Monokee Technical Profile

version 1.2

Table of Contents

Executive Summary

Monokee is a technology enabler that integrates Identity and Access Management (IAM) with disruptive and decentralized technologies to provide enterprise-grade security and compliance.

At its core, Monokee is an IAM framework suitable for enterprise ecosystems of all sizes, from Small and Medium Enterprises (SMEs) to large corporations, by providing Single Sign-On (SSO) with Multi-Factor Authentication (MFA) among many other identity-related functionalities.

Monokee works natively in a heterogeneous business ecosystem, including industrial, banking, and healthcare customers. The proprietary visual engine enables systems administrators to implement integrated governance policies for classic IAM scopes and domain or business-specific scenarios.

With the integration of MFA and dynamic risk and trust assessment, Monokee's Continuous Adaptive Trust (CAT) reduces the enterprise attack surface, thus minimizing the overall risk of identity theft and unauthorized access. The next-gen technology in user journey orchestration enables the extraction of security claims that can be used for compliance and risk analysis purposes. With our trusted partners, Monokee includes the support for Know Your Customers (KYC) and Anti Money Laundering (AML) technologies.

The future, however, is decentralized. Monokee fully embraces the new Self-Sovereign Identity (SSI) paradigm with native support for distributed technologies and direct integration of Verifiable Credentials (VC) in the SSO user journeys.

With the SSI integration, enterprises can offload the identity aspects of the authentication and authorization flows, further reducing the overall responsibilities and delegating to third-party trusted issuers the risks associated with user identities.

Monokee is built with a robust cybersecurity driver in terms of infrastructure regulatory requirements:

1. the microservices-based architecture guarantees isolation and reliability provided that each virtualized container ensures limited external access both at rest and while running;
2. strong authentication and authorization mechanisms are enforced inter-components to ensure data protection and prevent known threats;
3. regular code review processes and anti-malware controls are in place to minimize the risk associated with cyber threats and vulnerability exploits.

Monokee’s introduction has immediate OPEX savings on the:

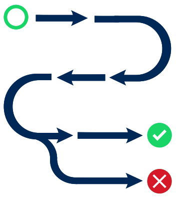
1. management costs associated with classic IAM KPI, such as the integration of SSO;
2. drastic decrease in help desk costs and ad-hoc technical training for all the integrated services;
3. simplification of identity-related procedures, such as password changes and multiple entities interaction.

There are also notable indirect and long-term OPEX savings associated with the reduced risk of security breaches and compliance with current regulatory requirements (e.g., GDPR fines are in the order of 4% global turnover or 20 million EUR).

Unique value proposition

These are the features that make Monokee unique and special against the competition.

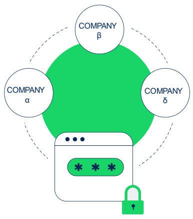
Visual Identity Orchestrator



A unique drag-and-drop framework for mapping the user journeys during all phases of the identity lifecycle, including provisioning, authentication, and authorization. Monokee enables enterprise teams to build user journeys with a codeless approach, drastically reducing the integration complexity and time.

Read about it in the *Visual Identity Orchestrator (V.I.O.)* section.

Multi-domain (patented)



With SSO functionalities, Monokee covers all requirements and enterprise use cases for identity federations.

Both cloud and on-premises tenants support Monokee’s unique and patented feature to create unlimited domains to guarantee isolation and segregation by default. It can be configured to enable users’ migration and sharing between domains in a single tenant.

Domains can be hidden/visible to each others depending on requirements.

Read about it in the *Patented multi-domain tenants* section.

Ready for Self-Sovereign Identity

Decentralized identity will sustain the upcoming Web 3.0, and the public sector will soon consider digital identity wallets as requirements for citizens.

Since 2021 Monokee has been fully compliant with industry standards and integrates all major SSI frameworks for Verifiable Credentials usage within enterprise federations.

Read about it in the *Decentralized IAM Framework* section.

Centralized IAM Framework

Companies must deal with increasing numbers of users logging into many work-related applications; in addition, administrators, privileged users, groups of users, and internal and external users have distinctive attributes and related application rights.

Centralizing all user's accounts into one identity comes with operational benefits, both for the user who logs in once to access all his applications and the system administrator, who can manage groups, roles, users, attributes, and applications from an all-in-one dashboard panel.

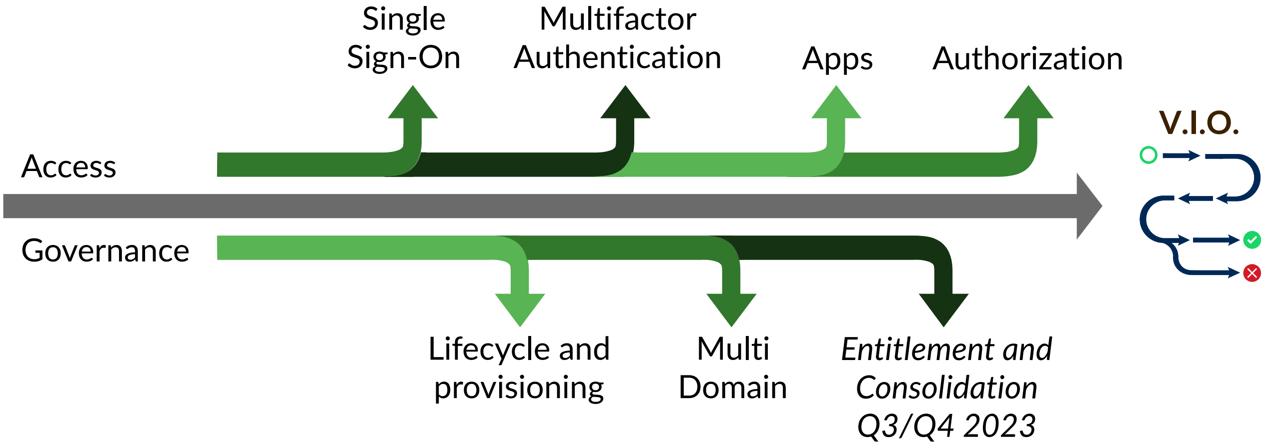

Single Sign-On
Multifactor Authentication
Apps
Authorization
V.I.O.
Access
Governance
Lifecycle and provisioning
Multi Domain
Entitlement and Consolidation Q3/Q4 2023

Figure 1: Monokee Centralised IAM Framework general overview.

As a centralized identity platform, Monokee revolves around access management with some light governance features.

Access Management

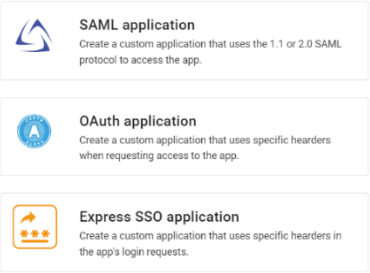
Monokee's core functionalities provide a complete suite of tools for access management. As such, it includes everything you might expect regarding the application catalog, Single Sign-On (SSO), Multi-Factor Authentication (MFA), Authorisation, and Orchestration.

Monokee Identity Provider is RBAC at its core, however, custom attributes are supported to achieve ABAC-like capabilities. For more information, refer to the *Identity Governance* section.

