

Reissue – darmowa wymiana certyfikatu

Wer. 1.2

assecO

 **Certum**
by assecO

Spis treści

1. Wstęp.....	3
2. Jak wykonać reissue?	3
Metoda CSR	5
Metoda generowania kluczy na karcie kryptograficznej.....	8

1. Wstęp

Reissue pozwala na wydanie nowej kopii certyfikatu z nowymi kluczami, ale taką samą datą końca ważności jak bazowy certyfikat.

Przykładowe powody do wykonania reissue:

- utrata klucza prywatnego,
- certyfikat z innym algorytmem lub długością klucza,
- problem z instalacją lub brak dopasowania certyfikatu do klucza prywatnego,
- zmiana serwera lub dostawcy usług hostingowych.



Wydanie certyfikatu reissue spowoduje automatyczne unieważnienie poprzedniego certyfikatu po upływie 14 dni od wydania nowej kopii certyfikatu. Jest to czas na wymianę certyfikatu w aplikacji czy na serwerze. Z uwagi na to, zachęcamy wszystkich użytkowników wykonujących reissue certyfikatu o niezwłoczne zainstalowanie nowej kopii certyfikatu w celu zapewnienia ciągłości działania zabezpieczenia strony internetowej.

2. Jak wykonać reissue?

Jako klient, możesz rozpocząć proces reissue z poziomu **Twojego konta** w sklepie, w zakładce **Produkty bezpieczeństwa**.

Jako partner, proces reissue certyfikatu rozpoczynasz z poziomu **Dashboardu**, skąd przechodzisz na listę certyfikatów.

Znajdź bazowy, ważny certyfikat, który chcesz wydać ponownie, otwórz jego szczegóły i użyj opcji **Reissue**.

← Powrót

Certyfikat dla zamówienia ORDER/0000234900/000

CN:

STATUS CERTYFIKATU Ważny

Dane subskrybenta

Imię	Nazwisko	Adres e-mail

Metoda weryfikacji
Dostarczenie dokumentów

Dane organizacji

Organizacja	Metoda weryfikacji
Asseco Data Systems S.A.	KRS 0000421310

Kraj	Województwo
Polska	pomorskie

Upoważnienie subskrybenta

Metoda weryfikacji
KRS 0000421310

Domeny do zabezpieczenia [2]

Domena

Certyfikaty pośrednie

Szczegóły

- Kategoria produktu
SSL (TLS)
- Produkt
Trusted MultiDomain SSL 4 domeny 365 dni - wydanie
- Data aktywacji certyfikatu
2023-11-03 11:46
- Data wygaśnięcia certyfikatu
2024-11-02 11:46
- Numer seryjny certyfikatu
54b1b0cdda9d52e9e12b3da3b85326b2

[Podgląd certyfikatu](#)

[Pobierz PEM](#)

[Pobierz DER](#)

[Unieważnij certyfikat](#)

