Poznań, 09.06.2026

Projekt

Systemy automatycznej identyfikacji

Temat projektu

Jak działa moduł karty na kluczu YubiKey

S2Inf1-IP
Wojciech Surdyka 165217

Spis treści

1. Wprowadzenie do technologii YubiKey

Rozdział przedstawia ogólną charakterystykę kluczy YubiKey oraz ich rolę w zwiększaniu bezpieczeństwa procesu uwierzytelniania. Omówiono w nim podstawowe standardy obsługiwane przez urządzenia YubiKey, dostępne rodzaje kluczy oraz zakres dalszej pracy w ramach projektu.

1.1. Sprzętowe klucze bezpieczeństwa

Współczesne systemy informatyczne są coraz częściej narażone na różnego rodzaju zagrożenia cybernetyczne, takie jak phishing, przejmowanie kont użytkowników czy wycieki danych uwierzytelniających. Szczególnie niebezpieczne są ataki phishingowe polegające na podszywaniu się pod zaufane podmioty w celu pozyskania danych logowania użytkownika.

Jednym ze sposobów ograniczenia skuteczności tego typu ataków jest stosowanie uwierzytelniania wieloskładnikowego (MFA – Multi-Factor Authentication). W rozwiązaniach tego typu oprócz hasła wymagany jest dodatkowy składnik potwierdzający tożsamość użytkownika. Coraz większą popularność zdobywają sprzętowe klucze bezpieczeństwa, które pełnią funkcję fizycznego tokena uwierzytelniającego.

Sprzętowe klucze bezpieczeństwa umożliwiają realizację silnego uwierzytelniania przy wykorzystaniu protokołów uwierzytelniania takich jak FIDO2, U2F czy PIV. W przeciwieństwie do kodów SMS lub aplikacji generujących hasła jednorazowe, klucze sprzętowe są odporne na wiele popularnych metod przechwytywania danych uwierzytelniających [1].

1.2. Historia i rozwój YubiKey

YubiKey jest rodziną sprzętowych kluczy bezpieczeństwa opracowaną przez szwedzką firmę Yubico. Urządzenia te zostały zaprojektowane w celu zapewnienia bezpiecznego i wygodnego uwierzytelniania użytkowników zarówno w środowiskach korporacyjnych, jak i zastosowaniach indywidualnych.

W kolejnych latach rozwoju producent rozszerzał funkcjonalność urządzeń o obsługę nowych standardów uwierzytelniania i kryptografii. Współczesne modele YubiKey wspierają między innymi FIDO2, FIDO U2F, OTP, OpenPGP oraz PIV, dzięki czemu jedno urządzenie może realizować wiele różnych funkcji związanych z bezpieczeństwem cyfrowym.

Obecnie klucze YubiKey są wykorzystywane przez przedsiębiorstwa, instytucje publiczne oraz użytkowników indywidualnych na całym świecie. Ich głównym zadaniem jest zwiększenie bezpieczeństwa procesu logowania i ograniczenie ryzyka przejęcia kont użytkowników [1][2].

1.3. Obsługiwane standardy uwierzytelniania

Klucze YubiKey obsługują wiele standardów uwierzytelniania i kryptografii, co pozwala na ich wykorzystanie w różnych środowiskach informatycznych. Do najważniejszych należą FIDO2, FIDO U2F, OTP, OATH, OpenPGP oraz PIV (Personal Identity Verification).

Do najważniejszych standardów należą:

- **FIDO2** - standard uwierzytelniania bezhasłowego, wykorzystujący kryptografię asymetryczną,

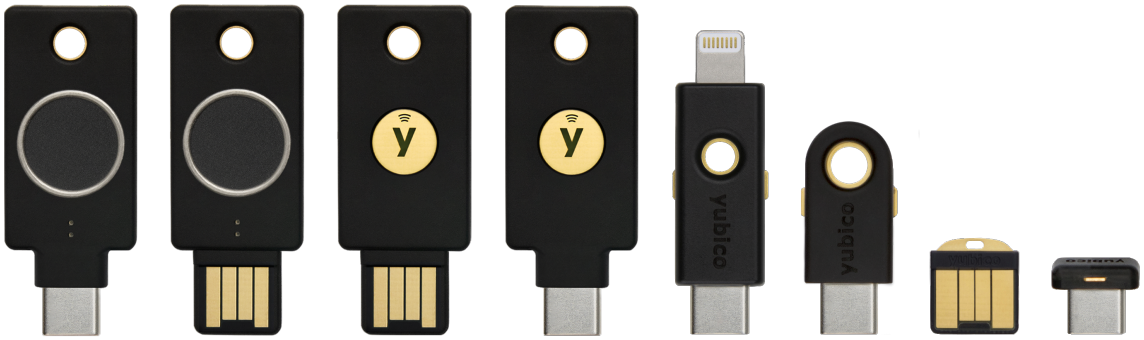
- **FIDO U2F (Universal Second Factor)** - standard drugiego składnika uwierzytelniania,
- **OTP (One-Time Password)** - mechanizm generowania jednorazowych haseł wykorzystywanych podczas logowania,
- **OATH (Initiative for Open Authentication)** - standard uwierzytelniania umożliwiający generowanie jednorazowych kodów dostępowych (HOTP i TOTP), wykorzystywanych jako dodatkowy składnik podczas logowania do systemu,
- **OpenPGP** - standard umożliwiający szyfrowanie danych i składanie podpisów cyfrowych,
- **PIV (Personal Identity Verification)** - standard kart inteligentnych, umożliwiający przechowywanie certyfikatów i wykonywanie operacji kryptograficznych [3].

