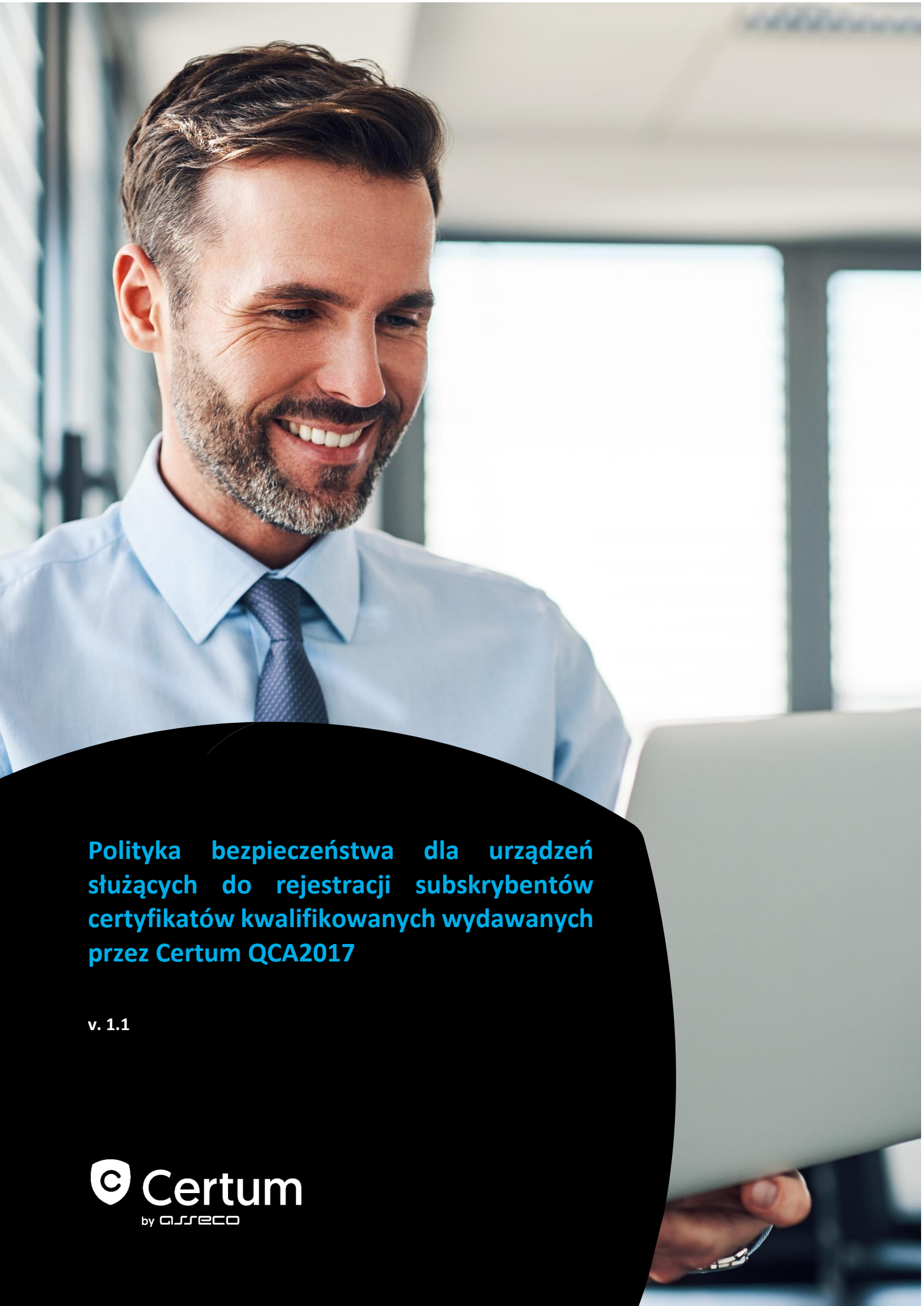

Polityka bezpieczeństwa dla urządzeń służących do rejestracji subskrybentów certyfikatów kwalifikowanych wydawanych przez Certum QCA2017

v. 1.1

Certum
by asseco

Klauzula: Prawa Autorskie

Wszelkie pytania związane z prawami autorskimi należy adresować do Asseco Data Systems S.A., ul. Jana z Kolna 11, 80-864 Gdańsk, Polska, e-mail: infolinia@certum.pl.

Spis treści

1	Urządzenie do rejestracji i identyfikacji	Urządzenie przy pomocy, którego realizowany jest proces identyfikacji (w tym zdalnej) oraz rejestracji posiadacza certyfikatu (klienta Certum).

Definicje

1	MDM	Mobile Devices Management. System do zarządzania urządzeniami mobilnymi.
2	Paperless	System wytwarzany przez Certum służący do rejestracji wniosków o wydanie certyfikatów kwalifikowanych.

