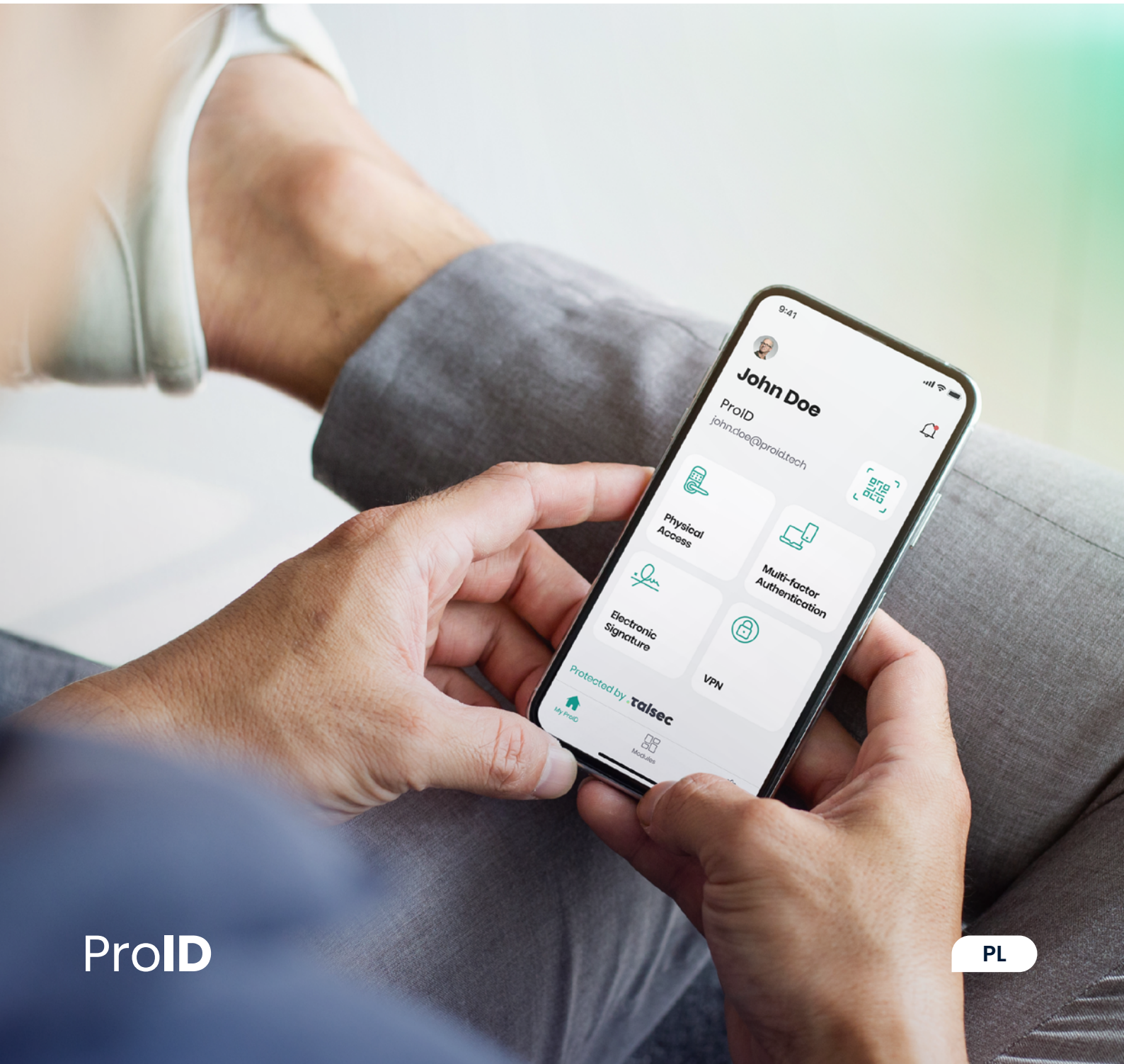
ProID

Biała księga
tożsamości pracowników



ProID

PL

ProID

Bezpieczna tożsamość cyfrowa dla pracowników i organizacji

Tożsamość cyfrowa jest dziś wszędzie, ułatwiając nam codzienne życie publiczne i zawodowe. Ale jak zapewnić, że jest ona naprawdę bezpieczna, a jednocześnie przyjazna dla użytkownika?