Application Catalogue

Monokee supports apps integrated with SAML 2.0 (including sign and encryption), OAuth2 and OpenID Connect (OIDC), generic token-based authentication including full JOSE support (JWT, JWE, JWK, JWA, and JWS), and custom legacy authentication.

Configurations for individual applications can be imported, exported, and provided as a template.



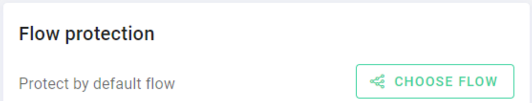
SAML application
Create a custom application that uses the 1.1 or 2.0 SAML protocol to access the app.

OAuth application
Create a custom application that uses specific hearders when requesting access to the app.

Express SSO application
Create a custom application that uses specific hearders in the app's login requests.

Figure 2: Add new application

Your application, your rules: individual applications can be protected by customizable access policies.



Flow protection

Protect by default flow

Figure 3: Example of application protection flow

Administrators can use data from users, roles, custom attributes, custom scripts, and external data sources to make a decision.

Individual applications can be associated directly with users but also with groups, and, in addition to the classic RBAC scheme, custom attributes may be valorized statically (i.e., based on individual users' attributes or groups) but also dynamically (i.e., based on APIs, policies, or runtime values)

Single Sign-On (SSO)

Monokee plays a hybrid role, depending on the process in which it is involved and the actor addressed.

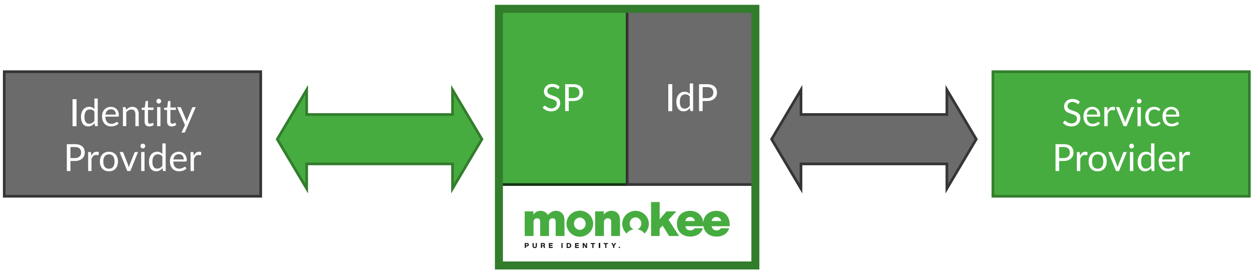


Figure 4: Monokee acts as Identity Provider or Service Provider depending on the role of the other actors.

Monokee supports multiple protocols in each phase independently.

For example, you can use a SAML application (SP) with Monokee as IdP but have the users come from another IdP using any given modern authentication protocol.

To achieve these bridging functionalities, Monokee extensively supports SSO protocols such as SAML 2.0, OAuth 2, OIDC, JOSE, Simple Web Tokens, and mTLS.

Custom authentication methods can be evaluated upon request.

Monokee is also OpenID Certified (including for 3rd party initiated OP).

Multi-Factor Authentication and Continuous Adaptive Trust

Enforcing a solid MFA strategy for a more secure business environment is extremely important but nonetheless often ignored. To ease enterprises in rolling out mandatory MFA for all accounts, monokee natively integrates several authentication factors:

- One-Time Password (OTP), both time-based (TOTP) or HMAC-based (HOTP)
- SMS (discouraged as of 2017)
- Hardware tokens and security keys
- WebAuthN and FIDO2
- Biometrics and Know Your Customer (KYC) providers

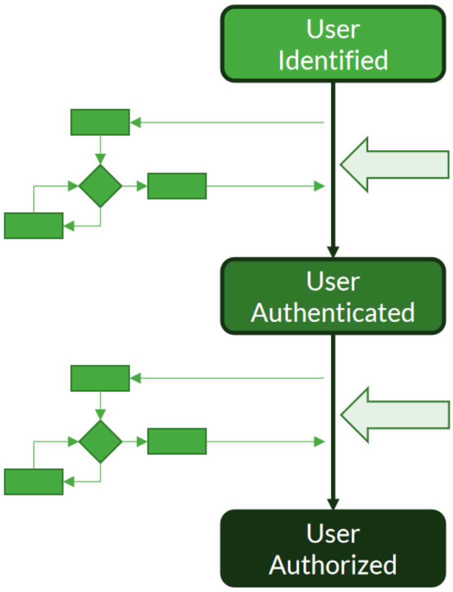
Unfortunately, a blind count of the authentication factors asked of the user is a naïve approach. Monokee enables security engineers to build custom policies for dynamic risk and trust management that include runtime conditions and behavioral parameters to achieve Continuous Adaptive Trust (CAT). With Monokee, you can move from MFA to CAT, integrating passwordless user journeys where the trust in the user identity is continuously adapted and evaluated.

Custom factors can increase security while reducing the frequency of additional authentication steps. Different entry barriers can be designed on security levels and threat indicators, enabling frictionless access to low-sensitivity areas while guaranteeing a security assurance level. CAT factors include user identity, access context, reputation analysis, and anomaly detection.

Authorization

Monokee supports dynamic and configurable authorization approaches: it is possible to combine multiple conditions to guarantee authorized access to the applications.

The image below summarises some examples of custom policies that can be designed within Monokee.



Custom policies

MFA example:

- For ***dev*** use **WebAuthN biometric auth**
- For ***hr*** use **TOTP with Google Auth**
- For ***management*** use **Yubiko Key**
- For ***sysadmin*** require both **FIDO2** and Any **Manager approval**

Custom policies

Application-level granularity example:

- For *ClientX-VPN* require attribute ABC and ManagerY approval
- For Any *Intranet App* require Trusted Device and Internal IP
- For *Salary Portal* require Email Verification if **not** Trusted Device

Figure 5: Monokee custom policies application in an authentication and authorization user journey.

Identity Governance and Administration (IGA)

Monokee includes an Identity Management (IdM) toolbox to complete the AM features for essential use cases such as lifecycle management, provisioning and de-provisioning, entitlements, and identity consolidation. Advanced functionalities may be achieved via third-party integrations with dedicated IGA vendors.

Patented multi-domain tenants

Monokee's patented feature permits to manage of multiple domains within the same tenant. Rather than managing a unique data source for users, identities, flows, and so forth, Monokee enables strong segregation between domains. For example, the IT department of a company can manage a tenant for the whole organization, while each other Business Unit (BU) is independent and completely isolated. However, the IT department might have specific privileged accounts that are enabled to travel across the other domains, thus allowing seamless interaction with the platform and streamlined configurations.

Domains can be joined in trusted relationships to enable seamless identity traveling between them (e.g., Administrators might manage both domains with different privileges and roles but with the same identity). These accounts are called Siblings.

Data segregation and isolation can be guaranteed by logically separating the data sources (i.e., using different cryptographic keys to protect the data) or using different data clusters.

