empowerID

TECHNICAL BRIEF · EMPOWERID IDENTITY FABRIC

Standards, protocols & technical differentiation

The open specifications behind EmpowerID Identity Fabric — and how one governance spine for people, machines, applications, and AI agents differs from legacy IAM suites and agent-only gateways.

July 2026 · v1.1 For security architects, evaluation teams, SI partners, and industry analysts

PURPOSE

This brief answers a common evaluation question: which open standards and protocols does EmpowerID Identity Fabric implement, and how does that architecture differ from traditional IAM suites and agent-only gateways? It is written to stand alone — as a PDF, an email attachment, or a data-room document — without requiring access to EmpowerID engineering repositories.

DOCUMENT

Document ID	EID-STANDARDS-2026-001
Version	1.1 · 28 July 2026
Classification	External — shareable

NOT IN SCOPE HERE

SOC 2 / ISO 27001 certificates, commercial licensing, exhaustive connector SKU lists, and signed customer references — provided separately under corporate and sales channels.

01 — WHY STANDARDS MATTER

Three things an evaluator needs

Enterprise evaluators, systems integrators, and industry analysts typically need more than a checkbox that says “OAuth supported”:

1 · Inventory

Which IETF, OpenID Foundation, and industry specifications apply to authentication, authorization, provisioning, continuous access, agent tools, and audit evidence — and at what maturity.

2 · Composition

How those specifications connect inside one architecture rather than sitting alongside each other as disconnected optional modules.

3 · Differentiation

What is structurally different from legacy IGA/IAM suites and from agent-only gateways, expressed in protocol and proof terms.

EmpowerID Identity Fabric is standards-first at every integration boundary: adopted protocols at the seams; centralized policy and tamper-evident evidence as platform primitives; one governance spine for workforce, partner/B2B, service/workload, and AI agent identities.

Standards by domain, and what each one buys

Domain	Open standards (representative)	Why it differentiates
Identity & authentication	OpenID Connect, OAuth 2.1, WebAuthn/FIDO2, CIBA, PKCE, PAR, DPoP, JARM, RAR, Resource Indicators, token exchange, token introspection	Deep OAuth/OIDC surface while coexisting with the workforce IdP (e.g. Okta, Entra) — the fabric federates rather than forcing rip-and-replace
Authorization	OpenID AuthZEN (evaluate, batch, search); PBAC / ABAC / RBAC / ReBAC	One externalized Policy Decision Point for applications, IGA guardrails, SoD, search scoping, delegation, and agent enforcement — not siloed product RBAC
Cross-app & agent identity	RFC 8693, On-Behalf-Of, ID-JAG (IETF OAuth draft; same wire as Okta Cross-App Access), RFC 9728 resource metadata, RFC 7523 JWT bearer at resource authorization servers, RFC 9207 issuer identification	Issue and consume ID-JAG at governed tool, orchestration, and AI gateway edges; AuthZEN at mint and on each action
Continuous access	OpenID Shared Signals Framework (SSF) 1.0, CAEP-aligned Security Event Tokens, RFC 8935 push, RFC 9493 subjects	Verified signal → policy → enforcement (push transmit/receive in production; poll and RISC on roadmap)
Provisioning & directory	SCIM 2.0, LDAP v3, virtual directory	Configuration-driven connectors and graph-backed membership — not a monolithic SQL “identity warehouse”
Agent execution	Model Context Protocol (MCP) incl. the 2026-07-28 revision, MCP enterprise-managed authorization (EMA) grant profiles, OAuth 2.1 at the gateway, RFC 8693 delegation narrowing	Dual policy enforcement (model traffic + tool calls) with capability without custody — credentials are not returned to the agent
Evidence	JWS (RS256), hash-chained receipts, JWKS verification, SCITT-upgradeable receipt format	Linked decision → execution → verification chain, not audit logs alone

ONE-LINE POSITIONING

Open standards at the boundaries; one event-driven governance spine — so any front door, whether ServiceNow, SAP GRC, SailPoint, Microsoft Copilot, a custom portal, or an AI agent, uses the same authorization contract and produces the same auditable outcomes.

03 — DESIGN PRINCIPLES

What to verify, and why it matters

EmpowerID Identity Fabric aligns with the Identity Fabric reference model: composable, API-first services for all identity types, integrated by policy and orchestration.