Spośród wszystkich funkcjonalności dostępnych w urządzeniach YubiKey szczególnie interesujący jest moduł PIV, umożliwiający wykorzystanie klucza jako karty inteligentnej. Funkcja ta pozwala na przechowywanie certyfikatów, realizację uwierzytelniania oraz wykonywanie operacji kryptograficznych bez ujawniania klucza prywatnego poza urządzeniem.

1.4. Rodzaje kluczy YubiKey

Firma Yubico oferuje kilka rodzin kluczy bezpieczeństwa różniących się funkcjonalnością i przeznaczeniem. Najpopularniejszą z nich jest seria **YubiKey 5**, obsługująca między innymi standardy FIDO2, OTP, OpenPGP oraz PIV.

Oprócz niej dostępne są również urządzenia **YubiKey Bio**, wyposażone w czytnik linii papilarnych, oraz **Security Key Series**, przeznaczone głównie do uwierzytelniania przy użyciu standardów FIDO2 i U2F. Poszczególne modele występują w wariantach USB-A, USB-C, NFC oraz Lightning, co pozwala na współpracę z różnymi urządzeniami i systemami operacyjnymi [4].



Rys. 1.1. Różne warianty fizycznych kluczy YubiKey [4]

1.5. Cel i zakres projektu

Celem projektu jest analiza działania modułu Smart Card wykorzystującego standard PIV, zaimplementowanego w kluczach YubiKey.

W ramach projektu przedstawione zostały funkcje modułu PIV, sposób komunikacji pomiędzy kluczem a systemem operacyjnym, mechanizmy przechowywania kluczy kryptograficznych i certyfikatów, proces uwierzytelniania oraz składania podpisu cyfrowego. Omówiono również

praktyczne zastosowania technologii YubiKey oraz mechanizmy bezpieczeństwa, wykorzystywane do ochrony tożsamości cyfrowej użytkowników.

2. Identyfikacja funkcji modułu Smart Card / PIV

W tym rozdziale przedstawiono podstawowe funkcje modułu Smart Card/PIV dostępnego w kluczach YubiKey. Opisano rolę standardu PIV, najważniejsze funkcje kryptograficzne modułu oraz wykorzystywane algorytmy i interfejsy komunikacyjne.

2.1. Standard PIV i rola modułu Smart Card

PIV (Personal Identity Verification) jest standardem kart inteligentnych zdefiniowanym przez amerykański standard FIPS 201. Umożliwia on wykorzystanie kart inteligentnych do przechowywania certyfikatów cyfrowych oraz wykonywania operacji kryptograficznych z użyciem kluczy prywatnych przechowywanych wewnątrz urządzenia.

Klucze YubiKey implementują standard PIV, dzięki czemu mogą pełnić funkcję klasycznej karty inteligentnej wykorzystywanej do uwierzytelniania użytkowników, podpisywania danych oraz szyfrowania informacji. W praktyce pozwala to na integrację YubiKey z istniejącą infrastrukturą bezpieczeństwa opartą na kartach inteligentnych.

Moduł Smart Card stanowi jedną z aplikacji dostępnych w urządzeniach YubiKey. Jego zadaniem jest bezpieczne przechowywanie materiału kryptograficznego oraz wykonywanie operacji kryptograficznych bez ujawniania klucza prywatnego systemowi operacyjnemu. Dzięki temu nawet w przypadku przejęcia kontroli nad komputerem atakujący nie uzyskuje bezpośredniego dostępu do kluczy użytkownika [5].

W ramach modułu PIV wykorzystywane są specjalne sloty przeznaczone do różnych zastosowań. Slot 9A służy do uwierzytelniania użytkownika, 9C do składania podpisów cyfrowych, 9D do zarządzania kluczami wykorzystywanymi podczas szyfrowania, natomiast 9E przeznaczony jest do uwierzytelniania samej karty [6]. W tabeli 2.1. przedstawiono wybrane, najważniejsze wykorzystywane sloty funkcjonalne.

Tabela 2.1. Najważniejsze sloty PIV wykorzystywane w kluczach YubiKey [6]

Slot	Przeznaczenie
9A	PIV Authentication
9C	Digital Signature
9D	Key Management
9E	Card Authentication
F9	Attestation

2.2. Funkcje kryptograficzne modułu PIV

Podstawowym zadaniem modułu PIV jest przechowywanie kluczy kryptograficznych i certyfikatów użytkownika. Klucze mogą zostać wygenerowane bezpośrednio na urządzeniu lub zaimportowane z zewnętrznego źródła. W obu przypadkach klucz prywatny pozostaje wewnątrz YubiKey i nie jest udostępniany aplikacjom działającym na komputerze [5].

Jedną z najważniejszych funkcji modułu jest tworzenie podpisu cyfrowego. Operacja polega na wykorzystaniu klucza prywatnego znajdującego się w odpowiednim slocie PIV do podpisania danych przekazanych przez aplikację. Sam klucz nigdy nie opuszcza urządzenia, a do systemu zwracany jest jedynie wynik operacji kryptograficznej [7].

