**Załącznik nr 1 do Zaproszenia**

**Opis przedmiotu zamówienia**

1. **Produkt** – programowa implementacja modułu autoryzacji podpisu o następujących cechach:
* umożliwia zdalne zarządzanie produktem uwierzytelnionemu Administratorowi (tworzenie Użytkowników, konfigurowanie produktu),
* umożliwia zdalne wykonanie podpisu cyfrowego uwierzytelnionemu Użytkownikowi, jedynie na danych przekazanych przez Użytkownika,
* komunikacja z produktem jest zapewniona z wykorzystaniem protokołu AMQP (implementacja RabbitMQ, zabezpieczony TLS).
1. **Założenia**
2. Zakłada się przyjęcie metodyki analizy podatności oraz demonstracji scenariuszy ataku zgodnie z Common Criteria. Za określenie metodyki odpowiedzialny jest Zamawiający. Zamawiający oczekuje od Wykonawcy znajomości i umiejętności zastosowania dedykowanych metodyk, takich jak: OWASP Application Security Verification Standard (ASVS), Penetration Testing Execution Standard (PTES), Open Security Testing Methodology Manual (OSTMM), NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.
3. Zespól Wykonawcy ma charakter ekspercki. Zakres wsparcia oferowanego przed zespół Wykonawcy obejmuje wkład do raportu, za którego treść odpowiedzialny pozostaje Zamawiający.
4. **Zakres wsparcia obejmuje:**
	1. identyfikację podatności, w tym przeszukiwanie baz znanych podatności,
	2. identyfikację możliwych podatności i/lub niepoprawnych konfiguracji produktu, na podstawie dostępnej dokumentacji, w tym dokumentacji testów bezpieczeństwa dewelopera, testów wykonanych przez Zamawiającego, oraz wiedzy eksperckiej Wykonawcy,
	3. analiza tzw. area of concern, pod kątem potencjalnych podatności, z wykorzystaniem udostępnionej przez Zamawiającego dokumentacji produktu,
	4. analiza kodu źródłowego produktu, zachowania/działania produktu, pod kątem wykrycia ewentualnych podatności,
	5. opracowanie zakresu ogólnego procesu *network protocol fuzzing*, jak również *fuzzing* dedykowanego dla protokołu AMQP,
	6. opracowanie scenariuszy ataków oraz ich adaptacja z uwzględnieniem wyników pośrednich,
	7. w szczególności, scenariusze ataków mogą dotyczyć:
		1. podatności zaimplementowanej funkcjonalności TLS,
		2. podatności procesów zarządzania sesją, uwierzytelnianiem i autoryzacją Użytkownika/Administratora;
		3. ataków kryptograficznych na mechanizmy szyfrowania, podpisu cyfrowego i znaczników czasowych (w tym metody identyfikacji podatnych komponentów w funkcjach kryptograficznych produktu).
5. **Ponadto, zakres wsparcia obejmuje:**
	1. Konsultacje w zakresie doboru i konfiguracji narzędzi w środowisku testowym produktu znajdującego się w siedzibie Zamawiającego,
	2. Konsultacje dotyczące wykonania opracowanych scenariuszy ataków lub asysta dla Zamawiającego przy wykonaniu części ataków,
	3. Konsultacje dotyczące właściwego udokumentowania danych wejściowych, przebiegu oraz rezultatów poszczególnych scenariuszy ataków.
6. **Rezultaty usługi wsparcia:**

Celem realizacji usług wsparcia jest wykazanie odporności/braku odporności na ataki zdefiniowane w scenariuszach ataków.

1. **Wynagrodzenie za usługi wsparcia**
	1. Zryczałtowana cena obejmuje następujące usługi:
		1. pakiet 200 roboczogodzin usługi wsparcia w celu realizacji pkt 3 i 4
		2. minimum 4 sesji warsztatowych (szkoleń) o długości 4 godzin każda dla zespołu Zamawiającego, w trakcie i po wykonaniu części usług wsparcia przedstawionych w pkt. 3 i 4. Celem warsztatów jest przekazanie Zamawiającemu wiedzy i umiejętności zastosowania zdefiniowanych scenariuszy ataków w odniesieniu do produktów IT o funkcjonalności zbliżonej jednakże innej niż funkcjonalność Produktu.
	2. Dodatkowe pakiety po 50 roboczogodzin (maksymalnie dwa), realizowane po uprzednim wskazaniu przez Zamawiającego potrzeby uruchomienia dodatkowego pakietu w celu zapewnienia pogłębionego wsparcia w obszarze niezidentyfikowanym na etapie opracowania opisu przedmiotu zamówienia – cena jednostkowa dodatkowego pakietu.
2. **Dodatkowe warunki dotyczące realizacji usługi wsparcia**
	1. Prace koncepcyjne i przygotowawcze mogą być realizowane w miejscu wg uznania Wykonawcy.
	2. Zapoznanie się i analiza dokumentacji może odbywać się wyłącznie w systemie wspomagającym działalność laboratoryjną Zamawiającego, znajdującym się w siedzibie Zamawiającego. W wyjątkowych wypadkach, zapoznanie się z dokumentacją może odbywać się na specjalnie zabezpieczonych stacjach roboczych, udostępnionych przez Zamawiającego.
	3. Prace testowe lub realizacja scenariuszy testowych może odbywać się wyłącznie w siedzibie Zamawiającego, w środowisku testowym Produktu.
	4. Wszelka komunikacja z zespołem Zamawiającego może odbywać się za pośrednictwem bezpiecznych kanałów komunikacyjnych, w tym z wykorzystaniem narzędzi PGP/GPG oraz systemu telekonferencyjnego, będącego pod kontrolą Zamawiającego.
	5. Wskazany przez Zamawiającego efekt prac Wykonawcy zostanie przedstawiony w formie pisemnej, w języku angielskim.
3. **Termin realizacji**
	1. Część usług opisana w pkt. 6 a) i) i b) powinna zostać zrealizowana do 31.05.2022.
	2. Część usług opisana w pkt. 6 a) ii) powinna zostać zrealizowana do 30.06.2022.
4. **Wybór oferty**
	1. Cr: cena zryczałtowana za godziny usług wsparcia wskazane w pkt. 6a) i) oraz ii)

Cr = (Cena oferty najniższej/cena oferty ocenianej)\*50

**Maksymalna wartość Cr = 50**

* 1. Cp – cena zryczałtowana za pakiet godzin usług wsparcia wskazany w pkt. 6b)

Cp = (Cena oferty najniższej/cena oferty ocenianej)\*20

**Maksymalna wartość Cp = 20**

* 1. S: Szkolenia wskazane w pkt. 6a) ii)

S = wybór z [10, 20, 30]

Mniej niż 4 sesje – oferta podlega odrzuceniu

4 sesje – 0 pkt

5 sesji – 10 pkt

6 sesji – 20 pkt

7 sesji - 30 pkt

**Maksymalna wartość S = 30**

* 1. Najkorzystniejsza ekonomicznie oferta: najwyższa wartość z (Cr+Cp+S)