W ciągu ostatnich kilku lat liczba cyberataków na organizacje wszystkich typów i rozmiarów dramatycznie wzrosła. Ataki te powodują długotrwałe przerwy w świadczeniu usług i ogromne straty finansowe. Wraz z postępującą cyfryzacją procesów biznesowych i rozwojem sytuacji międzynarodowej można oczekiwać, że cyberzagrożenia będą nadal rosły.

To smutna prawda, że 80% udanych cyberataków jest spowodowanych naruszeniem lub kradzieżą danych logowania samych pracowników lub uprzywilejowanych kont administratorów, którzy mają dostęp do wszystkich systemów i interfejsów. Jednak to samo niebezpieczeństwo dotyczy dostępu do interfejsów elementów technicznych (serwerów, infrastruktury OT, inteligentnych liczników itp.).

Ale bezpieczna tożsamość cyfrowa nie musi już straszyć. Rozwiązaniem nie jest stosowanie jeszcze dłuższych, bardziej złożonych i praktycznie niemożliwych do zapamiętania haseł. Jest na to inny sposób. Wygodny, przyjazny dla użytkownika, a jednocześnie tak bezpieczny, jak to tylko możliwe.

Platforma bezpieczeństwa dla przedsiębiorstw ProID

ProID to modułowa platforma do zabezpieczania organizacji skoncentrowana na pracy i tożsamości technicznej, w całości opracowana przez MONET+.

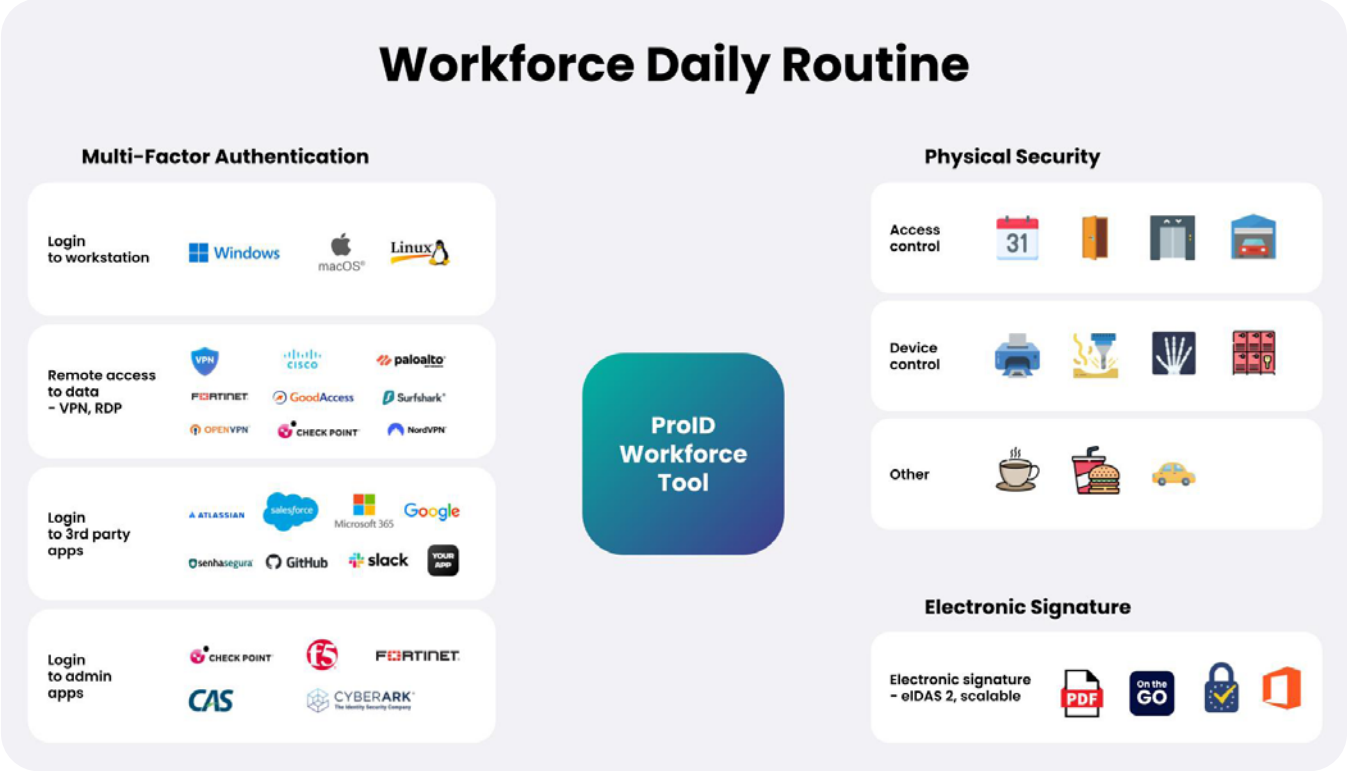
Zapewnia ochronę ponad 170 000 użytkowników w ponad 180 organizacjach z różnych branż - fintech, telekomunikacja, opieka zdrowotna, usługi użyteczności publicznej, produkcja, sektor publiczny i inne.