Moduł PIV umożliwia również uwierzytelnianie użytkownika. W tym przypadku certyfikat zapisany w slocie 9A wykorzystywany jest do potwierdzenia tożsamości podczas logowania do systemu lub usługi sieciowej.

Kolejną funkcją jest szyfrowanie i odszyfrowywanie danych. Do tego celu wykorzystywany jest slot 9D (Key Management), przeznaczony do przechowywania kluczy używanych podczas operacji związanych z ochroną poufności danych [6].

2.3. Obsługiwane algorytmy i interfejsy

Moduł PIV obsługuje algorytmy kryptografii asymetrycznej RSA oraz ECC (Elliptic Curve Cryptography). W zależności od wersji firmware urządzenia możliwe jest wykorzystanie kluczy RSA oraz krzywych eliptycznych P-256 i P-384. Algorytmy te wykorzystywane są podczas uwierzytelniania, podpisywania danych oraz szyfrowania informacji.

W celu zapewnienia współpracy z aplikacjami wykorzystującymi sprzętowe moduły kryptograficzne Yubico udostępnia bibliotekę YKCS11. Jest ona implementacją standardu PKCS#11, który definiuje sposób komunikacji aplikacji z urządzeniami przechowującymi klucze kryptograficzne. Dzięki temu z funkcji PIV mogą korzystać między innymi OpenSSL, OpenSSH, Firefox oraz aplikacje Java [8].

Od strony systemu operacyjnego YubiKey działający w trybie PIV jest widziany jako karta inteligentna (Smart Card). Pozwala to na wykorzystanie istniejących mechanizmów obsługi kart inteligentnych dostępnych w systemach Windows, Linux oraz macOS bez konieczności tworzenia dedykowanych rozwiązań dla każdego typu urządzenia.

3. Analiza komunikacji między kluczem a systemem

Rozdział opisuje sposób wymiany danych pomiędzy systemem operacyjnym a kluczem YubiKey działającym w trybie PIV. Szczególną uwagę zwrócono na rolę interfejsu CCID, komunikatów APDU oraz warstwy pośredniczącej pomiędzy aplikacją a urządzeniem.

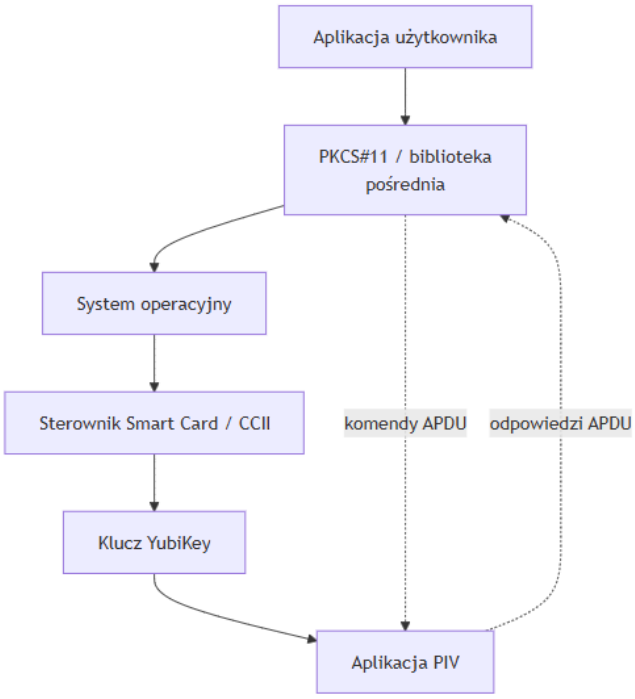
3.1. Mechanizm komunikacji

Komunikacja pomiędzy systemem operacyjnym a kluczem YubiKey działającym w trybie PIV odbywa się z wykorzystaniem mechanizmów typowych dla kart inteligentnych. Po stronie komputera aplikacja nie komunikuje się bezpośrednio z pamięcią klucza, lecz korzysta z warstwy pośredniej, którą stanowią sterowniki systemowe, biblioteki obsługi kart inteligentnych oraz interfejsy programistyczne, takie jak PKCS#11.

Jednym z najważniejszych elementów tej komunikacji jest interfejs CCID (Chip Card Interface Device). W dokumentacji Yubico wskazano, że interfejs CCID jest wykorzystywany wtedy, gdy przez USB aktywne są aplikacje takie jak PIV, OATH lub OpenPGP [9]. Dzięki temu YubiKey może być rozpoznawany przez system jako urządzenie typu Smart Card, czyli karta inteligentna dostępna przez standardowy mechanizm obsługi kart.

Właściwa wymiana poleceń między aplikacją a modułem PIV odbywa się za pomocą komunikatów APDU (Application Protocol Data Unit). APDU jest standardowym formatem komend i odpowiedzi wykorzystywanym w kartach inteligentnych. Polecenie APDU może służyć między innymi do wyboru aplikacji PIV, odczytu certyfikatu, weryfikacji PIN-u lub zlecenia wykonania operacji kryptograficznej [10].

