FIDO and the Shared Signals Framework

Orchestrating Agile and Secure IAM Workflows

October 2025

Authors:

Jacob Harlin, Microsoft

Josh Cigna, Yubico

Martin Gallo, HYPR

Sumana Malkapuram, Netflix

Apoorva Deshpande, Okta

Abstract

In today's fragmented enterprise security landscape identity and access management (IAM) systems often operate in silos. The need for cohesive, real-time coordination across platforms is more critical than ever. This paper introduces a strategic approach that combines FIDO-based strong authentication with the OpenID Foundation's Shared Signals Framework (SSF) to orchestrate agile and secure IAM workflows, enable stronger continuous authentication, and promote collaborative defense against identity threats.

FIDO protocols offer a robust foundation for user authentication as they leverage public-key cryptography to eliminate password-based vulnerabilities. However, authentication alone is insufficient for sustaining zero-trust principles. Once an authenticated session is established, its trustworthiness must be continuously evaluated. This broader need for continuous evaluation is where SSF comes in - enabling the secure exchange of identity and security events, such as risk signals and session revocations, across disparate systems and vendors.

This document explores how integrating SSF into IAM architectures enhances visibility and responsiveness throughout the user journey, including joiner-mover-leaver (JML) and account recovery scenarios. It also highlights how Continuous Access Evaluation Protocol (CAEP) and Risk Incident Sharing and Coordination (RISC) protocols, when layered atop FIDO2, empower organizations to make real-time, risk-informed decisions that reduce fraud and accelerate incident response.

This synthesis of FIDO and SSF represents a paradigm shift toward continuous, adaptive trust that enables organizations to move beyond static controls and toward dynamic, signal-driven security ecosystems.

Audience

This white paper is for enterprise security practitioners and identity and access management leaders whose responsibility is to protect the security and life cycle of online and identity access management. Specifically, the target audience should include those whose purviews cover activity monitoring for threat detection and response as well as IAM staff who support those goals. Additionally, IAM leadership and architects should review this document to understand opportunities the described technologies offer and the implications of implementing them.

Table of Contents

1 Introduction

The FIDO Authentication protocol has a proven track record of securing initial session authentication by leveraging strong public key infrastructure (PKI) based cryptography. Adoption of this technology has been a leap forward as a unified approach for secure and usable session establishment, however the ability to maintain, monitor, and manage ongoing sessions has historically remained fractured. This challenge is exacerbated by the reality of today's enterprise security landscape, where numerous security vendors and solutions often operate in silos with limited communication. These barriers hinder comprehensive security outcomes during adverse events, leading to localized mitigations rather than unified responses.

Shared signals offer a crucial pathway to facilitate a more holistic and effective response by providing a way to exchange security events across vendor boundaries. Ongoing management and monitoring are required to adopt the full zero-trust model. The OpenID Foundation’s Shared Signals Framework (SSF) aims to address these challenges. If you root an IAM program with a strong footing, such as FIDO based authentication, and combine it with strong ongoing activity monitoring enabled by an SSF, you can achieve substantial changes that reduce (and enable you to react to) fraud and maligned activities.

2 What is the Shared Signals Framework?

The Shared Signals Framework (SSF) standard simplifies the sharing of security events across related and disparate systems. The framework allows organizations to share actionable security events and enables a **coordinated** response to potential threats and security incidents. SSF is defined by the OpenID Foundation’s Shared Signals Working Group (SSWG). The SSF standards are still evolving, but evaluation of the specifications **provides** a clear picture of what the SSWG hopes to achieve and can inform practitioners around what can be done with these tools today. The goal of this framework is to define a common language and mechanism for communicating actionable security events in near real-time, that allows systems to respond more effectively and in a coordinated way to potential threats.

SSF helps bridge gaps between identity providers, relying parties, and other services by creating a unified way for entities to notify each other of relevant changes, such as risk signals or session status updates.