EIDAS 2 | NIS 2 | ISO 27001 | TISAX | DORA

info@proid.tech | +420 577 110 411 | www.proid.tech

ProID Workforce Bezpieczna tożsamość pracowników

ProID oferuje metody i narzędzia, które nie patrzą na kwestię bezpieczeństwa tylko z punktu widzenia rozwiązania określonej części. Wręcz przeciwnie, dąży do zapewnienia kompleksowego rozwiązania, które łączy wszystkie potrzeby pracownika podczas jego codziennej pracy.



ProID Workforce obejmuje wszystkie 3 podstawowe obszary cyfrowej tożsamości pracownika:

1. **Uwierzytelnianie wieloskładnikowe** - bezpieczne i przyjazne dla użytkownika logowanie do różnych systemów i aplikacji.
2. **Elektroniczne podpisywanie i pieczętowanie dokumentów** cyfrowych do najwyższego poziomu kwalifikacji.
3. **Fizyczna identyfikacja pracowników** za pomocą chipa zbliżeniowego (rozwiązania do drukowania, systemy obecności, dostępu i cateringu itp.)

ProID Workforce tools and management

ProID Workforce oferuje zweryfikowane narzędzia do identyfikacji pracowników, które są w stanie spełnić nawet najbardziej wymagające wymagania i scenariusze klientów:

1. Wielofunkcyjna karta inteligentna ProID i jej różne warianty.
2. Aplikacja mobilna ProID.





ProID Workforce obejmuje modułowe zarządzanie automatyzacją procesów i proste zarządzanie narzędziami ProID.

Wszystkie narzędzia można łączyć w ramach jednej organizacji zgodnie z potrzebami poszczególnych użytkowników, a jednocześnie każdy użytkownik może mieć wiele narzędzi w celu uzyskania najbardziej odpowiedniej kombinacji.

Cała platforma ProID może być dostarczana lokalnie do środowiska klienta lub używana jako usługa (SaaS).

Wielofunkcyjna karta inteligentna ProID

Karty inteligentne to sprawdzony i przetestowany sposób zabezpieczania tożsamości pracownika. W przeszłości były one wykorzystywane głównie do zabezpieczania dostępu do obszarów chronionych. Dodaliśmy do naszego portfolio dodatkowe funkcje, które sprawiają, że są one narzędziem zapewniającym zarówno bezpieczeństwo fizyczne, jak i logiczne.

