Security Assertion Markup Language (SAML)

Introduction

- It is a standard for authentication and authorization between the identity provider and the service provider.

- It is XML based and uses base64 encryption

- SAML is defined in terms of Protocols, Bindings, Assertion and Profiles

- SAML uses SSO - Single-Sign On - a term that means that a user can sign in once and use the same credentials can be reused to log into other service providers.

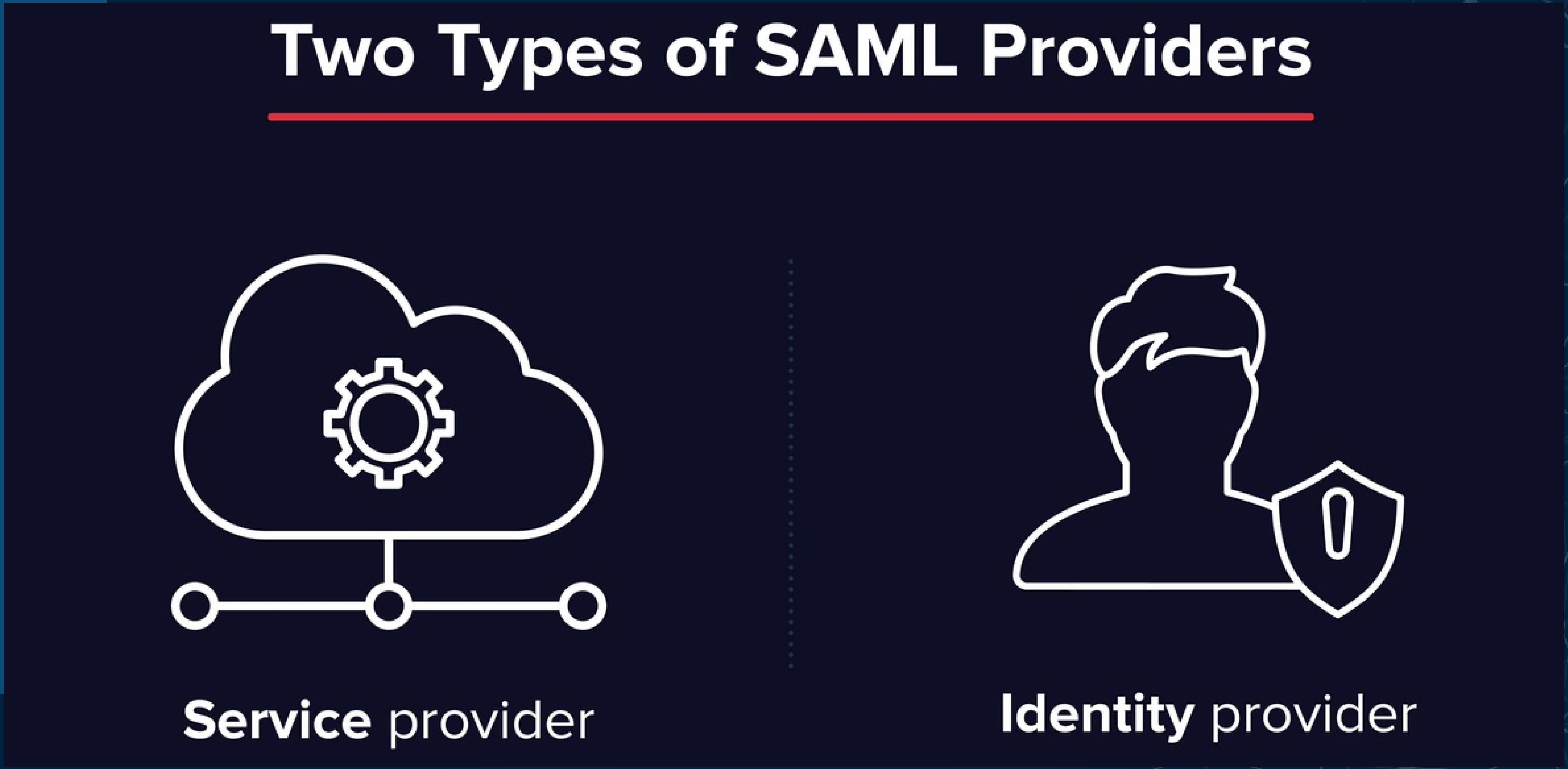
Uses

- It simplifies authentication and authorization.

- Makes it possible to keep the identity provider and service provider exist separately from each other.

- Secure method of passing user authentication & authorization between the Identity provider and service provider.