For example, Mobile Device Management (MDM) tools can transmit a device compliance change event to indicate a user’s laptop is no longer compliant with corporate policies. When this event is received by a downstream system, that service

may determine that the user's authenticated session should be terminated until such a time as the device moves back into a healthy state.

> **Note:** It is important to remember that SSF security events standardize and facilitate the sharing of information. They are not directives. Recipients need to determine the actions to take in case of a security event.

The SSF standard describes how to create and manage streams, which are used to deliver notification of events to the receiver using push (RFC 9835) and poll (RFC 8936) mechanisms. From a technical perspective, SSF describes using secure, privacy protected generic webhook transit with events delivered via HTTP in streams.

Software vendors can act as transmitters and receivers; however, they must establish independent unidirectional streams. Events are formatted as Security Event Tokens (SETs) (RFC 8417) and the entities involved are identified by Subject Identifiers for Security Event Tokens (RFC 9493). Additional Subject Members are also defined in the OpenID Shared Signals Framework Specification 1.0.

Since SETs do not describe the content or semantics of events, the SSWG is developing two standard profiles under SSF:

- Continuous Access Evaluation Profile (CAEP): For sharing access relevant state changes like token revocation or device posture.
- Risk Incident Sharing and Coordination (RISC): For sharing signals about "risky" behaviors, such as account compromise.

2.1 Continuous Access Evaluation Profile (CAEP)

To further simplify interoperability between various vendors, the SSWG has also defined the CAEP Interoperability Profile. This specification "defines the minimum required features from SSF and CAEP that an implementation MUST offer in order to be considered as an interoperable implementation". (CAEP Interoperability Profile)

Federated systems commonly assert the login only during initial authentication, which can create security risks if user properties (such as location, token claims, device status, or org membership) change during an active session. CAEP aims to enhance the "verify, then trust" mantra by defining a common event profile to communicate such changes as they happen. For example, early proposed examples suggest CAEP events can be used to:

- Tie risk signals to known identities (users and non-human identities (NHIs)
- Track sessions and behavioral changes over time

- Dynamically adjust access without requiring the user to re-authenticate

This list is non-exhaustive, and capabilities are expected to grow and evolve as CAEP is more widely adopted. Because CAEP is built upon SSF principles, interoperable push and poll of SETs can be sent in real-time between trusted entities. These entities can include identity providers, relying parties (RP), monitoring systems like Security Information and Event Management (SIEM) systems, MDM systems, or any security-focused software vendor.

When an entity receives a SET, they can then evaluate the event and decide whether to revoke tokens or transmit an updated security status to other services. Monitoring systems such as MDM, endpoint detection and response (EDR)/extended detection and response (XDR), SIEMs, or any security-focused software vendor can emit/consume CAEP events. As enterprise architectures evolve, CAEP can serve as a foundational tool for zero-trust strategies, enabling continuous and adaptive access evaluation that is informed by real-time context.

2.2 Key components of the Security Token Event (SET)

At the core of SSF is the Security Event Token (SET), a JWT based envelope defined by RFC 8417, that provides the foundational format for encoding and transporting these events.

“The intent of this specification is to define a syntax for statements of fact that SET recipients may interpret for their own purposes.” (RFC 8417)

Based on this principle, SETs provide a structured, interoperable format to convey claims (statements of fact) such as account changes, credential updates, or suspicious activity, without prescribing any particular enforcement action. This allows recipient systems to evaluate and respond to events in accordance with their own policies. Each profile (CAEP, RISC, SCIM) imposes specific constraints on the base SET and its associated subject identifiers (per RFC 9493), thereby defining clear semantics and expected behaviors for particular use cases.

The SET itself is composed of several key claims, which together define the issuer, audience, subject, and event full context. A full description is available within the official documentation from the OpenID foundation, RFC 8417, and RFC 9493. The following is a brief outline of these claims.

- **iss** (*issuer*) - Represents the entity that issued the token, such as https://idp.example.com/ (as per SET examples). This is used by the receiving service to verify that the event originates from a trusted provider.