1. Administracja urządzeń do identyfikacji i rejestracji

1. Urządzenia do rejestracji i identyfikacji muszą być zarządzanie przez administratorów Certum:
    a) W przypadku urządzeń mobilnych – poprzez system MDM Certum;
    b) W przypadku stacji roboczych – poprzez kontroler domeny Asseco Data Systems.
2. Za zgodą Certum dopuszczalne jest zarządzanie urządzeniami przez administratorów Partnera Certum:
    a) W przypadku urządzeń mobilnych – poprzez system MDM Partnera;
    b) W przypadku stacji roboczych – poprzez kontroler domeny Partnera.
3. Systemy MDM i kontrolery domen muszą umożliwiać wdrożenie zasad niniejszej polityki bezpieczeństwa bez możliwości zmiany zasad przez użytkownika urządzenia.

2. Ochrona danych rejestrowanych w procesie identyfikacji

1. Dane rejestrowane w procesie identyfikacji powinny być przetwarzane wyłącznie na urządzeniu w dedykowanej lokalizacji (folderze).
2. Dane rejestrowane w procesie identyfikacji nie mogą być kopiowane i przenoszone na zewnętrzne nośniki podłączone bezpośrednio do urządzenia lub online (do zdalnych nośników danych) jeśli nośniki te nie znajdują pod kontrolą Certum.
3. Dane rejestrowane w procesie identyfikacji muszą być regularnie usuwane z dedykowanej lokalizacji w sposób automatyczny, nie rzadziej niż raz na 24 godziny.

3. Wsparcie dla procesu składania zaawansowanego podpisu biometrycznego

1. Urządzenie do rejestracji i identyfikacji musi umożliwiać składanie zaawansowanego podpisu biometrycznego rejestrującego co najmniej trzy cechy biometryczne. Podpis składany jest pod oświadczeniem o wydanie certyfikatu. W tym celu urządzenie powinno rejestrować co najmniej następujące cechy:
    a) położenie rysika,
    b) dynamika prędkości rysika,
    c) nacisk rysika na ekran.

4. Wsparcie dla sprzętowej ochrony kluczy kryptograficznych

1. Urządzenie do rejestracji i identyfikacji musi umożliwiać bezpieczne przechowywanie kluczy służących do zestawienia połączenia TLS z uwierzytelnianiem klienta i serwera (2-way TLS) w lokalnym magazynie kluczy.
2. Klucze zapisane w lokalnym magazynie kluczy powinny być chronione sprzętowo, bez możliwości ich eksportu poza urządzenie. Import kluczy do magazyny powinien być możliwy z poziomu systemu MDM lub kontrolera domeny.
3. Przeglądarka przy pomocy, której użytkownik łączy się z systemem Paperless, powinna wspierać nawiązanie sesji TLS z uwierzytelnianiem klienta przy pomocy kluczy zapisanych w lokalnym magazynie kluczy.

5. Zarządzanie aktualizacjami systemowymi (w tym poprawkami bezpieczeństwa)

1. Urządzenia do identyfikacji i rejestracji powinny mieć zainstalowane wszystkie udostępnianie przez producenta aktualizacje systemowe, w tym poprawki bezpieczeństwa.
2. Zainstalowane aktualizacje bezpieczeństwa powinny eliminować podatności krytyczne i wysokie.
3. Zainstalowane aktualizacje bezpieczeństwa powinny być nie starsze niż 6 miesięcy.
4. W przypadku gdy aktualizacje bezpieczeństwa nie są wydawane przez dostawcę urządzenia, może być ono wykorzystane do komunikacji z systemami Certum, o ile wprowadzone zostaną alternatywne, zaakceptowane przez Certum, zabezpieczenia mitygujące prawdopodobieństwo wystąpienia ataków na integralność lub niezaprzeczalność procesu identyfikacji lub rejestracji.
5. Zabezpieczenia określone w pkt. 4 będą podlegały okresowym przeglądom w ramach analizy ryzyka. Jeśli poziom ryzyka wzrośnie i przestanie być akceptowalny przez Certum, Certum zastrzega sobie prawo do wycofania urządzeń z użytkowania w trybie natychmiastowym.

6. Akceptacja urządzeń do identyfikacji i rejestracji przez Certum

1. Urządzenie do identyfikacji i rejestracji podlegają ewidencji i akceptacji przez administratorów Certum.
2. Każdy nowy model urządzenia, przed wprowadzeniem do eksploatacji powinien być notyfikowany u administratorów Certum wraz z oświadczeniem, że spełnia wszystkie wymagania niniejszej polityki.
3. Notyfikowane urządzenie, po akceptacji przez administratorów Certum, może być używane w procesach identyfikacji i rejestracji dopiero po zainstalowaniu na nim klucza służącego do nawiązania dwustronnego uwierzytelniania TLS z modułem podpisywania wniosków o wydanie certyfikatów kwalifikowanych.
4. Instalację klucza przeprowadzają administratorzy Certum lub administratorzy Partnera wyłącznie na zaakceptowanych urządzeniach.

7. Usuwanie urządzeń do identyfikacji i rejestracji przez Certum

1. W przypadku naruszenia niniejszej polityki bezpieczeństwa administratorzy Certum mogą bez ostrzeżenia unieważnić certyfikat TLS służący do nawiązywania bezpiecznego połączenia z modułem podpisywania wniosków o wydanie certyfikatów kwalifikowanych.