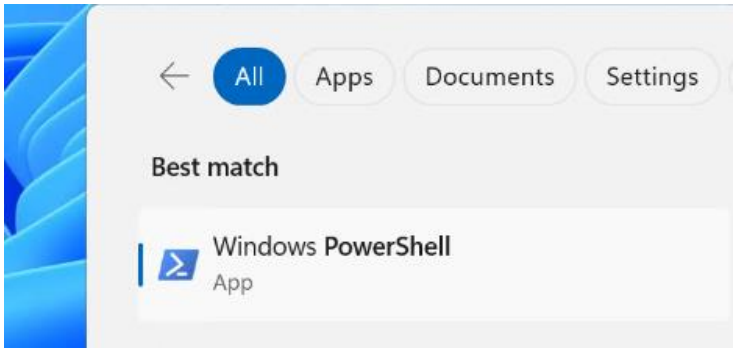
SecureBoot Windows 2026 Dodawanie Certyfikatów dla wybranych produktów NTT

Wstęp:

Microsoft od 2026 roku wymaga, aby w urządzeniach wspierających Windows 11 znajdował się nowy certyfikat, pozwalający na uruchomienie systemu. Jeśli Twoje urządzenie zostało wyprodukowane przed 2026 i zauważysz poniższy komunikat, odwiedź portal https://ntt.pl/support/ lub https://support.ntt.pl/ następnie wpisz numer seryjny urządzenia w celu zweryfikowania czy dostępna jest nowa wersja oprogramowania układowego zawierająca wymaganą poprawkę.
***Tylko dla wybranych urządzeń NTT.**

Aby sprawdzić czy twoje urządzenie zawiera poprawne certyfikaty należy uruchomić jako administrator aplikacje Power Shell:



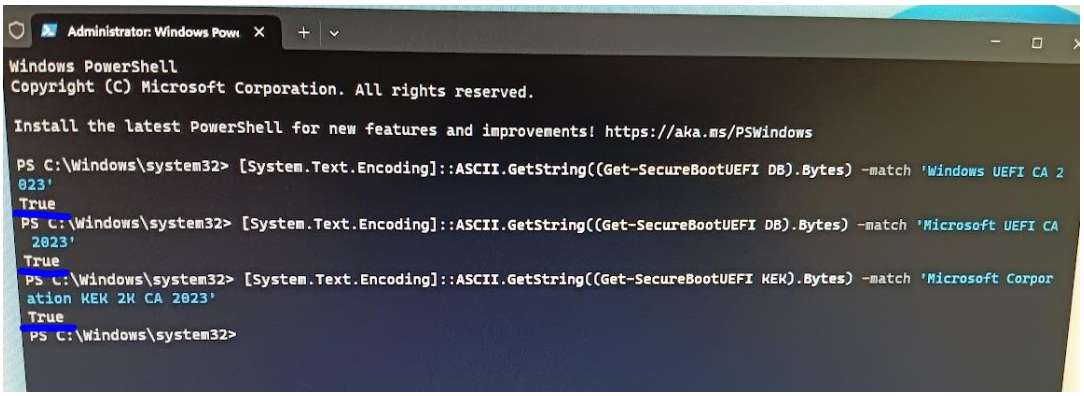
Następnie wkleić do konsoli poniższy tekst:

[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI DB).Bytes) -match 'Windows UEFI CA 2023'

[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI DB).Bytes) -match 'Microsoft UEFI CA 2023'

[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI KEK).Bytes) -match 'Microsoft Corporation KEK 2K CA 2023'

Jeśli w konsoli pojawi się komunikat „True”- twoje urządzenie posiada wymagane certyfikaty i nie trzeba przeprowadzać poniższej aktualizacji. Jeśli pokaże się „False”- zapoznaj się z poniższymi wytycznymi.



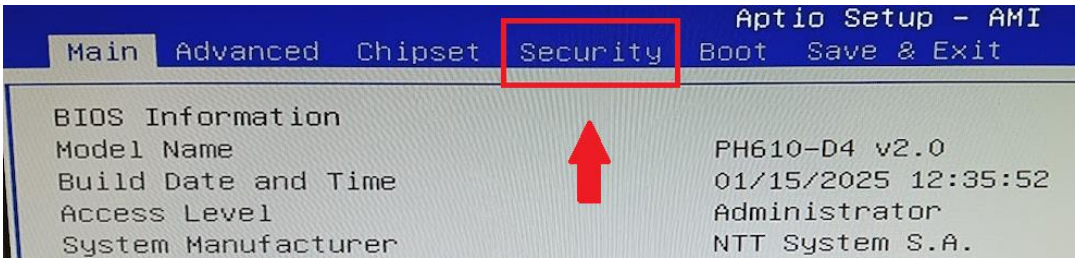
Jeśli po uruchomieniu urządzenia zauważysz poniższy komunikat (*lub podobny, ale z tytułem SecureBoot Violation na czerwonym tle) zastosuj się do dalej wymienionych wytycznych.

Odłącz wszystkie urządzenia podłączone do portów USB (z wyjątkiem myszki i klawiatury), następnie wykonaj ponowne uruchomienie urządzenia.

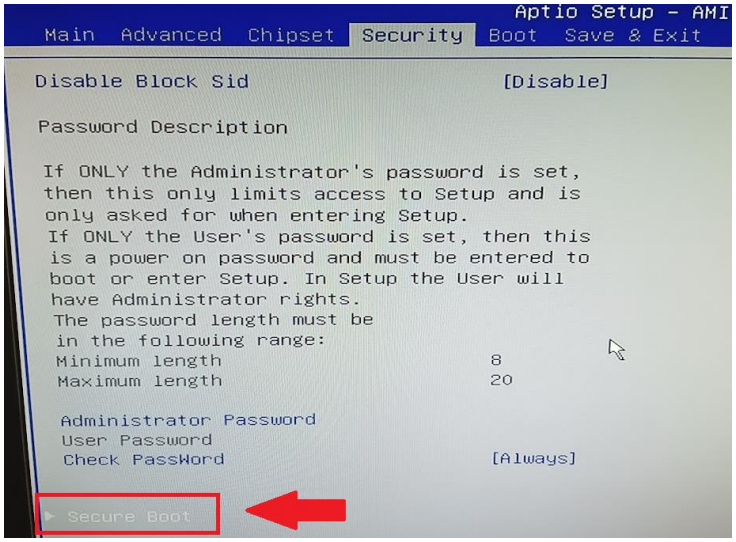
Sprawdź czy w portalu Support znajduje się poprawka dla twojego urządzenia

Jeśli znajduje się plik z poprawką, zrestartuj urządzenie na którym występuje komunikat o naruszeniu SecureBoot. Podczas ponownego uruchamiania od razu zacznij wciskać klawisz „Delete" znajdujący się na klawiaturze. To pozwoli wejść do ustawień BIOS.

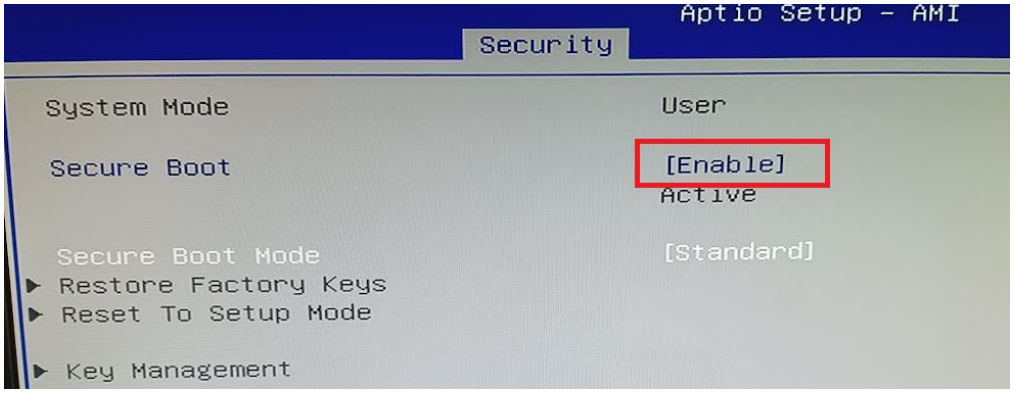
Przejdź do zakładki Security:

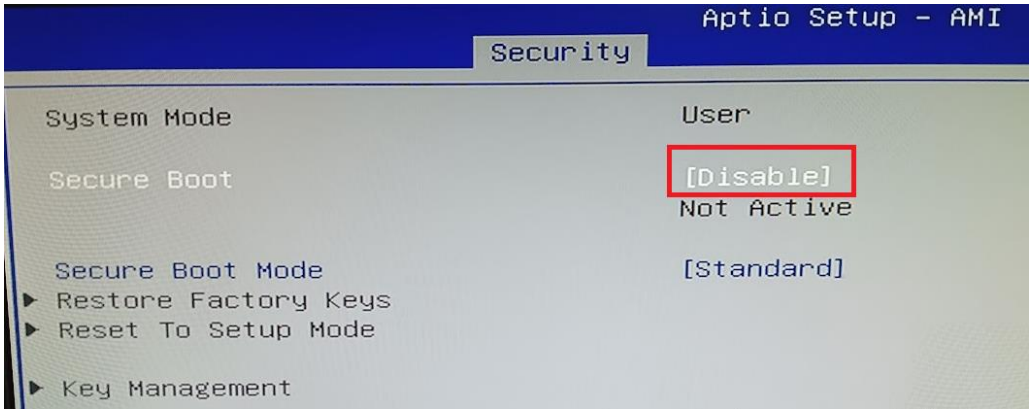


Odszukaj i uruchom funkcje „Secureboot":

