Warszawa, 01-09-2021 r.

Nazwa projektu: *Wysoce konfigurowalne rozwiązanie eSignature dla szkolnictwa wyższego" (eSignForStudy). Numer INEA/CEF/ICT/A2020/2271208*

WYKONAWCY
Strona internetowa

WYJAŚNIENIE
treści zapytania ofertowego w postępowaniu nr WMIM/ZP-371/38-07/2021
na dostawę sieciowego urządzenia serwerowego z modułem kryptograficznym (HSM)

Zamawiający informuje, że w przedmiotowym postępowaniu wpłynęły pytania do treści Zapytania ofertowego z dnia 26 sierpnia 2021 r., zwanego dalej *Zapytaniem*, na które udziela się następujących odpowiedzi.

Pytanie 1. *W Zapytaniu zapisali Państwo, że HSM ma mieć certyfikację normy FIPS 140-2 lub FIPS 140-3 i jednocześnie mieć zgodność z eIDAS i być na liście kwalifikowanych urządzeń do tworzenia podpisów i pieczęci Unii Europejskiej. Takich urządzeń nie ma na rynku.*
Wszystkie urządzenia, które są zgodne z eIDAS i mogą się dostać na listę, muszą mieć certyfikacje Common Criteria Protection Profile 419 221-5. Nie ma także urządzeń, które mają równocześnie certyfikacje FIPS oraz Common Criteria. Prosimy o wyjaśnienie tej rozbieżności.
Odpowiedź Według wiedzy Zamawiającego na rynku są dostępne urządzenia HSM posiadające jednocześnie dwie certyfikacje. Zamawiający oczekuje dostarczenia takiego urządzenia.
Jednocześnie Zamawiający wymaga, w zależności od potrzeb, możliwości konfiguracji urządzenia w trybie zgodności z certyfikacją: FIPS 140-3 lub FIPS 140-3 albo eIDAS/Comonn Criteria z profilem bezpieczeństwa 419 221-5.

Pytanie 2. *Punkt k) Urządzenie powinno pozwalać na całkowitą zdalną administrację bez konieczności asysty operatorów przy urządzeniu.*
Czy Zamawiający przewiduje możliwość niezdalnego wyłączania i włączania prądu i inicjalnie nastawiania np.: adresu IP, żeby HSM był dostępny w sieci i być zgodnym z tym wymaganiem?
Odpowiedź Zamawiający podtrzymuje wymaganie wyspecyfikowane w pkt. k.

Pytania 3. *Punkt o) Moduł HSM musi posiadać możliwość ładowania własnego kodu wykonywalnego, który jest uruchamiany wnętrz modułu HSM i pozwala rozszerzyć funkcje urządzenia HSM. Wraz z urządzeniem musi zostać dostarczony pakiet dla programistów (SDK) pozwalający na tworzenie, kompilowanie i ładowanie takiego kodu.*

The sole responsibility of this publication lies with the project consortium. The European Union is not responsible for any use that may be made of the information contained therein.

Co-financed by the Connecting Europe Facility of the European Union

INEA/CEF/ICT/A2020/2271208

HSM zgodne z eIDAS i certyfikacją Common Criteria Protection Profile 419 221-5 nie mają ani prawnej, ani technicznej możliwości ładowania własnego kodu na urządzenie.
HSM zgodne z FIPS 140-2 lub FIPS 140-3 mają, ale nie są na liście ww. ani nie można na nie wydać pieczęci kwalifikowanej.
Prosimy o wyjaśnienie i doprecyzowanie wymagania.
Odpowiedź
Certyfikacja Common Criteria Protection Profile 419 221-5 nie definiuje i nie wyklucza posiadania funkcjonalności opisanej w punkcie o).

Pytanie 4.
Punkt 2c. HSMy w dzisiejszych czasach nie wspierają skrótu SHA-1. W modelach zgodnych z eIDAS jak i FIPS tą funkcja nie jest dostępna w żadnym certyfikowanym modelu.
Prosimy o wyjaśnienie i doprecyzowanie wymagania lub modyfikację.
Odpowiedź
Zamawiający rezygnuje z wymagania funkcji skrótu SHA-1.

Pytanie 5.
Czy karty inteligentne i czytnik kart, jedno i drugie jest konieczne do zarządzania HSM, ma być także dostarczone w ramach zamówienia?
Odpowiedź
Zamawiający nie wymaga dostawy kart i czytników kart inteligentnych w ramach zamówienia.

Pytanie 6.
Czy w ramach zamówienia oczekują Państwo szkolenia? Jeśli tak, prosimy o podanie liczby osób na szkolenie.
Odpowiedź
Zamawiający nie oczekuje szkolenia.

Pytanie 7.
Czy w ramach zamówienia oczekują Państwo wsparcia przy wdrożeniu?
Odpowiedź
Zamawiający nie oczekuje wsparcia przy wdrożeniu.

Pytanie 8.
Czy w ramach zamówienia ma być dostarczona pieczęć kwalifikowana na HSM zgodna z certyfikacją Common Criteria Protection Profile 419 221-5?
Odpowiedź
Tak, zamawiający wymaga dostawy pieczęci kwalifikowanej na dostarczany HSM ważnej 2 lata wraz ze zdalnym wsparciem technicznym zgodnej z certyfikacją Common Criteria Protection Profile 419 221-5.

W związku z wyjaśnieniami termin składania ofert, o którym mowa w Rozdziale VI Zapytania upływa w dniu **8 września 2021 r.** o godz. $12^{\underline{00}}$.

Co-financed by the Connecting Europe Facility of the European Union

INEA/CEF/ICT/A2020/2271208