Rola systemu operacyjnego polega na wykryciu urządzenia, udostępnieniu odpowiedniego sterownika oraz przekazywaniu komunikatów między aplikacją użytkownika a kluczem YubiKey. Z punktu widzenia programu korzystającego z PIV urządzenie może być traktowane jak standardowa karta inteligentna. Ułatwia to integrację z istniejącymi rozwiązaniami, ponieważ aplikacja nie musi znać szczegółów sprzętowych konkretnego modelu YubiKey.



Rys. 3.1. Uproszczony schemat komunikacji pomiędzy aplikacją a modułem PIV w kluczu YubiKey

3.2. Przykładowy przebieg komunikacji

Przykładowy przebieg komunikacji rozpoczyna się od podłączenia klucza YubiKey do komputera przez USB lub od użycia go przez NFC, jeżeli dany model i środowisko pracy obsługują taki sposób połączenia. Po wykryciu urządzenia system operacyjny udostępnia aplikacjom odpowiedni interfejs komunikacyjny.
Następnie aplikacja, na przykład program podpisujący dokument albo narzędzie administracyjne, wysyła polecenie do modułu PIV. Polecenie to zostaje opakowane w komunikat APDU i przekazane przez system operacyjny do urządzenia. Dokumentacja Yubico pokazuje, że odpowiedzi APDU zawierają nie tylko dane, ale również bajty statusu **SW1** i **SW2**, które informują o powodzeniu albo błędzie wykonania operacji [10].

Po otrzymaniu polecenia YubiKey wykonuje żądaną operację. Może to być odczyt certyfikatu, sprawdzenie kodu PIN, wygenerowanie podpisu cyfrowego albo zwrócenie informacji o błędzie. Jeżeli operacja zakończy się powodzeniem, urządzenie zwraca odpowiedź APDU. Typowym kodem oznaczającym sukces jest **90 00** [10].

W przypadku większych danych, na przykład certyfikatu, odpowiedź może zostać podzielona na kilka części. Dokumentacja Yubico opisuje mechanizm, w którym aplikacja otrzymuje informację, że dostępne są kolejne bajty danych, a następnie wysyła dodatkowe polecenie **GET RESPONSE** aby odebrać dalszą część odpowiedzi [10].

4. Prezentacja sposobu przechowywania kluczy i certyfikatów

W tym rozdziale omówiono sposób organizacji kluczy kryptograficznych i certyfikatów w module PIV. Przedstawiono znaczenie klucza prywatnego, klucza publicznego, certyfikatu X.509 oraz slotów PIV wykorzystywanych do przechowywania tych danych.

4.1. Klucze kryptograficzne i certyfikaty

Moduł PIV w kluczu YubiKey wykorzystuje kryptografię asymetryczną, czyli pary kluczy składające się z klucza prywatnego i klucza publicznego. Klucz prywatny służy do wykonywania operacji takich jak podpis cyfrowy lub odszyfrowywanie danych, natomiast klucz publiczny może być udostępniany innym podmiotom i wykorzystywany do weryfikacji podpisu albo szyfrowania danych dla właściciela klucza.

W kontekście PIV klucz publiczny jest zwykle powiązany z certyfikatem **X.509**. Certyfikat zawiera informacje identyfikujące właściciela oraz jego klucz publiczny. Dzięki temu system, aplikacja lub usługa sieciowa mogą sprawdzić, czy dany klucz publiczny należy do określonego użytkownika. W dokumentacji Yubico wskazano, że zajęty slot PIV zawiera zwykle klucz prywatny, klucz publiczny oraz certyfikat X.509 [11].

Istotną cechą YubiKey jest możliwość przechowywania klucza prywatnego wewnątrz urządzenia. W takim modelu aplikacja działająca na komputerze nie otrzymuje kopii klucza prywatnego, lecz jedynie zleca urządzeniu wykonanie operacji kryptograficznej. Zwiększa to bezpieczeństwo, ponieważ nawet w przypadku zainfekowania systemu operacyjnego atakujący nie powinien uzyskać bezpośredniego dostępu do samego klucza prywatnego.

