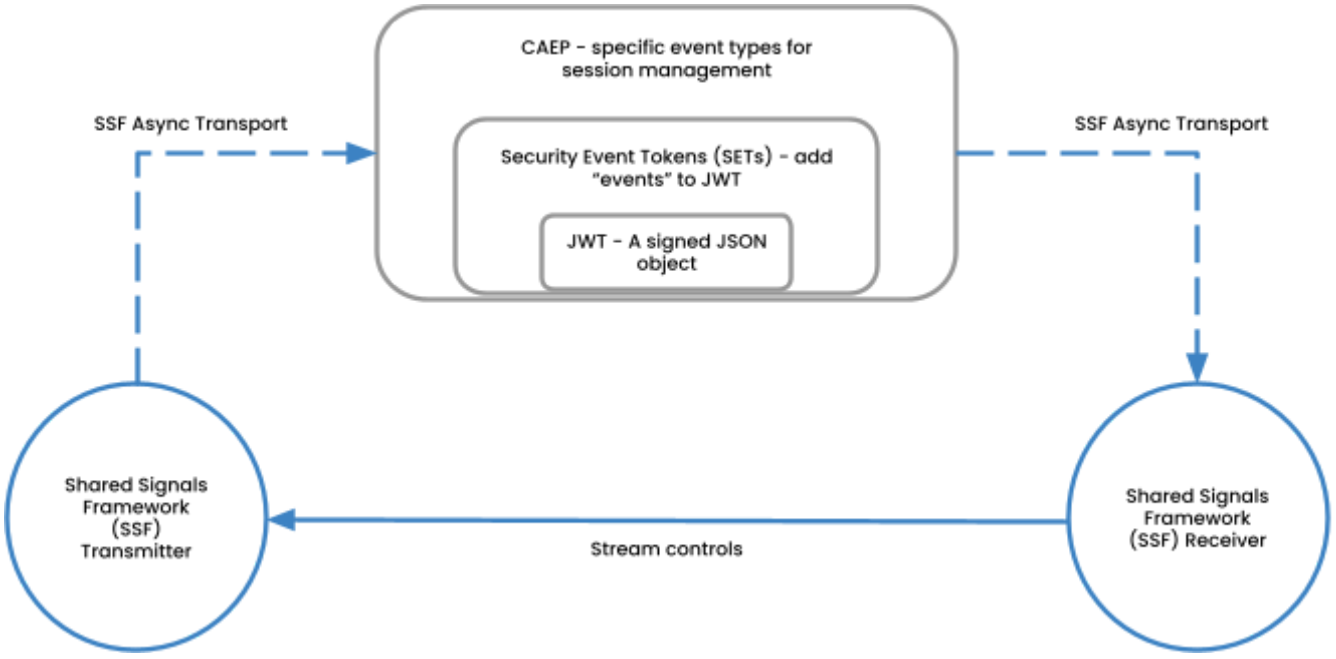
Why CAEP and SSF?

Single sign-on enables users to access hundreds of cloud services. However conditions that assert the validity of the login can change instantaneously, and at different services such as your identity provider, device management service or even a cloud application. The Continuous Access Evaluation Profile (CAEP) and the Shared Signals Framework (SSF) are standards from the OpenID Foundation, which communicate signals relevant to the user's access posture so that each service can re-evaluate whether the user should continue to be signed in. In short, it helps instantaneously close doors that single sign-on leaves open.

Who Uses It Today?

Leading companies like Apple, Disney, Jamf, Okta and SGNL support CAEP and SSF in production today. The United States Internal Revenue Service (IRS), login.gov and ID.me operate production services that exchange Risk Incident Sharing and Coordination (RISC) events, which are also transported using SSF.

CAEP and SSF in a Nutshell



- SSF provides a reliable asynchronous transport with negotiation for specific event types and subjects
- SETs contain the information relevant for the security event
- CAEP is the profile that describes events specific to session properties / security.

About OpenID

Founded in 2007, the OpenID Foundation (OIDF) is a global open standards body committed to helping people assert their identity wherever they choose. We are a global & vibrant community where identity peers and thought leaders convene to craft the identity ecosystems of tomorrow. Our mission is to lead the global community in creating identity standards that are secure, interoperable and privacy-preserving. Find out more at openid.net.

2025 Interop participants