- aud (*audience*) - Specifies the intended recipient of the token. Depending on the deployment, the recipient may be the relying party application, an identity provider, or another trusted service. This helps ensure that only the designated service processes the security event.
- **jti** (JWT ID – unique event identifier) - A unique identifier for this specific event within the security stream. Helps with tracking and deduplicating events to avoid processing the same event multiple times.
- **iat** (*Issued At Timestamp*) - Indicates the exact Unix timestamp when the event was generated. Helps determine the event's freshness and prevent replay attacks.
- **sub_id** (*subject identifier*) - Structured information that describes the subject of the security event.
- **events** (*Security Events Information*) - The core claim that contains details about the specific security event. This is a mapping from an event type identifier (for example, https://schemas.openid.net/secevent/risc/event-type/account-disabled) to an event-specific JSON object that typically includes attributes such as subject, contextual metadata (for example, reason, timestamp, and risk level), and any profile-defined parameters required to interpret and act on the event.
- **event_timestamp** - Represents the date and time of an event. Uses NumericDate
- **txn** (*Transaction Identifier*) - OPTIONAL - Represents a unique transaction value. Used to correlate SETs to singular events.

2.3 Risk Incident Sharing and Coordination (RISC)

While CAEP defines a standardized messaging transport for communicating session-related state changes between trusted parties during active sessions, additional security events that might compromise an identity outside of a single session must also be addressed. This is where Risk Incident Sharing and Coordination (RISC) comes into play.

RISC is designed to share security events that are related to potential threats, credential compromises, and account integrity across federated systems. RISC hopes to define profiles that enable each recipient system to assess and act upon security events based on their unique risk policies, rather than mandating specific enforcement actions.

RISC SETs might also empower standards compliant systems (via the System for Cross-Domain Identity Management (SCIM) standard for example) to communicate

“statement of fact” assertions, with the goal to enable simpler automation and coordination across an asynchronous federated environment.

It is important to remember that RISC, like CAEP, suggests a framework of profiles and roles for platforms to leverage.

- SETs only state provable assertions. They do not issue specific directives.
- Receivers may need to leverage profiles that are not yet established, to always take prescribed actions based on SETs received from transmitters. However, those profiles need to be understood by the transmitter/receiver pair.
- The ultimate goal is to enable more automation and faster reactivity across sessions through the sharing of SETs.

3 SSF and user journeys

When you plan for implementation of IAM tools and capabilities, it is a common practice to consider the user journeys that need to be supported. These user journeys include day-to-day authentication and authorization processes, as well as more impactful (but less common) JML and recovery processes. Both CAEP and RISC methodologies can be used to enhance these workflows, building off strong authentication backed with FIDO2. With FIDO2 you are able to make decisions about users with certainty and with SSF you can track actions and react more quickly and accurately based on identity signals and user behaviors.

While the adoption of SSF is expected to grow, it will be up to the individual practitioner or organization to best determine how to leverage these capabilities. At the time of writing, the proposed workflows (as well as many of the transmitter and receiver interfaces) all need to be manually created and configured. Instead, it is recommended that you evaluate how these suggestions can enrich existing workflows and request delivery of these capabilities from your vendors and implementers.

3.1 Onboarding (joiners) and upgrading (movers) access

One journey that affects every end user is the joiner, or onboarding, process which generally establishes accounts for a user before they start at an organization. Accounts are created and entitlements are granted, with the expectation that they will not be used immediately. This timeframe is normally documented as “Day Zero -1.” This timeframe varies depending on organizational practices, but in order to ensure a speedy onboarding process most mid to large sized organizations follow this trend.

The risk here is that it is easy to perform OpenSource Intelligence Gathering (OSINT) and enumerate accounts that fall into the “pending start day” category. The current set of IAM tools may lack the intelligence or agility to dynamically enable and disable

accounts based on a strong identity proofing workflow and business demands of “hitting the ground running” often mean that these accounts are active and unmonitored before a user starts.

