ACE MULTIPASS
Cybersécurité - Méthodes agiles

TRAINING DATASHEET

Training Provider

Identity Management & Federation Training

A 4-day course dedicated to identity and access management (IAM): authentication, authorisation, cryptography, PKI, federation and SSO, through to cloud IAM (Azure, AWS) and mobility (BYOD/MDM) — to design, assess and drive an enterprise IAM strategy.

DURATION	PRICE	SCHEDULE
4 days	**€2,800**	**9:00 am - 5:00 pm** *(1.5-hour lunch break at midday)*

LEARNING OBJECTIVES

By the end of the course, participants will be able to:

- Distinguish and implement identification, authentication and authorisation mechanisms, including strong and multi-factor authentication.
- Choose a suitable access control model (DAC, MAC, RBAC, ABAC).
- Master the fundamentals of cryptography and design a public key infrastructure (PKI).
- Build a strategy for managing certificates and certification authorities.
- Implement identity federation and single sign-on (SSO) with industry-standard protocols (SAML, OpenID Connect).
- Deploy IAM in cloud environments (Azure, AWS) and for mobile/BYOD use.
- Assess and build a comprehensive IAM strategy suited to their organisation's context.

TARGET AUDIENCE AND PREREQUISITES

Anyone responsible for corporate security (CISOs, systems/network security managers) and professionals tasked with designing or assessing an identity management strategy (enterprise, B2B, Internet).

Basic knowledge of systems, networks and IT security. Proficiency with the Windows operating system.

PROGRAMME

Module 1 · The Stakes of an Identity Management Strategy (1.5 h)

- Why structure identity management: security, compliance, user experience, cost control.
- What identity and access management (IAM) covers: scope, stakeholders, identity lifecycle.
- The main approaches by context: internal enterprise, B2B, consumer (Internet).

Module 2 · Identification, Authentication and Authorisation (2 h)

- Distinguishing identification, authentication and authorisation: three often-confused concepts.
- Strong authentication: principles and use cases.
- Biometrics as an authentication factor: possibilities and limitations.
- Multi-factor authentication (MFA) with mobile devices.

Module 3 · Identity Administration and Governance (1 h)

- The identity lifecycle: creation, modification, suspension, deletion.
- Governance principles: access reviews, segregation of duties, traceability.
- The role of administration processes in reducing risk.

Module 4 · Directories and Authentication Databases (2 h)

- Centralised directory vs federated approach: advantages and limitations of each model.
- LDAP v3 directories: structure, schema, replication.
- Securing directory access: LDAPS, LDAP/TLS.
- Controlling and auditing access to directory objects, certificate publication.

Module 5 · Access Control Models (1.5 h)

- Comparing the main authorisation methods: DAC, MAC, RBAC, ABAC.
- Access control lists (ACLs): how they work and use cases.
- Choosing the right model for the organisational context.

Module 6 · Cryptography Concepts for IAM (2 h)

- Symmetric and asymmetric encryption: principles and respective uses.
- Hashes and digital signatures: ensuring integrity and authenticity.
- The digital certificate as a building block of trust.

Module 7 · Hardware Implementation of Cryptography (1 h)

- Storing private keys on hardware tokens (smart cards, YubiKey…) and hardware security modules (HSMs).
- Using hardware containers to protect keys.
- Comparing security levels depending on the storage method chosen.

Module 8 · Public Key Infrastructure (PKI): The Fundamentals (2 h)

- X.509 v3 certificates and their role in a PKI.
- Defining an identity in a public key infrastructure.
- Determining certificate lifetimes and controlling access through attribute certificates.

Module 9 · Building a Certificate Management Strategy (2 h)

- Securing private keys: automatic archival, key recovery agent.
- Mapping identities to certificates and distributing trusted certificates.
- Publishing certificate revocation lists (CRLs) and managing the certification authority hierarchy (root, intermediate, issuing CA).
- Strengthening security with an offline root CA; assessing trust in external CAs and complying with a certificate policy.

