Jak poprawnie przygotować żądanie CSR?

ZANIM ZACZNIESZ

Do przygotowania kluczy i podpisania żądania wymagane jest oprogramowanie klasy OpenSSL. Zalecane jest używanie aktualnej, stablinej wersji.
Na rynku istnieje również wiele alternatywnych rozwiązań np. KeyStore Explorer, Google Tink itp. Poniższa instrukcja opiera się na openSSL i zakłada, że na komputerze jest już prawidłowo zainstalowany software. Komendy mają przykładowy charakter. Należy zwrócić szczególną uwagę na nazwy tworzonych plików. Powielanie komend może spowodować nadpisywanie danych!

W przypadku żądania do certyfikatu OV potrzebna będzie również aplikacja Szafir do podpisania żądania CSR w formacie CAdES PKCS#7.

GENEROWANIE ŻĄDANIA CERTYFIKATU DV

Dla nowej pary kluczy
Za pomocą jednej komendy wygeneruj klucz prywatny w pliku: key.pem oraz żądanie CSR w pliku req.pem.
Dla certyfikatu DV jedynym polem w temacie certyfikatu jest CN. Ta sama wartość musi być również zawarta w rozszerzeniu subjectAltName.
openssl req -new -subj "/CN=domena-testowa.pl" -addext "subjectAltName = DNS:domena-testowa.pl" -newkey rsa:2048 -keyout key.pem -out req.pem –nodes

Dodatkowe domeny można określić w powyższej komendzie, zmieniając odpowiednio przełącznik -addext:

-addext "subjectAltName = DNS:domena-testowa.pl,DNS:subdomena1.domena-testowa.pl,DNS:subdomena2.domena-testowa.pl"

Dla istniejącej pary kluczy

openssl req -new -subj "/CN=domena-testowa.pl" -addext "subjectAltName = DNS:domena-testowa.pl" -key key.pem -out req.pem

GENEROWANIE I PODPISANIE ŻĄDANIA CERTYFIKATU OV

Dla nowej pary kluczy

Za pomocą jednej komendy wygeneruj klucz prywatny w pliku: key.pem oraz żądanie CSR w pliku req.pem.

Dla OV, w temacie certyfikatu, oprócz nazwy własnej CN podaj obowiązkowo pola C - kraj (country), ST - województwo (state), L -miejscowość (locality), O - nazwa organizacji (organization). Domena podana w nazwie własnej musi być również zawarta w rozszerzeniu subjectAltName.

openssl req -new -utf8 -subj "/C=PL/ST=mazowieckie/L=Warszawa/O=Nazwa Organizacji/CN=domena-testowa.pl" -addext "subjectAltName = DNS:domena-testowa.pl" -newkey rsa:2048 -keyout key.pem -out req.pem –nodes

Dodatkowe domeny można określić w powyższej komendzie, zmieniając odpowiednio przełącznik -addext:

-addext "subjectAltName = DNS:domena-testowa.pl,DNS:subdomena1.domena-testowa.pl,DNS:subdomena2.domena-testowa.pl"

Dla istniejącej pary kluczy

openssl req -new -utf8 -subj "/C=PL/ST=mazowieckie/L=Warszawa/O=Nazwa Organizacji/CN=domena-testowa.pl" -addext "subjectAltName = DNS:domena-testowa.pl" -key key.pem -out req.pem

Podpisanie żądania

W konfiguracji aplikacji Szafir wybieramy format podpisu CAdES (PKCS#7) i zaznaczamy opcję: Zapisz podpisywane dane razem z podpisem.

Podpisz utworzony w openssl plik żądania **req.pem** i wynikowy podpisany plik **req.pem.sig** wskaż w zamówieniu.