Profiles built on Shared Signal Frameworks (specifically RISC) can be leveraged to enhance this process. You can develop workflows that use the successful establishment of FIDO credentials via strong ID Proofing workflows, or initial detection of the use of pre-registered FIDO credentials, to trigger account enablement via IAM systems. With this workflow, accounts can sit inactive during the Day Zero - time frame and will only be dynamically activated once a successful strong authentication has been detected.

Role or access changes (known as mover workflows) can follow a pattern similar to that of the onboarding enhancement. New accounts can be created in a disabled state, awaiting specific triggers (such as date and time) in conjunction with authentication. RISC also opens the door to more dynamic access elevation, where the signaling framework can be used to trigger approval workflows in IAM ticketing and provision systems to temporarily grant higher privileges or roles.

Creative use of the shared signals frameworks, paired with a FIDO backed Root of Trust (RoT), can strengthen and enhance joiner and mover user journeys. These emerging techniques should be evaluated and adopted in a timely manner, to raise the bar for all IAM practitioners.

3.2 Device recovery/replacement

Another common user journey is establishment of a user on a new device. While it is similar to the onboarding journey, pre-existing permissions, accounts, and roles add complexity to this journey. This is also a common area of attack as attackers can abuse this workflow to enroll their own devices or otherwise compromise the pre-existing identity via unsecured channels.

A best practice for device loss workflows is to lock down access as soon as a lost device is reported. You can leverage RISC signals to inform RISC consumer systems of the new device registration activity as part of an automated workflow that helps disable access as needed. Once a new device is issued, an identity can be re-established on the new device with a FIDO2 authentication workflow. The workflow can then leverage RISC signals to have IAM provisioning systems re-enable access.

Similar workflows can be leveraged if the FIDO2 authenticator needs to be replaced. This includes the loss of a device that contains a synced credential or a hardware token that contains a device-bound credential. Identity proofing workflows need to be leveraged to securely re-establish identity before a new credential can be bound to a

user's account. After this workflow is complete, RISC signals can be leveraged to re-enable sensitive access that was disabled when the credential was reported missing.

3.3 Offboarding (Leaver events in JML)

Offboarding workflows fall into two categories: planned and unplanned. Planned offboarding remains fairly unimpacted by SSF. It is possible to leverage CAEP signals to trigger termination of any active sessions after the user signs off for the last time. However, the SSF is more useful for unplanned offboarding events. A workflow can evaluate CAEP signals, and any open sessions can be identified and ended. As part of this workflow FIDO credentials should be de-associated from the user's accounts, ensuring that the user can no longer log in. Both of these controls can ensure that unplanned offboarding events are well controlled and executed across the board.

3.4 Session tracking

Within the scope of modern identity security, session tracking plays a pivotal role in maintaining the integrity and security of user sessions. While authentication methods like FIDO effectively protect the initial login, they are significantly enhanced when complemented by session tracking. This involves the continuous monitoring of a session's behavior and context throughout its entire lifecycle, from creation to termination. Such ongoing evaluation is crucial for identifying risk signals that may indicate potential security threats, such as session hijacking or unauthorized access attempts.

Platforms within a networked environment use CAEP events to send a range of signals to an authentication system responsible for managing sessions. You can utilize session tracking data so that as events are received, the authentication system can implement appropriate security measures, such as enforcing step-up authentication or terminating sessions. These events originate from multiple, diverse platforms, which each act as both transmitters and receivers within the SSF. This interconnected network offers valuable insights into potential security threats, enabling each platform to contribute to and enhance session tracking across the entire network.

To illustrate the impact of session tracking, we will explore use cases that compare an environment that uses only WebAuthn authentication with an environment that uses an enhanced approach that incorporates continuous authentication and shared signals. This comparison highlights how continuous session tracking can significantly bolster security and mitigate risks.

The following table describes some possible ways to design these workflows. The table outlines the traditionally observed behaviors of systems and how security policies can be enhanced with the inclusion of SSF capabilities. When compared side by side, you can see the advantages provided by the adoption of SSF signaling.