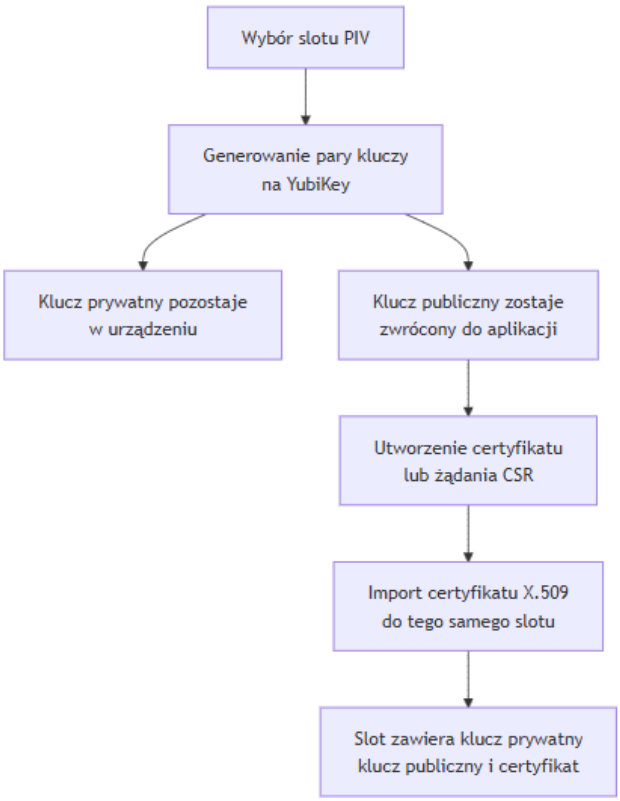
4.2. Sloty PIV i generowanie kluczy

Dane wykorzystywane przez moduł PIV są organizowane w slotach. Każdy slot ma określone przeznaczenie. Podstawowe sloty to 9A, 9C, 9D i 9E, wykorzystywane odpowiednio do uwierzytelniania, podpisu cyfrowego, zarządzania kluczami oraz uwierzytelniania karty [6]. Dokumentacja Yubico wskazuje również, że YubiKey 4 i 5 obsługują 24 sloty PIV, a każdy z nich może przechowywać certyfikat X.509 wraz z odpowiadającym mu kluczem prywatnym [6].

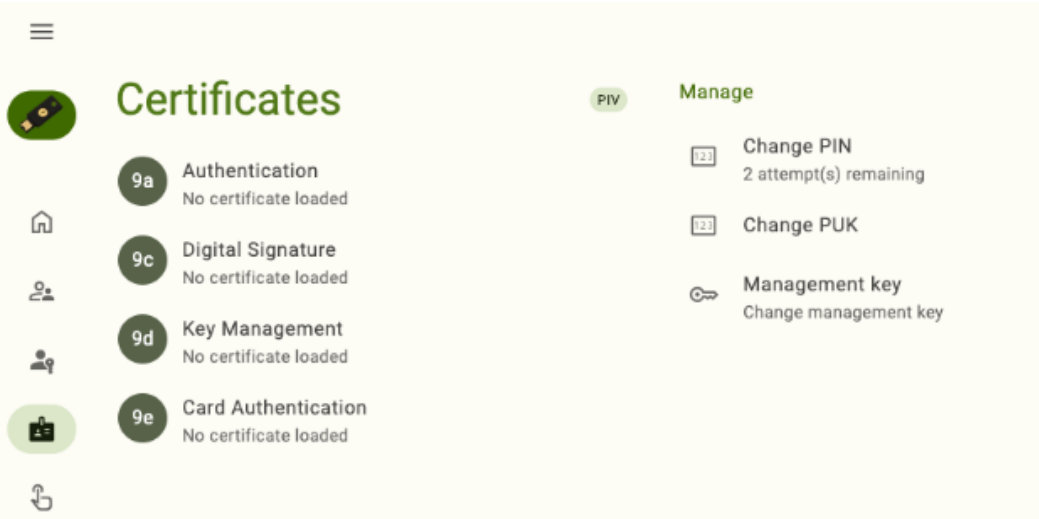
Klucz może zostać wygenerowany bezpośrednio na urządzeniu albo zaimportowany z zewnętrznego źródła. W przypadku generowania klucza na YubiKey urządzenie tworzy parę kluczy, a na zewnątrz zwracany jest klucz publiczny. Następnie na podstawie klucza publicznego można utworzyć certyfikat samopodpisany albo żądanie certyfikatu, które zostanie przekazane do urzędu certyfikacji [11].

Po wygenerowaniu certyfikatu należy zaimportować go do tego samego slotu PIV, w którym znajduje się odpowiadający mu klucz prywatny. W efekcie slot zawiera zestaw danych potrzebnych do wykonywania operacji kryptograficznych: klucz prywatny, klucz publiczny i certyfikat X.509 [11].

Ważnym mechanizmem związanym z generowaniem kluczy jest atestacja. YubiKey od wersji 4.3 posiada klucz i certyfikat atestacyjny w slocie F9. Atestacja pozwala potwierdzić, że dany klucz prywatny został wygenerowany na urządzeniu YubiKey, a nie zaimportowany z zewnątrz [12].



Rys. 4.1. Przykładowy proces tworzenia klucza i certyfikatu w module PIV



Rys. 4.2. Widok slotów PIV w aplikacji Yubico Authenticator [15]

5. Omówienie procesu uwierzytelniania i podpisu cyfrowego

Rozdział przedstawia praktyczne wykorzystanie modułu PIV w procesie uwierzytelniania oraz tworzenia podpisu cyfrowego. Opisano, w jaki sposób certyfikat i klucz prywatny zapisane w YubiKey mogą zostać użyte do potwierdzenia tożsamości użytkownika i zabezpieczenia dokumentów.

5.1. Proces uwierzytelniania

Uwierzytelnianie przy użyciu PIV polega na potwierdzeniu tożsamości użytkownika za pomocą certyfikatu oraz klucza prywatnego przechowywanego w urządzeniu. W typowym scenariuszu wykorzystywany jest slot 9A, czyli PIV Authentication. Certyfikat i odpowiadający mu klucz prywatny zapisane w tym slocie mogą być używane między innymi do logowania do systemu operacyjnego lub usługi wymagającej uwierzytelniania certyfikatowego [6].