Principle	What to verify in evaluation	Standards implication
API and event parity	Governed actions are available via documented APIs and asynchronous events	Security is not UI-only; integrators and agents are first-class callers
Contract integration	Services integrate via APIs and events, not shared databases	AuthZEN, SCIM, and LDAP at boundaries; propagation via events
Bring-your-own front door	Existing ITSM, GRC, or IGA portals can drive the same workflows	Same application authorization contracts for human UI and machine callers
Fail-closed enforcement	Deny when the decision service is unavailable, where policy requires	Obligations (e.g. step-up MFA, audit) enforced at the Policy Enforcement Point
Explicit maturity	Draft and roadmap items are labeled as such	ID-JAG is an implemented IETF draft; FAPI alignment is not claimed as formal FAPI certification

04 — STANDARDS INVENTORY

The specifications, domain by domain

Every row below carries a maturity tag. Colour is a reading aid only — the word is authoritative.

PRODUCTION	Included in standard platform deployment; used on live paths
IMPLEMENTED	Engineering-complete; may still be completing operational qualification
EMERGING	Built to a public draft or profile; the specification may still evolve
ROADMAP	Planned; not represented as generally available in this document
NOT A FOCUS	Out of scope for the fabric unless covered by EmpowerID Identity Governance or a partner

4.1 · Authentication and session

Standard / specification	Platform role	Maturity	Notes
OpenID Connect	SSO and ID tokens	Production	Identity & Federation Service
OAuth 2.1	Authorization code, client credentials, token endpoints	Production	Platform baseline
PKCE (RFC 7636)	Public and native client protection	Production	
PAR (RFC 9126)	Pushed authorization requests	Production	
JARM	JWT-secured authorization response	Production	
`private_key_jwt`	Confidential client authentication	Production	
CIBA (OpenID)	Decoupled / out-of-band authentication	Production	
WebAuthn / FIDO2	Passkeys; passwordless-capable authentication	Production	
TOTP	Authenticator-app MFA	Production	
Temporary Access Pass	Bootstrap and recovery	Production	
Password storage	argon2id, lockout, policy	Production	Implementation detail; listed for completeness
DPoP (RFC 9449)	Sender-constrained tokens	Production	Composable with token exchange and ID-JAG
Token introspection (RFC 7662)	Resource-server validation	Production	

Standard / specification	Platform role	Maturity	Notes
JWT / JWS / JWKS	Signing, verification, key rotation	Production	Keys supplied at deployment time

> **Evaluation note.** Adaptive risk step-up and SAML/WS-Federation IdP capabilities should be confirmed against your deployment scope if SAML-centric federation is required. This brief emphasizes OIDC/OAuth-first integration.

4.2 · OAuth authorization and rich requests

Standard / specification	Platform role	Maturity	Notes
RAR (RFC 9396)	Fine-grained `authorization_details`	Production	Linked to AuthZEN and delegation
Resource Indicators (RFC 8707)	Per-API audience binding	Production	ID-JAG consumption, MCP, Experience API
RFC 8693 Token Exchange	Delegation, OBO, agent narrowing	Production	Agent delegation rail uses narrowing semantics
On-Behalf-Of (OBO)	User context via services and agents	Production	Token exchange profiles
RFC 9207	Authorization server issuer identification (`iss` in the response)	Production	Mix-up defence; enforced at the MCP edge
FAPI-aligned baseline	PAR + DPoP + JARM + `private_key_jwt`	Implemented	Automated baseline tests; not formal OpenID FAPI certification

4.3 · Cross-application access — ID-JAG and Cross-App Access

Standard / specification	Platform role	Maturity	Notes
ID-JAG — Identity Assertion Authorization Grant (`draft-ietf-oauth-identity-assertion-authz-grant`)	Propagate identity for app-to-app and agent-to-resource calls	Emerging, implemented	Interoperates on the same wire as Okta Cross-App Access (XAA)
RFC 8693 (Step 1 — issuance)	Exchange for `typ=oauth-id-jag+jwt` assertion	Production	AuthZEN decision at mint
RFC 7523 JWT bearer (Step 2 — consumption)	Resource AS exchanges assertion for access token	Implemented, live-verified	Central replay and mint authority
RFC 9728	Protected Resource Metadata (`id_jag_supported` , caching)	Production	Governed Tool Gateway, orchestration MCP, AI Gateway
RFC 8707	Audience binding on consumption	Production	Confused-deputy controls
Assertion hygiene	Short lifetime (`exp ≤ 300s`), pairwise `sub` , `act` delegation chain, `client_id`	Production	Meets or exceeds the draft's security profile
Replay control	`jti` single-use with release-on-failure	Production	A transient downstream error does not burn a valid assertion
DPoP across the mint	`cnf.jkt` sender constraint preserved through consumption	Implemented	Composes RFC 9449 with RFC 7523