Najważniejsze cechy:

- Zgodność z FIDO2 - uwierzytelnianie bezhasłowe, również bezdotykowe.
- Bestsellerowe, sprawdzone narzędzie do zapewnienia cyfrowej tożsamości pracownika.
- Bezpieczne przechowywanie kluczy cyfrowych i certyfikatów.
- Działa nawet w trybie offline.
- Certyfikowane narzędzie wymienione na zaufanej liście UE.

Możliwe zastosowania:

- **Karta identyfikacyjna pracownika**
  Spełnia funkcję kart osobistych dzięki możliwości graficznej personalizacji kart.
- **Uwierzytelnianie wieloskładnikowe**
  Narzędzie do weryfikacji MFA w systemach i aplikacjach (MS, Linux, MacOS), VPN, RDP i aplikacjach innych firm.
- **Funkcja zbliżeniowa**
  Karty obsługują większość technologii zbliżeniowych/producentów (Mifare DESfire, HID, Legic itp.) i mogą być podłączone do systemów obecności, rejestrów płatności (np. obiadów) i urządzeń zewnętrznych (drukarek, kołowrotów, wind...).
- **Podpis elektroniczny**
  Karty Chip są wyposażone w certyfikowany chip QSCD i umożliwiają tworzenie kwalifikowanych podpisów elektronicznych zgodnie z obowiązującymi przepisami i regulacjami UE.
- **Tryb offline**
  Nie zależy ona od uwierzytelniania certyfikatem online.

Dostarczamy również powiązane produkty (czytniki kart, drukarki do drukowania itp.) oraz szeroką gamę modułów dla administratorów i administratorów.

Aplikacja mobilna ProID

Telefon komórkowy stał się integralną częścią rutyny pracy większości pracowników. Jest to urządzenie, które mają przy sobie zawsze i wszędzie i są przyzwyczajeni do rozwiązywania na nim coraz większej liczby zadań. Uczyniliśmy z niego nowe narzędzie bezpieczeństwa korporacyjnego.

Nasza aplikacja mobilna ProID jest dostępna zarówno dla systemu Android, jak i iOS i obsługuje dostęp bez hasła przy użyciu danych biometrycznych.

Najważniejsze cechy:

- Bardzo przyjazna dla użytkownika metoda o wysokim poziomie bezpieczeństwa.
- Eliminacja haseł (wsparcie biometryczne).
- Integracja wielu metod (powiadomienia push, generowanie OTP, SMS).
- „Tryb wyspowy“ (scenariusze offline) w przypadku sytuacji kryzysowych.
- Możliwość pełnego wdrożenia lokalnego.
- Obsługuje bezstykową identyfikację użytkownika (Legic, HID, NXP itp.).

Możliwości korzystania z aplikacji ProID Mobile:

- **Uwierzytelnianie wieloskładnikowe**

  Narzędzie do weryfikacji MFA w systemach i aplikacjach, VPN, RDP i aplikacjach innych firm lub aplikacjach niestandardowych.

- **Funkcje zbliżeniowe**

  Umożliwia funkcje zbliżeniowe, takie jak sterowanie kołowrotami i windami, odblokowywanie zamków lub sterowanie urządzeniami zewnętrznymi (dla SDK Legic Connect, HID i Mifare 2Go).

- **Podpis elektroniczny**

  IUmożliwia tworzenie zaawansowanych i kwalifikowanych podpisów elektronicznych bezpośrednio z telefonu komórkowego.

Moduły zarządzania narzędziami ProID

Aby uprościć zarządzanie narzędziami ProID Workforce, oferujemy modułowe zarządzanie dla użytkowników i administratorów organizacji. Centralizuje ono i automatyzuje złożone operacje związane z zarządzaniem narzędziami. W prosty sposób wdraża wymagane procesy i umożliwia łatwą konfigurację wymagań dotyczących zarządzania cyklem życia narzędzi ProID.

Najważniejsze cechy:

- Znaczne przyspieszenie i automatyzacja wszystkich procesów.
- Eliminacja błędów.
- Zapewnienie bezpieczeństwa systemu organizacji.
- Oszczędność kosztów i czasu.
- Intuicyjne sterowanie.