Podczas logowania system lub aplikacja sprawdza certyfikat użytkownika i zleca wykonanie operacji kryptograficznej z użyciem klucza prywatnego. Klucz prywatny nie jest kopiowany do komputera. YubiKey wykonuje operację wewnątrz urządzenia, a następnie zwraca wynik. Dzięki temu system może potwierdzić, że użytkownik posiada właściwy klucz prywatny powiązany z certyfikatem.

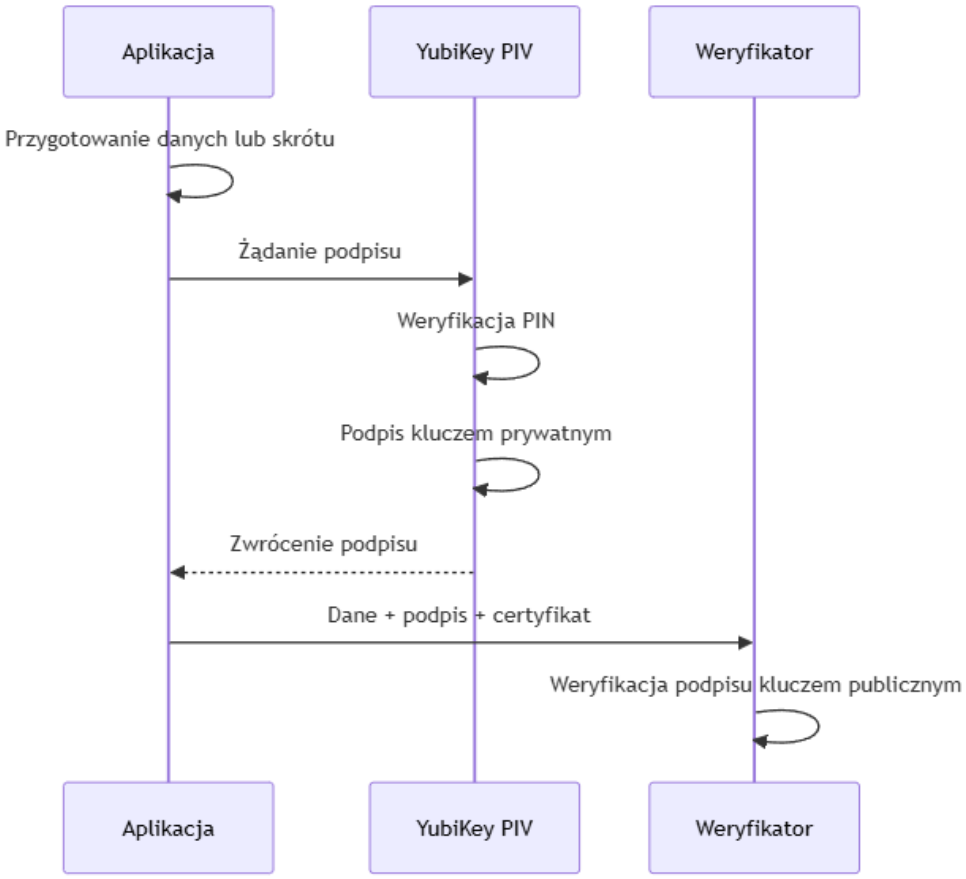
W praktyce uwierzytelnianie PIV może być używane w środowiskach korporacyjnych, na przykład do logowania do systemu Windows, dostępu do zasobów firmowych lub uwierzytelniania w usługach wykorzystujących infrastrukturę klucza publicznego. Yubico opisuje YubiKey jako urządzenie zgodne z PIV, które może działać jako karta inteligentna w środowisku Microsoft Windows [13].

5.2. Proces podpisu cyfrowego

Podpis cyfrowy jest operacją kryptograficzną, która pozwala potwierdzić autentyczność i integralność danych. W module PIV do podpisu cyfrowego przeznaczony jest przede wszystkim slot 9C, czyli Digital Signature. Według dokumentacji Yubico slot ten służy do podpisywania dokumentów, plików lub programów, a przed każdą operacją podpisu wymagane jest podanie PIN-u użytkownika [6].

Proces podpisu można przedstawić w kilku etapach (rys. 5.1). Najpierw aplikacja przygotowuje dane do podpisania lub ich skrót kryptograficzny. Następnie wysyła żądanie podpisu do modułu PIV. YubiKey sprawdza, czy użytkownik ma prawo wykonać operację, na przykład przez weryfikację PIN-u. Następnie urządzenie wykonuje podpis za pomocą klucza prywatnego znajdującego się w odpowiednim slocie i zwraca gotowy podpis do aplikacji.

Weryfikacja podpisu odbywa się już poza YubiKey. Odbiorca dokumentu lub aplikacja weryfikująca używa klucza publicznego zawartego w certyfikacie X.509, aby sprawdzić, czy podpis został utworzony właściwym kluczem prywatnym i czy dane nie zostały zmienione po podpisaniu.



Rys. 5.1. Uproszczony proces tworzenia i weryfikacji podpisu cyfrowego z użyciem YubiKey PIV

6. Analiza zastosowań i mechanizmów bezpieczeństwa YubiKey

W niniejszym rozdziale przedstawiono przykładowe zastosowania YubiKey oraz najważniejsze mechanizmy bezpieczeństwa stosowane w urządzeniu. Omówiono zarówno praktyczne scenariusze użycia, jak i ograniczenia wynikające z konieczności poprawnej konfiguracji oraz fizycznego posiadania klucza.

