

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup **certyfi­katów niekwalifiko­wanych** niezbędnych **do komunikacji z Węzłem Krajowym**.
2. Na potrzeby komunikacji systemu Zamawiającego z Węzłem Krajowym (system login.gov.pl) Zamawiający wymaga zestawu certyfi­katów (2 sztuki), ze specjalnymi kluczami na krzywych eliptycznych, co jest wymogiem Węzła Krajowego, służące do:
 - Podpisywania żądań,
 - Deszyfracji asercji.
3. Certyfikaty muszą spełniać następujące **wymagania** (zgodnie z wymaganiami Ministerstwa Cyfryzacji):
 - 1) Algorytm podpisu ECDSA with SHA256;
 - 2) Krzywa eliptyczna: NIST Curve P-256;
 - 3) Długość klucza prywatnego: 256 bit;
 - 4) Zgodność ze standardem X.509 v.3 (RFC5280);
 - 5) Zabezpieczony funkcją skrótu SHA2;
 - 6) Wysoki poziom zaufania gwarantujący jednoznacz­ną identyfikację użytkownika/właściciela, na którego wystawiono certyfi­kat;
 - 7) Wymagane rozszerzenie Key Agreement dla certyfikatu do deszyfracji;
 - 8) Wymagane rozszerzenie Digital Signature dla certyfikatu do podpisu;
 - 9) Wymaganie adresu OCSP dla certyfikatu do deszyfracji i podpisu;
 - 10) Wymaganie adresu CRL dla certyfikatu do deszyfracji i podpisu.
4. Okres ważności certyfikatu : 24 miesiące.
5. Przedmiot zamówienia zostanie dostarczony w terminie maksymalnie 3 dni roboczych od dnia złożenia zamówienia lub zawarcia umowy.