Integrated Authentication System: Secfense Suite + Thales CMS + YubiKey

Solution Overview

The combination of three complementary components Secfense Suite, Thales Certificate Management System, and YubiKey enables the creation of a comprehensive and flexible user authentication architecture tailored to diverse technical scenarios and security requirements across the organization.

1. Secfense Suite

Secfense provides an intermediary layer between the user and the application, enabling:

- Deployment of FIDO-based Multi-Factor Authentication (MFA) for any web application without modifying application code, even in legacy or unsupported systems.
- Integration with identity providers (IdPs) using SAML and OpenID Connect standards, allowing passwordless (passkey-based) login to:
    - SaaS platforms (e.g., HubSpot, WorkForce),
    - VPNs,
    - applications supporting identity federation.

2. Thales Certificate Management System (CMS)

Thales CMS allows for:

- Centralized lifecycle management of X.509 certificates used in PKI environments,
- Automation of certificate issuance, renewal, and revocation,
- Integration with operating systems (e.g., Windows) and solutions supporting certificate-based authentication (e.g., RDP login, desktop applications, VPN).

3. YubiKey Hardware Tokens

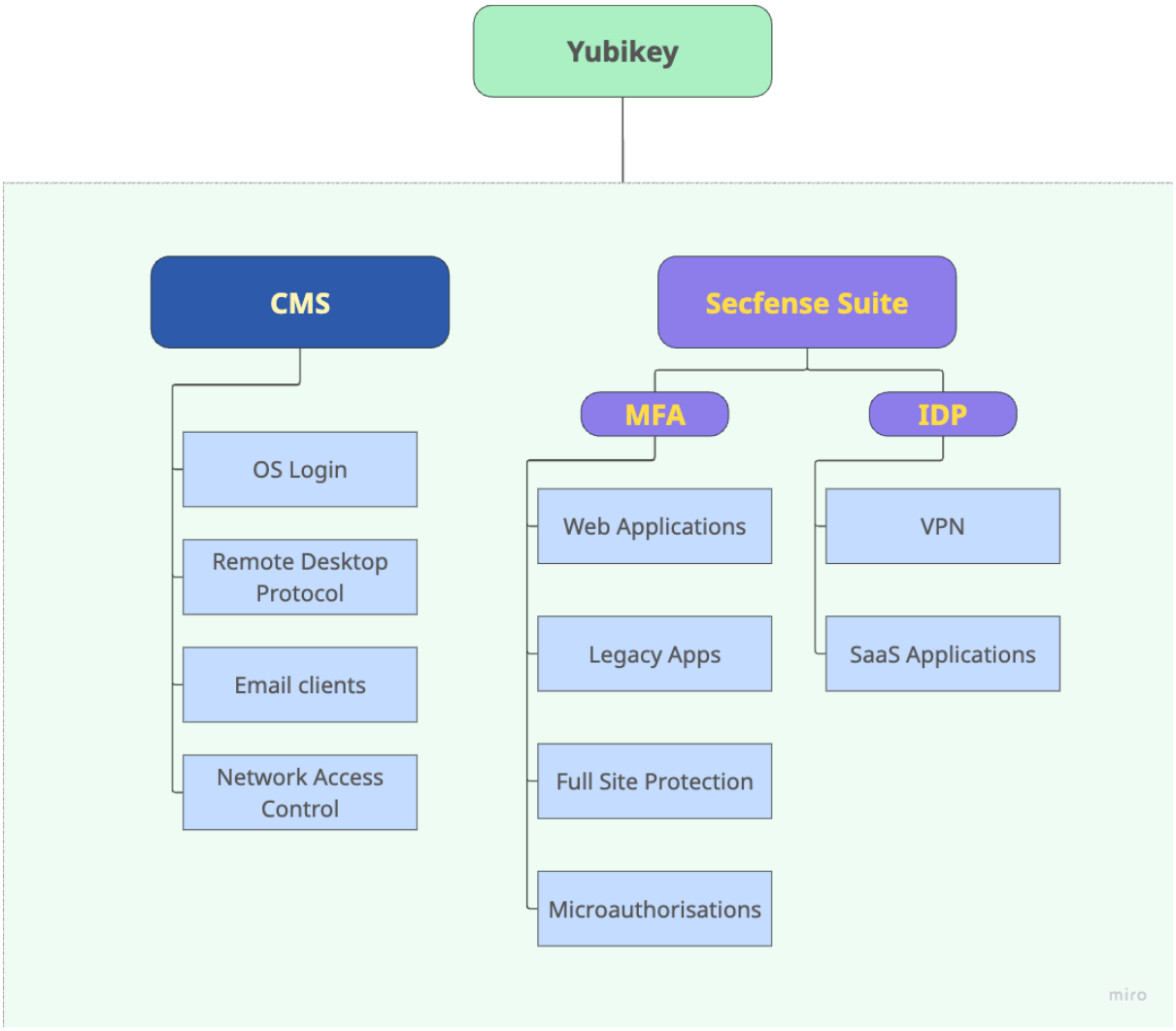
YubiKey devices from Yubico serve a dual purpose:

- **FIDO2/WebAuthn authenticator** - enabling passwordless login (passkeys) in line with current FIDO Alliance standards,
- **Client certificate carrier** - supporting PKI-based authentication (e.g., operating system logins, VPN, and network service access).

Key Benefits of the Integration

Flexibility - full coverage of authentication scenarios: from modern web applications to legacy, business-critical systems.
Security enhancement - passwordless user workflows, strong identity assurance using certificates and hardware tokens.
Fast deployment - MFA and identity federation can be added without code changes, thanks to Secfense's unique reverse proxy approach.
Regulatory compliance - alignment with GDPR, NIS2, DORA, and PSD2 through strong, phishing-resistant digital identity mechanisms.

Use Cases
Applicable across industries such as banking, public administration, critical infrastructure, healthcare, energy, and manufacturing.


Yubikey
CMS
OS Login
Remote Desktop Protocol
Email clients
Network Access Control
Secfense Suite
MFA
IDP
Web Applications
Legacy Apps
Full Site Protection
Microauthorisations
VPN
SaaS Applications
miro