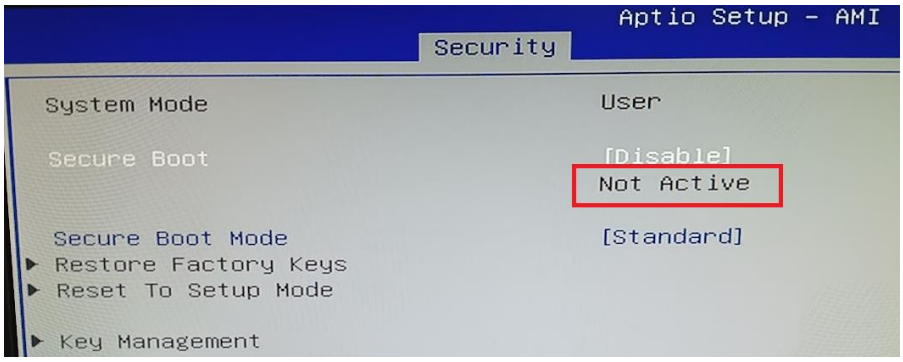


Przełącz poniższą funkcje z „Enabled" na Disabled:





Zapisz ustawienia klawiszem „F10”.
Urządzenie po ponownym uruchomieniu załaduje system operacyjny Windows (bez czerwonego komunikatu), tym samym możliwe jest uruchomienie oprogramowania do aktualizacji BIOS, pobranej z portalu Support. Dalsze kroki aktualizacji zawarte są w oprogramowaniu do aktualizacji oraz w dokumencie PDF dostarczonym z aplikacją.
***Jeśli komunikat nadal jest widoczny pomimo przełączenia funkcji na „Disabled” i zrestartowaniu urządzenia- sprawdź czy Status funkcji zmienił się na „Not Active”:**

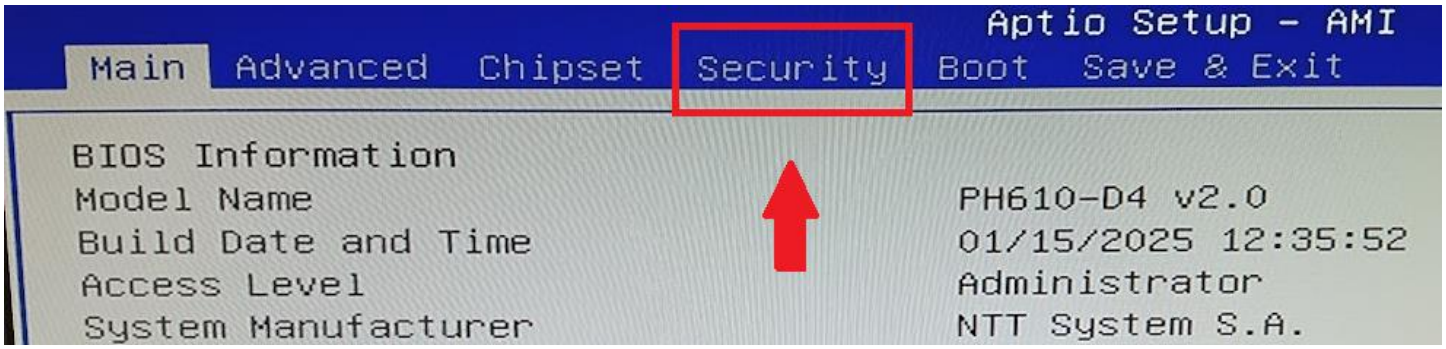


Jeśli widoczny status to „Active”. Wykonaj ponownie powyższe kroki.

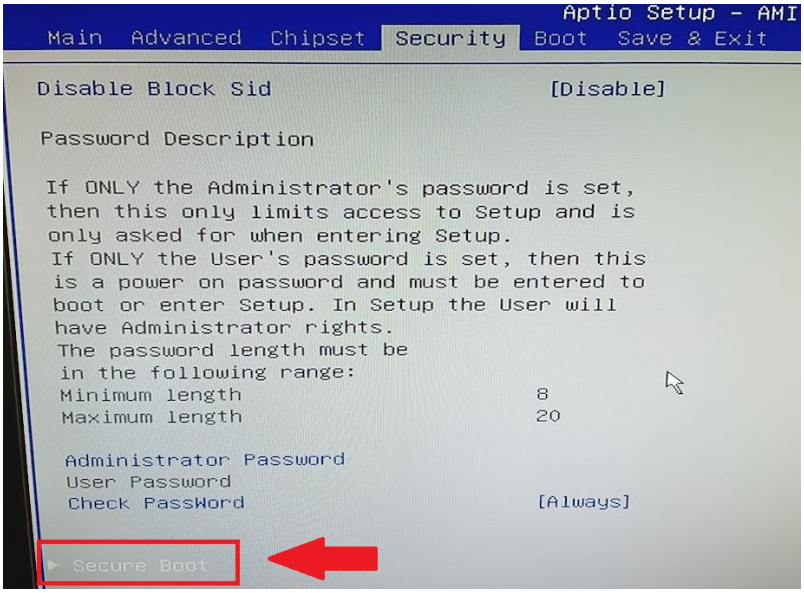
Po aktualizacji BIOS funkcja Secureboot automatycznie się aktywuje z poprawnymi dla Windows 11 2026 certyfikatami oraz komunikat o naruszeniu SecureBoot powinien zniknąć.
Nie jest wymagane ponowne wchodzenie w ustawienia oprogramowania układowego.

Urządzenia dla których nie została dostarczona aktualizacja oprogramowania układowego (BIOS) na portalu Support.

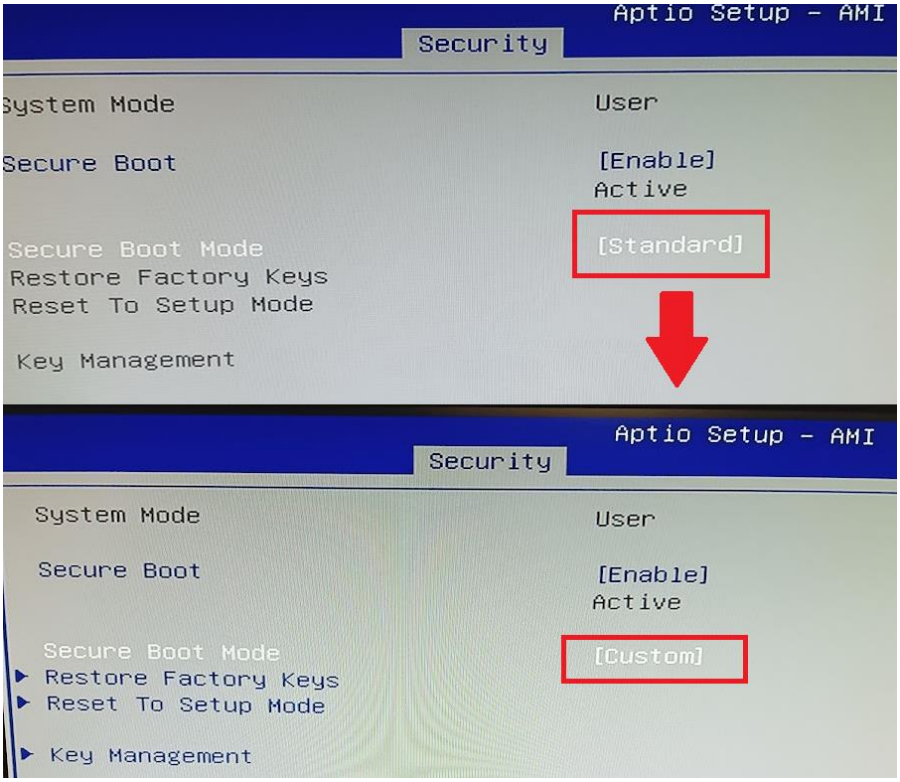
Pobierz paczkę z najnowszymi certyfikatami dla Secureboot 2026:
https://update.ntt.pl/file/1841/9ae3ef068c3af071e5f7cff64006f1ca
Wypakuj zawartość paczki bezpośrednio na pendrive, bądź inną pamięć masową (może być również dysk systemowy, który podłączony jest do urządzenia jako główny dysk, ale zalecamy używać pendrive)
Podłącz pendrive do dowolnego portu USB urządzenia.
Zrestartuj urządzenie na którym występuje komunikat o naruszeniu SecureBoot. Podczas ponownego uruchamiania od razu zacznij wciskać klawisz „Delete” znajdujący się na klawiaturze. To pozwoli wejść do ustawień BIOS.
Przejdź do zakładki Security:



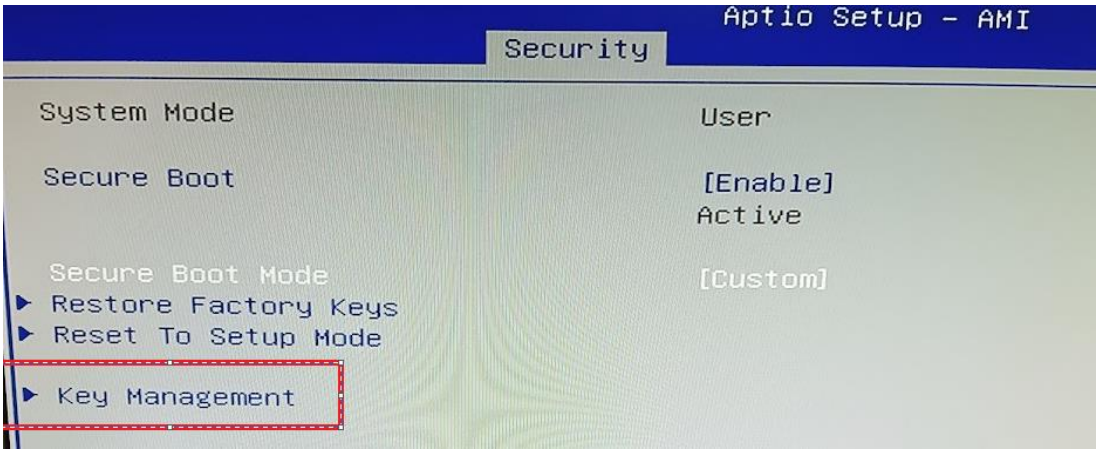
Odszukaj i uruchom funkcje „Secureboot”:



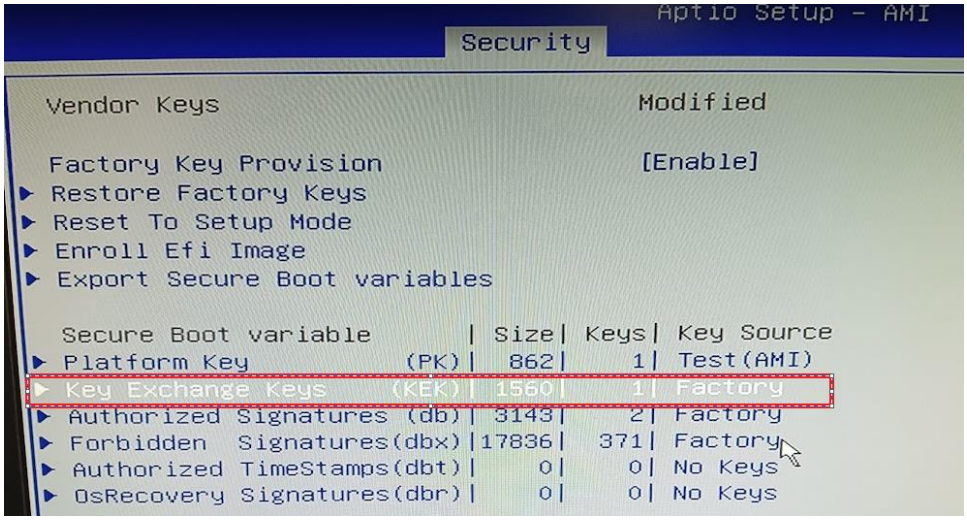
Przełącz funkcje Secureboot Mode ze „Standard” na „Custom”



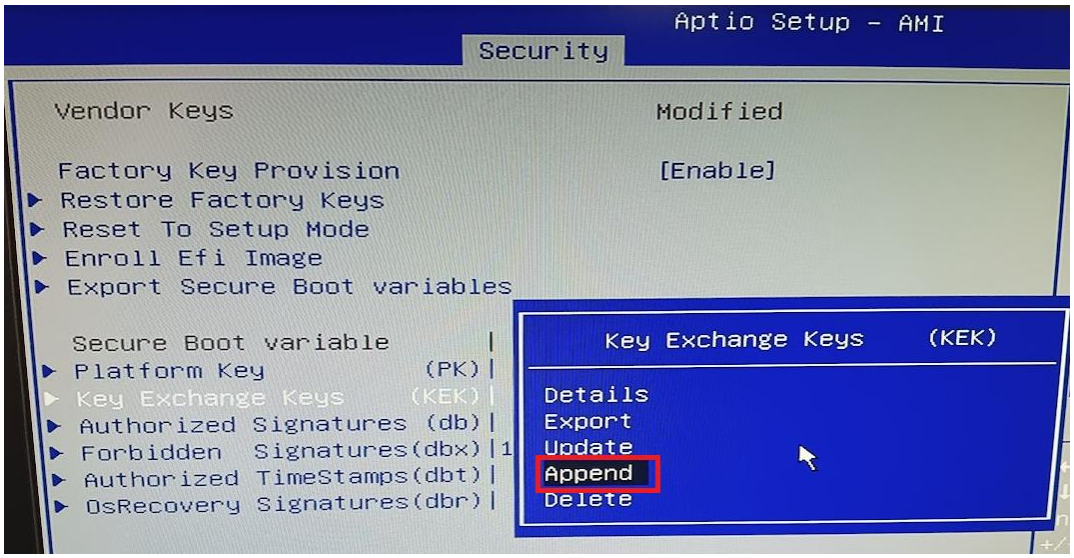
Przejdź do funkcji „Key Managment”:



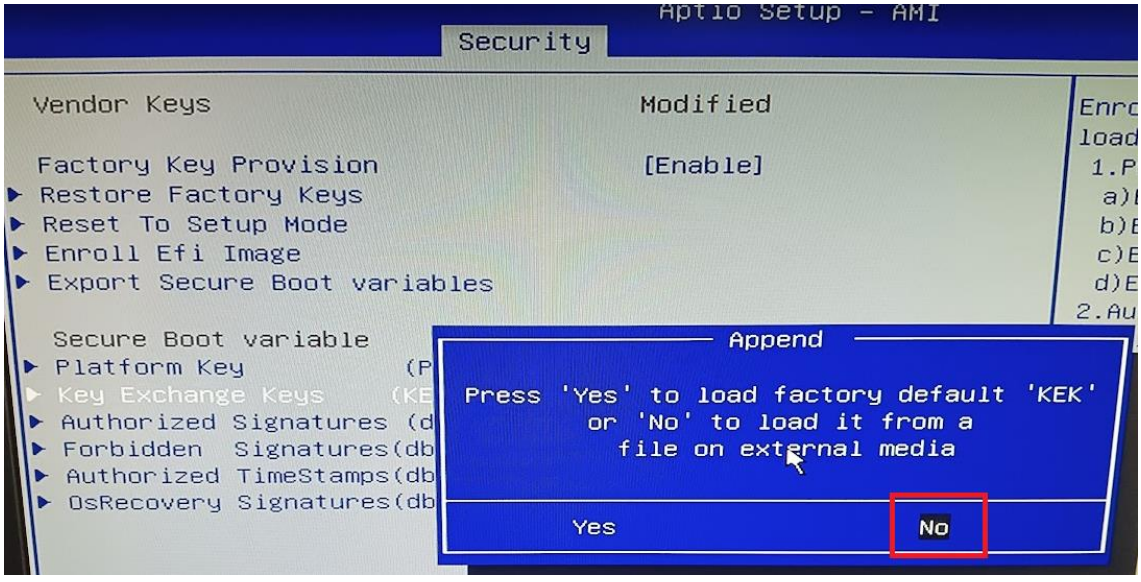
Przejdź do zakładki „Key Exchange Keys” klawiszem Enter znajdującym się na klawiaturze urządzenia:



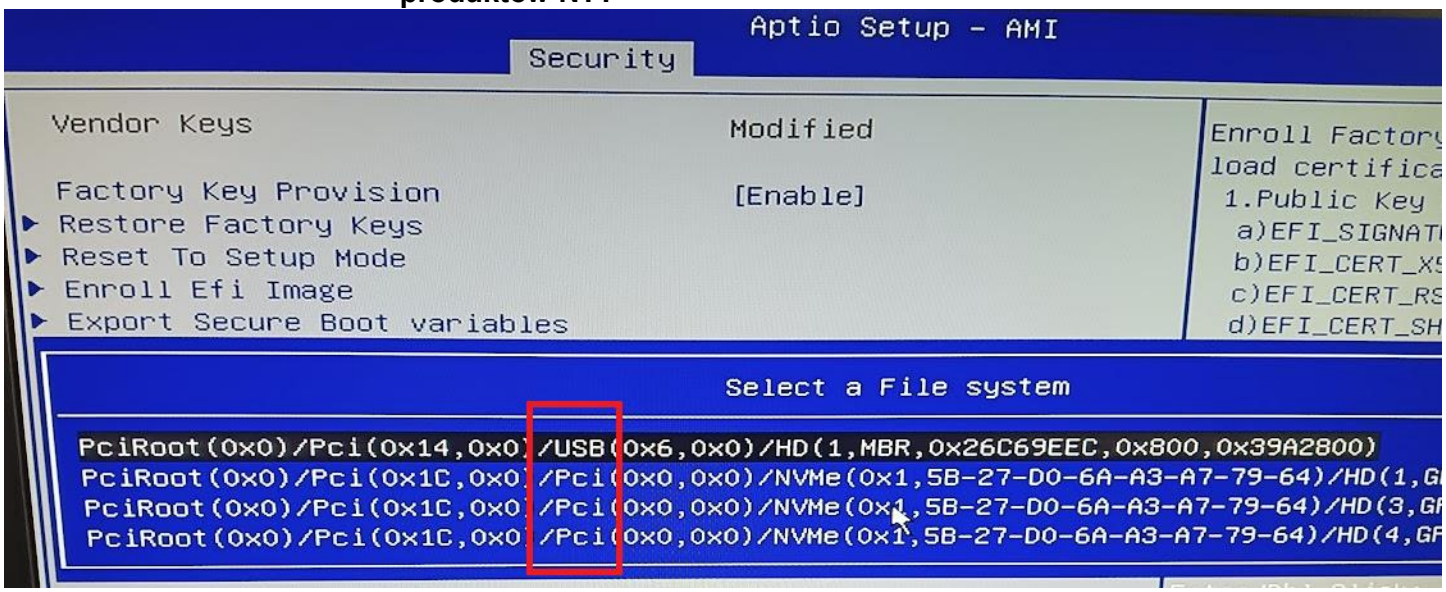
Wybierz opcje „Append”:



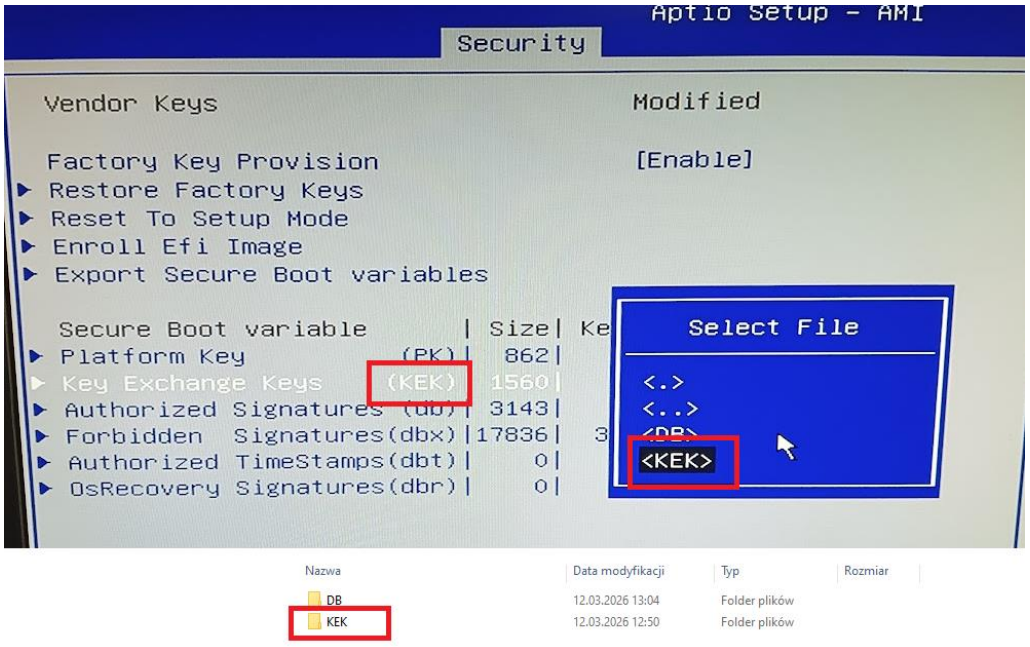
Zaznacz i przejdź do opcji „No” za pomocą strzałek na klawiaturze urządzenia, potwierdzając wybór klawiszem Enter.



Wybierz urządzenie na którym znajdują się wymagane certyfikaty. Pendrive oraz inne pamięci masowe podłączone do portu USB będą opisane jako „USB”. Dyski systemowe podłączone do wewnętrznych portów urządzenia (SATA/M.2) jako PCIE. Wybór urządzenia możliwy jest za pomocą strzałek znajdujących się na klawiaturze urządzenia, potwierdzenie wyboru, klawisz Enter:

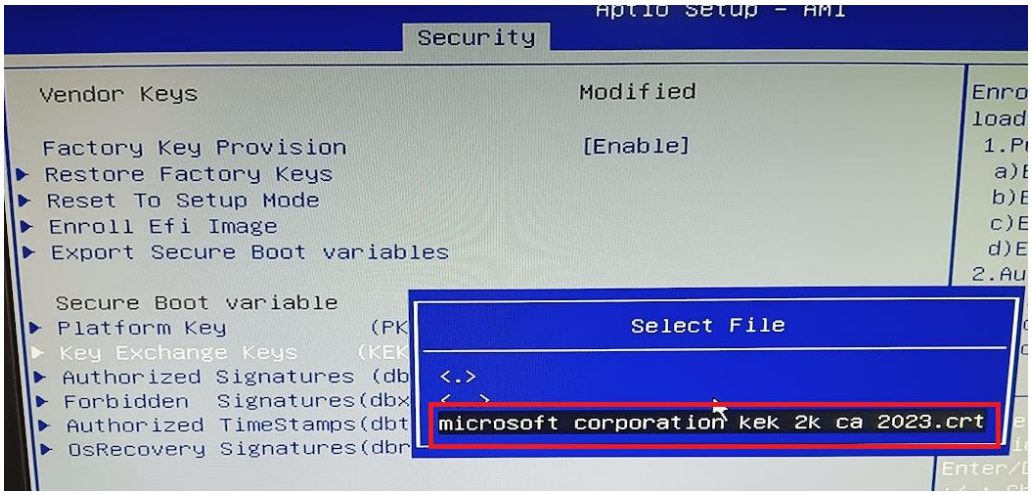


Po wybraniu odpowiedniego urządzenia zawierającego aktualne certyfikaty należy wybrać folder który odpowiada aktualnie dodawanym certyfikatom. Za pomocą strzałek na klawiaturze podłączonej do urządzenia należy wybrać folder z certyfikatem. Potwierdzenie klawiszem Enter:

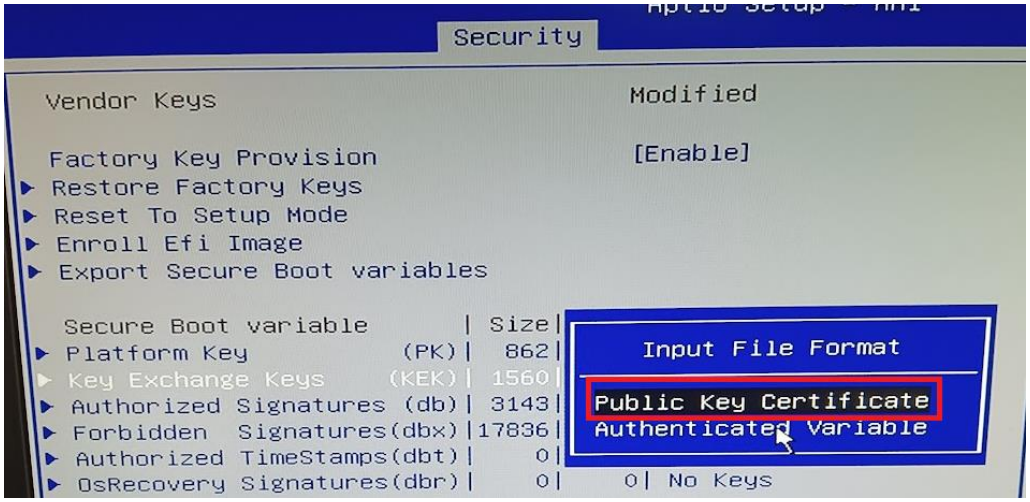


***Przykład- Key Exchange Keys (KEK)- folder KEK na urządzeniu pamięci masowej**

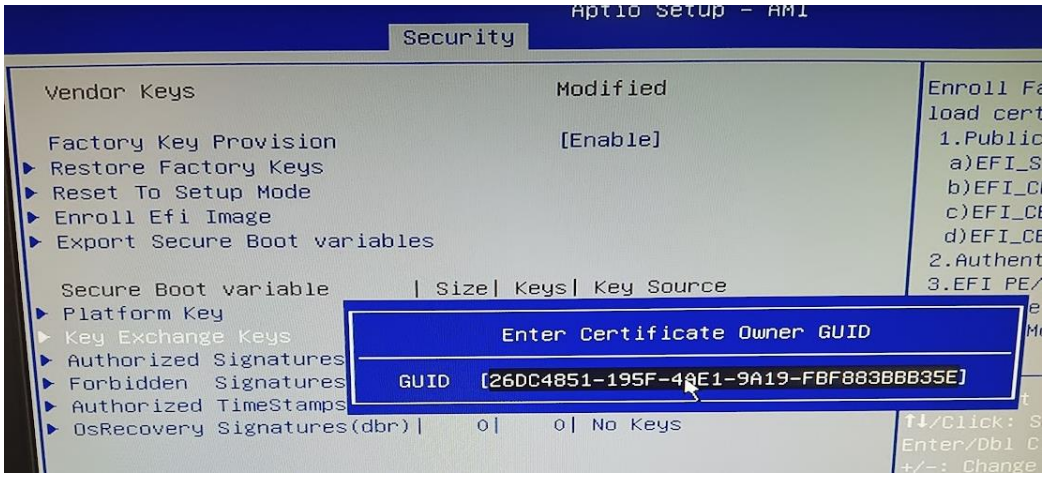
Po potwierdzeniu wejścia w folder „KEK”, należy wskazać za pomocą strzałek znajdujących się na klawiaturze certyfikat aktualnie dodawany, zatwierdzić wybór klawiszem Enter:



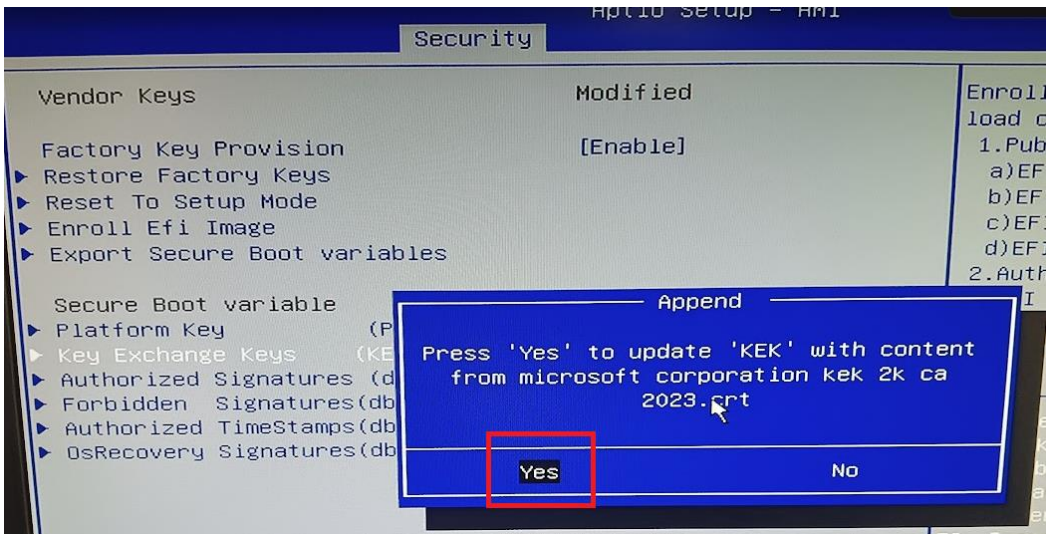
Po potwierdzeniu wybrania certyfikatu należy wybrać opcje „Public Key Certificate”:



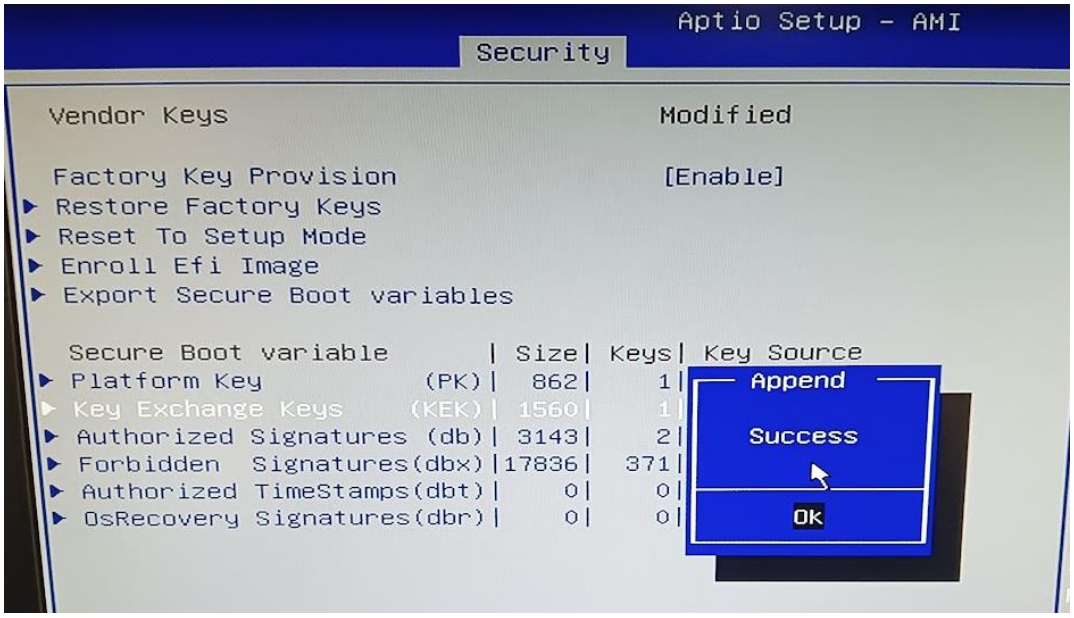
Wcisnąć klawisz Enter po pojawieniu się poniższego okna:



Zaznacz i przejdź do opcji „Yes” za pomocą strzałki na klawiaturze urządzenia, potwierdzając wybór klawiszem Enter.

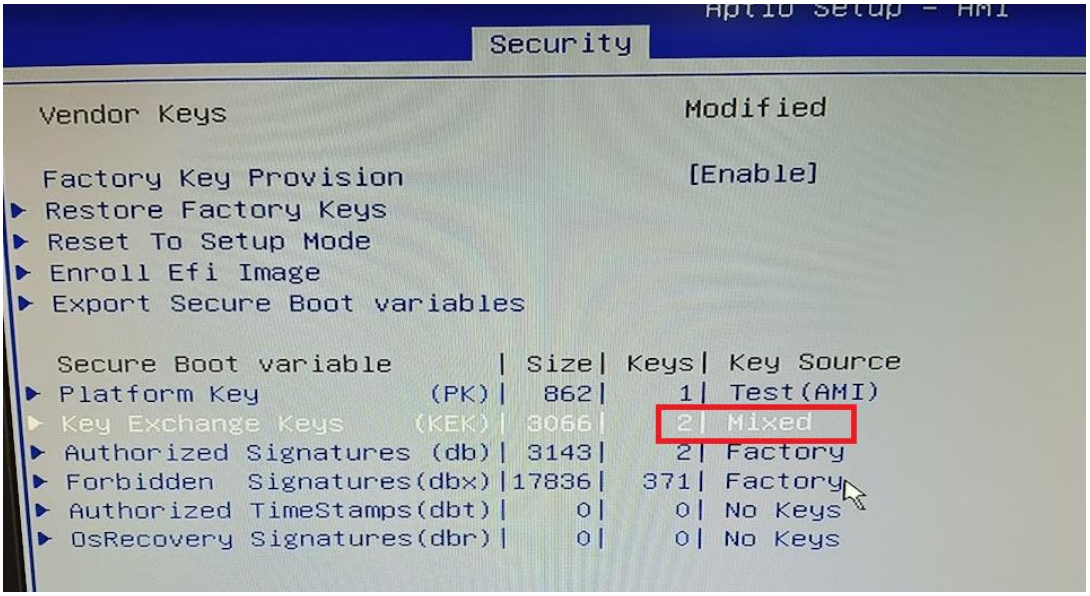


Potwierdź sukces klawiszem Enter.

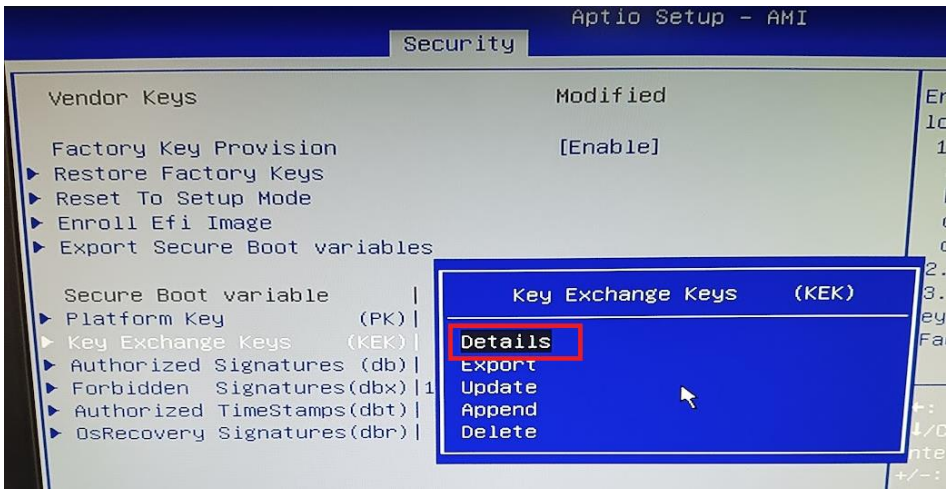


Jeśli pojawi się komunikat „Failed”- powtórz cały proces dodawania certyfikatu od miejsca uruchomienia funkcji „Key Exchange Keys”.