Możliwości wykorzystania modułów ProID:

- **Organizacje pod kontrolą**

  Moduły oferują doskonały przegląd wszystkich narzędzi, użytkowników i certyfikatów w organizacji, niezależnie od jej wielkości.
- **Pokrycie ważnych scenariuszy**

  Wdrażanie użytkowników, przypisywanie narzędzi użytkownika i zarządzanie nimi, zarządzanie kluczami i certyfikatami, drukowanie kart itp. Wszystko to w czasie rzeczywistym i bez skomplikowanych czynności.
- **Część bezpieczeństwa wewnętrznego**

  Moduły stanowią centralną bazę danych oraz kopię zapasową certyfikatów i kluczy na wypadek scenariuszy kryzysowych, w tym możliwość wyszukiwania i rejestrowania.
- **Role użytkowników**

  Moduły są przeznaczone dla administratorów i administratorów, a także dla działów HR (wydawanie lub drukowanie kart inteligentnych) i użytkowników końcowych (automatyczne odnawianie wygasających certyfikatów, przechowywanie QPIN itp.)
- **W chmurze lub lokalnie**

  Moduły mogą być instalowane zarówno w siedzibie klienta na jego serwerach i stacjach roboczych, jak i obsługiwane jako usługa (SaaS).

Przegląd przypadków użycia





Identyfikacja wizualna	✓	✗
Logowanie do komputera	✓	✓
Logowanie do VPN	✓	✓
Logowanie do RDP	✓	✓
Logowanie do różnych aplikacji (M365, Gsouite, ...)	✓	✓
Podpis elektroniczny	✓	✓
Kontrola dostępu	✓	✓
Kontrola urządzenia	✓	✓
FIDO2	✓	✗

ProID eSign - System zdalnego kwalifikowanego podpisu elektronicznego

Wraz z cyfryzacją dokumentów i ideą „bez papieru" konieczne jest zapewnienie, że takie dokumenty mają taką samą wagę prawną jak dokumenty drukowane. Jest to możliwe dzięki takim środkom jak kwalifikowany podpis elektroniczny, pieczęć lub znacznik czasu. Jednym z najskuteczniejszych sposobów ich tworzenia przez organizacje jest praca zdalna. Eliminuje to wykorzystanie zasobów z przechowywanym certyfikatem, podpis jest dostępny z dowolnego miejsca, działa również na telefonie komórkowym i pozwala na centralne zarządzanie wszystkimi certyfikatami.

Nasz system Remote Sign łączy wygodę zdalnego podpisywania z maksymalnym bezpieczeństwem. Jest instalowany bezpośrednio w organizacji jako „on-premise", wraz ze wszystkimi niezbędnymi komponentami.

Częścią rozwiązania jest nasz własny certyfikowany moduł SAM, który znajduje się na zaufanej liście UE. Służy on do autoryzacji procesu podpisywania.

Dlaczego warto wybrać to rozwiązanie?

- Zapewnia wygodę użytkownika, jest łatwy w użyciu i eliminuje potrzebę fizycznej obecności w oddziale.
- Intuicyjne sterowanie, bez hasła.
- Cyfrowe zarządzanie i tworzenie dokumentów z pełną mocą prawną łatwo i z dowolnego miejsca.
- Niezależność od urządzenia, może być używana na laptopie, tablecie i telefonie komórkowym.
- Certyfikowane rozwiązanie zgodne z eIDAS 2.

Możliwości wykorzystania systemu eSign:

- **Podpis, pieczęć, stempel**
  Kwalifikowany podpis elektroniczny, kwalifikowana pieczęć elektroniczna i znacznik czasu z dowolnego miejsca i urządzenia, w tym smartfonów i tabletów.
- **Integracja z systemami organizacyjnymi**
  Możliwość połączenia z zarządzaniem dokumentacją lub istniejącymi aplikacjami (CRM, ERP, systemy fakturowania i zamawiania itp.).
- **Możliwości biznesowe**
  Sama organizacja może być dostawcą podpisu elektronicznego dla swoich klientów, dostawców lub spółek zależnych.