Module 10 · Authentication and Identity Propagation Protocols (2 h)

- Identity propagation protocols: SAML, SOAP.
- Securing XML exchanges: XML Encryption, XML Signature.
- The role of these protocols in interoperability between systems.

Module 11 · Federated Identity Management and SSO (2 h)

- The principle of single sign-on (SSO) and its benefits.
- Ensuring interoperability through claims and open industry standards.
- The identity metasystem vision: federating without centralising.

Module 12 · Case Study: Federation with Microsoft ADFS (1 h)

- Local authentication and remote access in an ADFS architecture.
- Designing claims-based applications with SAML.
- Abstracting the WS-Trust and WS-Federation protocols: what they bring in practice.

Module 13 · Identity Federation with Microsoft Azure (1.5 h)

- Extending on-premises Active Directory to Azure.
- Implementing single sign-on with Azure for SaaS applications.
- Ensuring identity interoperability and portability across environments.

Module 14 · Federation with AWS and Multi-Cloud Interoperability (1.5 h)

- Amazon AWS federation: authenticating with Amazon IAM roles.
- Connecting a federated Microsoft identity to Amazon services and instances.
- Simplifying cross-system identity management with the SCIM protocol.

Module 15 · Identity Management for Mobility and BYOD (1.5 h)

- The specific IAM challenges of mobile devices and BYOD.
- Enrolling mobile devices using certificates.
- Configuring SCEP (Simple Certificate Enrollment Protocol), with examples using an MDM (Microsoft Intune) and network devices.

Module 16 · Wrap-up: Building a Comprehensive IAM Strategy (1.5 h)

- Review of the key building blocks covered during the course.
- Evaluation grid for an identity management solution in an enterprise, B2B or Internet context.
- Key success factors and common pitfalls of an IAM project.

LIST OF WORKSHOPS AND DEMOS

- Workshop 1: exploiting protocol weaknesses
- Demo 2: simulating a Diffie-Hellman key exchange
- Workshop 3: installing and configuring an SSH server
- Workshop 4: using OpenSSL for secure exchanges
- Workshop 5: Microsoft certificate store
- Workshop 6: deploying a Microsoft root certification authority
- Workshop 7: deploying a Microsoft intermediate certification authority
- Workshop 8: configuring and issuing a user certificate
- Workshop 9: certificate-based web authentication
- Workshop 10: secure email exchange
- Workshop 11: Firefox web authentication and electronic signing of PDF and Word documents
- Workshop 12: smart card user enrollment by an enrollment agent
- Workshop 13: certificate archival and recovery
- Workshop 14: configuring SSO with ADFS
- Demo 15: installing and configuring Azure AD Connect
- Demo 16: using AWS SSO to integrate with Azure AD
- Demo 17: AWS IAM federation with Azure AD

- Demo 18: configuring the Simple Certificate Enrollment Protocol (SCEP)

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Each session can be adapted to the needs of people with disabilities. Participants concerned are invited to let us know before the start of the course so that we can examine possible arrangements together: room access conditions, adaptation of materials and teaching methods, or rescheduling of the session.

TEACHING AND TECHNICAL RESOURCES

Sessions are delivered using a variety of tools: audiovisual materials, documents handed out to trainees, practical exercises with their solutions for operational courses, and real-world case studies or lessons learned for more theoretical sessions.

At the end of each session, ACE-MULTIPASS gives trainees a satisfaction questionnaire, the results of which are then reviewed by the teaching team.

An attendance sheet is signed every half-day and handed in at the end of the course; a certificate of attendance is also issued to trainees who have attended the entire session.

TRAINER EXPERTISE

Our trainers are chosen for their expertise in the fields they teach. Each one is selected by our teaching team, which checks both their technical command of the subject and their ability to teach and lead a group. They generally have at least five to ten years of professional experience and hold or have held positions of responsibility in their sector.

ASSESSMENT METHODS

Throughout the course, the trainer measures trainees' progress through various exercises: multiple-choice questionnaires, role-plays or practical exercises.

A positioning test is also carried out before and after the course to measure the skills acquired by each participant.