SAML PROVIDER TYPES



Two Types of SAML Providers

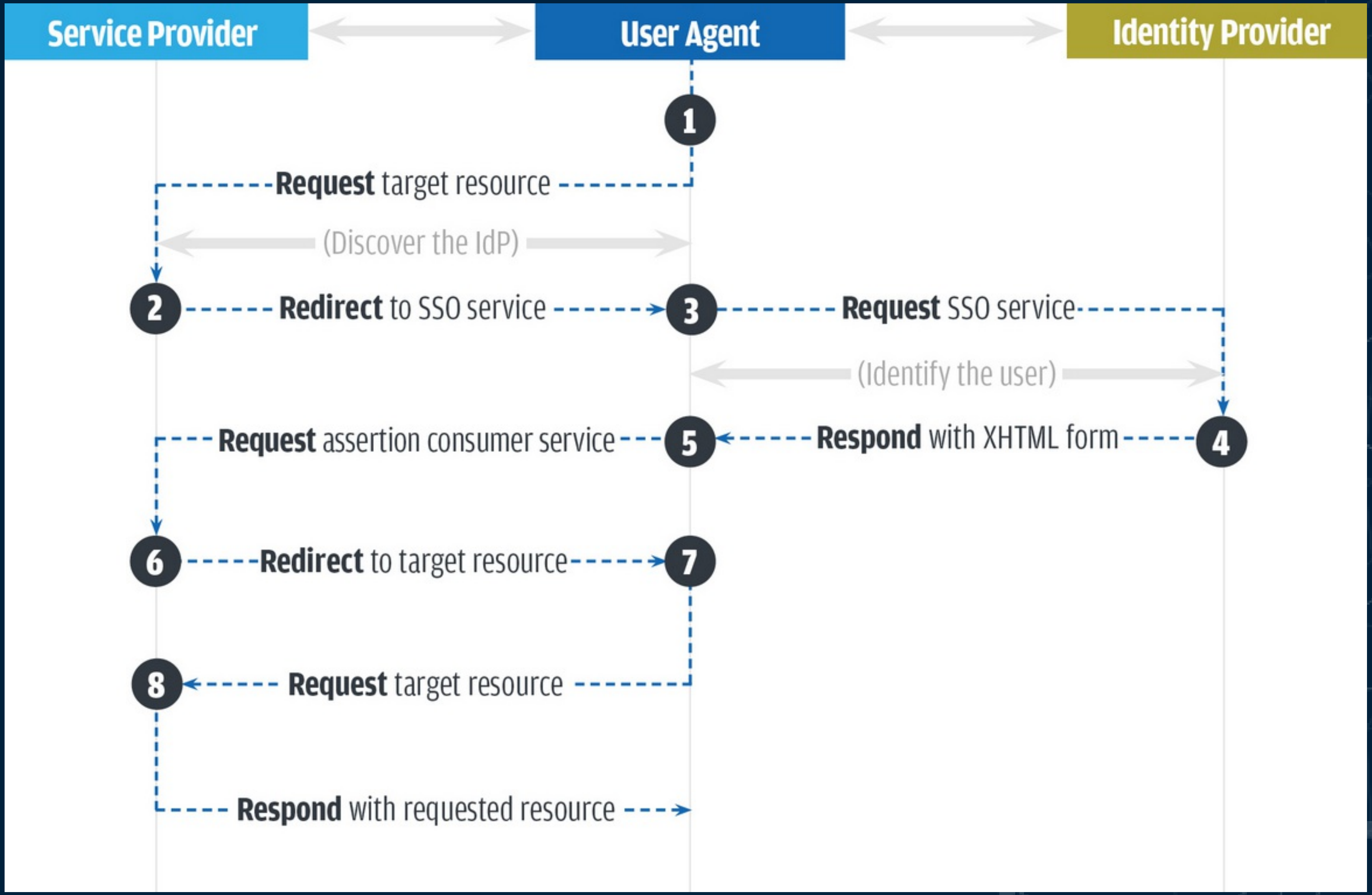
Service provider

Identity provider

SAML PROVIDER TYPES (CONTINUED)

- A SAML provider is a system that helps a user access a service they need. There are two primary types of SAML providers, service provider, and identity provider.
- A service provider needs the authentication from the identity provider to grant authorization to the user.
- An identity provider performs the authentication that the end user is who they say they are and sends that data to the service provider along with the user's access rights for the service.
- An Example of identity provider would be OneLogin An Example of service provider would be Salesforce

SAML FLOW



Service Provider

User Agent

Identity Provider

1 **Request** target resource

(Discover the IdP)

2 **Redirect** to SSO service

3 **Request** SSO service

(Identify the user)

4 **Respond** with XHTML form

5 **Request** assertion consumer service

6 **Redirect** to target resource

7 **Request** target resource

8 **Respond** with requested resource

Why use SAML

- Standard
  - Designed to work well with any system independent of implementation.
  - Open approach without any interoperability issues
- Security
  - Does not store identities therefore no breach in security
  - Uses public key infrastructure to protect asserted identities
- User experience
  - User's access multiple applications with a single set of credentials entered once

SAML Protocols

- Assertion Query and Request Protocol
- Authentication Request Protocol
- Artifact Protocol
- Name Identifier Management Protocol
- Single Logout Protocol
- Name Identifier Mapping Protocol

SAML Assertions

- Authentication
- Attribute
- Authorization decision

SAML Bindings

Mappings from SAML request-response message exchanges into standard messaging or communication protocols are called SAML protocol bindings.

SAML Profiles

- Web Browser SSO Profile
- Enhanced Client and Proxy (ECP) Profile
- Identity Provider Discovery Profile
- Single Logout Profile
- Name Identifier Management Profile
- Artifact Resolution Profile
- Assertion Query/Request Profile
- Name Identifier Mapping Profile