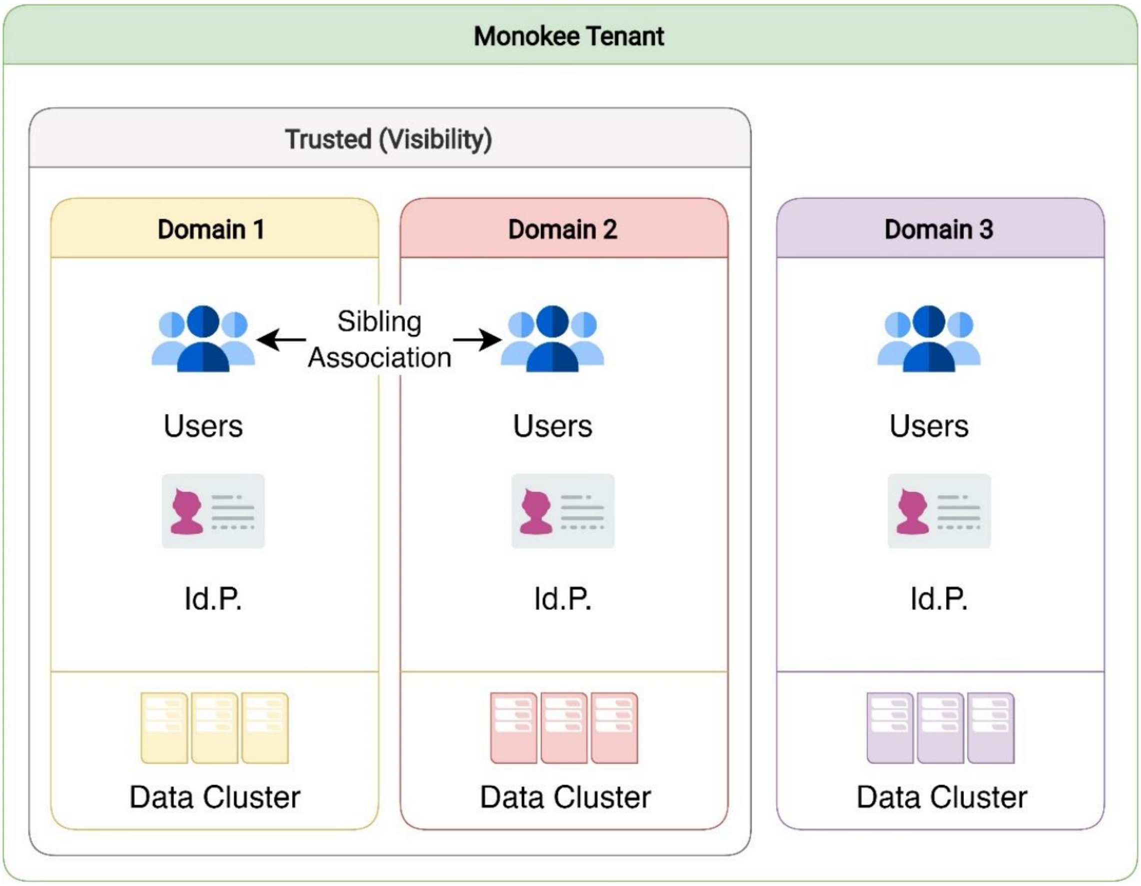


Figure 6: Monokee tenant with multiple domains.

Lifecycle, Provisioning, Entitlement

As mentioned in the previous sections, Monokee is designed to work with identities obtained from any given source. However, Monokee Identity is RBAC with the addition of custom attributes. Custom attributes are generic `key:value` pairs for users and groups. The values can be statically assigned by administrators or calculated at runtime directly in the flows.

Each governance workflow can be designed via the *Visual Identity Orchestrator (V.I.O.)*. Specifically, administrative flows provide the tools for onboarding, offboarding, and general access privileges management.

Self-service flows can be deployed to offload first-level ticketing for user support, including registration, password management, applications, and access requests.

Direct provisioning for third-party applications can be achieved via SCIM, Just-In-Time provisioning, or customized API calls.

Visual Identity Orchestrator (V.I.O.)

At its core, Monokee features a complete orchestration tool for managing identities, applications, and user journeys.

Monokee's VIO permits the planning and execution of user journeys for each application. These flows can be monitored and analyzed to infer security properties and statistical information. Security engineers can dynamically adapt them to organizations' requirements and ecosystem changes. By using the VIO, security engineers and administrators can reduce development and operational costs while increasing usability and awareness.

Below, see Gartner's six key value points for Identity Orchestration and how Monokee perfectly fits the description.

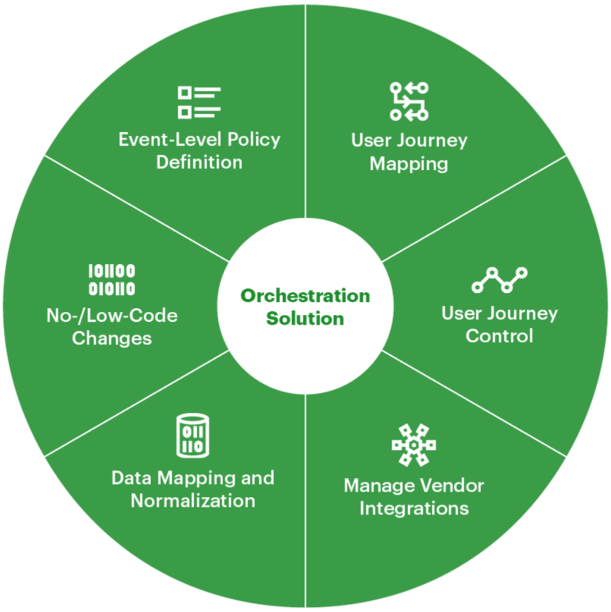

Event-Level Policy Definition
User Journey Mapping
No-/Low-Code Changes
Orchestration Solution
User Journey Control
Data Mapping and Normalization
Manage Vendor Integrations

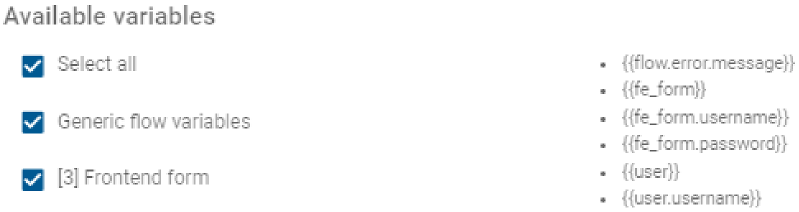
Figure 7: Gartner's six key value points for Identity Orchestration.

Entry-level policy definition

With Monokee, it is possible to integrate hundreds of custom factors in your policy to trigger external tools or obtain augmented information. Custom API calls can be included in any user journey to get information or trigger external events.

No-code/Low-code changes

Monokee's VIO integrates a drag-and-drop canvas for the configuration, personalization, and refinement of user journeys. Variables can be easily copy-pasted from the helper panel. Custom frontend and backend scripts can be included upon request.



Available variables

☑ Select all

☑ Generic flow variables

☑ [3] Frontend form

- {{flow.error.message}}
- {{fe_form}}
- {{fe_form.username}}
- {{fe_form.password}}
- {{user}}
- {{user.username}}

Figure 8: Monokee variable helper panel.