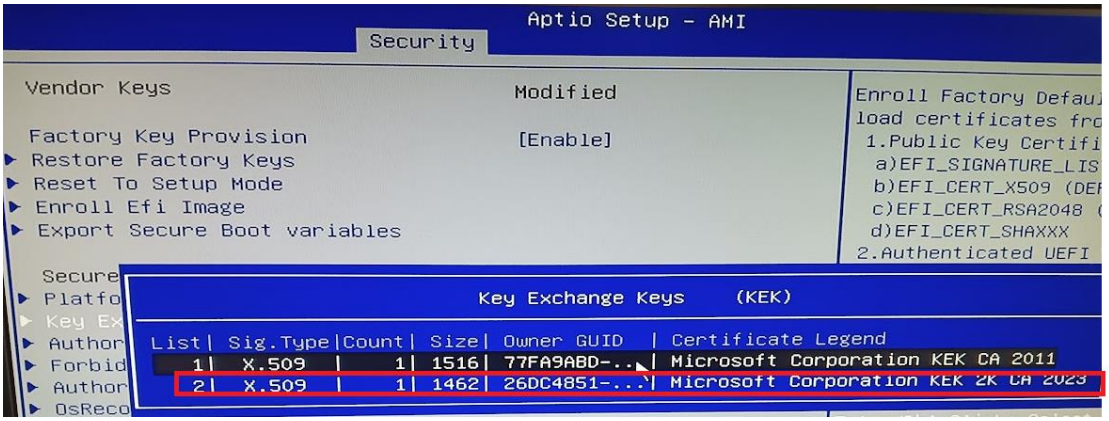
Po poprawnym dodaniu można zauważyć, że status „Key Source” zmienił się na mixed.



W celu upewnienia się, że certyfikat został dodany prawidłowo, zalecamy przejść ponownie do funkcji „Key Exchange Keys” a następnie uruchom opcje „Details”:

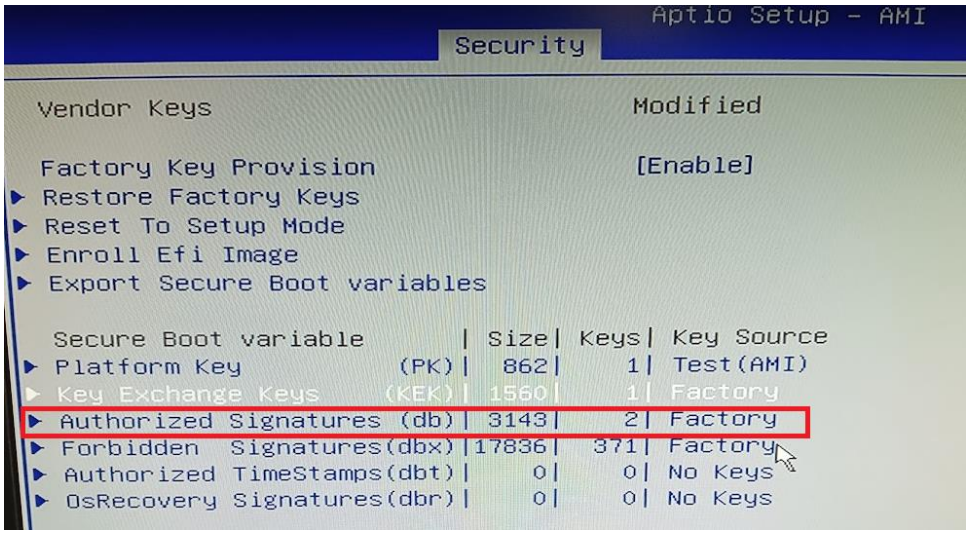


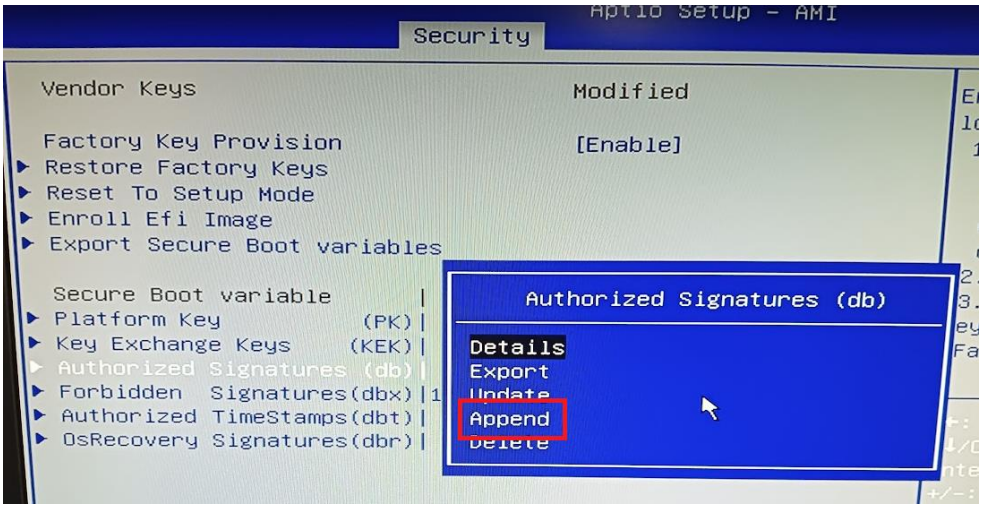
Certyfikat KEK 2K CA 2023 powinien znajdować się na liście:

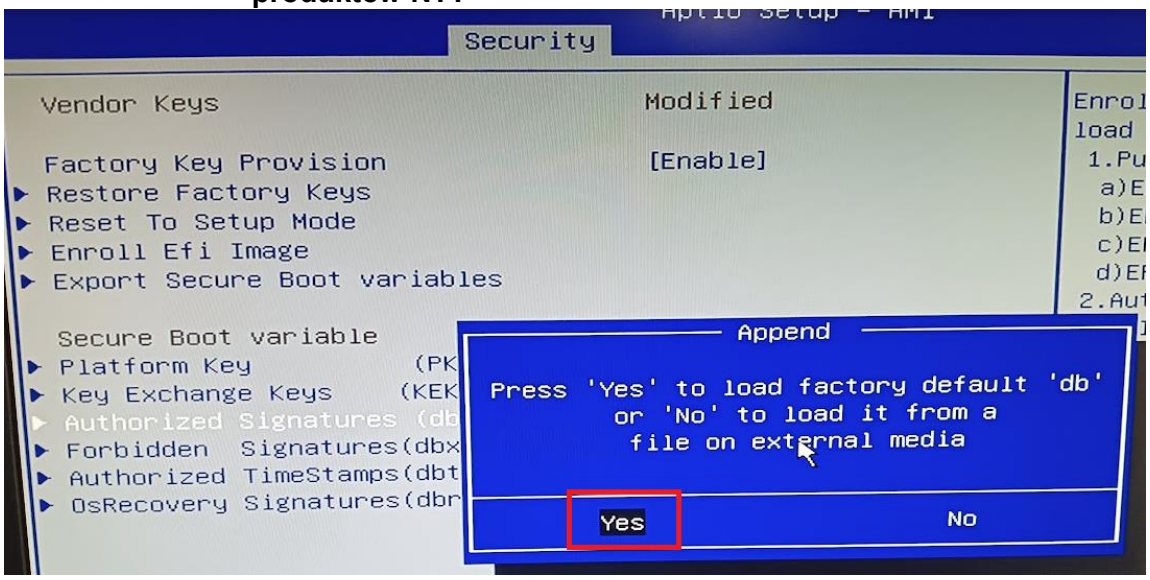


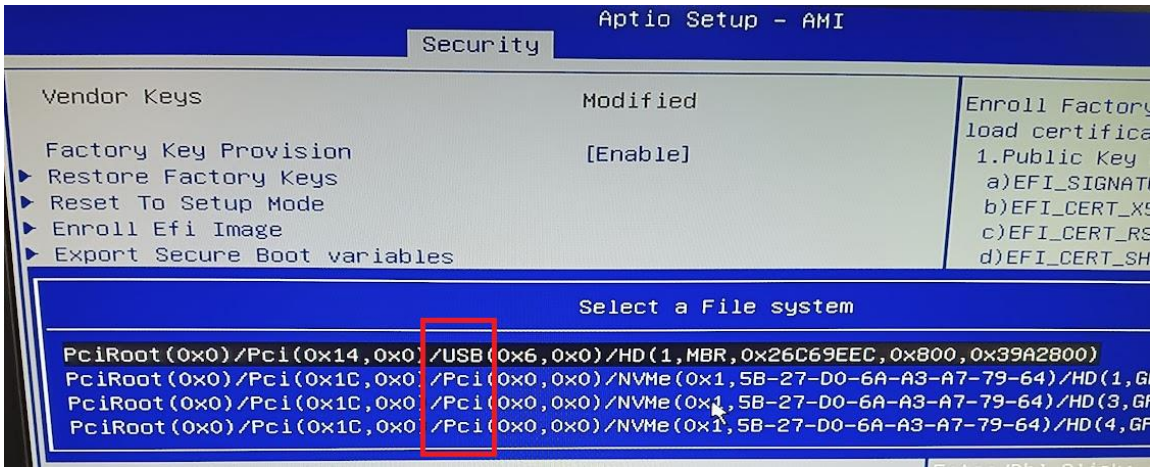
Jeśli nie jest widoczny, należy ponownie przejść proces dodawania certyfikatu zaczynając od funkcji „Key Exchange Keys”.

