

AMFA — AMITRONIC MFA

AMITRONIC MFA Platform · AMFA-900-HA

W OFERCIE

AMFA to platforma uwierzytelniania wieloskładnikowego, którą budujemy w Polsce, dla organizacji, które muszą udowodnić kontrolę dostępu: urzędów, jednostek samorządu, szpitali i firm przetwarzających dane wrażliwe. Spina logowanie do systemu Windows, aplikacji webowych i serwerów, tak aby użytkownik potwierdzał tożsamość jednym spójnym mechanizmem — a administrator miał jedno miejsce do zarządzania polityką i pełny ślad audytowy.

100%

Ruchu administracyjnego pod MFA

0

Zależności od chmury zewnętrznej

2+

Węzły klastra — minimum

WDROŻENIE

W sieci organizacji, bez chmury

TOŻSAMOŚĆ

Active Directory przez LDAPS

DOSTĘPNOŚĆ

Klaster od 2 węzłów w górę

LICENCJA

Bezterminowa + 12 mies. aktualizacji

Zastosowanie i wartość dla organizacji

Bez chmury i bez wycieku tożsamości

Cała infrastruktura działa w sieci organizacji. Dane uwierzytelnienia, hasła i tokeny nie opuszczają jej środowiska.

Jeden mechanizm dla wszystkich systemów

Windows, aplikacje webowe oraz serwery Linux i SSH — jedna polityka, jedno miejsce obsługi i jeden rejestr zdarzeń.

Wysoka dostępność w standardzie

Model AMFA-900-HA pracuje w klastrze co najmniej dwuwęzłowym z klastrową bazą danych; liczbę węzłów zwiększa się wraz z obciążeniem, a awaria jednego nie przerywa logowania.

Ślad audytowy zamiast samego alertu

Każde uwierzytelnienie, odmowa i zmiana polityki trafia do rejestru — audyt odpowiada na pytanie „kto, kiedy i jak się zalogował”.

Typowe zastosowania

Logowanie do Windows w domenie

Sytuacja: użytkownicy potwierdzają tożsamość wyłącznie hasłem domenowym, hasła bywają współdzielone, a część komputerów pracuje poza siecią organizacji. **Rozwiązanie:** własny dostawca poświadczeń prowadzi hasło i drugi składnik na jednym ekranie logowania; klucz FIDO2 działa także bez połączenia z serwerem, a stan konta (wygasłe, wyłączone, wymagana zmiana hasła) rozstrzyga się w tym samym kroku.

Aplikacje webowe, których nie da się zmienić

Sytuacja: aplikacje wewnętrzne i serwisy (m.in. Joomla, WordPress) nie mają MFA, a ich modyfikacja jest kosztowna lub niemożliwa. **Rozwiązanie:** brama uwierzytelniająca przed aplikacją dokłada drugi składnik bez zmian w kodzie; kolejne systemy dołączają przez Keycloak (OIDC/SAML).

Dostęp administracyjny do serwerów

Sytuacja: SSH i konta administracyjne stoją poza jednolitą polityką i poza wspólnym rejestrem. **Rozwiązanie:** moduł PAM obejmuje logowanie i sesję SSH, polityki działają per grupa i aplikacja, a zdarzenia trafiają do jednego rejestru audytowego.

Przebieg uwierzytelnienia

KROK 01

Nazwa użytkownika i hasło domenowe weryfikowane w Active Directory przez LDAPS — platforma nie przechowuje haseł; stan konta rozstrzyga się w tym samym kroku. Gdy polityka na to pozwala, hasło można pominąć i zalogować się samym kluczem FIDO2/passkey.

KROK 02

Gdy katalog wymaga zmiany hasła, Windows prowadzi jej formularz na ekranie logowania — bez pomijania drugiego składnika.

KROK 03

Potwierdzenie czynnikiem: klucz FIDO2/WebAuthn (z PIN-em lub bez), kod TOTP/HOTP albo kod odzyskiwania. W trybie offline klucz jest weryfikowany na stacji — logowanie działa bez połączenia z serwerem.

KROK 04

Ustanowienie sesji, powiązanie z urządzeniem i wpis zdarzenia do rejestru audytu.

Możliwości platformy

Metody potwierdzania tożsamości

Kilka czynników obok siebie — dobieranych polityką per użytkownik, grupa i aplikacja.

- Hasło z Active Directory (uwierzytelnianie przez LDAPS)
- Kody jednorazowe TOTP (aplikacja mobilna, token sprzętowy)
- Tokeny HOTP — walidacja w silniku MFA oraz lokalnie na stacji
- FIDO2 / WebAuthn — klucze sprzętowe i biometria platformy, z PIN-em lub bez
- Logowanie offline kluczem FIDO2 — gdy stacja nie ma łączności z serwerem
- Jednorazowe kody odzyskiwania dla sytuacji awaryjnej
- Zaufane przeglądarki z czasem życia i możliwością odwołania

Logowanie do Windows i stan konta

Ekran logowania Windows prowadzi całą procedurę — łącznie z tym, co dyktuje katalog.