Data mapping and normalization

Monokee has been successfully deployed for seamless integration for systems and vendors that operate with different protocols, messages, or data formats.

User journey mapping

Each flow can be designed with a drag-and-drop canvas and connected to any given application. Custom blocks can be used to catch events of interest or specific conditions.

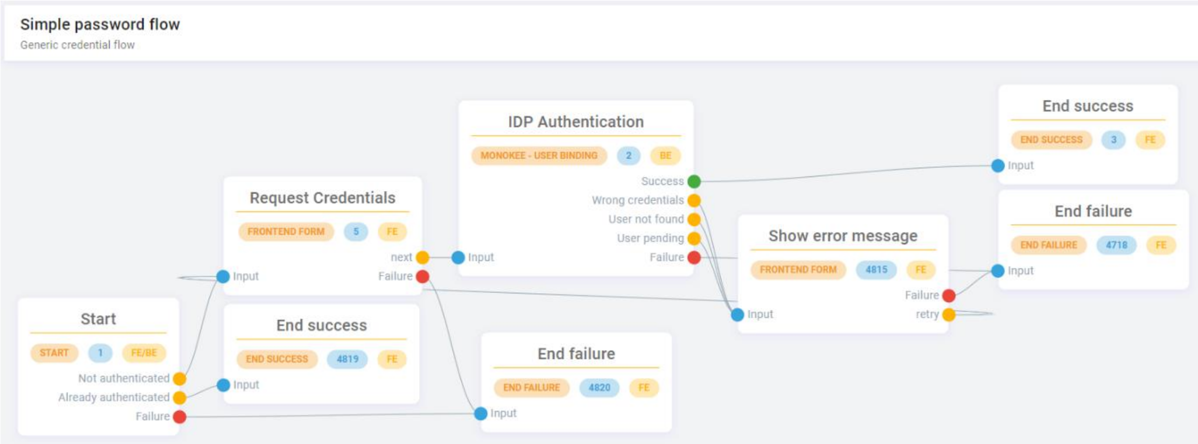


Figure 9: Monokee's VIO for a generic credential authentication flow.
The user lands on the ***Start*** *node; if he is already authenticated, nothing is changed and the* ***End success*** *node is triggered. If the user is not authenticated, he will be prompted with a credentials request and authenticated (****IDP Authentication****). If the credentials don't match the stored ones, an error message will be displayed with a button to retry. Catch-all* ***End failure*** *nodes are connected to every node to enable error management.*

User Journey Control

Administrators may trigger dynamic and highly customization policies directly at runtime. Monokee supports both direct events handling and webhooks for triggering user journeys.

Manage Vendors Integration

Monokee natively integrates and manages thousands of third-party applications via modern authentication protocols or custom injection for legacy ones. Partners may customize nodes to provide additional features specific to third-party vendors not yet supported.

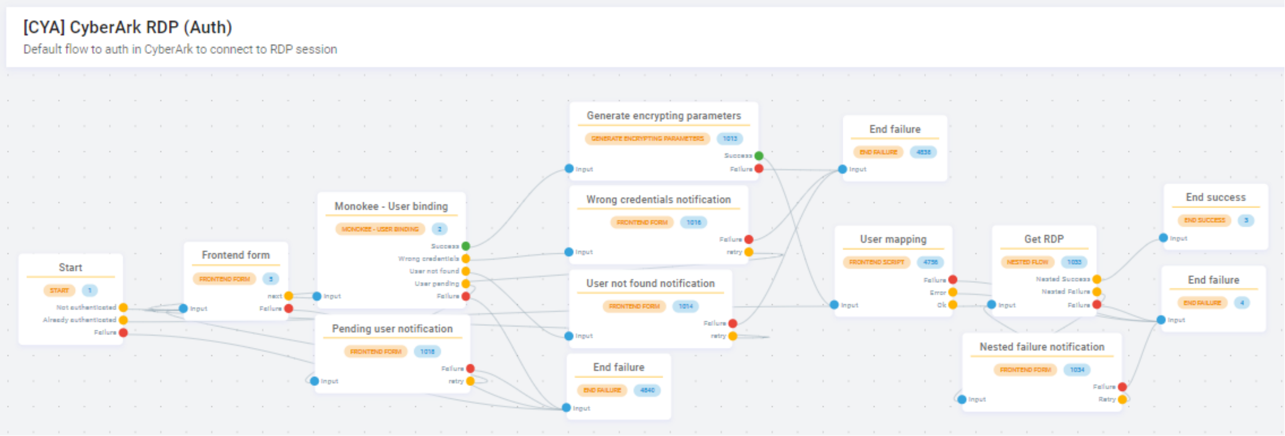
Privileged Access Management (PAM)

Like the IGA functionalities, Monokee only covers a minimum amount of features in the Privileged Access Management (PAM) and is designed to cover the minimum requirements of small to medium organizations. For larger ones, Monokee supports full integration with third-party solutions.

Monokee currently does not support password vaulting, activities control, in-session monitoring, privilege evaluation, or attestation. For these requirements, integration with a third-party partner is advised.

Privileged remote access management

Monokee can be integrated with Zero-Trust solutions to grant just-in-time access to internal machines via RDP or Web HTML5 connections. Access can be granted temporarily and with customized flows that may include explicit policy acceptance, confirmation, or third-party approval.



[CYA] CyberArk RDP (Auth)

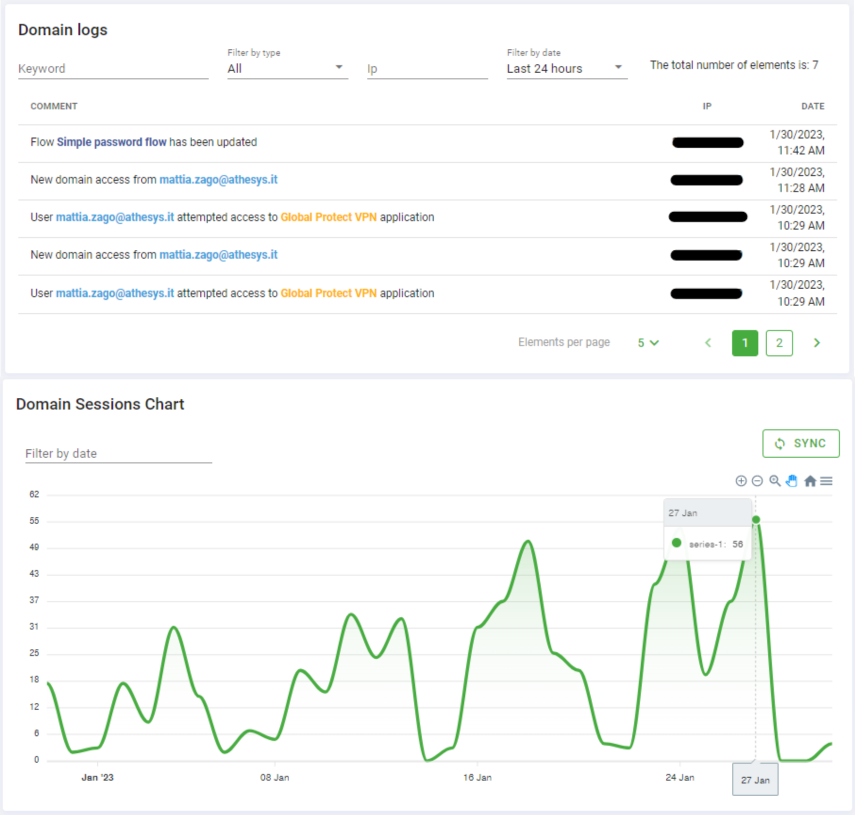
Default flow to auth in CyberArk to connect to RDP session

Figure 10: Example of Monokee user journey for PAM RDP session.
The user is authenticated and mapped to a user on the target PAM solution.
*A dedicated **Nested Flow** is used to get the correct RDP file to send to the user.*

User activity recording and real-time visibility

Monokee VIO can be deployed for the protection of any given resource. Unique and individual sessions are established for each user, including privileged ones. Monokee enabled administrators to certify access to resources for compliance purposes.