User Journey - Adding continuous access and session evaluation to a high assurance authentication

Scenario	FIDO (Point-in-Time Authentication)	FIDO + SSF (Continuous Assessment and Signals)	CAEP/RISC events
Initial authentication	User logs in using WebAuthn	User logs in using WebAuthn.	NA
Session establishment	Session is established and remains valid until expiration or logout	Session is established with continuous monitoring enabled. If a disallowed event signal is received (for example, credential compromise, risk alert, or policy violation), the session can be revoked or re-evaluated immediately instead of waiting for expiration or logout	*CAEP* session-established
Threat intelligence alert	No visibility or action	A threat intelligence system (for example, EDR/XDR or an anti-phishing platform) watches for a phishing campaign targeting a user group. If a phishing campaign is detected, the system acts as a transmitter and sends a RISC **credential-compromise** event to the Identity Provider (IdP), which functions as the SSF receiver in this scenario. Upon receiving the event, the IdP correlates the	*RISC*: credential-compromise *CAEP:* session-revoked

Scenario	FIDO (Point-in-Time Authentication)	FIDO + SSF (Continuous Assessment and Signals)	CAEP/RISC events
		identity, flags the session, and revokes it as necessary. The IdP can then act as a transmitter and issue a *CAEP* session-revoked event to other downstream SSF receivers, such as SaaS applications or partner services. This enables receivers to take appropriate actions (for example, terminating sessions or prompting re-authentication) based on the trust change initiated by the IdP.	
Session hijack or replay (post threat alert)	Session remains valid and an attacker can reuse the stolen session token (for example, via fixation or XSS), as FIDO-only systems do not have post-authentication visibility.	Signals (for example, from threat intelligence platforms) elevate risk and those events are transmitted to receivers like the IdP, which then terminates the session. This prevents the reuse of any compromised session tokens.	CAEP: risk-level-changed
Step-up authentication (post threat alert)	Not triggered	After receiving a *RISC* credential-compromise event from a threat intelligence system, the Identity Provider (IdP) flags the session as high-risk and prompts the user to authenticate using FIDO WebAuthn. Once the user completes strong re-	*CAEP:* assurance-level-change

Scenario	FIDO (Point-in-Time Authentication)	FIDO + SSF (Continuous Assessment and Signals)	CAEP/RISC events
		authentication, the IdP issues a *CAEP* assurance-level-change event to reflect the increased assurance level. This event can also be transmitted to downstream consumers such as audit platforms or relying parties, enabling consistent assurance tracking.	

4 Filling gaps – compliments to FIDO and conclusion

As demonstrated, by the use cases outlined above, both CAEP and RISC pair well with FIDO authentication standards to improve overall security postures and practices for enterprises and organizations. These cases only cover the largest areas where these frameworks should be adopted and integrated into current tools and workflows. In addition to our recommendation of implementing these standards, a robust and well planned SSF/FIDO program can provide buffers/flagging against potential false positive signaling and help make the tasks of attributing improper activities and detection of rogue actors easier for Network Operations Centers (NOCs).

SIEM systems rely on credible data from endpoints. SSF helps to normalize the structure of many tasks that historically have required bespoke connectors. Shared signals (such as CAEP session state changes or RISC credential-compromise events) can add clarity and deeper insight into principal (the user or entity associated with the event) and system behavior. Additionally, SSF-enabled SIEM or IAM tools can be leveraged to strengthen current step-up authentication practices, providing native ways to track high privilege interactions without the need for full reliance on single point of failure third party systems.

In the past, passive signals were used for dark web monitoring. With shared signals coordination we now have the capabilities to send notifications and cycle credentials automatically for systems that do not support strong authentication. Accounts with leaked credentials can either be auto-disabled and shunted to a reset workflow that is backed by a strong authentication with FIDO or automatically rotated with credentials

that are vaulted and retrievable with IDV or FIDO authentication. Stolen credentials may not be limited to usernames and passwords and can also include stolen synced passkeys and or certificates. CAEP can be leveraged to communicate out of context credentials, and the shared signals should be leveraged as part of a risk-based authentication workflow.