Systemy zarządzania certyfikatami technologicznymi

Nie tylko ludzie, ale także różne urządzenia i sprzęt techniczny mają już tożsamość cyfrową. Co więcej, liczba takich elementów technologicznych rośnie wykładniczo, podobnie jak związane z nimi zagrożenia bezpieczeństwa.

Infrastruktura OT, serwery, czujniki, systemy pomiarowe, zaawansowane maszyny produkcyjne, sprzęt szpitalny i wiele innych urządzeń komunikuje się z sieciami korporacyjnymi i codziennie odbiera lub wysyła poufne dane. Atak może spowodować upadek całej organizacji i zakłócić jej działanie na wiele dni. Właśnie dlatego rozszerzyliśmy nasze rozwiązanie tożsamości o część, która chroni wrażliwe elementy techniczne.

Dlaczego warto wybrać to rozwiązanie?

- Uniwersalne zastosowanie do zarządzania tożsamościami elementów technicznych w całej organizacji.
- Możliwość powiązania z tożsamością pracownika.
- Wykorzystanie najnowocześniejszych algorytmów kryptograficznych.
- Oparty na technologii infrastruktury klucza publicznego.

Możliwości wykorzystania systemów:

- **Centralny punkt zarządzania**
  Systemy zapewniają centralną lokalizację do bezpiecznego przechowywania materiałów kryptograficznych, wykonywania operacji kryptograficznych i kontrolowania dostępu w oparciu o role użytkowników.
- **Rozwiązanie typu „wszystko w jednym“**
  Systemy są zintegrowane z modułami zarządzania certyfikatami, domeną PKI i urzędem certyfikacji.
- **KMS (system zarządzania kluczami)**
  Umożliwia szyfrowaną komunikację między urządzeniami, serwerami i aplikacjami, import i dystrybucję kluczy kryptograficznych.
- **Zarządzanie cyklem życia certyfikatu (CLM)**
  Skutecznie zarządza cyklem życia certyfikatów technologicznych. Zapewnia krytyczne scenariusze (zautomatyzowane wydawanie, sprawdzanie tożsamości i żądania certyfikatów...), a także procesy wspierające centralne zarządzanie certyfikatami.
- **Support for global protocols**
  The systems work with widely used protocols and ensure their integration into a single interface (ACME, SCEP, EST, Proprietary protocol...).
- **Obsługa protokołów globalnych**
  Systemy współpracują z powszechnie używanymi protokołami i zapewniają ich integrację w ramach jednego interfejsu (ACME, SCEP, EST, zastrzeżony protokół...).

O Monet+

ProID jest produktem firmy Monet+

Tożsamość cyfrowa i płatności elektroniczne.

Zawsze. Gdziekolwiek.

Monet+ jest wiodącą czeską firmą programistyczną z prawie 30-letnim doświadczeniem w zakresie bezpiecznej tożsamości cyfrowej i rozwiązań płatniczych. Niezależnie od tego, czy chodzi o logowanie do systemów korporacyjnych, zarządzanie kontami bankowymi za pośrednictwem aplikacji mobilnych, uwierzytelnianie za pomocą danych biometrycznych, czy zdalne podpisywanie dokumentów, Monet+ zapewnia narzędzia, dzięki którym odbywa się to w bezpieczny sposób. Nasze rozwiązania zasilają i zabezpieczają również codzienne transakcje, pozwalając użytkownikom płacić kartami bankowymi w sklepach, kupować bilety transportu publicznego, a nawet z łatwością ładować pojazdy elektryczne.

Obsługując zróżnicowaną gamę 450 klientów publicznych i prywatnych, Monet+ jest wspierany przez zespół ponad 350 oddanych ekspertów. Naszym celem jest zapewnienie, że tożsamości cyfrowe i płatności są bezpieczne, dostępne i niezawodne - zawsze i wszędzie.

Więcej informacji na stronie

www.proid.tech