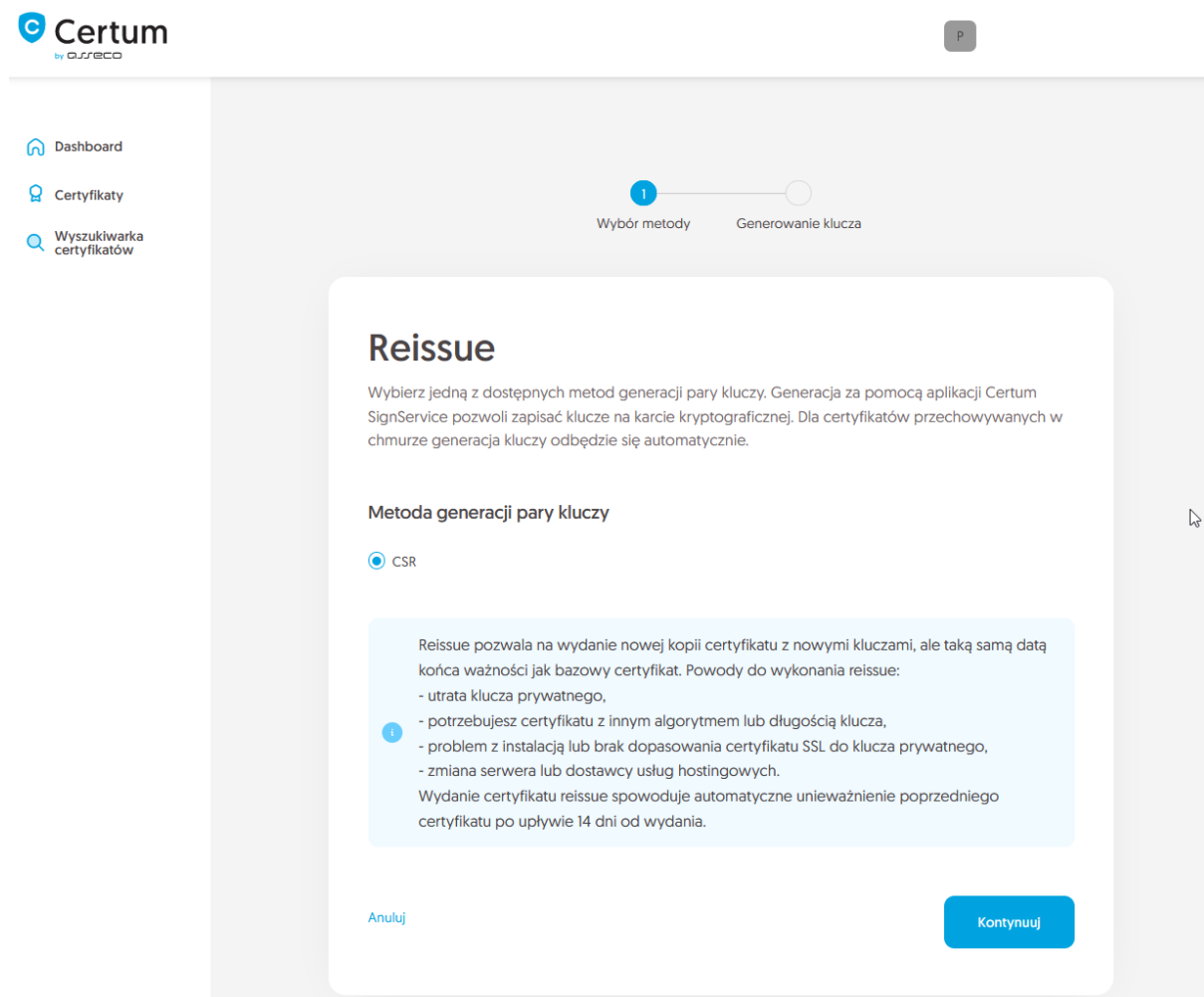
[Reissue](#)

W kolejnym kroku wybierz sposób dostarczenia kluczy dla nowej kopii certyfikatu. Zależnie od produktu, otrzymasz do wyboru metody:

- **CSR** – żądanie podpisania certyfikatu, wygenerowane poprzez generator np. [Certum Tools](#) lub aplikację/serwer, na którym będzie zainstalowany certyfikat
- **Generowanie pary kluczy na karcie** – klucze zostaną zapisane na karcie kryptograficznej.

Wybierając metodę generowania pary kluczy na karcie, wybierz również algorytm i długość klucza. Twój wybór powinien zależeć od algorytmu i długości klucza wspieranych przez aplikację, w której używasz certyfikatu lub rekomendację np. Twojego działu IT.

Metoda CSR



The screenshot shows the Certum SignService interface. At the top left is the Certum logo with 'by asreco' underneath. A navigation sidebar on the left contains 'Dashboard', 'Certyfikaty', and 'Wyszukiwarka certyfikatów'. At the top right is a 'P' button. A progress bar at the top center shows two steps: 'Wybór metody' (selected with a blue circle containing '1') and 'Generowanie klucza'. The main content area is titled 'Reissue' and contains the following text:

Wybierz jedną z dostępnych metod generacji pary kluczy. Generacja za pomocą aplikacji Certum SignService pozwoli zapisać klucze na karcie kryptograficznej. Dla certyfikatów przechowywanych w chmurze generacja kluczy odbędzie się automatycznie.

Metoda generacji pary kluczy

CSR

Reissue pozwala na wydanie nowej kopii certyfikatu z nowymi kluczami, ale taką samą datą końca ważności jak bazowy certyfikat. Powody do wykonania reissue:

- utrata klucza prywatnego,
- potrzebujesz certyfikatu z innym algorytmem lub długością klucza,
- problem z instalacją lub brak dopasowania certyfikatu SSL do klucza prywatnego,
- zmiana serwera lub dostawcy usług hostingowych.

Wydanie certyfikatu reissue spowoduje automatyczne unieważnienie poprzedniego certyfikatu po upływie 14 dni od wydania.