CAEP, RISC, and FIDO provide a risk-averse way to enable federated login. Implementation of both enhanced session tracking and strong authentication creates a workflow in which external users can leverage federated login processes and security teams can more closely monitor and attribute activity and behavior. In the Customer Identity space, these enhanced signals can provide more secure ways to allow end users to authenticate using their existing trusted identity provider accounts (for example Google, Apple or enterprise Identity Providers) instead of creating new local credentials, through enhanced session tracking and strong, phishing resistant authentication.

When practitioners and vendors embrace RISC and CAEP frameworks for signaling, they strengthen not only their own environments but also the broader information security ecosystem. A common, interoperable signaling language increases the ability of systems across organizational boundaries to track and correlate user and process activity, detect inappropriate behavior, and respond consistently. In this way, the adoption of SSF moves security practice toward a more collaborative, standards-based model that prioritizes shared defense and ecosystem resilience. When SSF is put into practice, it enables external entities to be better informed in real time, improving collective security and ensuring that end users are more effectively protected.

5 SET examples

This section contains several mockup examples of the makeup of SETs. These are provided to add clarity to the contents and capabilities of each component of the SSF. They describe the information systems can expect to receive and what data points can be included in a token.

5.1 CAEP example tokens

CAEP provides a standardized way to communicate access property changes in real time. It defines Security Event Tokens (SETs), which are sent by transmitters using the SSF framework. Upon receiving a CAEP event, the receiver can dynamically adjust access permissions, which reinforces zero-trust security principles and ensures security decisions remain context aware and adaptive.

The following are examples of key CAEP Security Event Tokens (SETs).

5.1.1 Session revoked

Session revoked: Indicates an active session has been terminated

Event transmission example.

```
{
  "iss": "https://idp.example.com/",
  "iat": 1742418748,
  "aud": "https://sp.example.com",
  "sub_id": {
    "format": "iss_sub",
    "iss": "https://sp.example.com",
    "sub": "12345"
  },
  "events": {
    "https://schemas.openid.net/secevent/caep/event-type/session-revoked": {
      "event_timestamp": 1742418748
    }
  },
  "jti": "unique-event-id"
}
```

5.1.2 Credential changes

Token claims change: Signals changes in token claims such as roles, entitlements, and group memberships that affect access control

Credential change: Signals that a user's credentials have been changed (for example, deleted, updated, created, or revoked). Examples of credentials include passwords, fido2-platform, and fido2-roaming.

Event transmission example

```
{
  "iss": "https://idp.example.com/",
  "iat": 1742422524,
  "aud": "https://sp.example.com",
  "sub_id": {
    "format": "iss_sub",
    "iss": "https://sp.example.com",
    "sub": "12345"
```



```
  },
  "events": {
    "https://schemas.openid.net/secevent/caep/event-type/credential-change": {
      "credential_type": "fido2_platform",
      "change_type": "delete",
      "event_timestamp": 1742422524
    }
  },
  "jti": "YjYyMmUwYzgtMmU3MS00YmI2LTgyZWUtMjFmMjFmYTg1Yjk3"
}
```


5.1.3 Assurance level or compliance change

Assurance level change: Indicates that the assurance level of user's authentication has changed, impacting session security.

Device compliance change: Signals a change in the security posture of a user's device. For example, a previously compliant device is now non-compliant.

Transmission event for device compliance example.


```
{
  "iss": "https://idp.example.com/",
  "iat": 1742422620,
  "aud": "https://sp.example.com",
  "sub_id": {
    "format": "iss_sub",
    "iss": "https://sp.example.com",
    "sub": "12345"
  },
  "events": {
    "https://schemas.openid.net/secevent/caep/event-type/device-compliance-change": {
      "previous_status": "compliant",
      "current_status": "not-compliant",
      "event_timestamp": 1742422620
    }
  },
  "jti": "MTNiN2U2ZGEtZmRlMS00ZDliLWEwY2EtY2NmZTdkZGNkNjY0"
}
```


5.2 RISC example tokens

The following examples show the key RISC SETs.

