



## Załącznik nr 1: Szczegółowy opis parametrów technicznych i funkcjonalności

1. Zamawiający planuje zakup kluczy sprzętowych U2F, zwanych dalej „Urządzeniami”, w jednym z dwóch wariantów:

### Wariant 1:

LP.	Nazwa produktu	Liczba
1	Klucze sprzętowe U2F (Typ C) - Klucze dla użytkowników o podwyższonym stopniu bezpieczeństwa	200
2	Klucze sprzętowe U2F (Typ A) - Klucze dla pozostałych pracowników, w tym klucze backupowe i do kont dodatkowych.	2600

### ALBO

### Wariant 2:

LP.	Nazwa produktu	Liczba
1	Klucze sprzętowe U2F (Typ C) - Klucze dla użytkowników o podwyższonym stopniu bezpieczeństwa	200
2	Klucze sprzętowe U2F (Typ B) - Klucze dla pozostałych pracowników, w tym klucze backupowe i do kont dodatkowych.	2600

2. Wykonawca zrealizuje przedmiot zamówienia w terminie **15 dni kalendarzowych** od zawarcia umowy – niezależnie od wariantu.
3. Wykonawca zobowiązuje się realizować przedmiot zamówienia zgodnie z zasadą Do No Significant Harm (DNHS), o której mowa w art. 17 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/852 Zamawiający zobowiązuje Wykonawcę do postępowania zgodnie z zasadą DNSH (z ang. „Do No Significant Harm” – tzn. Nie Czyni Znaczącej Szkody) dot. niewspierania ani nieprowadzenie działalności gospodarczej, która czyni znaczące szkody dla któregośkolwiek z celów środowiskowych, w rozumieniu art. 17 rozporządzenia (UE) 2020/852 (Rozporządzenie PE i Rady UE 2020/852 z dnia 18 czerwca 2020 r. – tzw. Taksonomii), a także wymaganiami stawianymi w ramach realizacji Krajowego Planu Odbudowy i Zwiększania Odporności.
4. Wykonawca realizując przedmiot zamówienia, zobowiązuje się do postępowania z odpadami, w tym zużytym sprzętem elektronicznym, zgodnie z obowiązującymi przepisami prawa.
5. Szczegółowy opis parametrów technicznych i funkcjonalności:



### **1) Klucz sprzętowy typu A**

1. Urządzenie musi posiadać wsparcie dla platform Microsoft Windows, Mac OS X, Linux.
2. Urządzenie musi umożliwiać współpracę z mobilnymi systemami operacyjnymi iOS oraz Android.
3. Urządzenie musi być kompatybilne z przeglądarkami: Chrome, Edge, Opera, Safari, Firefox w aktualnych wersjach.
4. Urządzenie musi być kompatybilne z serwisami: Google, Microsoft, Twitter, Facebook, Instagram, YouTube.
5. Urządzenie musi posiadać możliwość potwierdzenia logowania dotknięciem przycisku - obowiązkowa interakcja użytkownika podczas logowania.
6. Urządzenie musi posiadać złącze USB-C.
7. Urządzenie musi posiadać moduł NFC.
8. Urządzenie musi obsługiwać protokoły FIDO2/WebAuthn, FIDO U2F, karta inteligentna (PIV), OTP, OATH-TOTP, OATH-HOTP, statyczne hasło i Challenge-Response.
9. Urządzenie musi posiadać wsparcie dla PKCS#11.
10. Urządzenie musi obsługiwać algorytmy kryptograficzne: RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384.
11. Urządzenie musi być odporne na zgniecenie.
12. Urządzenie musi posiadać klasę szczelności min. IP68.
13. Urządzenie do działania nie może wymagać baterii.
14. Urządzenie do działania nie może wymagać połączenia internetowego.
15. Urządzenie nie może być typem pendrive, czyli posiadać miejsce do przechowywania danych: pliki, katalogi.
16. Urządzenie nie może działać po Bluetooth.
17. Urządzenie musi posiadać możliwość wygrawerowania loga/kodu.
18. Urządzenie musi być tak fizycznie skonstruowane, by uniemożliwić jego rozłożenie na części i ponowne złożenie.
19. Urządzenie nie może obsługiwać logowania za pomocą biometrii.
20. Urządzenie musi umożliwiać przechowywanie na nim kodów OTP, zamiast np. w aplikacji mobilnej.
21. Do działania Urządzenia nie mogą być potrzebne żadne dodatkowe sterowniki wymagające samodzielnego pobrania i instalacji nadzorowanej przez użytkownika.
22. Urządzenie musi posiadać specjalne oczko umożliwiające zawieszenie urządzenia.
23. Urządzenie musi być wyprodukowane w Unii Europejskiej.

24. Urządzenie musi być objęte co najmniej 12 miesięczną gwarancją producenta Urządzenia.
25. Urządzenie powinno działać prawidłowo z konfiguracją serwera VPN na urządzeniach Fortinet.
26. Wraz z Urządzeniem ma być dostarczona przejściówka z USB-C na USB-A.