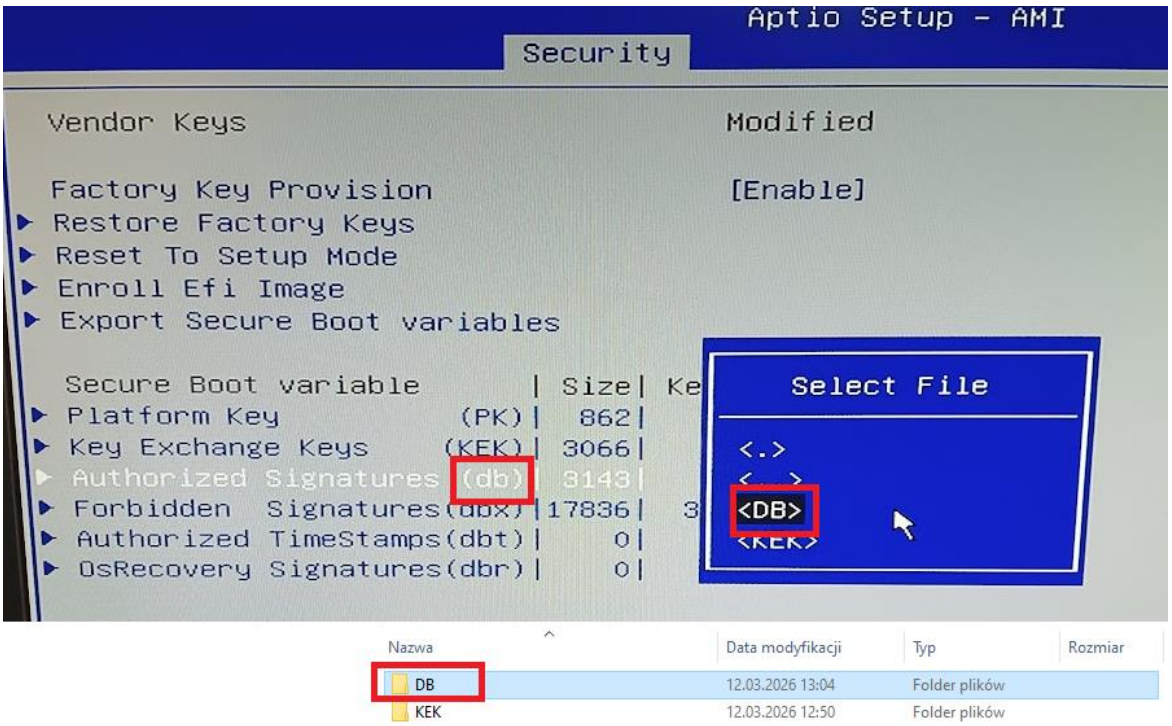
<u>Analogicznie należy dodać pozostałe trzy certyfikaty znajdujące się na urządzeniu do którego zostały wypakowane, za pomocą funkcji „Authorized Signatures (db)”.</u>





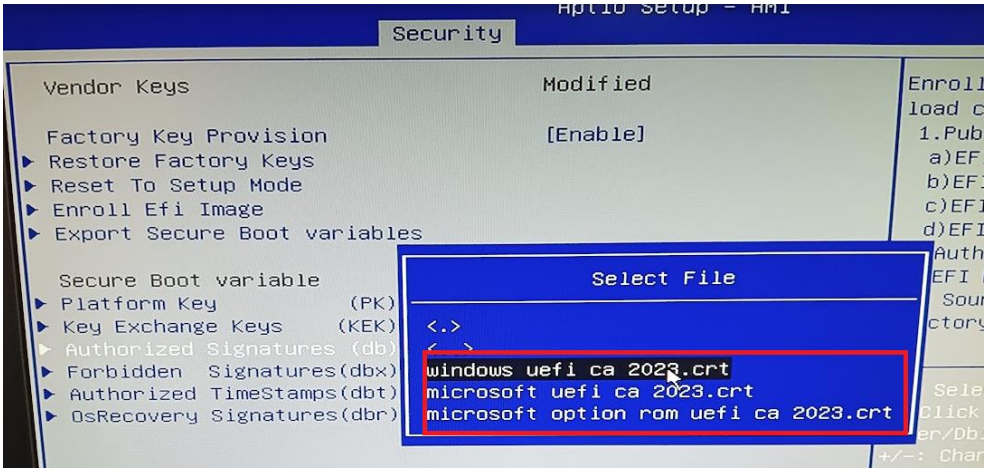


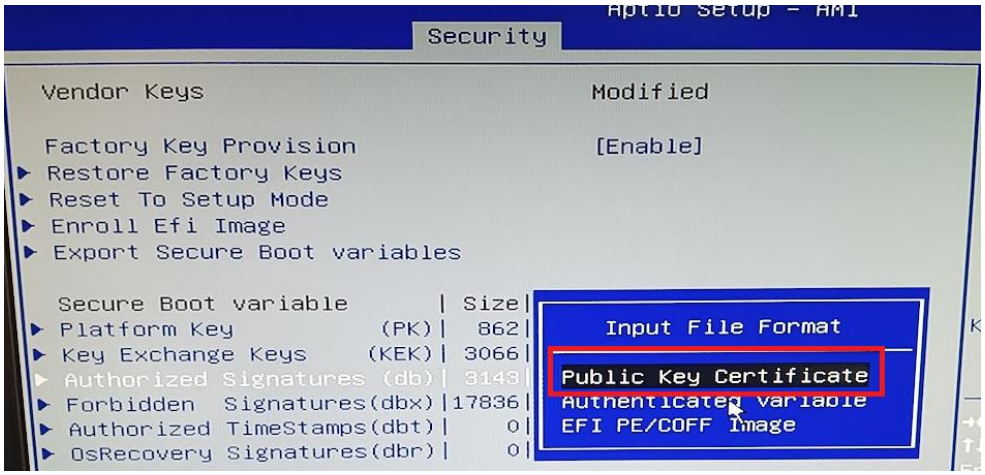


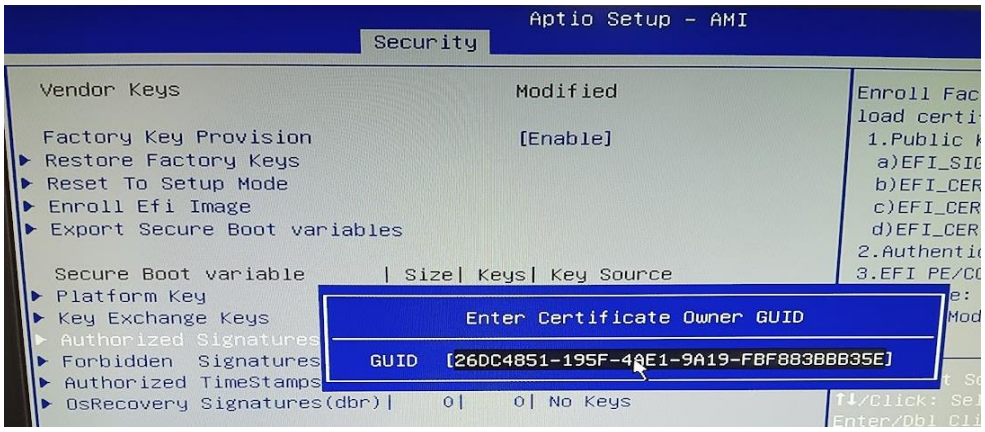


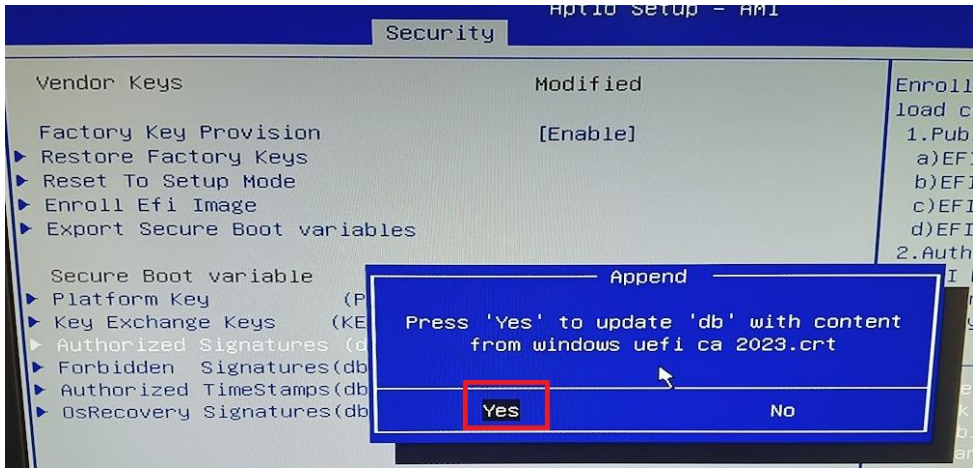
***Przykład- Authorized Signatures (db) folder DB na urządzeniu pamięci masowej**