Clients can integrate custom automatic analysis functions to evaluate user journeys and identify anomalies and threats. Monokee also supports direct and authenticated exports toward Security Information and Event Management (SIEM) systems and Security Operations Center (SOC) management tools.



Domain logs

Keyword

Filter by type: All

Ip

Filter by date: Last 24 hours

The total number of elements is: 7

COMMENT	IP	DATE
Flow Simple password flow has been updated	[redacted]	1/30/2023, 11:42 AM
New domain access from mattia.zago@athesys.it	[redacted]	1/30/2023, 11:28 AM
User mattia.zago@athesys.it attempted access to Global Protect VPN application	[redacted]	1/30/2023, 10:29 AM
New domain access from mattia.zago@athesys.it	[redacted]	1/30/2023, 10:29 AM
User mattia.zago@athesys.it attempted access to Global Protect VPN application	[redacted]	1/30/2023, 10:29 AM

Elements per page 5 ‹ 1 2 ›

Domain Sessions Chart

Filter by date

Figure 11: Monokee Dashboard

Decentralized IAM Framework

The identity landscape is evolving from well-known identity federations to fully decentralized solutions. The Self-Sovereign Identity (SSI) paradigm was designed to solve the existing problems with paper-based ids in the digital realm by shifting the models toward user-centric, trustworthy, and privacy-preserving ones.

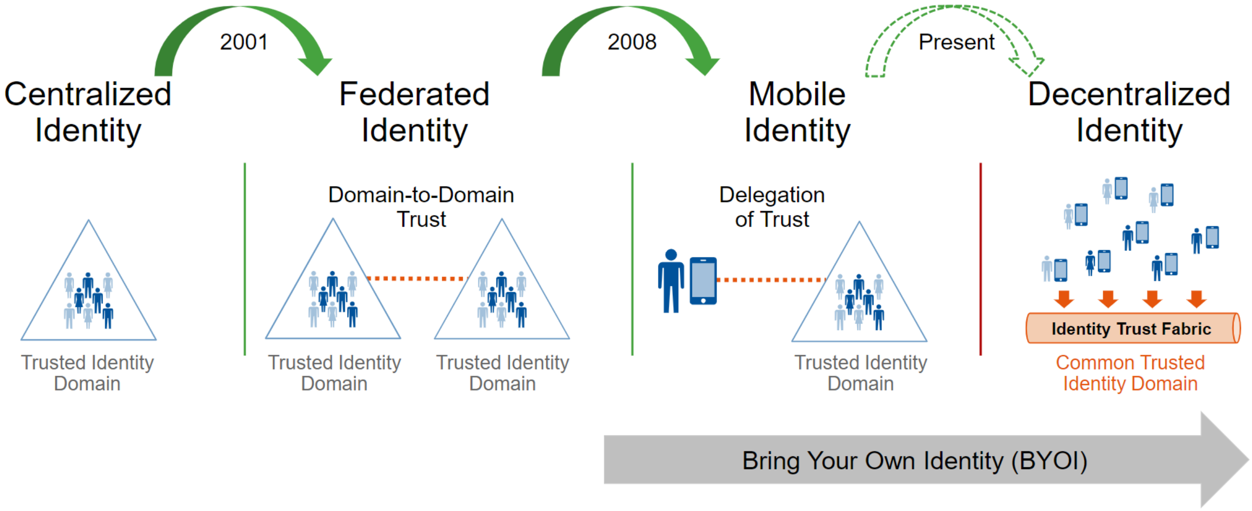


Figure 12: Identity evolution

With trends showing that a decentralized identity model will become a new standard, Monokee is SSI-ready.

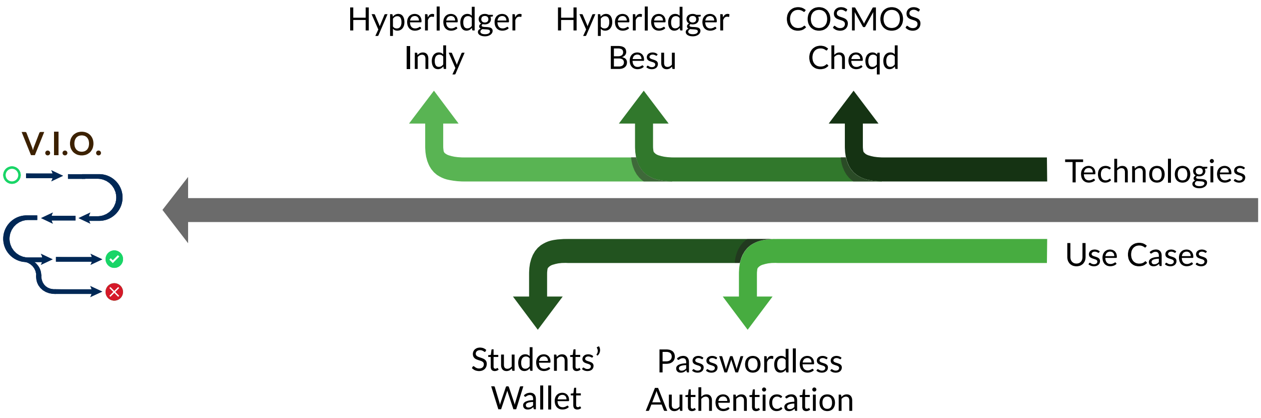


Figure 13: Monokee Decentralised IAM Framework general overview.

Monokee is a trusted partner of multiple SSI vendors and contributes to public projects and communities to streamline the adoption of SSI technologies in enterprise environments.

W3C® DIF TRUST Over IP FOUNDATION

Figure 14: Monokee is dedicating resources to the SSI community.

sovrin cheqd Indicio

Figure 15: Monokee is a trusted partner of the most important SSI vendors worldwide.

