SOLUTION BRIEF · 2026

SSF / CAEP Continuous Access on the EmpowerID Identity Fabric

Governed effects, not a signal feed — policy-decided enforcement for people and AI agents, with evidence you can defend.

Document EID-SSF-CAEP-SOLUTION-2026-GD

Version 1.0 (general distribution)

Date 2026-07-19

Audience Security & identity leaders · Architects

Why continuous access matters

When a credential is compromised, a delegation is revoked, or an entitlement is removed, every minute of continued access is risk. SSF and CAEP are the open standards for sharing those security events between systems. This brief describes how EmpowerID turns those signals into governed, provable enforcement on the Identity Fabric — for your workforce and your AI agents — and what makes that structurally different from a typical "signal distributor + session revoke" deployment.

THE QUESTION THIS BRIEF ANSWERS

When a security signal arrives, does access actually change — everywhere, immediately — and can you prove it did?

1 · Our implementation model — governed effects, not a signal feed

EmpowerID treats SSF/CAEP as a **governed-effects control plane** on the same event-driven spine used for identity governance, authorization, orchestration, and agent execution — not as a standalone notification integration.

Design choice	What EmpowerID does
Authoritative source	Session, credential, delegation, grant, and entitlement transitions originate from the IdP and platform governance plane — committed as durable facts before fan-out.
Policy on egress and enforcement	The PDP evaluates both whether a signal may be transmitted and how it must be enforced. Reactions are not hard-coded in receivers.
Dual enforcement surfaces	**Human path:** BFF session invalidation with upstream delegation–session correlation. **Agent path:** pre-dispatch denial at the agent execution boundary before tools or credentials are invoked.
Trusted context only	Enforcement and authorization consume validated signal context attached by the platform. Client-supplied SSF claims are not trusted.
Separated evidence	Delivery acknowledgment, authorization disposition, and enforcement disposition are distinct immutable facts — not one mutable "handled" flag.
Loop-safe topology	Locally originated signals fan out on an internal channel only. Externally received SETs are validated and enforced internally but never retransmitted, preventing SSF echo loops.
Operator visibility	Signal → policy decision → enforcement outcome is joined in an operator timeline for causal audit and incident response.

CATEGORY CLAIM

Many vendors excel at **collecting and delivering** SETs. EmpowerID implements what happens **after** a trusted signal is accepted: AuthZEN evaluation, authority mutation, runtime enforcement, and auditable proof — on one fabric.

