

Two New CAEP Event Types

Atul Tulshibagwale, CTO, SGNL

CAEP Events

- Descriptions of events that impact session properties
- Non-prescriptive
- Current Event Types
 - Session Revoked
 - Credential Change
 - Assurance Level Change
 - Device Compliance Change
 - Token Claims Change

New Event Types

- Session Established
 - Indicates that a new session is observed at the Transmitter
 - Can bind user to environmental properties seen at the Transmitter
 - IP Address
 - User Agent fingerprint
- User Present
 - Indicates that a user with an existing session was observed to be present at the Transmitter
 - Can provide observed environmental properties (same as in the “established” event)

Use Cases

- Session Established
 - Notify completion of a federated identity exchange initiated from an IdP
 - Notify a new session creation at an application that maintains persistent session state
 - Optionally binds a session to its context at the Transmitter so that the Receiver may detect session hijacking
- User Present
 - Detect application usage
 - Detect lateral movement
 - Detect impossible travel across applications

Event Specific Claims

- Apply to both events, Session Established and User Present
- Optional **ctx** claim, containing the following optional fields
 - **ip**: The RFC 4001 string representation of the IP address
 - **uaf**: A unique fingerprint that represents the user agent
- The **uaf** value **MUST** be the same for all sessions belonging to the same user at the same Transmitter. It **MAY** be different for different users' sessions at the same Transmitter

Best Practices for These Events

- Session Established Event
 - Subject Identifier SHOULD contain session identifier
 - Receiver can correlate “established” with “present” events
 - Subject Identifier MAY contain a device identifier
- User Present Event
 - Subject identifier SHOULD contain session identifier to correlate with “established” event
 - Subject identifier MAY contain a device identifier