Warunki korzystania z certyfikatów TLS/SSL

Zamawiając certyfikat SSL Zamawiający zobowiązuje się do:

1. dostarczania do KIR prawdziwych i dokładnych informacji dotyczących danych podmiotu certyfikatu (subskrybenta) przez cały okres ważności certyfikatu w postaci zarówno danych zawartych w zamówieniu, jak również danych zawartych w żądaniu wygenerowania certyfikatu zawierającym klucz publiczny, dla którego ma być przygotowany certyfikat;
2. ochrony klucza prywatnego powiązanego z kluczem publicznych, dla którego KIR wyda certyfikat poprzez kontrolowanie używania klucza prywatnego, zapewnienie poufności klucza prywatnego, zapewnienie ochrony wszelkich informacji z nim związanych;
3. weryfikacji danych zawartych w wydanym certyfikacie;
4. instalacji certyfikatu tylko na serwerze obsługującym nazwę lub nazwy domenowe wymienione w certyfikacie wydanym przez KIR;
5. stosowania certyfikatu zgodnie z prawem oraz zawartą Umową;
6. niezwłocznego zaprzestania używania certyfikatu oraz związanego z nim klucza prywatnego i zgłoszenia do KIR wniosku o unieważnienie certyfikatu w następujących przypadkach:
    a. nieprawidłowych lub nieprawdziwych danych zawartych w certyfikacie,
    b. zaistnienia podejrzenia niewłaściwego wykorzystania certyfikatu,
    c. kompromitacji klucza prywatnego,
    d. zaprzestania używania klucza prywatnego powiązanego z kluczem publicznym umieszczonym w certyfikacie w chwili wygaśnięcia certyfikatu lub jego unieważnienia,
    e. innych przewidzianych Kodeks postępowania certyfikacyjnego KIR dla zaufanych certyfikatów niekwalifikowanych;
7. postępowania zgodnie z instrukcjami przekazanymi przez KIR w przypadku kompromitacji klucza prywatnego lub użycia niezgodnie z przeznaczeniem.