A quick overview of SSI:

- *Why should you care about SSI?* According to Gartner, by 2024, it will enable a multi-billion-dollar market. Besides the market opportunities, this revolutionary paradigm will be demanded by the general public and enforced by the public sector.
- *How does it work?* The architecture and technical details may vary depending on the framework. Still, at its core is the concept of trustless trust, which is the idea of building trust chains that replace people, agents, and intermediaries with software and distributed consensus. On top of that, individuals may decide precisely what information to share with which actors, often in the form of Zero-Knowledge Proofs (ZKPs) anonymous credentials.
- *Where can it be used?* Monokee enables seamless integration of distributed technologies in B2B and B2C services that can apply to innovative use cases such as the IoT and smart cities scenarios or generic autonomous projects.
- *When was it introduced?* A few examples of successful SSI introduction are available, primarily the introduction of Sovrin in British Columbia (Canada) in 2019 and the IATA Travel Pass in 2021. The European Union will implement a universal wallet for digital identity as part of the new eIDAS 2.0 agreement in 2024.
- *What do you need?* Surprisingly, with Monokee, you will not need anything else. The whole stack is already integrated to accept, issue, and verify Verifiable Credentials (VCs) with support in the VIO for Hyperledger Indy and generic W3C VCs.

Technologies for the Self-Sovereign Identity (SSI)

Monokee is natively integrated with all major technologies, such as Hyperledger Indy and Besu, but also generic W3C Verifiable Credentials.

Monokee's distributed agents can issue credentials for commercial networks such as Sovrin, Indicio, and Cheqd, but also private networks compatible with Hyperledger Indy and Hyperledger Besu.

Monokee natively supports the issue and verification of the recommended W3C Verifiable Credentials data model.

For mobile users, Monokee has developed a customized wallet based on Hyperledger Aries, while also supporting all compatible third-party wallets. For desktop users, Monokee supports Metamask-based wallets.

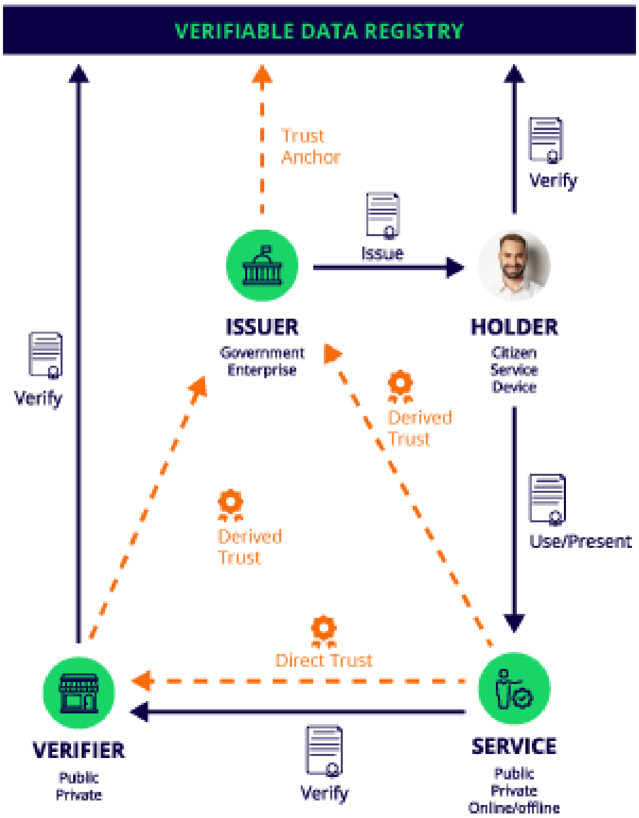


Figure 16: Generic overview of Hybrid-SSI technologies for integrated services

Infrastructure and Modularity

Monokee's infrastructure is designed to be:

- *Modular and customizable*:
  - White label support.
  - Partner extensions.
  - Enable only the required services.
  - Installation in the cloud or on-premises.
  - Support for workforce identities and customer identities.
- *CI/CD driven*:
  - Containerized codebase and services
  - Specific module version pinning
  - Modules hot swap
- *Scalable and secure*:
  - Isolated microservices
  - Load balancing reverse proxy
  - Individual HA for modules
  - The data layer in a separate cluster
  - Encryption by default (with modern AES-256, TLS 1.3 supported)