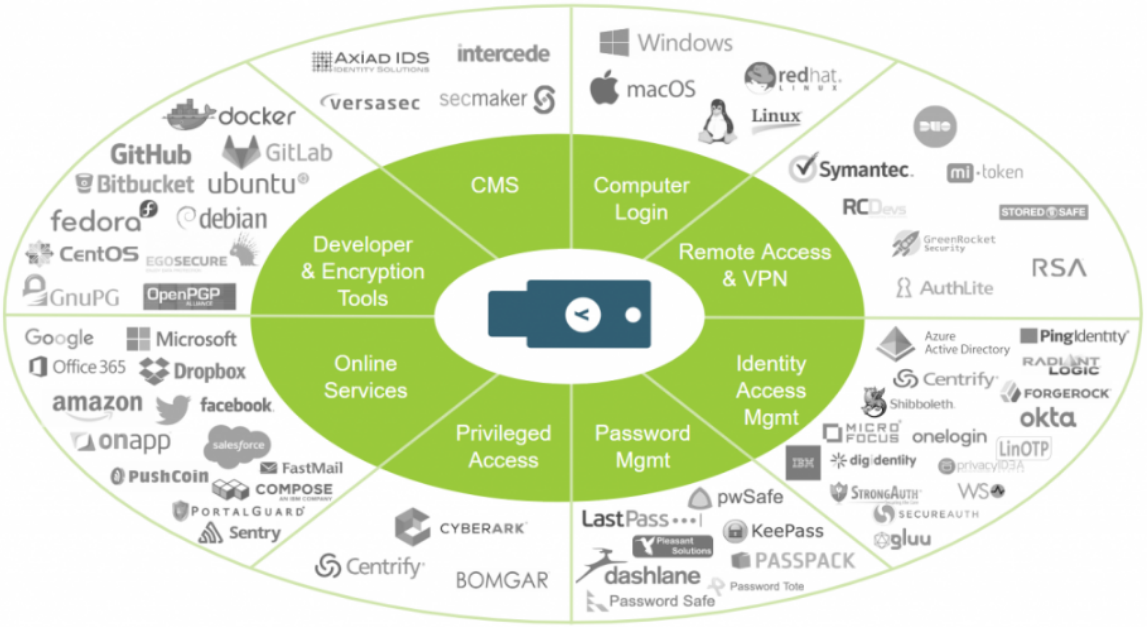
6.1. Praktyczne zastosowania

YubiKey z modułem PIV może być wykorzystywany w różnych scenariuszach (rys. 6.1) wymagających silnego uwierzytelniania lub ochrony kluczy kryptograficznych. Jednym z podstawowych zastosowań jest logowanie do systemów operacyjnych przy użyciu mechanizmów kart inteligentnych. Yubico wskazuje, że YubiKey może identyfikować się jako Microsoft USB CCID smart card reader oraz karta PIV zgodna z NIST SP 800-73 [13].

Kolejnym zastosowaniem jest uwierzytelnianie SSH. Yubico udostępnia instrukcję konfiguracji YubiKey z PIV do uwierzytelniania w OpenSSH przez PKCS#11. W takim scenariuszu klucz prywatny znajduje się w slocie PIV, a serwer SSH wykorzystuje odpowiadający mu klucz publiczny do potwierdzenia tożsamości użytkownika [14].

YubiKey może być także wykorzystywany w środowiskach korporacyjnych do dostępu do VPN, aplikacji firmowych lub systemów wymagających certyfikatów użytkownika. Zastosowanie PIV jest szczególnie naturalne tam, gdzie organizacja posiada własną infrastrukturę PKI i wykorzystuje certyfikaty X.509 do kontroli dostępu.

Innym przykładem jest podpisywanie dokumentów lub kodu. Moduł PIV pozwala przechowywać klucz prywatny i certyfikat używany przez aplikacje podpisujące. Dzięki temu podpis może być wykonany z użyciem klucza sprzętowo chronionego, a nie pliku z kluczem prywatnym przechowywanego na dysku komputera.



Rys. 6.1. Przykładowe obszary zastosowań kluczy YubiKey w usługach i systemach informatycznych [2]

6.2. Mechanizmy bezpieczeństwa

Podstawowym mechanizmem bezpieczeństwa w YubiKey jest sprzętowa ochrona klucza prywatnego. Klucz prywatny może być wygenerowany i przechowywany wewnątrz urządzenia, a operacje kryptograficzne wykonywane są bez jego ujawniania systemowi operacyjnemu. Takie podejście ogranicza ryzyko kradzieży klucza z dysku lub pamięci komputera.

Drugim ważnym mechanizmem jest PIN. W przypadku PIV PIN zabezpiecza dostęp do operacji takich jak uwierzytelnianie, odszyfrowywanie oraz tworzenie podpisu cyfrowego. Dokumentacja Yubico wskazuje, że PIN, PUK i Management Key są kluczowe dla działania aplikacji PIV, a producent zaleca zmianę wartości domyślnych przed rozpoczęciem używania urządzenia [15].
Dodatkową ochronę stanowi Management Key, który jest wymagany przy operacjach administracyjnych, takich jak generowanie, importowanie lub usuwanie kluczy i certyfikatów w slotach PIV [15]. Dzięki temu zwykłe użycie klucza, na przykład podpis lub logowanie, jest oddzielone od operacji konfiguracyjnych.