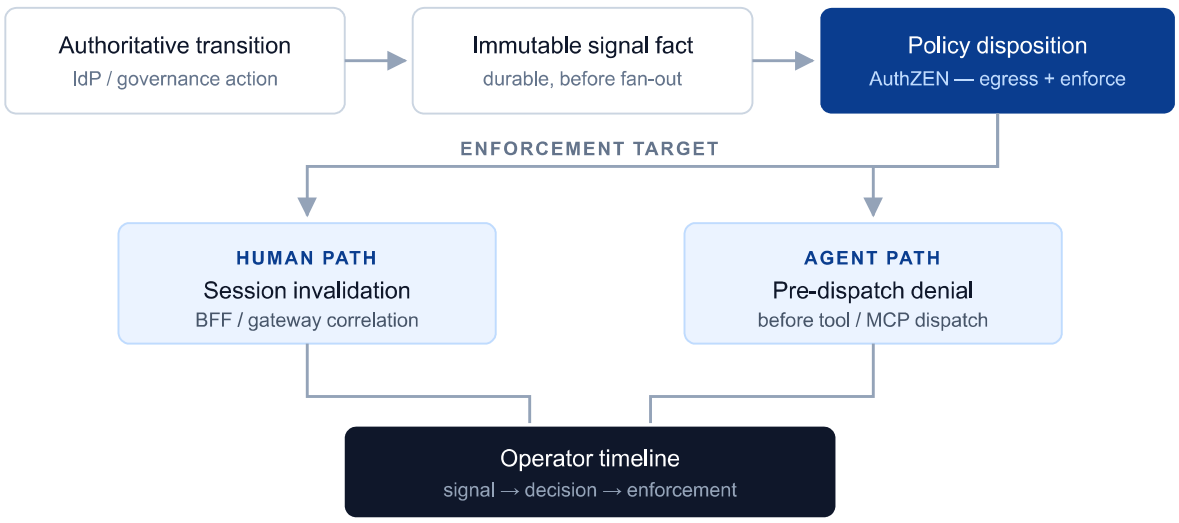

Figure 1 — Governed-effects control loop

2 · What is unique about EmpowerID's approach

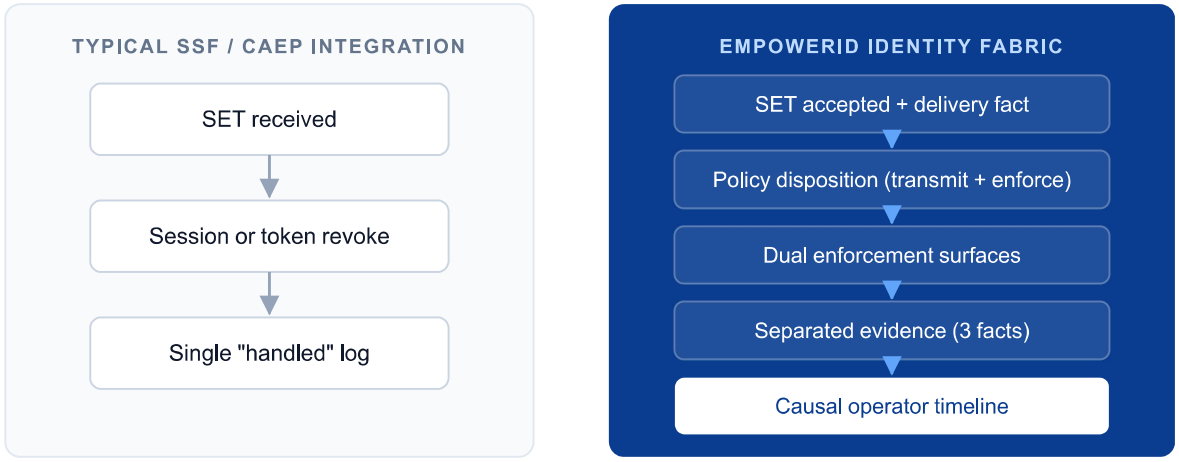

Figure 2 — Typical integration vs EmpowerID

2.1 · Pre-dispatch denial while credentials still look valid

Most continuous-access implementations stop at session termination or token revocation at the IdP. EmpowerID additionally enforces at the **agent execution boundary**: a delegated agent can be blocked before tool/MCP dispatch even when the underlying credential has not yet expired. That is a different semantic from "401 because the session is dead."

> **PROOF POINT**
> *A trusted signal changes effective authority, stops an unsafe agent action before dispatch, and leaves an explainable record of why.*

2.2 · Agent-native signals on the same contract as CAEP

EmpowerID extends CAEP with typed platform events for connected-agent and governance lifecycles, carried on the same canonical envelope and processing pipeline as standard CAEP events:

Event	Role
`CAEP session-revoked`	Human and agent sessions
`CAEP credential-change`	Password and PAT lifecycle
`delegation-revoked`	Connected-agent delegation
`oauth-grant-revoked`	OAuth grant lifecycle
`entitlement-revoked`	Recertification / remediation path

Subject binding supports opaque session correlation, identity URI (ARN), and complex delegation subjects — so enforcement can target the right runtime object, not only a user id.

2.3 · Policy-governed egress, not "fire and forget" transmit

The IdP is an SSF **transmitter** (RFC 8935 push) with discovery, signing, durable inbox, and delivery ledger. Uniquely, whether and where to transmit is a policy decision — aligned with the same AuthZEN application model used for human and agent authorization elsewhere on the fabric.

2.4 · Evidence you can defend in an audit

Typical integrations log "signal received" and "session killed." EmpowerID separates:

1. **Delivery fact —** the SET was accepted and acknowledged.
2. **Authorization disposition —** policy allowed, denied, or deferred enforcement.
3. **Enforcement disposition —** sessions terminated, authority revoked, or pre-dispatch denial applied.

Your security and audit teams can answer: *which signal caused which enforcement action, under which policy decision?*

2.5 · Same fabric as IGA and Agent Governance & Execution

SSF/CAEP is not a bolt-on SKU. It reuses:

- Identity provider transitions and signing

- AuthZEN PDP and application registry
- API gateway enforcement and session correlation
- Agent orchestration and execution guard
- Analytics and operator UI (Signal Timeline)

Continuous access therefore scales with the same proof and policy model as access requests, agent delegation, and recertification — not a parallel security silo.

3 · End-to-end control loop

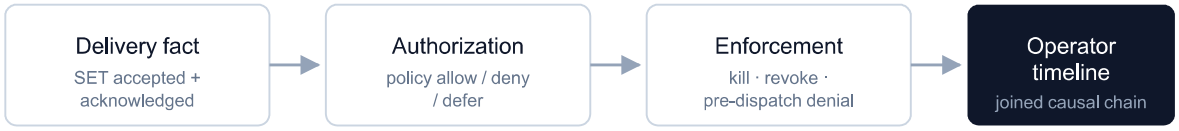

Figure 3 — Separated evidence vocabulary

Platform roles

Layer	Implementation role
Identity provider	SSF transmitter (RFC 8935 push), CAEP/SSF receiver, signing, durable inbox, delivery ledger
Policy decision point	AuthZEN evaluation; trusted signal context only
API gateway	RFC 8935 receiver, enforcement consumer, delegation–session correlation, session invalidation
Agent execution plane	Authority guard before tool dispatch
Analytics & operations UI	Immutable signal facts; Signal Timeline for causal chain

4 · Standards and interoperability

Mechanism	Status
SSF push (RFC 8935)	Supported
Discovery `/.well-known/ssf-configuration`	Supported
Receiver `POST /api/caep/events` (`application/secevent+jwt`)	Supported
SSF poll (RFC 8936)	Roadmap

Canonical wire envelope v2 with golden interop fixtures. Implementation profile available on request (not a conformance certificate).

5 · Proven scope today

Integration-proven paths:

Path	Effect
Agent tool dispatch	Pre-dispatch denial at authority checkpoint; tool not invoked
Human LLM / gateway session	Session invalidation and revocation bridge

The end-to-end control loop is demo-proven with reproducible verification. Production qualification and formal OpenID SSF transmitter conformance are on a defined path; detail available on request.

6 · See it in action

- **Live demo:** watch a trusted signal change authority, stop an unsafe agent action before dispatch, and leave a defensible record — end to end in about 15 minutes.
- **Technical deep dive:** implementation profile, interop detail, and evidence pack available under evaluation.

Contact your EmpowerID representative to schedule a demonstration.

General distribution — may be shared with customers and partners. EmpowerID Identity Fabric SSF/CAEP continuous access. Version 1.0, 2026-07-19. EmpowerID (master brand) · EmpowerID Identity Fabric (platform) · Commercial solution: Agent Governance & Execution.