Standard / specification	Platform role	Maturity	Notes
Issuer discovery metadata	`identity_chaining_requested_token_types_supported`, `authorization_grant_profiles_supported`	Production	Lets clients negotiate ID-JAG and the MCP EMA flow
MCP EMA grant profiles	Enterprise-managed authorization advertised on protected-resource metadata	Advertised; interop open	Two-sided EMA interop with a third-party IdP/client is not complete — no certification claim
Inbound federation	Accept foreign federation grants (e.g. Okta, Entra) and materialize governed local agent identity	Implemented	Public trust framework for foreign issuers continues to mature

WHAT ID-JAG DOES

Answers *which application may call which other application's API, on whose behalf* — with short-lived, audience-bound assertions brokered by the identity provider.

WHAT IT DOES NOT DO ALONE

It does not replace enterprise authorization, segregation of duties, recertification, or fulfillment proof. The fabric treats ID-JAG as one credential leg into a deeper spine: AuthZEN decisions at mint and on each tool or model call, rich authorization requests, a delegation graph, and hash-chained receipts.

Resource surfaces that consume ID-JAG (verified June 2026)

- EmpowerID Governed Tool Gateway (MCP)
- EmpowerID Orchestration Service (MCP integration)
- EmpowerID AI Gateway (LLM provider proxy edge)

> Proof point. On the AI Gateway path, a consumed ID-JAG resolves to a delegated identity chain and receives an explicit policy denial from the centralized PDP when the model or action is not permitted — demonstrating that credential acceptance and authorization decision are separate, composed layers.

4.4 · Authorization — AuthZEN and policy model

Standard / specification	Platform role	Maturity	Notes
OpenID AuthZEN	Evaluation, batch, and search APIs	Production	Single PDP for the platform
PBAC / ABAC / RBAC / ReBAC	Hybrid authorization; graph as policy information	Production	Relationship access via graph-backed attributes
AuthZEN constraints	Spend caps, egress, data scope, rate limits, sensitive data patterns	Production	Enabled in standard deployment
AuthZEN obligations	MFA, consent, audit hooks	Production	Enforced at the PEP (recommended AuthZEN split)

Enforcement surfaces sharing one contract: Experience API layer, Governed Tool Gateway, orchestration and agent execution paths, Identity & Federation Service token boundary, Identity Graph & Membership Service, and search post-authorization filtering.

4.5 · Continuous access — SSF and CAEP

Standard / specification	Platform role	Maturity	Notes
OpenID SSF 1.0	Signal transmitter and receiver	Production (HTTP push)	Administrator-provisioned streams
CAEP	Continuous access evaluation event types	Production (event production)	Mapped to platform contracts
RFC 8935	SET push delivery	Production	Signed `secevent+jwt`
RFC 9493	Subject identifier shape in SETs	Production	
RFC 8936	Poll delivery	Roadmap	
RISC	Account compromise profile	Roadmap	
Stream Management API	Dynamic stream lifecycle	Roadmap	

> **Scope statement.** Push-based SSF transmit and receive is production-grade. Not every execution path (e.g. all MCP batch or WebSocket modes) yet participates in the same centralized continuous-enforcement scope; rollout is documented internally and shared under technical diligence. Operational qualification drills and OpenID transmitter conformance evidence are in progress.

4.6 · Provisioning, directory, and integration

Standard / specification	Platform role	Maturity	Notes
SCIM 2.0	Identity synchronization	Production	Ingestion and connectors
LDAP v3	Virtual directory read; governed write	Production	Identity Virtualization Service
SAP RFC/BAPI	SAP fulfillment and read	Production	Dedicated SAP integration service
JSON-RPC 2.0	MCP transport	Production	Governed Tool Gateway

Event streaming (e.g. Apache Kafka) is the platform integration backbone for high-volume propagation; it is an operational seam rather than an identity standard.

