IAM

AIRLOCK IAM

Access for all users. Seamlessly.

Airlock IAM is generally used in combination with Airlock WAF and Airlock API gateway within the Airlock Secure Access Hub. Airlock IAM's role is to manage and authenticate users and to forward the relevant identity information to the desired application in an appropriate form.

Customer IAM (cIAM)

Unlike workforce IAM systems, cIAM systems, such as Airlock IAM, focus on managing external users accessing in-house systems. cIAM systems are designed for simple scalability and large numbers of users. They also provide a seamless user experience, with optimised, integrated user interfaces for on-boarding and self-services. Airlock IAM's capacity for handling social identities (BYOI) and a high degree of flexibility in the authentication process (adaptive authentication) are two of its greatest strengths.

Strong authentication, broad selection

Strong authentication with two factors, also known as multi-factor authentication or MFA, is often used to ensure that a login is not compromised by the vulnerabilities of any single authentication method.

Flexible combination options are especially important here and Airlock IAM is compatible with a range of solutions, including use with a password, Mobile TAN (mTAN), a Matrix card, email OTP, Kobil SecOVID, OneSpan DIGIPASS, Swisscom Mobile ID (mobile signature services), client certificates such as X.509 or SwissID, as well as CRONTO Visual Transaction Signing from OneSpan, FUTURAE Authentication Suite and many more.

Adaptive authentication

Airlock IAM can dynamically manage user access in a range of ways, striking the perfect balance between security and user-friendliness for all requirements. In particular, it is possible to consider a user's access history as well as the real-time circumstances of the access attempt, for example, from the workplace, home or on the road.

Supported concepts include:

- RBAC/ABAC (role/attribute-based access)
- Risk-based authentication
- Step-up and step-down authentication
- Re-authentication and time-out functions
- Complex access policies via rules and logical operators

Single sign-on (SSO)

The Secure Access Hub decouples the individual accesses from the applications and can, therefore, act as a smart identity switch. Depending on where an access attempt is being forwarded to, the identity of the authenticated user can be represented differently. This enables transparent, single sign-on that combines high levels of security with high user acceptance.

Airlock IAM supports a range of SSO standards and formats, including SAML 2.0 assertions, Kerberos tickets, OAuth 2.0 tokens, OpenID Connect 1.0 tickets, HTTP headers, URL tickets, and others.

Social registration and BYOI

Users want to register and log in quickly and easily, re-using existing identities to avoid the need to set up yet another password. If users bring their identities with them for external access, this is called Bring Your Own Identity. The alternative to a clutter of passwords are the standards OAuth 2.0 and OpenID Connect 1.0.

These allow the re-use of user identities and give users control. Should you not wish to rely entirely on an external identity provider, such as Facebook, Airlock IAM can add a second factor to these identities to enable strong authentication.

Comprehensive user self-service options

Setting up user accounts and registration processes typically elicit a lot of questions from users. Targeted user guidance and an optimised user experience are, therefore, crucial if helpdesks are to avoid being swamped with calls.

Airlock IAM provides dozens of optimised, integrated UIs for registration, onboarding and self-services. These include kiosk and portal functions for managing the user's own data, independent registration, also available via social media channels, and management of relevant accounts and tokens, including migration workflows. The integrated consent-management system also makes it possible to meet the General Data Protection Regulation (GDPR) requirements for connected applications, quickly and easily.

Deployment

Docker image, self-contained application

Features:

- **User authentication**
  - Password authentication
  - Wide spectrum of authentication methods for strong authentication
  - X.509 client certificate
  - Adaptive and risk-based
  - «Remember Me»
  - RADIUS server
  - Workflow-based
- **Request authentification**
  - Authentification of REST calls
  - JWT, Basic Auth, Client certificate
- **User directories:**
  Databases, LDAP, MSAD
- **User-, token- and role administration incl. helpdesk-tool**
- **User self-services**
  - Password-reset
  - Registration of second factor
  - Administration of second factor
  - Kiosk- and portal functions for user's own user data
- **Single sign-on (SSO)**
  - Large range of supported protocols
- **Login REST API**
- **Admin REST API**
- **SAML 2.0 IdP and SP**
- **OAuth 2.0 and OpenID Connect 1.0**
  - As authorisation server / OP
  - As client / RP
  - Authorisation code flow, implicit flow, client credentials flow
  - Dynamic client registration, discovery
  - Various other functions
- **Social registration and social account linking**
- **GDPR consent enforcement**
- **Multitenancy**
- **Highly scalable**
- **Security at bank level**
- **Individually extendable**