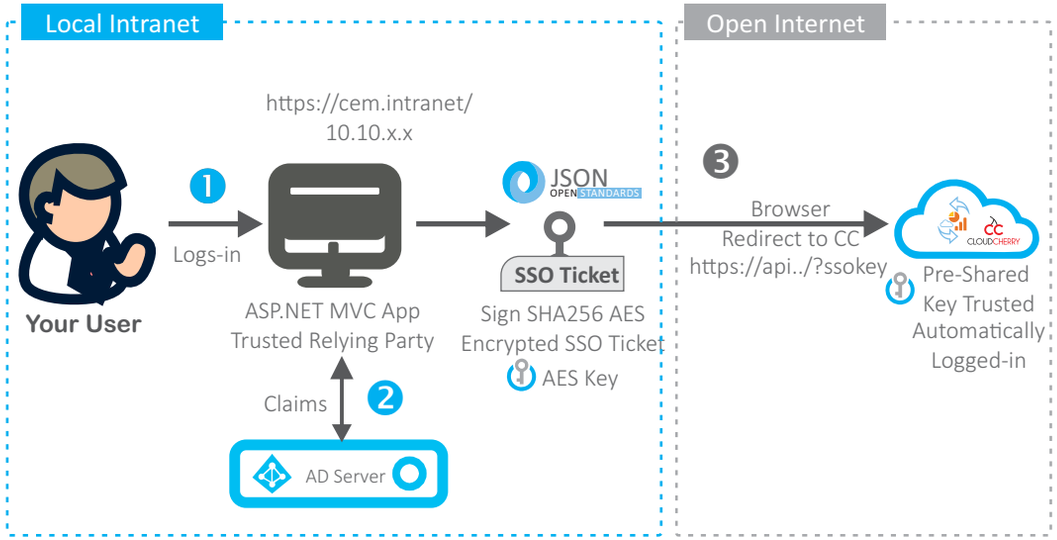
JSON Web Token -vs- SAML <SingleSignOn/>

JSON SSO

AVAILABLE 2017



Local Intranet

1. Local intranet user on browser accessing local intranet server (Part of local AD/Domain) hosting the SSO ASP.NET MVC application
2. Local intranet application using [WS-Federation Passive Protocol] to check for claims locally, if valid claims found, then create/sign JSON SSO ticket

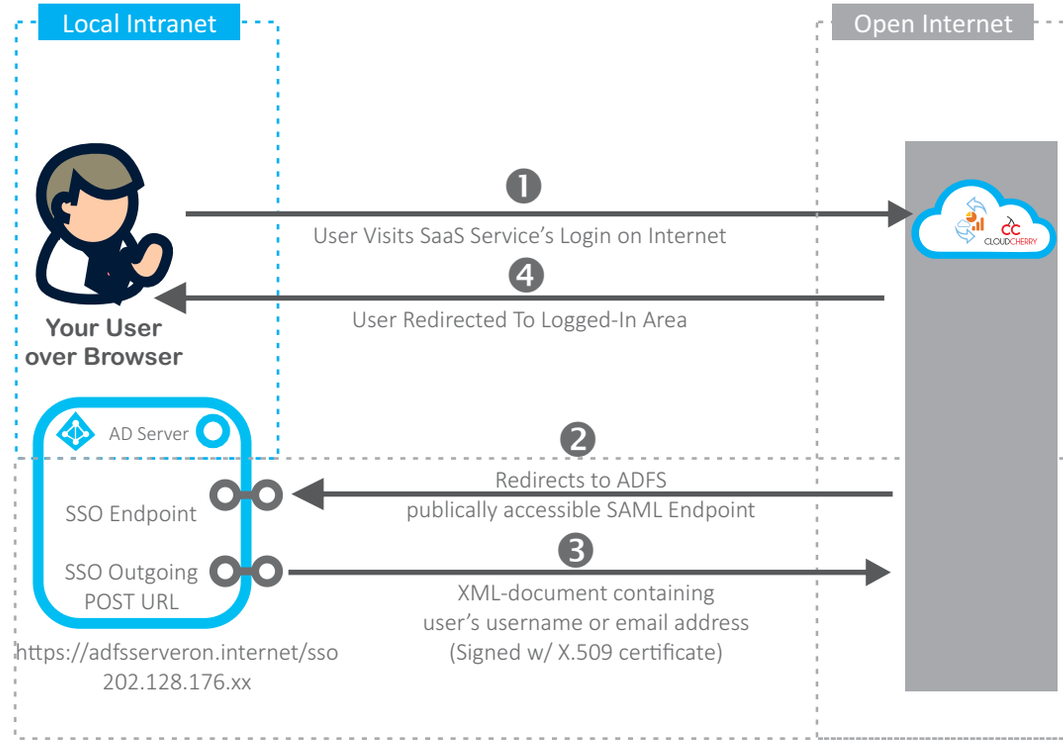
Internet

3. User's browser forwards to open internet for access to CEM dashboard

Key Features

- Enables sign-on w/o separate login/password (SSO)
- **Modern Open Standard(JSON) Recommended w/ oAuth 2/OpenID**
- **Supports Windows Integrated Authentication**
- **Highly Secure (Complete SSO flow is local, zero internet exposure of AD)**
- **NSA Grade Encryption AES256 w/ SHA256 Hashed Key (first and only publicly accessible cipher approved by the National Security Agency (NSA) for top secret information)**

SAML



Open Internet

1. Local Intranet User on Browser accessing remote SaaS application, is redirected to publicly accessible Web SAML 2 SSO End-point
2. ADFS authenticates using SAML 2 Request from SaaS App
3. ADFS POST's XML document containing username/email back to SaaS App
4. SaaS application setups session and redirects users into logged in area

Key Features

- (Same) Enables sign-on w/o separate login/password (SSO)
- **Legacy XML Standard**
- **Less secure based on configuration (Almost all implementations require ADFS Server or reverse proxy exposure to Open Internet to enable receiving SAML login request)**