4.7 · Agent governance and tools

Standard / specification	Platform role	Maturity	Notes
MCP (Model Context Protocol)	Tool discovery; HTTP, WebSocket, SSE	Production	PDP-governed allowlists and schema discipline
OAuth 2.1 / OIDC	Client authentication at gateway	Production	
RFC 8693 + DPoP	Delegation and secretless access patterns	Production	Credential Control / OAuth Vault patterns
MCP revision 2026-07-28	Discover-first stateless core, Streamable HTTP validation, scope step-up → `403` + `WWW-Authenticate`, RFC 9207 `iss` hardening	Preview — governance-first	Runs on the same AuthZEN PEP; consumes ID-JAG at this edge. Public conformance suite not yet passed — see §8
Vault KV (OpenBAO-compatible)	Secret storage	Production	PDP-governed access and governed disclosure UX
Cross-cloud model runtime	One governance socket over managed model providers — verified delegated identity, kill switch, budget hold, per-turn signed receipt	Implemented — 3 providers	Vendor APIs rather than an identity standard; listed because enforcement is the same PEP

Internal engineering shorthand “ARIA” maps to the customer-facing EmpowerID AI Gateway, EmpowerID Governed Tool Gateway, and EmpowerID Execution Control Plane — dual enforcement plus orchestrated execution.

4.8 · Evidence and configuration audit

Standard / specification	Platform role	Maturity	Notes
JWS RS256	Signed decision and execution receipts	Production	Reporting & Evidence Service
Hash-chained receipts	Tamper-evident sequences	Production	
JWKS	Verification keys	Production	
SCITT	Supply-chain transparency for receipt registration	Roadmap	Receipt format designed to be upgradeable; not claimed today
Config-Change Ledger	Audit of external-system configuration changes	Production	Connector and system definitions

How the standards compose

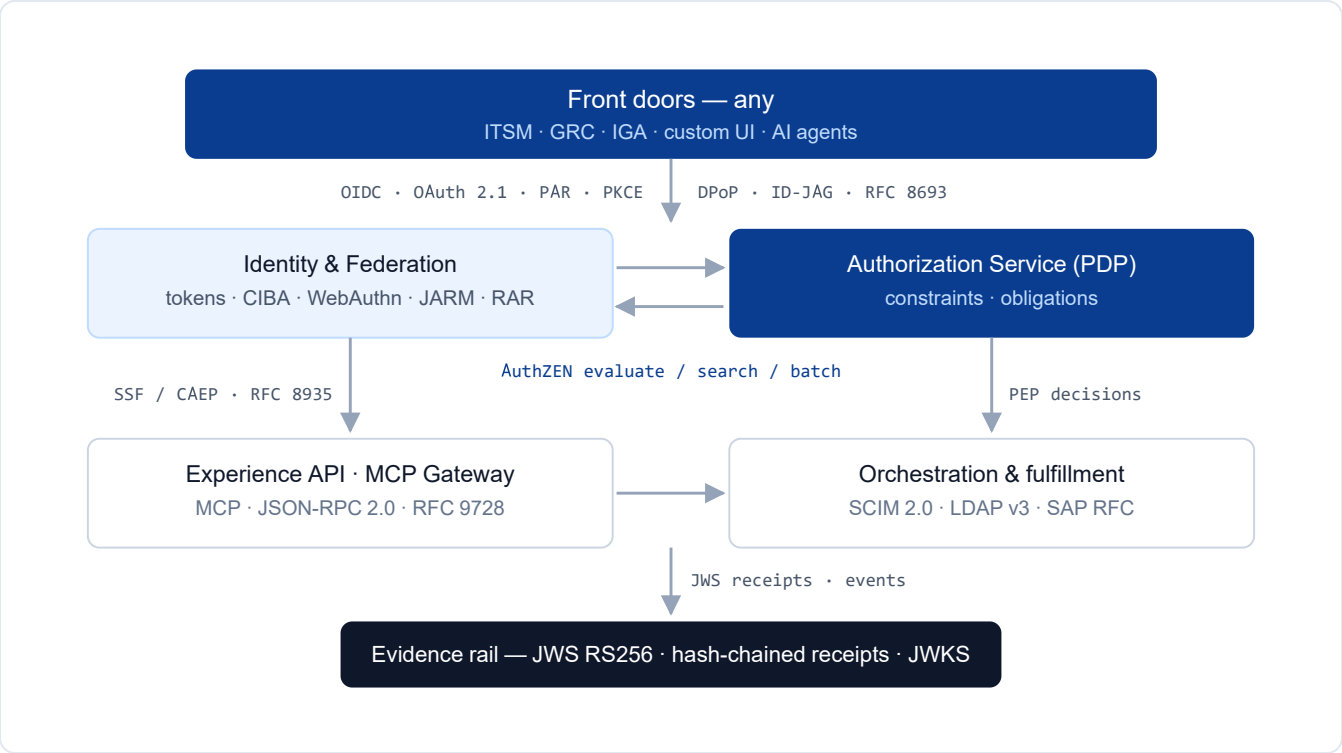

Figure 1 — Standards at each boundary. Cross-service integration uses documented APIs and events, never direct access to a peer service's database.