At the bottom of the card are two buttons: 'Anuluj' and 'Kontynuuj'.

Po wybraniu metody CSR, możesz przejść dalej do podania CSR. Na tym etapie będziesz mógł pobrać aplikację [Certum Tools](#) do wygenerowania CSR lub dostarczyć własny.

Po wklejeniu CSR, zostanie on zweryfikowany czy jest poprawny. W razie wystąpienia błędu CSR, zostaniesz o nim poinformowany komunikatem błędu.

- [Dashboard](#)
- [Certyfikaty](#)
- [Wyszukiwarka certyfikatów](#)

Wybór metody 2
Generowanie klucza


Reissue - Dane CSR

Wprowadź dane żądania podpisania certyfikatu [CSR] lub użyj aplikacji Certum Tools do wygenerowania nowego CSR.

```

Lt.FN9bFKx9i.fenLdvM3rB4zdeuwiw6e9+9o4k/G4IeWH/VChP0oqgE1aGnckzaP
2F0pFWvLeZ2AB71cV82dtrvVT8k/w1mH0h4vILLRi:61+qImSRo4FrvjHPclreBYI
umnkF80TqYtUGGD2fS3j5mkQDUKOYAQAk2wgop4teT+SEIGB/zwHvRB22cKWA41V
kH+QhcER+DV8I8wSuFJjpZjeJ1u3FCc4FDWcuLCtu+u1d57uC8PHSdSpFNT1qN
nsq1Q97cIQyp48+2kdTKD8BLAko+99P4tsjgMBAgMBAAEwDQYJKo2IhvcNAQEL
BQADggEBAGNrvQdE4oLeVnMMp9ZVcD/F2FVtWbUjAarrfkMvaQbfP9qXcF77
QBeDIdKf5pE4+jP7YhF85F3eT/tBtSKa06ahJgutHFJkHrVvjM9yLux9eVecVvt
Lq09yphWv7UhsIeeqn2uUBRRw/5vFg1kc2/rCkk9Obkubv7T8u766G4MUqCUaX
mEj8FUwT2EQT2p8CXcNlase5n2//GMe8zeQlkumB2krIT+ReeLHRyHko4uCh1F1pE
ma07kIqosD1sIDR/OtWMTImPnwxJ9L7dj4k4z2rcv9aj/q4BjIaAv2kpw12Zw4kr
LvZ8HzeqMg+bn4009SD97W790AOfc#Q=
-----END CERTIFICATE REQUEST-----

```

 Dane poprawne

[Pobierz aplikację Certum Tools](#)

[Cofnij](#)

[Kontynuuj](#)

Pozytywna weryfikacja CSR i przejście w procesie dalej, zleci nową kopię certyfikatu do wydania.

- [Dashboard](#)
- [Certyfikaty](#)
- [Wyszukiwarka certyfikatów](#)



Sukces!

Nowa kopia certyfikatu została przekazana do wydania, wydanie powinno nastąpić w ciągu 5 minut. Przejdź do szczegółów certyfikatu reissue, skąd będziesz mógł go pobrać.

[Przejdź do dashboardu](#)

Po wydaniu, nową kopię certyfikatu znajdziesz jako nowy certyfikat na Dashboardzie lub na liście certyfikatów.

Tym samym, bazowy certyfikat zostanie przekazany do unieważnienia w ciągu 14 dni. Przypominamy:



Wydanie certyfikatu reissue spowoduje automatyczne unieważnienie poprzedniego certyfikatu po upływie 14 dni od wydania nowej kopii certyfikatu. Jest to czas na wymianę certyfikatu na serwerze. Z uwagi na to, zachęcamy wszystkich użytkowników wykonujących reissue certyfikatu o niezwłoczne zainstalowanie nowej kopii certyfikatu w celu zapewnienia ciągłości działania zabezpieczenia strony internetowej.

Metoda generowania kluczy na karcie kryptograficznej

Po wybraniu metody generowania pary kluczy na karcie, wybierz algorytm i długość klucza.

Certum
by **czsreco**

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów

Wybór metody Generowanie klucza

Reissue

Wybierz jedną z dostępnych metod generacji pary kluczy. Generacja za pomocą aplikacji Certum SignService pozwoli zapisać klucze na karcie kryptograficznej. Dla certyfikatów przechowywanych w chmurze generacja kluczy odbędzie się automatycznie.

