

## Bezpieczeństwo danych w telefonach i tabletach

### 1. Kryteria i wymagania o charakterze innym niż cena lub koszt związane z bezpieczeństwem danych dla telefonów i tabletów

- 1) Stosowanie przez Zamawiających wymagań OPZ lub dodatkowo punktowanych w ramach kryteriów zapisów, **zgodnie z którymi producent urządzenia ma zapewnić odpowiedni poziom bezpieczeństwa** poprzez:
    - a) Oświadczenie producenta, że oferowane urządzenia posiadają certyfikat zgodności z normą Common Criteria (CC) jako podstawowe wymaganie bezpieczeństwa teleinformatycznego – wymóg rekomendowany.
    - b) Oświadczenie producenta, że oferowane inne produkowane przez niego urządzenia w tej samej kategorii produktowej (telefony/tablety/komputery itp.) posiadają certyfikat zgodności z normą Common Criteria (CC) – wymóg minimalny, ale zapewniający o poziomie bezpieczeństwa samego procesu produkcyjnego.
  - 2) Stosowanie przez Zamawiających wymagań w OPZ lub dodatkowe punktowanie w ramach kryteriów zapisów, które **wymuszają szyfrowanie danych na urządzeniu oraz zabezpieczenie dostępu do urządzenia** za pomocą co najmniej PIN-u, hasła o odpowiednim poziomie skomplikowania lub metod biometrycznych.
  - 3) Stosowanie przez Zamawiających wymagań w OPZ lub dodatkowe punktowanie w ramach kryteriów zapisów, zgodnie z którymi **urządzenie powinno umożliwiać przechowywanie danych wrażliwych w izolowanym kontenerze będącym oddzielną przestrzenią roboczą zaszyfowaną sprzętowym kluczem kryptograficznym**, wymagającą uwierzytelnienia (na przykład za pomocą biometrii).
  - 4) Stosowanie przez Zamawiających wymagań w OPZ lub dodatkowe punktowanie w ramach kryteriów zapisów, zgodnie z którymi **producent urządzenia powinien zapewnić narzędzia do monitorowania i zdalnego wymuszania instalacji najnowszych wersji systemu operacyjnego („firmware”) na urządzeniach**, w celu zapewnienia poprawy procesów bezpieczeństwa.
  - 5) Stosowanie przez Zamawiających zapisów w OPZ lub dodatkowe punktowanie w ramach kryteriów zapisów, zgodnie z którymi **oprogramowanie urządzeń mobilnych powinno udostępniać odpowiednie interfejsy dla systemów zarządzania, monitorowania i kontroli urządzeń mobilnych („MDM”)** umożliwiające kontrolę wszystkich obszarów wykorzystania urządzeń uwzględniony w polityce bezpieczeństwa.
- ### 2. Kryteria i wymagania o charakterze innym niż cena lub koszt dotyczące bezpieczeństwa Oprogramowania (Wymaganie stosowane przykładowo przez Centrum Informatyki Resortu Finansów).
- 1) Oprogramowanie lub sprzęt wykorzystywane do świadczenia usługi nie może być zabronione do stosowania przez administrację któregokolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).

- 2) Oprogramowanie lub sprzęt wykorzystywane do świadczenia usługi nie może być czasowo wstrzymane do stosowania przez administrację któregośkolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
- 3) Oprogramowanie wykorzystane do świadczenia usługi musi być na aktualnej liście oprogramowania dopuszczonego do kupowania lub stosowania przez administrację każdego z Państw członkowskich NATO (North Atlantic Treaty Organization) jeśli w porządku prawnym tego/tych krajów stosuje się takie listy.

#### Przykład zamówienia

Zakup usługi kompleksowej ochrony bramy internetowej oraz stacji roboczych i serwerów. Znak sprawy PN/38/18/AQOO (Zamawiający: Centrum Informatyki Resortu Finansów).