What is structurally different

6.1 · Compared with legacy IGA / IAM suites

Common suite pattern	EmpowerID Identity Fabric pattern	Standards angle
Monolith with embedded RBAC	Externalized AuthZEN PDP	Open evaluation and search APIs; policies as versioned configuration
Overnight batch SoD	Preventive SoD at the PDP (milliseconds, fail-closed)	Same engine as application authorization
Single relational identity warehouse	Graph + transactional grants + analytics evidence store	LDAP/SCIM at the edge; events for propagation
Governance only through vendor UI	Bring-your-own front door + API/event parity	ID-JAG and MCP for non-human callers
Agents added later	Agent Governance & Execution on the same spine	MCP, RFC 8693, ID-JAG, Credential Control

6.2 · Compared with agent-only gateways

Common agent-gateway pattern	Fabric pattern	Standards angle
Tool routing and static API keys	Governed Tool Gateway PEP + AuthZEN per tool	MCP + OAuth + AuthZEN
Credentials held in the agent	Capability without custody	Token exchange; secrets not returned to the agent
Weak enterprise IGA	Entitlement ledger and access certification engines	SCIM/LDAP fulfillment with proof chain
Ad hoc cross-app trust	ID-JAG issue and consume on resource planes	Same IETF draft wire as industry Cross-App Access
Foreign agent tokens trusted implicitly	Inbound federation materializes a governed local identity with delegation lineage	RFC 7523 jwt-bearer; foreign JWKS validation, `typ` gate, replay control, capability ∩ ceiling
Identity governed, model runtime ungoverned	Same PEP governs the agent's model traffic across cloud providers	Kill switch, budget hold, per-turn signed receipt on a verified delegated identity

6.3 · Compared with “we support OAuth” marketing

Differentiation is composition — four things working together, not four features listed separately:

`ID-JAG + AuthZEN`

Cross-app identity leg plus per-action authorization.

`Constraints + obligations`

Enforced in standard deployment, not optional demos.

`SSF/CAEP → policy → enforce`

Continuous access as verified signals, not session TTL alone.

`Proof chain`

Signed receipts linked to decisions and fulfillment.

07 — PLATFORM SCALE

Protocols at enterprise volume

Metrics below illustrate that adopted protocols operate at enterprise scale in reference deployments (mid-2026 baseline). Your sizing may differ.

Indicator	Illustrative value
Independently deployable fabric services	15+
AuthZEN application contracts / policies	115 / 227
Event topics in production	30+
Dynamic group (ABAC) rules published via events	176,000+
MCP tools via Governed Tool Gateway	167+ (400+ tool definitions on the full governance surface)
Typical PDP decision latency	Sub-10 ms
Typical search index lag	Under 5 seconds

08 — BOUNDARIES

Maturity and scope statements

Read this section before reusing any part of this brief in an RFP response.

Topic	Accurate statement
FAPI	Aligned building blocks and automated tests — not formal OpenID FAPI product certification
ID-JAG / XAA	IETF draft; interoperable with Okta Cross-App Access wire; issuance production-grade; consumption live-verified with ongoing hardening
SSF	Push transmit/receive in production; poll, RISC, and stream management on roadmap; continuous enforcement scope is expanding
SoD	Engine production-ready; customer/function catalog content must be populated for turnkey rule libraries
Access certification	Engine production-ready; production certification campaigns depend on customer rollout
Privileged access	Governed secrets vault, disclosure, and secretless agent access in production; session recording, shared-account checkout, and rotation automation on roadmap
MCP 2026 transport	Governance-first preview slice; the public conformance suite has not been passed — no “MCP 2026 certified”, “passed the official suite”, or “first to” claim is authorised
MCP EMA	Grant profiles are advertised on protected-resource metadata; two-sided interop with an external IdP/client is not complete — no “EMA certified” claim
Inbound agent federation	On-behalf-of and autonomous foreign-agent paths are live and hardened; the public trust framework for foreign issuers continues to mature
Connector catalog	Depth and configuration velocity versus incumbent SKU count — position with evidence, not parity claims
Decentralized identity / verifiable credentials	Not a current fabric focus; enterprise federation via OIDC (and SAML where deployed)
Intellectual property	Some Credential Control patterns may be subject to patent review before deep implementation disclosures

09 — NEXT STEP

Suggested technical deep-dive agenda

A 90-minute session for security architects and evaluation teams.