## **2) Klucz sprzętowy typu B**

1. Urządzenie musi posiadać wsparcie dla platform Microsoft Windows, Mac OS X, Linux.
2. Urządzenie musi umożliwiać współpracę z mobilnymi systemami operacyjnymi iOS oraz Android.
3. Urządzenie musi być kompatybilne z przeglądarkami: Chrome, Edge, Opera, Safari, Firefox w aktualnych wersjach.
4. Urządzenie musi być kompatybilne z serwisami: Google, Microsoft, Twitter, Facebook, YouTube.
5. Urządzenie musi posiadać możliwość potwierdzenia logowania dotknięciem przycisku - obowiązkowa interakcja użytkownika podczas logowania.
6. Urządzenie musi posiadać złącze USB-C.
7. Urządzenie musi posiadać moduł NFC.
8. Urządzenie musi obsługiwać protokoły FIDO2/WebAuthn, FIDO U2F.
9. Urządzenie musi obsługiwać algorytmy kryptograficzne: ECC p256, ECC p384.
10. Urządzenie musi być odporne na zgniecenie.
11. Urządzenie musi posiadać klasę szczelności IP68.
12. Urządzenie do działania nie może wymagać baterii.
13. Urządzenie do działania nie może wymagać połączenia internetowego.
14. Urządzenie nie może być typem pendrive, czyli posiadać miejsce do przechowywania danych: pliki, katalogi.
15. Urządzenie nie może działać po Bluetooth.
16. Urządzenie musi posiadać możliwość wygrawerowania loga/kodu.
17. Urządzenie musi być tak fizycznie skonstruowane, by uniemożliwić jego rozłożenie na części i ponowne złożenie.
18. Urządzenie nie może obsługiwać logowania za pomocą biometrii.
19. Do działania Urządzenia nie mogą być potrzebne żadne dodatkowe sterowniki wymagające samodzielnego pobrania i instalacji nadzorowanej przez użytkownika.

20. Urządzenie musi posiadać specjalne oczko umożliwiające zawieszenie urządzenia.
21. Urządzenie musi być wyprodukowane w Unii Europejskiej.
22. Urządzenie musi być objęte co najmniej 12 miesięczną gwarancją producenta Urządzenia.
23. Wraz z Urządzeniem ma być dostarczona przejściówka z USB-C na USB-A.

### 3) Klucz sprzętowy typu C

1. Urządzenie musi posiadać wsparcie dla platform Microsoft Windows, Mac OS X, Linux.
2. Urządzenie musi umożliwiać współpracę z mobilnymi systemami operacyjnymi iOS oraz Android.
3. Urządzenie musi być kompatybilne z przeglądarkami: Chrome, Edge, Opera, Safari, Firefox w aktualnych wersjach
4. Urządzenie musi być kompatybilne z serwisami: Google, Microsoft, Twitter, Facebook, YouTube.
5. Urządzenie musi posiadać możliwość potwierdzenia logowania dotknięciem przycisku - obowiązkowa interakcja użytkownika podczas logowania.
6. Urządzenie musi posiadać złącze USB-C.
7. Urządzenie musi obsługiwać protokoły FIDO2/WebAuthn, FIDO U2F.
8. Urządzenie musi obsługiwać algorytmy kryptograficzne: ECC p256, ECC p384.
9. Urządzenie musi być odporne na zgniecenie.
10. Urządzenie musi posiadać klasę szczelności IP68.
11. Urządzenie do działania nie może wymagać baterii.
12. Urządzenie do działania nie może wymagać połączenia internetowego.
13. Urządzenie nie może być typem pendrive, czyli posiadać miejsce do przechowywania danych: pliki, katalogi.
14. Urządzenie nie może działać po Bluetooth.
15. Urządzenie musi posiadać możliwość wygrawerowania loga/kodu.
16. Urządzenie musi być tak fizycznie skonstruowane, by uniemożliwić jego rozłożenie na części i ponowne złożenie.
17. Urządzenie musi obsługiwać logowanie za pomocą biometrii
18. Do działania Urządzenia nie mogą być potrzebne żadne dodatkowe sterowniki wymagające samodzielnego pobrania i instalacji nadzorowanej przez użytkownika.



19. Urządzenie musi posiadać specjalne oczko umożliwiające zawieszenie urządzenia.
20. Urządzenie musi być wyprodukowane w Unii Europejskiej.
21. Urządzenie musi być objęte co najmniej 12 miesięczną gwarancją producenta Urządzenia.
22. Wraz z Urządzeniem ma być dostarczona przejściówka z USB-C na USB-A.

Zamówienie dofinansowane ze środków Unii Europejskiej, Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności; Inwestycja: C3.1.1.

Cyberbezpieczeństwo - CyberPL , infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; Cyberbezpieczeństwo - Cyberbezpieczny Rząd – w ramach projektu pn. „Cyberbezpieczeństwo w PIP”, na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10- CR.01-001/24/0036/KPOD.05.10- CR.01-001/25/2025