5.2.1 Account credential change required

Indicates an event requiring a credential update for the subject, typically due to detected compromise or reuse. For example, this helps prevent credential stuffing attacks across federated accounts.

```
{
  "iss": "https://idp.example.com",
  "iat": 1710525600,
  "jti": "account-cred-change-required-001",
  "aud": "https://sp.example.com",
  "events": {
    "https://schemas.openid.net/secevent/risc/event-type/account-credential-change-required": {
      "subject": {
        "sub": "user123",
        "email": "user@example.com"
      },
      "reason": "Detected credential reuse from known breach",
      "required_action": "Force password reset",
      "timestamp": 1710525600
    }
  }
}
```

5.2.2 Account enabled

Notifies that a previously disabled account has been re-enabled. This allows relying parties to reinstate access where appropriate (for example, after resolving a false positive).

5.2.3 Account purged

Notifies that the subject's account has been permanently deleted and should no longer be recognized by relying parties.

5.2.4 Account disabled

Notifies that the subject's account has been disabled and is no longer accessible. This helps prevent unauthorized access (for example, after fraud detection or HR termination).

Transmission event for account disabled for fraud detection.

```
{
  "iss": "https://idp.example.com",
  "iat": 1710525600,
  "jti": "account-disabled-event-002",
  "aud": "https://sp.example.com",
  "events": {
    "https://schemas.openid.net/secevent/risc/event-type/account-disabled": {
      "subject": {
        "sub": "user123",
        "email": "user@example.com"
      },
      "reason": "Fraudulent activity detected",
      "timestamp": 1710525600
    }
  }
}
```

5.2.5 Identifier changed/recycled

Notifies when a user's identifier (for example, email or username) has changed or is reassigned. Helps prevent unauthorized access using outdated identifiers.

```
{
  "iss": "https://idp.example.com",
  "iat": 1710525600,
  "jti": "identifier-changed-event-003",
  "aud": "https://sp.example.com",
  "events": {
    "https://schemas.openid.net/secevent/risc/event-type/identifier-changed": {
      "subject": {
        "sub": "user123",
        "old_email": "olduser@example.com",
        "new_email": "newuser@example.com"
      },
      "timestamp": 1710525600
    }
  }
}
```


6 Document history

Change	Description	Date
Initial publication	White paper first published.	October 2025

7 References

Internet Engineering Task Force (IETF). (2020, November 30). Poll-Based Security Event Token (SET) Delivery Using HTTP. IETF Datatracker. https://datatracker.ietf.org/doc/rfc8936/

Internet Engineering Task Force (IETF). (2020, November). Push-Based Security Event Token (SET) Delivery Using HTTP. IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc8935

Internet Engineering Task Force (IETF). (2018, July). Security Event Token (SET). IETF Datatracker. RFC 8417https://datatracker.ietf.org/doc/html/rfc8417

Internet Engineering Task Force (IETF). (2023, December). Subject Identifiers for Security Event Tokens. IETF Datatracker. https://datatracker.ietf.org/doc/rfc9493/

OpenID. (2025, August 29). OpenID Continuous Access Evaluation Profile 1.0. OpenID. https://openid.net/specs/openid-caep-1_0-final.html

OpenID. (2024, June 25). CAEP Interoperability Profile 1.0 - draft 00. OpenID. https://openid.net/specs/openid-caep-interoperability-profile-1_0-ID1.html

OpenID. (2025, August 29). OpenID RISC Profile Specification 1.0. OpenID. https://openid.github.io/sharedsignals/openid-risc-1_0.html

OpenID. (2025, August 29). OpenID Shared Signals Framework Specification 1.0. OpenID. https://openid.net/specs/openid-caep-1_0-final.html