Metoda generacji pary kluczy

CSR Generowanie pary kluczy na karcie

ALGORYTM KLUCZA I DŁUGOŚĆ KLUCZA

Wybierz algorytm i długość klucza

Metoda CSR pozwoli uzyskać certyfikat wraz z kluczem w formie do przenoszenia i instalacji z pliku. Pamiętaj, by zapisać klucz prywatny, który wygenerowałeś wraz z CSR.

Wygenerowanie kluczy na karcie spowoduje, że wydany certyfikat zostanie zainstalowany na karcie kryptograficznej i jej podłączenie do komputera będzie wymagane zawsze, gdy certyfikat jest używany. Wspierane są tylko karty Certum.

Reissue pozwala na wydanie nowej kopii certyfikatu z nowymi kluczami, ale taką samą datą końca ważności jak bazowy certyfikat. Powody do wykonania reissue:

- utrata klucza prywatnego,
- potrzebujesz certyfikatu z innym algorytmem lub długością klucza,
- problem z instalacją lub brak dopasowania certyfikatu SSL do klucza prywatnego,
- zmiana serwera lub dostawcy usług hostingowych.

Wydanie certyfikatu reissue spowoduje automatyczne unieważnienie poprzedniego certyfikatu po upływie 14 dni od wydania.

Anuluj Kontynuuj

Po przejściu dalej, upewnij się, że posiadasz kartę włożoną do czytnika, czytnik podłączony do komputera, a sama karta ma zainicjalizowany profil zwykły z nadanym kodem PIN. W procesie wymagane jest również posiadanie zainstalowanej na komputerze aplikacji proCertum CardManager, w której możesz również sprawdzić status karty i kodów PIN i PUK. Jeśli karta jest nowa, zapraszamy do zapoznania się z instrukcją [jak nadać kod PUK i PIN dla profilu zwykłego karty](#).

The screenshot shows the Certum SignService interface. At the top left is the Certum logo. A navigation sidebar on the left contains 'Dashboard', 'Certyfikaty', and 'Wyszukiwarka certyfikatów'. At the top right is a 'P' button. A progress indicator at the top center shows two steps: 'Wybór metody' (completed) and 'Generowanie klucza' (active). The main content area is titled 'Reissue' and contains the following text:

W celu wygenerowania pary kluczy, pobierz i uruchom aplikację **Certum SignService**.

[Pobierz aplikację Certum SignService](#)

1. Pobierz i zainstaluj aplikację **Certum SignService**.
2. Pobierz i zainstaluj aplikację **proCertum CardManager**, jeśli jej nie posiadasz lub jest nieaktualna.
3. Podłącz czytnik do komputera i włóż kartę do czytnika.
4. Otwórz aplikację **proCertum CardManager** i sprawdź czy profil zwykły karty jest zainicjalizowany. Jeśli profil nie jest zainicjalizowany, aplikacja poprosi Cię o nadanie kodów PIN i PUK.
5. Rozpocznij generację kluczy przyciskiem **Wygeneruj klucze**.
6. Zaakceptuj komunikat z przeglądarki o zgodę na uruchomienie aplikacji **Certum SignService**.
7. Gdy pojawi się okno aplikacji **Certum SignService**, wprowadź PIN do profilu zwykłego karty.
8. Odczekaj na wygenerowanie kluczy, może to zająć do kilku minut.

Below the list is a blue information box: **i** Po zakończeniu generacji, zostaniesz przeniesiony do kolejnego okna procesu.

At the bottom left is a 'Cofnij' button, and at the bottom right is a yellow 'Wygeneruj klucze' button.

Do wygenerowania kluczy na karcie potrzebujesz również zainstalowaną na komputerze aplikację Certum SignService. Aplikacja Certum SignService po uruchomieniu generowania kluczy, poprosi o zgodę na uruchomienie się i podanie kodu PIN profilu zwykłego karty w celu wygenerowania na niej kluczy.

The screenshot shows the same Certum SignService interface as above, but with a browser security warning dialog box overlaid. The dialog box text is:

Allow this site to open the certumkoalaservice link with CertumSignService?

