11 questions to ask before choosing an identity management solution

Choosing an Identity and Access Management (IAM) solution commits your organisation for several years. Dedicated or shared infrastructure, European hosting, pricing models, reversibility and regulatory compliance are all criteria that providers will not necessarily highlight. This document brings together the questions to ask and the warning signs to identify in the answers.

> **How to use this document**
>
> Ask these 11 questions to every IAM provider you evaluate, then compare their answers. An evasive answer, or no answer at all, is information in itself.

HOSTING AND SOVEREIGNTY

01 Where is my identity data physically hosted?

User directories, password hashes, session tokens and login logs are among the most sensitive data in your information system (IS): if they are compromised, access to all your applications can be gained. Some providers advertise "Europe" while subcontracting to infrastructures located outside the European Union. Ask for the specific country, the datacenter and the list of hosting subcontractors.

Warning sign : *a vague answer ("our European datacenters"), refusal to specify where the directory and secrets are stored, or reliance on Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP) without a guaranteed location.*

02 Is my data exposed to US extraterritorial laws (Cloud Act, FISA)?

Two US laws apply to companies incorporated under US law, regardless of where the data is stored. The Cloud Act (2018) allows authorities to require access to the data they hold. The Foreign Intelligence Surveillance Act (FISA), Section 702, provides the legal basis for surveillance programmes targeting non-US persons—it was this legislation that led the Court of Justice of the European Union to invalidate the Privacy Shield in 2020 (Schrems II judgment). Okta/Auth0, Microsoft and any provider whose parent company is American are subject to these laws.

Warning sign : *the provider is a US company or the subsidiary of a US company. GDPR compliance and hosting in Europe are not sufficient to eliminate this risk.*

03 Is my identity directory isolated or shared with other customers?

On an identity platform, multi-tenancy means that your accounts, secrets and tokens coexist with those of other organisations in the same database. This creates neighbour-related risks: cross-tenant data leakage, log correlation and shared service outages. A dedicated instance fully isolates your directory (application, database and file system).

Warning sign : *the provider cannot confirm complete isolation of your directory, or stores the identities of multiple customers in a shared database.*

COMPLIANCE AND REGULATIONS

04 Which certifications apply, and do they cover the solution I am purchasing?

ISO 27001 (information security management), HDS (French Health Data Hosting certification), SecNumCloud (ANSSI qualification) and SOC 2 demonstrate a level of maturity that has been independently audited. A key point is that a certification often applies to the platform or the provider,

rather than to each individual product, and some certifications (such as HDS) may require a separate contract at an additional cost. Ask for the exact scope of the certification and the conditions under which it applies to your solution.

Warning sign : *certifications presented without specifying their scope, confusion between certification of the platform and certification of the purchased solution, or conditions (such as a separate contract or additional cost) omitted.*

05 Does the service provide the information required for my NIS2 compliance?

The NIS2 Directive requires organisations to maintain control over their digital supply chain. Your IAM solution is part of that supply chain: you must be able to document your provider's security measures and incident notification procedures during an audit.

Warning sign : *the provider is unable to provide certifications, documented security measures or incident notification procedures that can be used as part of your own compliance documentation.*

06 Who is responsible for security updates, and how are vulnerabilities monitored?

Security flaws affecting Keycloak or its underlying libraries are published as publicly referenced vulnerabilities (CVEs). In a self-managed model, your team is responsible for applying the fixes. In a managed model, verify who is responsible for deploying patches and how vulnerability monitoring is organised.

Warning sign : *the provider does not specify who deploys security patches or how vulnerabilities are monitored and addressed.*

SERVICE AVAILABILITY AND SECURITY

07 What is the availability SLA, and what does it cover?

An SLA of 99.9% allows for approximately nine hours of downtime per year; at 99.99%, less than one hour. Verify the scope of the SLA, how maintenance windows are handled, and whether contractual penalties apply if the target is not met.

Warning sign : *an SLA below 99.9%, unplanned maintenance included in the availability calculation, or the absence of contractual compensation.*

08 Which strong authentication methods are available?

An identity service should support multi-factor authentication without relying on a single technology: passkeys and WebAuthn, one-time passcodes, mobile authenticator applications, as well as step-up authentication, which requires an additional authentication factor only for sensitive actions. Verify the range of available methods and their compatibility with your use cases.

Warning sign : *multi-factor authentication limited to a proprietary application, no support for passkeys/WebAuthn, or authentication methods based on proprietary technology.*

REVERSIBILITY AND OPEN STANDARDS

09 Can I recover all my identities, including password hashes?

With an identity service, reversibility is not limited to exporting the list of users: without password hashes, a migration requires all your users to reset their credentials. Ask about the export format (for example, the Keycloak JSON realm export), the exact scope of the recoverable data, and the conditions for exporting secrets.

Warning sign : *password hashes cannot be exported, secret exports are restricted depending on the pricing plan or available only on request, the export format is proprietary, or there is no documented migration procedure.*

10 Is the solution based on open identity standards, and can it federate my existing directories?

OAuth 2.0, OpenID Connect (OIDC) and SAML v2 ensure interoperability with your applications; LDAP / Active Directory federation and brokering with other identity providers prevent the duplication of user accounts. A solution that implements these standards only partially, or through proprietary extensions, locks you into its ecosystem.

Warning sign : *partial support for standards, no support for SAML v2, or LDAP / Active Directory federation and identity brokering limited to proprietary connectors.*

TOTAL COST AND PRICING MODEL

11 Is the pricing transparent and predictable, and what exactly does it cover?

Monthly Active User (MAU) and provisioned-user pricing models can lead to unexpected costs as your organisation grows or experiences usage spikes. Verify whether a public pricing schedule exists, how much notice is given before price increases, and what options are available if prices rise. Then distinguish what is included in the advertised price from what is charged as a paid option (Service Level Agreement [SLA], support, migration), and check whether any exit fees apply.

Warning sign : *no public pricing schedule, price increases without prior notice, critical options (SLA, 24/7 support) not clearly distinguished from the base price, or exit fees charged upon termination.*

Keycloak as a Service by Clever Cloud

Managed Keycloak, hosted in France, with maintenance and vulnerability monitoring handled by our teams.

INCLUDED IN THE OFFER – STARTING AT €47/MONTH

Managed Keycloak · dedicated infrastructure and isolated resources · built-in monitoring (metrics and dashboards included, no paid tier) · IP filtering (admin, per realm, and within the authentication flow) · strong authentication: passkeys, WebAuthn, and email OTP · domain-based registration filtering (whitelist/blacklist) · autoscaling · open standards (OAuth 2.0, OIDC, SAML v2, SCIM in preview, LDAP/AD) · realm export, including password hashes · cluster provisioning via Terraform · termination with no penalty fee.

OPTIONAL OR AVAILABLE AS A DEDICATED OFFER

99.99% availability SLA, 24/7 support and response time commitments (Premium option) · SecNumCloud-qualified zone available on request through our partner Cloud Temple.

ABOUT CLEVER CLOUD

A French company certified to ISO 27001:2022 and HDS (French Health Data Hosting certification, covering all six activities). HDS hosting applies to eligible services under a separate contract. SecNumCloud certification is currently in progress.

clever.cloud/product/managed-keycloak-as-a-service/