Uwaga, funkcja Authorized Signatures (db) wymaga dodania trzech certyfikatów. Dlatego cały proces należy powtórzyć oddzielnie dla wszystkich trzech certyfikatów znajdujących się w folderze „DB”:

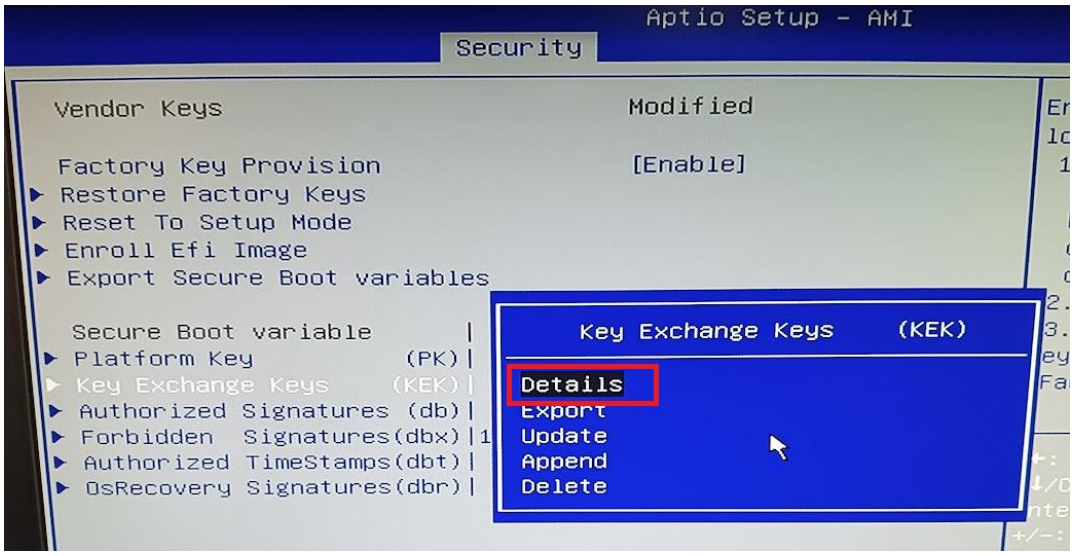


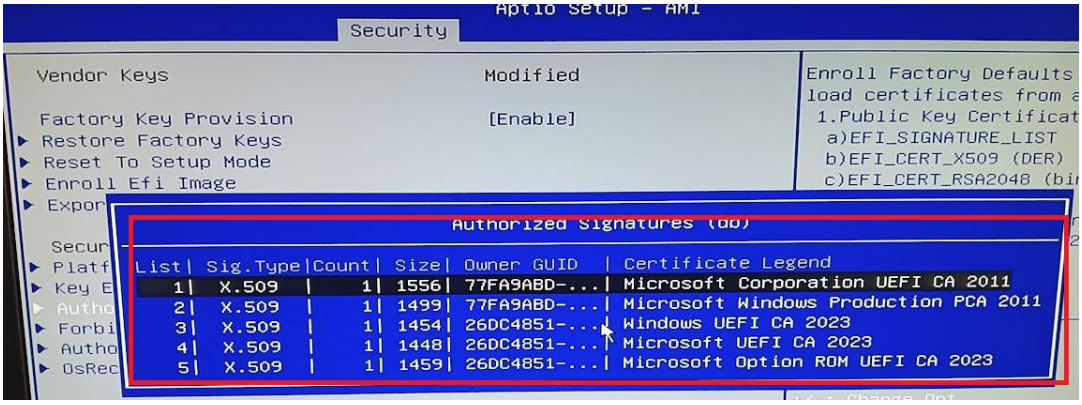






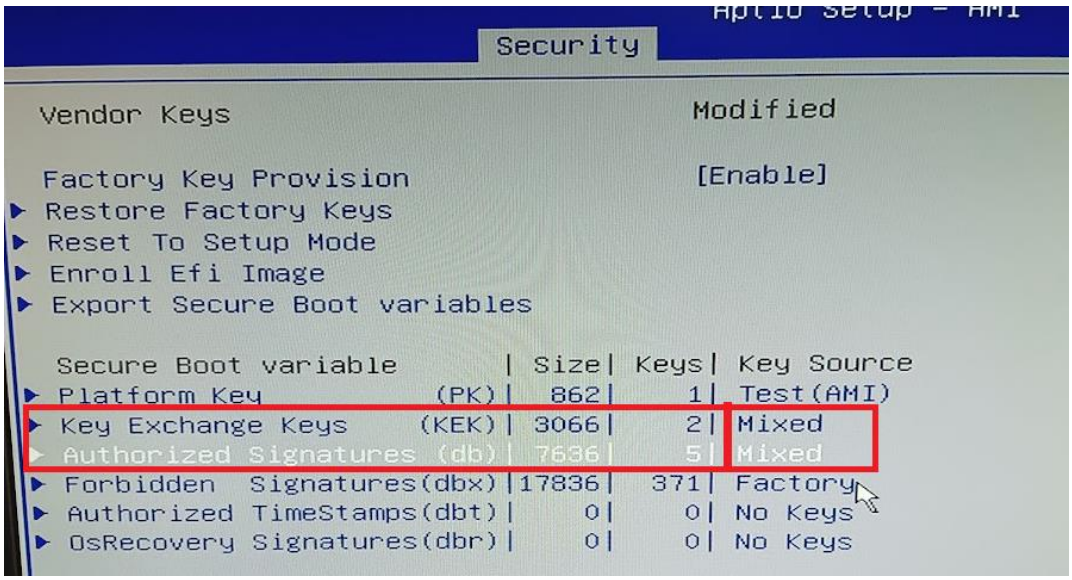
Po wybraniu „Yes” i potwierdzeniu informacji o sukcesie, należy ponownie przejść do funkcji Authorized Signatures (db) i wykonać te same kroki dla pozostałych certyfikatów znajdujących się w folderze „DB” w taki sposób, aby po wejściu do zakładki „Details” znajdowały się wszystkie zaznaczone poniżej certyfikaty:



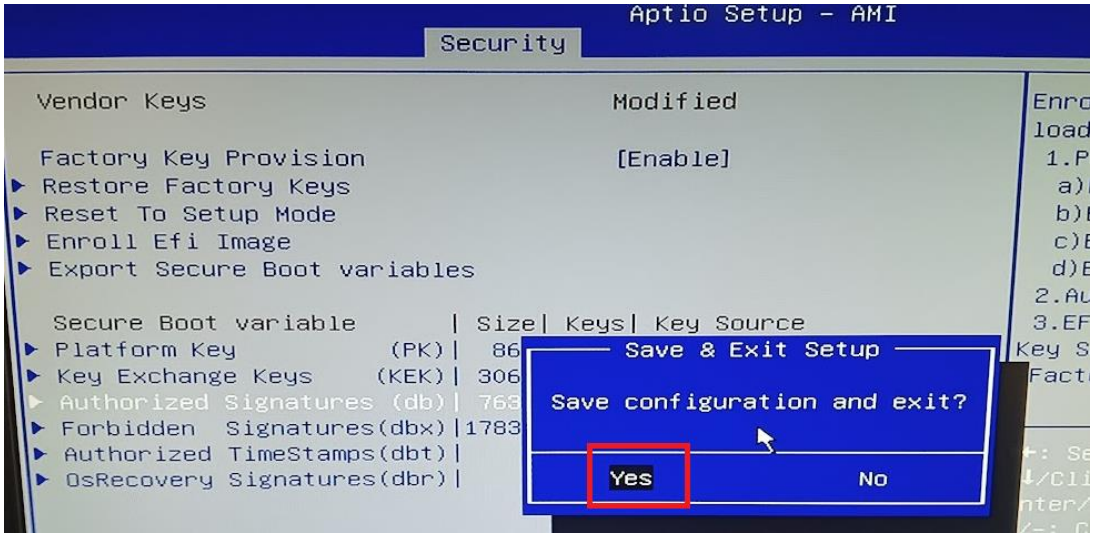


Na liście mogą znajdować się również inne certyfikaty, ale ważne jest aby lista zawierała wymienione wyżej certyfikaty.

Po poprawnym dodaniu można zauważyć, że status „Key Source” zmienił się na Mixed i zawiera minimum 5 kluczy (może być więcej).



Jeśli zawiera, należy klawiszem „F10” zapisać zmiany.



Po przeprowadzonej ręcznej aktualizacji, system Windows powinien się uruchomić bez czerwonego komunikatu.

Uwaga, każde załadowanie ustawień fabrycznych usunie ręcznie dodane certyfikaty.