

---

# Identity and Access Management Architecture: Sign-On, Federation and Governance Training Course

13 – 17 September 2027  
Tokyo





## Identity and Access Management Architecture: Sign-On, Federation and Governance Training Course

Ref: 347\_22276 Date: 13 – 17 September 2027 Location: Tokyo Fees: 6900 GBP

### Programme Summary

Identity and access management architecture, covering sign-on, federation and governance, is the subject of this one-week training course for enterprise architects, security leaders and heads of digital platforms at a managerial level, ending in an identity target architecture pack for one organisation. Identity estates grow by acquisition and project, leaving duplicate sign-in paths and access nobody reviews. The programme moves from protocol principles and estate diagnosis, through single sign-on and federation design, to access governance, then to a worked architecture pack. Mars Training Centre UK delivers this programme in identity and access management architecture.

### The Business Case

When identity is built application by application, users hold more access than they need, leavers keep accounts and audit evidence takes weeks to assemble. Leaders who agree one sign-in design, clear ownership and a lifecycle for every account can reduce exposure and answer assurance questions quickly.

- Unauthorised Access Exposure: Falls as dormant, orphaned and excessive entitlements are found and removed.
- Audit Evidence Effort: Shortens as access reviews and approvals leave a standard trail.
- Sign-In Friction: Eases as applications share one federated sign-in design.

### Principles and Evidence Base

- OAuth 2.0: Its authorisation framework underpins the delegation patterns reviewed in Sessions 1 and 3.
- OpenID Connect: Its identity layer on OAuth 2.0 shapes the sign-in patterns designed in Session 3.
- SAML 2.0: Its assertion exchange informs the federation with partners and legacy applications in Session 3.
- Least privilege and role-based access control: These principles structure the entitlement diagnosis of Session 2 and the governance rules of Session 4.

### Intended Participants

- Enterprise architects who set the target design for identity across applications and platforms.
- Security leaders who own access risk, privileged access and audit evidence.
- Heads of digital platforms who connect customer, partner and workforce applications.
- Governance leads who run access reviews and joiner, mover and leaver processes.

The programme serves banks, healthcare providers, public agencies and technology-led enterprises.



## Learning Outcomes

1. Participants will be able to evaluate an identity estate against the roles of OAuth 2.0, OpenID Connect and SAML 2.0.
2. Participants will be able to diagnose orphaned, excessive and privileged access across applications.
3. Participants will be able to construct a single sign-on and federation design for workforce, customer and partner users.
4. Participants will be able to prioritise authentication strength and access control rules by risk.
5. Participants will be able to design a joiner, mover and leaver lifecycle with access certification.
6. Participants will be able to justify a target architecture and migration roadmap to a design authority.

## Programme Structure

### Day 1: Identity and Access Management Architecture Principles

What must an identity and access management architecture decide, and which protocols carry those decisions?

- Identity Domain and Trust Boundary Map
- OAuth 2.0 Authorisation Flow Review
- OpenID Connect Sign-In Pattern Review
- SAML 2.0 Assertion Exchange Review
- Workforce, Customer and Partner Identity Split

### Day 2: Diagnosing Identity Estate and Access Risk

Where do accounts, entitlements and sign-in paths carry risk that nobody owns?

- Account and Entitlement Inventory
- Identity Provider Sprawl Assessment
- Orphaned and Privileged Account Review
- Authentication Strength and Assurance Level Check
- Access Request and Approval Trail Audit

### Day 3: Designing Single Sign-On and Federation

How are users, applications and partners connected through one sign-in design without widening trust?

- Single Sign-On Reference Architecture
- Federation Trust Design for Partners
- Multi-Factor Authentication Policy Matrix
- Role-Based Access Control Model
- Session and Token Lifetime Rules



## Day 4: Access Governance and Identity Lifecycle

How does access stay correct from joining to leaving, and who proves it?

- Joiner, Mover and Leaver Workflow
- Access Certification Campaign Design
- Separation of Duties Rule Set
- Privileged Access Approval Pattern
- Identity Audit Evidence Pack

## Day 5: Applying Identity and Access Management Architecture to One Organisation

Is the target architecture ready for a design authority to approve?

- Applying the Session 2 Inventory to the Chosen Organisation
- Testing Session 3 Sign-On Design Against Risk
- Mapping Session 4 Lifecycle Controls to Systems
- Sequencing the Migration Roadmap
- Completing the Identity Target Architecture Pack

## Methodology

The programme is built around structured exercises on anonymised identity estates from banking and healthcare settings. Participants work in small teams, trace sign-in paths, rank access risks and draft a target design as an architecture board would, without writing code.

- Suggested activity: Tracing three applications from sign-in to entitlement and listing the trust assumptions.
- Suggested activity: Ranking a set of orphaned and privileged accounts by risk.
- Suggested activity: Drafting a leaver workflow that removes access in every system.

## Capstone Output

Each participant completes an identity target architecture pack for one organisation. It holds an estate inventory summary, a sign-on and federation design, an authentication policy, a lifecycle and certification model and a phased roadmap. The pack is used to brief a design authority and to plan the migration.

## Frequently Asked Questions

### Is identity and access management architecture suitable for leaders who do not write code?

Yes. Identity and access management architecture is set at managerial level and assumes familiarity with application landscapes, not programming or product administration.



## **Which protocols does identity and access management architecture rest on in this training?**

Identity and access management architecture rests on OAuth 2.0, OpenID Connect and SAML 2.0 for sign-on and federation, with least privilege and role-based access control for governance.

## **How is the architecture pack from identity and access management architecture used at work?**

You use the pack from identity and access management architecture to brief a design authority, guide platform teams and sequence the migration of applications.

## **How does identity and access management architecture differ from a cyber security strategy programme?**

Identity and access management architecture centres on how users and applications authenticate and what each may access, while a cyber security strategy programme centres on enterprise-wide threat and control policy.