YubiKey jest również istotny w kontekście odporności na phishing. Według Yubico urządzenia te wykorzystują sprzętowo wspieraną kryptografię klucza publicznego, a klucze prywatne są przechowywane na YubiKey jako niekopiowalne i sprzętowo powiązane z urządzeniem [16]. W przypadku FIDO2 odporność na phishing jest szczególnie silna, ponieważ uwierzytelnianie jest powiązane z konkretną usługą. W przypadku PIV bezpieczeństwo wynika przede wszystkim z użycia certyfikatów, kluczy prywatnych i infrastruktury PKI.

Do ograniczeń rozwiązania należy zaliczyć konieczność posiadania fizycznego klucza oraz poprawnej konfiguracji środowiska. Utrata urządzenia może utrudnić dostęp do systemów, dlatego w praktyce stosuje się zapasowe klucze albo procedury odzyskiwania dostępu. Dodatkowo wdrożenie PIV w organizacji wymaga zrozumienia certyfikatów, slotów PIV, PIN-u, Management Key oraz infrastruktury PKI.

7. Podsumowanie

Celem projektu było przedstawienie sposobu działania modułu karty Smart Card/PIV w kluczach YubiKey. W pracy omówiono ogólną ideę sprzętowych kluczy bezpieczeństwa, ich zastosowanie w uwierzytelnianiu wieloskładnikowym oraz wybrane standardy obsługiwane przez urządzenia YubiKey. Szczególną uwagę poświęcono standardowi PIV, który umożliwia wykorzystanie klucza jako karty inteligentnej przechowującej certyfikaty i wykonującej operacje kryptograficzne.

Jeden z ważniejszych wniosków to, że moduł PIV może służyć do bezpiecznego przechowywania kluczy prywatnych, certyfikatów X.509 oraz wykonywania operacji takich jak uwierzytelnianie, podpis cyfrowy i odszyfrowywanie danych. Istotną cechą tego rozwiązania jest fakt, że klucz prywatny nie musi opuszczać urządzenia, co znacząco ogranicza ryzyko jego przejęcia przez złośliwe oprogramowanie lub nieuprawnionego użytkownika.

W projekcie przedstawiono również mechanizm komunikacji pomiędzy systemem operacyjnym a kluczem YubiKey. Komunikacja ta opiera się na standardowych rozwiązaniach stosowanych w kartach inteligentnych, takich jak CCID i APDU, dzięki czemu YubiKey może współpracować z istniejącymi systemami operacyjnymi oraz aplikacjami korzystającymi z interfejsów Smart Card i PKCS#11.

Analiza zastosowań pokazała, że YubiKey z modułem PIV może być wykorzystywany między innymi do logowania do systemów operacyjnych, uwierzytelniania SSH, dostępu do zasobów firmowych, pracy z VPN oraz podpisywania dokumentów lub kodu. Rozwiązanie to jest szczególnie przydatne w środowiskach, w których istotne jest bezpieczne zarządzanie tożsamością użytkowników oraz ochrona kluczy kryptograficznych.

Podsumowując, moduł karty na kluczu YubiKey stanowi praktyczne i bezpieczne rozwiązanie łączące funkcje fizycznego tokena, karty inteligentnej oraz sprzętowego magazynu kluczy kryptograficznych. Jego największą zaletą jest możliwość wykonywania operacji kryptograficznych bez ujawniania klucza prywatnego poza urządzeniem. Jednocześnie skuteczne wykorzystanie tej technologii wymaga poprawnej konfiguracji, znajomości podstaw infrastruktury klucza publicznego oraz odpowiedniego zabezpieczenia samego urządzenia.

Źródła

Dostęp: 09.06.2026

[1] https://delkom.pl/blog-wpis/klucze-uwierzytelniajace-yubico-czym-jest-i-jak-dziala-yubikey-249

[2] https://www.yubico.com/products/how-the-yubikey-works

[3] https://developers.yubico.com/PIV/Introduction/YubiKey_and_PIV.html

[4] https://docs.yubico.com/hardware/yubikey/yk-tech-manual/yk5-intro.html

[5] https://docs.yubico.com/software/yubikey/tools/pivtool/Introduction.html

[6] https://developers.yubico.com/PIV/Introduction/Certificate_slots.html

[7] https://docs.yubico.com/software/yubikey/tools/pivtool/piv-tool-command.html

[8] https://developers.yubico.com/yubico-piv-tool/YKCS11

[9] https://docs.yubico.com/yesdk/users-manual/yubikey-reference/transports/overview.html

[10] https://docs.yubico.com/yesdk/users-manual/yubikey-reference/apdu.html

[11] https://developers.yubico.com/yubico-piv-tool/Actions/key_generation.html

[12] https://docs.yubico.com/yesdk/users-manual/application-piv/attestation.html

[13] https://www.yubico.com/authentication-standards/smart-card/

[14] https://developers.yubico.com/PIV/Guides/SSH_with_PIV_and_PKCS11.html

[15] https://docs.yubico.com/software/yubikey/tools/authenticator/auth-guide/piv-certificates.html

[16] https://www.yubico.com/solutions/multi-factor-authentication/