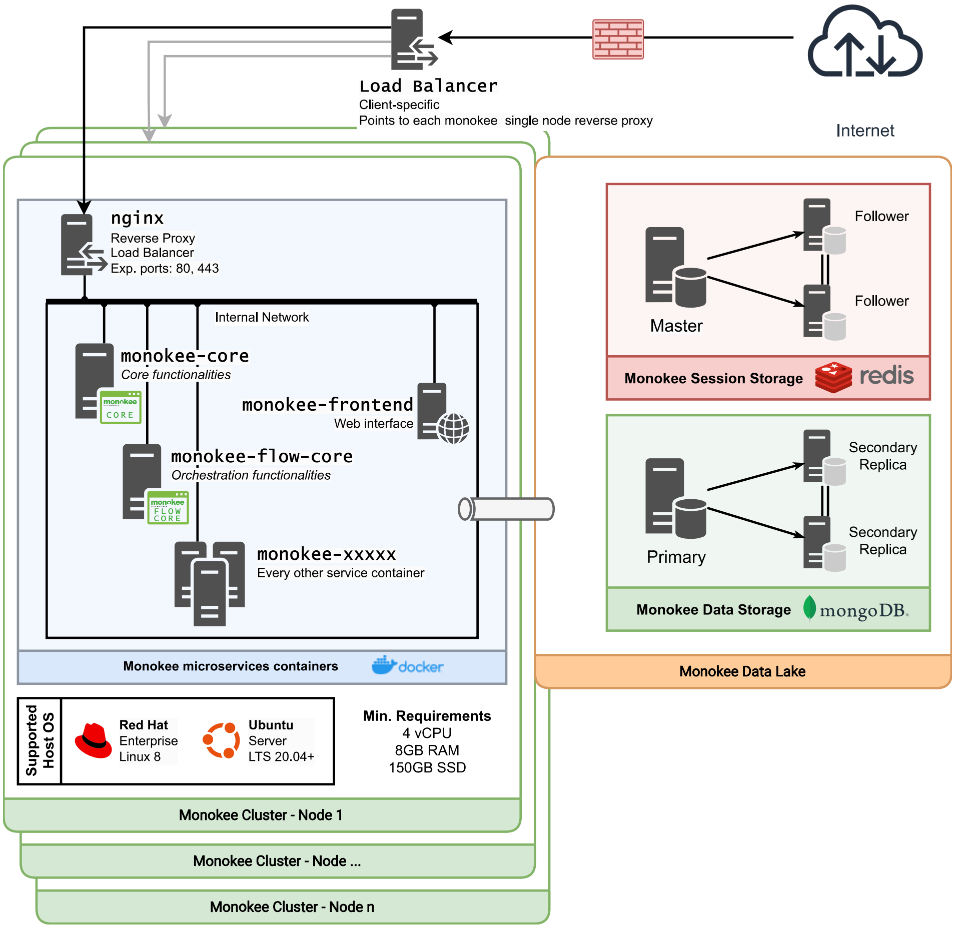


Figure 17: Monokee infrastructure

Microservice Architecture

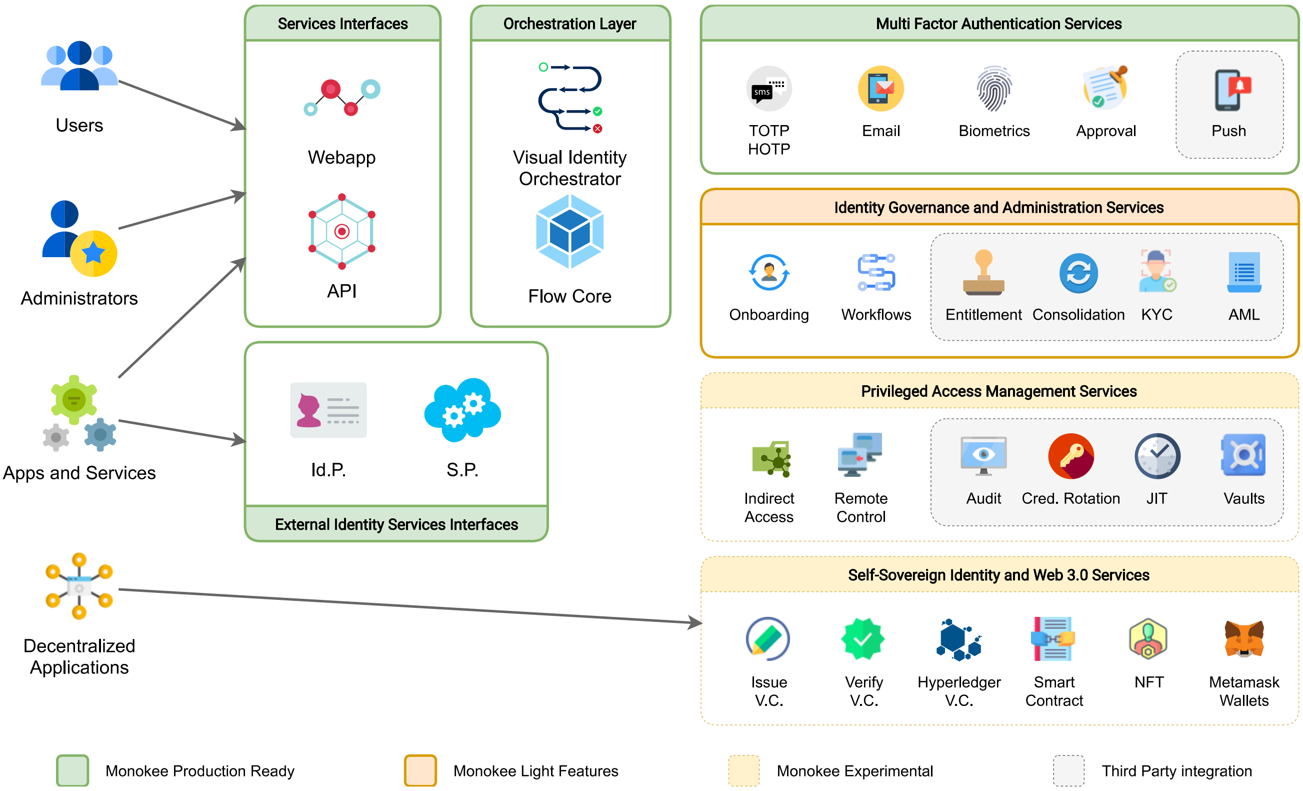


Figure 18: Monokee microservice architecture.

Standalone vs Toolchain mode

Given the modular nature of Monokee, it can be integrated as a standalone solution that covers all the requirements of small to medium organizations or in a toolchain mode where it delegates other aspects of identity management to dedicated third-party tools.

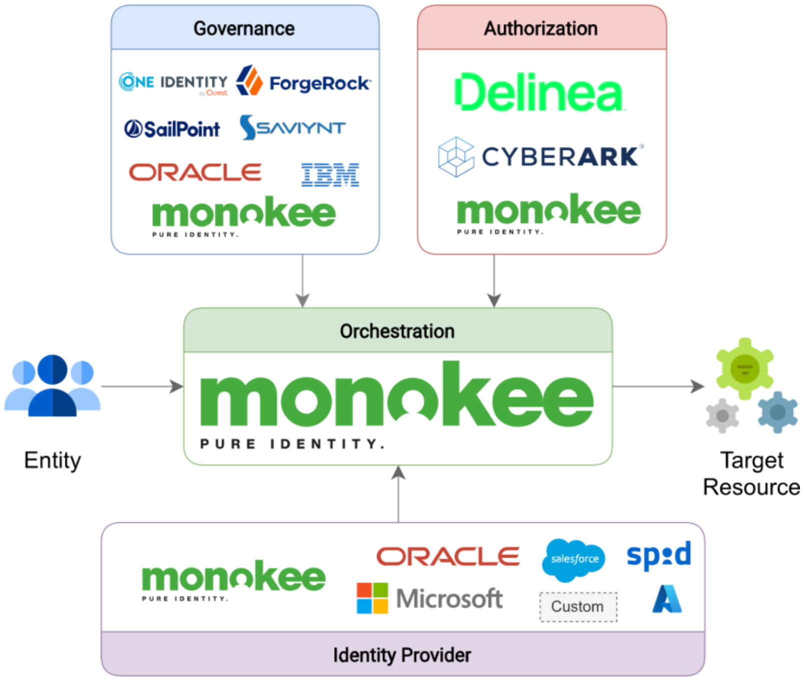
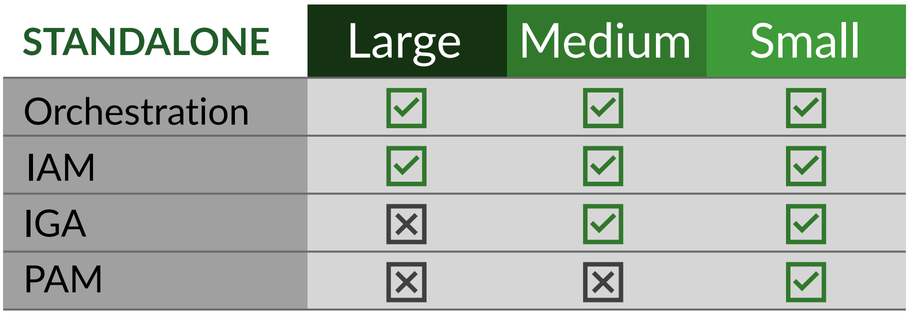


Figure 19: Monokee modularity

Either way, Monokee can be installed in-cloud or on-premises.

On the one hand, in the standalone mode, the light IGA features described in the previous section (Identity Governance and Administration (IGA)) usually cover all the requirements for Small and Medium Enterprises (SMEs). For smaller organizations, the audit and Zero-Trust protection of the network infrastructure offered by Privileged Access Management (PAM) are generally enough to cover the needs.

With Monokee as a standalone solution, SMEs can cover all the requirements without needing external licensing and skilled personnel.



STANDALONE	Large	Medium	Small
Orchestration	☑	☑	☑
IAM	☑	☑	☑
IGA	☒	☑	☑
PAM	☒	☒	☑

Figure 20: Monokee coverage for SMEs

On the other hand, in the toolchain mode, Monokee orchestrates all modules and third-party components, providing a unique location for administrators to manage user identities and application workflows. With this solution, Monokee integrates with third-party solutions for IGA, PAM, and IDM, and it is ideal for large enterprises and custom scenarios.