- Własny dostawca poświadczeń: nazwa użytkownika, hasło domenowe i drugi składnik w jednym oknie
- Wygasłe i wyłączone konto rozstrzygane od razu, z czytelnym komunikatem na ekranie logowania
- Wymuszona zmiana hasła przeprowadzana na ekranie logowania, bez omijania drugiego składnika
- Wykluczenia z MFA: konta, grupy domenowe i kontrolery domeny (także po identyfikatorze SID)
- Filtr kont obsługiwanych przez dostawcę (lista dozwolonych i wykluczonych)
- Obsługa bez ingerencji w system: instalator nie nadpisuje ustawień wdrożeniowych

Integracje i zasięg

MFA tam, gdzie użytkownik realnie pracuje — nie tylko w jednej aplikacji.

- Logowanie do Windows (Credential Provider, domena AD)
- Aplikacje webowe za bramą uwierzytelniającą (m.in. Joomla, WordPress)
- Keycloak jako dostawca tożsamości — OIDC/SAML dla kolejnych systemów
- Linux: moduł PAM dla logowania i sesji SSH
- Źródło tożsamości: Active Directory przez LDAPS — AMFA nie tworzy drugiej bazy użytkowników

Polityka i administracja

Jedna konsola do polityki, sesji, aplikacji i audytu — każde pole z realnego źródła.

- Polityki per użytkownik, grupa i aplikacja (łańcuch hasła i czynników, ważność sesji)
- Sesje aktywne, unieważnione i zaufane przeglądarki — z odwoływaniem dostępu
- Polityka MFA i jednorazowe kody awaryjne wydawane z panelu
- Rejestry: zdarzenia uwierzytelniania, zmiany administracyjne, wysyłki powiadomień
- Powiadomienia o zdarzeniach: e-mail/SMTP i kanały webhook
- Eksport zdarzeń do syslog (UDP, TCP, TLS) z rejestrem wysyłek
- Rejestr aplikacji i tras — ten sam, po którym idzie routing

Wysoka dostępność i eksploatacja

Architektura projektowana pod utrzymanie, nie pod demo.

- Dwa węzły bramy za adresem wirtualnym (VIP)
- Klaster bazy danych z automatycznym przełączaniem i jawną listą adresów
- Konfiguracja deklaratywna wersjonowana razem z produktem
- Health checks i gotowość komponentów widoczne w panelu
- Ścieżka aktualizacji z kopią poprzedniej wersji i możliwością wycofania

W skrócie

- Bez chmury zewnętrznej — dane uwierzytelnienia nie opuszczają organizacji
- Active Directory jako jedyne źródło tożsamości
- Windows, Linux i aplikacje webowe w jednym mechanizmie
- Klaster od dwóch węzłów, aktualizacja z możliwością wycofania

Matryca możliwości

LOGOWANIE WINDOWS	Własny dostawca poświadczeń: hasło domenowe + drugi składnik; tryb offline kluczem FIDO2
SERWERY LINUX / SSH	Moduł PAM dla logowania i sesji; polityki per grupa i aplikacja
APLIKACJE WEBOWE	Brama uwierzytelniająca przed aplikacją — bez zmian w kodzie (Joomla, WordPress)
SSO DLA KOLEJNYCH SYSTEMÓW	Keycloak jako dostawca tożsamości: OIDC i SAML
CZYNNIKI	FIDO2/WebAuthn (klucz, passkey, biometria platformy), TOTP, HOTP, kody odzyskiwania
ŹRÓDŁO TOŻSAMOŚCI	Active Directory przez LDAPS — bez drugiej bazy użytkowników

AUDYT I INTEGRACJE ZDARZEŃ	Rejestr uwierzytelnień i zmian, eksport syslog (UDP/TCP/TLS), powiadomienia e-mail i webhook
WYSOKA DOSTĘPNOŚĆ	Klaster od dwóch węzłów, adres wirtualny (VIP), klaster bazy danych
ADMINISTRACJA	Jedna konsola: polityki, sesje, aplikacje, zaufane przeglądarki