Time	Topic	Sections
0–15 min	Identity Fabric thesis and bring-your-own front door	§3, §5
15–35 min	AuthZEN, constraints, obligations, enforcement map	§4.4
35–50 min	ID-JAG / Cross-App Access — issue and consume	§4.3
50–65 min	SSF / CAEP continuous access	§4.5
65–80 min	Agent governance — MCP, Credential Control, dual PEP	§4.7, §6.2
80–90 min	Maturity, roadmap, partner deployment models	§8

Optional half-day add-on: full service catalog and KuppingerCole Identity Fabric mapping (separate analyst briefing available from EmpowerID).

APPENDIX A

Master reference table

ID	Name	Role on EmpowerID Identity Fabric
RFC 7636	PKCE	OAuth public clients
RFC 7662	Token introspection	Resource validation
RFC 7523	JWT bearer grant	ID-JAG Step 2 at resource AS
RFC 8693	OAuth 2.0 Token Exchange	Delegation, OBO, ID-JAG Step 1, agents
RFC 8707	Resource Indicators	Audience binding
RFC 8935	SET Push Delivery	SSF push
RFC 8936	SET Poll Delivery	Roadmap
RFC 9126	PAR	Pushed authorization requests
RFC 9396	RAR	Rich authorization requests
RFC 9449	DPoP	Sender-constrained tokens
RFC 9493	Subject identifiers	SSF/CAEP subjects
RFC 9207	AS issuer identification	Mix-up defence; MCP edge hardening
RFC 9728	Protected Resource Metadata	ID-JAG discovery
OAuth 2.1	OAuth consolidation (IETF)	Platform baseline
OIDC	OpenID Connect	SSO, ID tokens
CIBA	Client Initiated Backchannel Authentication	Decoupled authentication
WebAuthn / FIDO2	W3C / FIDO Alliance	Passkeys

ID	Name	Role on EmpowerID Identity Fabric
JARM	JWT Secured Authorization Response	Authorization response mode
AuthZEN	OpenID Authorization API	PDP evaluate / search / batch
SSF 1.0	Shared Signals Framework	Continuous access transport
CAEP	Continuous Access Evaluation Profile	Event semantics
SCIM 2.0	System for Cross-domain Identity Management	Provisioning
LDAP v3	Lightweight Directory Access Protocol	Virtual directory
MCP	Model Context Protocol	Agent tools
MCP 2026-07-28	MCP revision — stateless core, Streamable HTTP, EMA	Governed Tool Gateway preview slice
SCITT	Supply-chain transparency (IETF)	Receipt registration — roadmap
ID-JAG (IETF draft)	Identity Assertion Authorization Grant	Cross-app access (same wire as XAA)

APPENDIX B

Optional follow-on materials

Request from your EmpowerID account team or partner channel manager.

Material	Audience	Contents
Identity Fabric — Service Catalog & Capability Whitepaper	Architects, SI partners	Full service inventory, KuppingerCole building-block map, deployment bundles
Identity Fabric — Market Compass Brief (2026)	Executives, analysts	Shorter narrative and KC lens table
Cross-App Access (ID-JAG) Technical Brief	Security architects	Issue/consume flow, interoperability with Okta XAA, live verification summary
Competitive benchmark	Under NDA	Vendor comparison matrix

DOCUMENT CONTROL

Version history and disclaimer

Version	Date	Change
1.0	2026-07-28	Initial external draft
1.1	2026-07-28	Shareable edition: self-contained text, customer-facing naming, removed internal-only references

Disclaimer. This document describes product direction and implemented capabilities as of the publication date. Specifications marked *draft* or *roadmap* may change. Metrics are illustrative for reference deployments. Nothing herein modifies a signed agreement. Forward-looking statements are subject to delivery priorities and customer configuration.

Verify the composition, not the checklist

Book the 90-minute deep dive and watch ID-JAG mint under an AuthZEN decision, a CAEP signal narrow live authority, and a signed receipt chain close the loop.

Request a technical deep dive

info@empowerID.com · empowerid.com

empowerID