

Mis à jour le 24/08/2026

S'inscrire

Formation eIDAS 2.0

1 jour (7 heures)

Présentation

La réglementation eIDAS 2.0 fait évoluer l'identité numérique européenne avec le portefeuille européen d'identité numérique, les services de confiance et de nouvelles exigences d'interopérabilité.

Notre formation eIDAS 2.0 vous permettra de comprendre les évolutions réglementaires et techniques du cadre européen d'identité numérique, ainsi que leurs impacts pour les organisations publiques et privées.

Vous apprendrez à identifier le rôle du European Digital Identity Wallet, des attestations électroniques d'attributs, des parties utilisatrices et des prestataires de services de confiance dans les parcours d'identification et de partage de données.

À l'issue de la formation, vous serez en mesure d'analyser un cas d'usage eIDAS 2.0, de qualifier les exigences de sécurité, de protection des données et de conformité, puis de préparer l'intégration d'un portefeuille numérique dans votre système d'information.

Cette formation aborde également les mécanismes de divulgation sélective, les niveaux de garantie, les signatures et cachets électroniques, les listes de confiance et les bonnes pratiques de gouvernance pour construire des services numériques fiables à l'échelle européenne.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le cadre réglementaire et les évolutions introduites par eIDAS 2.0
- Identifier les acteurs, composants et flux du portefeuille européen d'identité numérique

- Différencier les services de confiance, les attestations d'attributs et les mécanismes d'identification électronique
- Évaluer les exigences de sécurité, d'interopérabilité et de protection des données d'un cas d'usage
- Préparer une démarche d'intégration eIDAS 2.0 adaptée à une organisation

Public visé

- Architecte sécurité
- Responsable IAM
- Chef de projet identité numérique
- Consultant cybersécurité
- Responsable conformité numérique

Pré-requis

- Connaissance des concepts d'IAM et de gestion des identités
- Notions de sécurité des échanges numériques et de cryptographie
- Compréhension générale des enjeux de conformité et de protection des données
- Expérience de projets de dématérialisation ou de services numériques

Pré-requis techniques

- Poste de travail sous Windows 10 ou 11, macOS ou Linux
- Navigateur récent, Google Chrome, Mozilla Firefox, Microsoft Edge ou Safari
- Connexion Internet stable autorisant l'accès aux ressources de démonstration
- Lecteur de documents au format PDF et outil de prise de notes

Programme de notre formation eIDAS 2.0

[Jour 1 - Matin]

Comprendre le cadre européen de l'identité numérique

- Panorama de la réglementation eIDAS et des évolutions apportées par eIDAS 2.0
- Enjeux métier et réglementaires de l'identité numérique européenne pour les services publics et privés
- Rôles et responsabilités des États membres, fournisseurs de portefeuilles, émetteurs d'attributs, parties utilisatrices et prestataires de services de confiance
- Fonctionnement du European Digital Identity Wallet : identité, justificatifs, authentification, présentation en ligne et hors ligne
- Principes de protection des données, consentement, pseudonymes et divulgation sélective des attributs
- Atelier pratique : cartographier deux parcours eIDAS 2.0, un accès à un service en ligne et un contrôle de justificatif, puis identifier les acteurs, données échangées et points de conformité

Concevoir des usages conformes et interopérables

- Les attestations électroniques d'attributs : données d'identification, attributs qualifiés et non qualifiés, émission et vérification
- Les services de confiance : signature électronique, cachet électronique, horodatage, certificats et archivage électronique
- Niveaux de garantie, sécurité du portefeuille, gestion des clés, authentification forte et révocation
- Interopérabilité technique : protocoles, interfaces, formats d'échange, architecture de référence et intégration au système d'information
- Gouvernance de mise en oeuvre : analyse de risques, listes de confiance, qualification des parties utilisatrices et feuille de route de déploiement
- Atelier pratique : concevoir un scénario d'intégration pour une partie utilisatrice, définir les attributs minimaux demandés, les contrôles de confiance et les mesures de sécurité, puis restituer une feuille de route opérationnelle

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.