Architektura i warstwy systemu

KLIENCI I SYSTEMY CHRONIONE	Windows (logowanie) (Credential Provider) · Przeglądarka (aplikacje webowe) · Linux / SSH (moduł PAM) · Aplikacje SSO (OIDC / SAML)
AMITRONIC WEB MFA GATEWAY	Brama uwierzytelniająca (własny komponent AMITRONIC) · Warstwa HTTP / TLS (węzeł 1 i 2 za VIP) · Memoryz sesji i wyzwań (kontrola stanu logowania)
SILNIKI I KATALOGI	Silnik MFA (polityki, czynniki, tokeny) · Keycloak (dostawca tożsamości) · Active Directory (katalog użytkowników (LDAPS))
DANE I CIĄGŁOŚĆ	Baza konfiguracji i sesji (klaster HA) · Ścieżka kopii zapasowych (odtworzenie do punktu w czasie) · Rejestry audytowe (retention wg polityki)

Założenia projektowe: Adres wirtualny (VIP) prowadzi ruch do aktywnego węzła bramy; drugi węzeł przejmuje obsługę przy awarii. Baza danych pracuje w klastrze z automatycznym wyborem lidera — brak pojedynczego punktu awarii na warstwie danych. Katalog Active Directory pozostaje źródłem tożsamości — AMFA nie tworzy drugiej bazy użytkowników.

Wariant i licencja

AMFA-900-HA Konfiguracja klastrowa z wysoką dostępnością Organizacje od kilkudziesięciu użytkowników, w tym jednostki z wymogami ciągłości działania - Dwa węzły bramy za adresem wirtualnym (VIP) - Klaster bazy danych z automatycznym przełączaniem - FIDO2/WebAuthn, TOTP, HOTP i kody odzyskiwania - MFA dla Windows, Linux/SSH, aplikacji webowych i SSO	Licencja i utrzymanie Licencja — Bezterminowa — bez limitu czasu i bez opłat od liczby użytkowników Aktualizacje w cenie — 12 miesięcy od zakupu: nowe wersje, poprawki, nowe integracje i czynniki Po 12 miesiącach — Dostęp do aktualizacji utrzymuje pakiet odnowienia — z opcją wsparcia Wsparcie — W pakiecie odnowienia albo jako odrębna umowa wsparcia Pakiety odnowienia: Pakiet aktualizacji · Pakiet aktualizacji i wsparcia
---	--

Wymagania techniczne

ŚRODOWISKO	Serwery wirtualne lub fizyczne w sieci organizacji (Linux)
KATALOG	Active Directory z dostępem LDAPS lub katalog lokalny
BAZA DANYCH	PostgreSQL (w konfiguracji HA — klaster z automatycznym przełączaniem)
SIEĆ	Adres wirtualny dla warstwy bramy, ruch TLS na 443
STACJE KLIENCKIE	Windows 10/11 (logowanie domenowe), przeglądarki aktualne
KLUCZE FIDO2	Dowolne klucze zgodne z WebAuthn lub biometria platformy

Wsparcie w wymaganiach zgodności

AMFA wspiera realizację wymagań w zakresie silnego uwierzytelniania i kontroli dostępu, które pojawiają się w audytach i regulacjach. Zakres zastosowania zależy od konfiguracji polityk w danej organizacji.

- **ISO/IEC 27001** — Kontrola dostępu i uwierzytelnianie: polityki, rejestry zdarzeń i przegląd uprawnień.
- **NIS2 / KSC** — Wymogi dotyczące silnego uwierzytelniania i zarządzania dostępem do systemów krytycznych.
- **RODO** — Przetwarzanie danych uwierzytelniających wyłącznie w infrastrukturze organizacji — bez transferu do chmury.
- **Zamówienia publiczne** — Dokumentacja techniczna i zakres prac przygotowane pod opis przedmiotu zamówienia.

AMFA nie jest certyfikatem ani deklaracją zgodności. Zgodność potwierdza organizacja w ramach własnego systemu zarządzania bezpieczeństwem; AMITRONIC dostarcza narzędzia i dokumentację wspierające ten proces.

Plan rozwoju produktu

- Potwierdzenie mobilne (push) — w przygotowaniu
- Rozszerzone raporty zgodności w panelu — w przygotowaniu
- Dodatkowe konektory aplikacji — planowane

AMITRONIC Amadeusz Kusz

Gaj 32, 13-334 Łąkorz · NIP 8771483213 · REGON 387488898
795 665 160 · biuro@amitronic.pl

Pilotaż i wdrożenie

Uruchamiamy pilotaż na wybranej grupie kont
i jednej aplikacji, bez wpływu na pozostałych użytkowników.
<https://support.amitronic.pl>

Dokument ma charakter informacyjny i nie stanowi oferty w rozumieniu art. 66 § 1 Kodeksu cywilnego. Nazwy produktów i znaki towarowe osób trzecich należą do ich właścicieli. Zastrzeżenia dotyczące zgodności odnoszą się do wymagań wskazanych w dokumencie; ostateczny zakres potwierdza analiza środowiska zamawiającego.