WS-Trust Identity provider. A SAML assertion in WS-Trust is a kind of security token.