Roadmap

- *2023 – Identity Governance and Administration, Identity Management*
  - Entitlements and entitlements certifications
  - Automatic Identity Consolidation
  - Governance Workflows
  - Multi-domain and Trust Relationships management
- *2023 – Self-Sovereign Identity and WEB 3.0*
  - Anonymous Credentials and Selective Disclosure
  - Full interoperability W3C VC and did:monokee
  - eIDAS 2.0 EU Wallets native integration
- *2023 – Additional Security Features*
  - Extended cryptographic support (Searchable Encryption, ZKP)
  - Behavioural biometrics and user profiling
- *2024 – Privileged Access Management and Zero-Trust*
  - Visibility and Analytics, including AI/ML
  - Privileged Session Monitoring and Tracking
  - Application Vaults and Credentials Rotations

Innovation and technology coverage

Since the beginning, Monokee pioneered most ground-breaking identity technologies.

In 2020 the European Commission granted Monokee the Seal of Excellence in the area of the Open Disruptive Innovation Scheme.

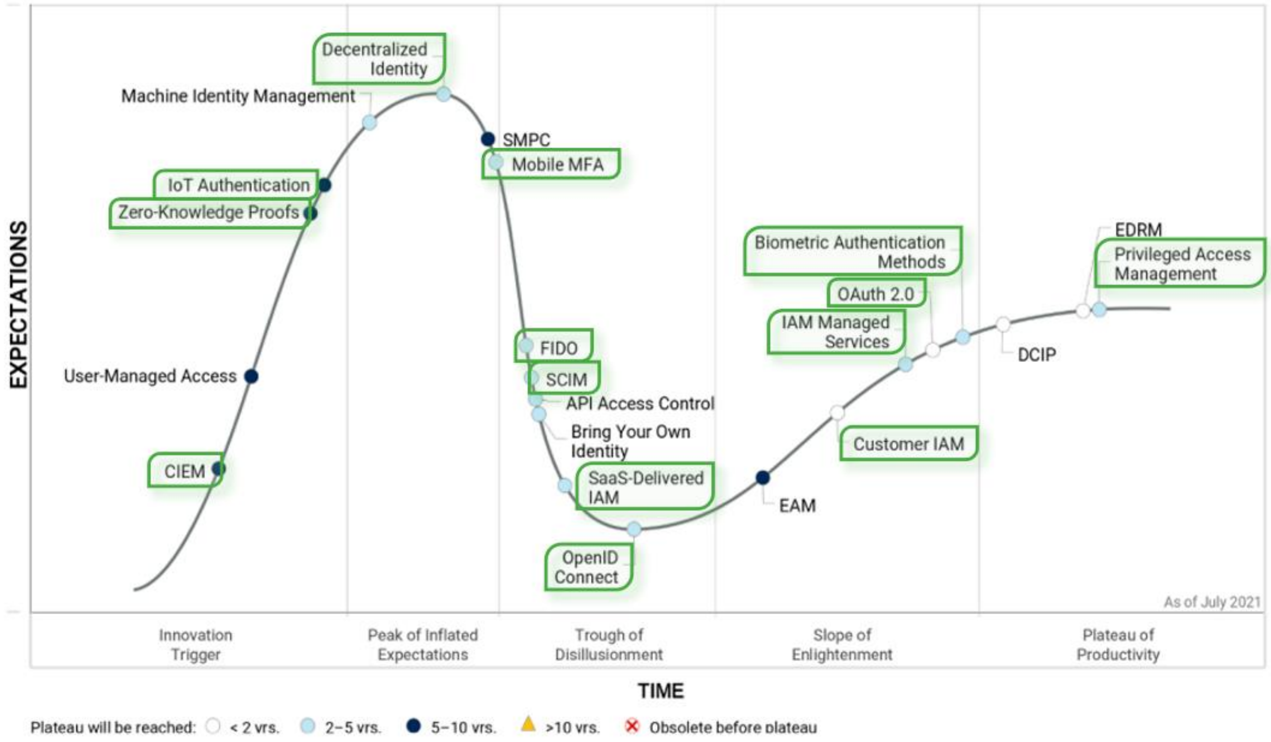


Figure 21: Technology coverage compared to Gartner Identity Hype Cycle 2021

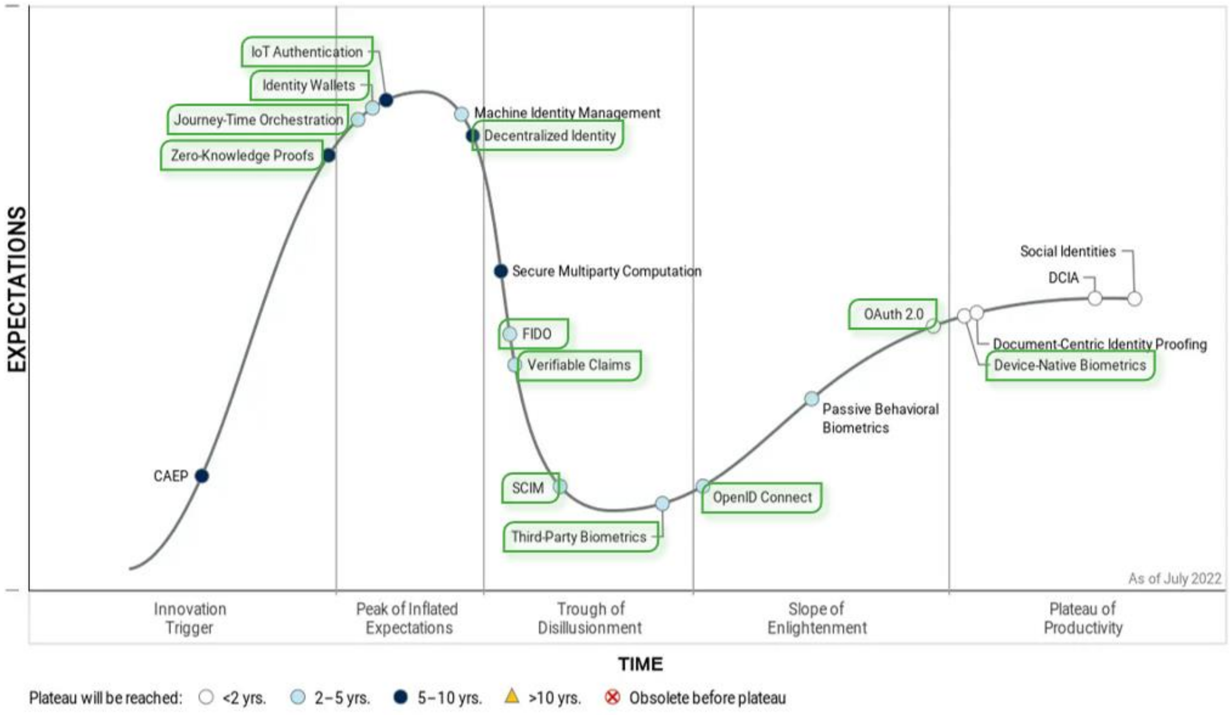


Figure 22: Technology coverage compared to Gartner Identity Hype Cycle 2022.