[Choose a different application.](#)

Always allow <http://100.101.10.90:4300> to open certumkoalaservice links


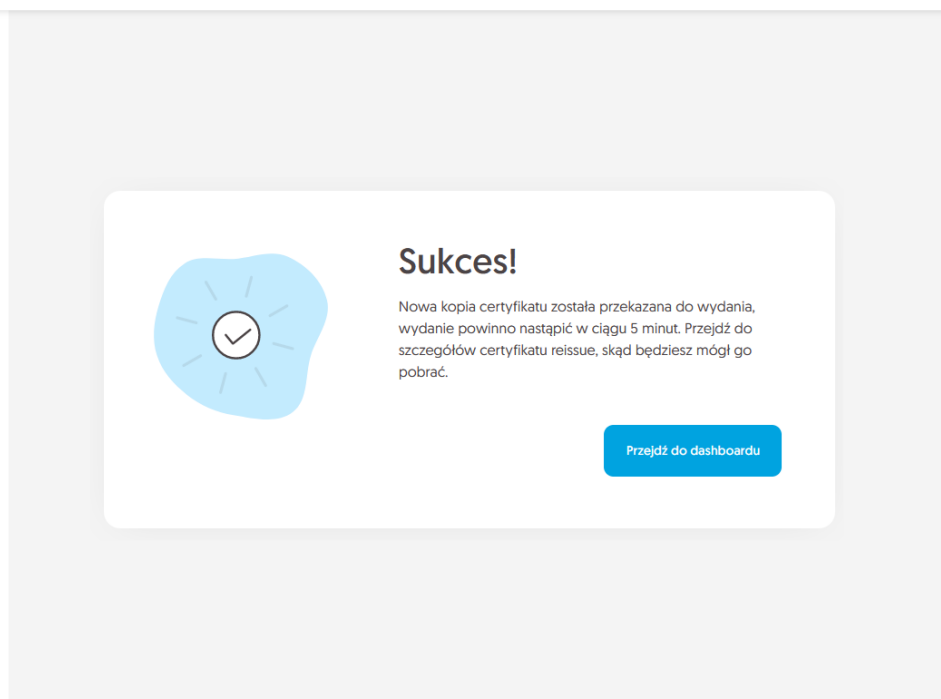
At the bottom of the dialog are 'Open Link' and 'Cancel' buttons. The background interface is dimmed.



The screenshot shows a window titled "Certum SignService" with a close button in the top right corner. The window contains the following elements:

- Logo:** A blue icon of a computer monitor with a pen nib writing on it, followed by the text "Certum SignService" in a large, bold, black font, and "by GISECO" in a smaller, blue font below it.
- Section Header:** "Generacja nowej pary kluczy" (Generation of a new key pair) in bold black text.
- Dane karty (Card Data):** A section with a light gray background containing two rows of text:
 - Nazwa czytnika: ACS ACR39U ICC Reader 0
 - Numer karty: 2268 9624 6429 8967
- Dane klucza (Key Data):** A section with a light gray background containing two rows of text:
 - Algorytm: RSA
 - Wielkość: 2048
- Input Field:** A text box labeled "PIN profilu zwykłego:" (Regular profile PIN) with a vertical cursor. Below the box is the text "[od 4 do 8 znaków]" (from 4 to 8 characters).
- Warnings:** Two lines of bold black text:
 - W zależności od algorytmu i wielkości klucza generacja może potrwać do kilku minut**
 - W trakcie operacji nie wyjmuj karty z czytnika**
- Buttons:** Two buttons at the bottom right: "Ok" and "Anuluj" (Cancel).

Po wpisaniu kodu PIN rozpocznie się proces generowania klucza na karcie. Może to zająć do kilkudziesięciu sekund. Po wygenerowaniu klucza nowa kopia certyfikatu zostanie przekazana do wydania.

 Dashboard Certyfikaty Wyszukiwarka
certyfikatów

Po wydaniu, nową kopię certyfikatu do zainstalowania na karcie znajdziesz jako nowy certyfikat na Dashboardzie lub na liście certyfikatów. Wydany certyfikat można będzie pobrać z wiadomości e-mail o utworzeniu certyfikatu lub z widoku szczegółów certyfikatu: w dogodnym kodowaniu **PEM** lub **DER** lub zainstalować na karcie, również z poziomu szczegółów certyfikatu.

Tym samym, bazowy certyfikat zostanie przekazany do unieważnienia w ciągu 14 dni. Przypominamy:



Wydanie certyfikatu reissue spowoduje automatyczne unieważnienie poprzedniego certyfikatu po upływie 14 dni od wydania nowej kopii certyfikatu. Jest to czas na wymianę certyfikatu w aplikacji czy na serwerze. Z uwagi na to, zachęcamy wszystkich użytkowników wykonujących reissue certyfikatu o niezwłoczne zainstalowanie nowej kopii certyfikatu w celu zapewnienia ciągłości działania zabezpieczenia strony internetowej.