

# Зменшення розміру файлу CACertificates.p7b

- [Загальний опис](#)
- [Передумови](#)
- [Виконання](#)
  - [1. Підготовка .cer](#)
  - [2. Генерація CACertificates.p7b](#)
  - [3. Опціонально: Редагування CAs.json](#)
  - [4. Перевірка працездатності згенерованого CACertificates.p7b](#)

## Загальний опис

Файл CACertificates.p7b зберігає в собі сертифікати, що використовуються для валідації підписів/автентифікації користувачів в реєстрах Платформи. Даний файл зберігається в ресурсі Secret системи OKD(Kubernetes). З часом розмір цього файлу перевищив 1 MiB, що створює проблему «Secret exceeds max size», так як OKD(Kubernetes) дозволяє зберігати не більше 1 MiB даних в цьому виді ресурсу. Тому було створено інструкцію, яка пропонує вирішення даної проблеми, шляхом зменшення розміру файлу CACertificates.p7b через його генерацію з попереднім видаленням старих сертифікатів.

## Передумови

- **Середовище:** Unix-подібна ОС, bash.
- **Пакет:** openssl ≥ 3.1.4
- **Скрипт генерації CACertificates.p7b:** прикладено до інструкції

## Виконання

### 1. Підготовка .cer

1.1 Завантажте архів з скриптом генерації CACertificates.p7b та розпакуйте його. Створіть папку .cer за шляхом знаходження скрипту генерації CACertificates.p7b.

1.2 Завантажте архів із сертифікатами з IIT за [посиланням](#) та розпакуйте архів в папку .cer за шляхом знаходження скрипту генерації CACertificates.p7b.

1.3 Перевірте кожен сертифікат в папці .cer на актуальність/необхідність та видаліть застарілі/непотрібні файли. Перевірити на файли можна двома шляхами:

a) Вручну:

1. Відкрити кожен сертифікат вручну через утиліту зчитування сертифікатів (на приклад в Windows) та перевірити, що поле "Valid from ... to ..." є актуальним або чи є зазначений емітент необхідним.
2. Видалити неактуальні/непотрібні.

b) За допомогою скриптів у директорії .cer:

1. Відобразити всі неактуальні на сьогоднішній день файли командою:

```
for f in *.cer; do if [ "$(openssl x509 -inform der -in "$f" -noout -enddate | cut -d= -f2 | xargs -I{} date -d "{}" +%s)" -lt "$(date +%s)" ]; then echo "$f"; fi; done
```

2. Видалити неактуальні на сьогоднішній день сертифікати наступною командою:

```
for f in *.cer; do if [ "$(openssl x509 -inform der -in "$f" -noout -enddate | cut -d= -f2 | xargs -I{} date -d "{}" +%s)" -lt "$(date +%s)" ]; then rm "$f"; fi; done
```

## 2. Генерація CACertificates.p7b

2.1 У директорії скрипта генерації надайте права на виконання скрипта генерації:

```
chmod +x main.sh
```

2.2 Запустіть скрипт:

```
./main.sh
```

**Результат** — файл CACertificates.p7b у робочій папці.

2.3 Переконайтесь, що його розмір  $\leq 1000$  КБ наступною командою:

```
du -k CACertificates.p7b
```

Приклад виконання команди:

```
$ du -k CACertificates.p7b
724    CACertificates.p7b
```

Якщо ліміт перевищено — видаліть ще сертифікати в кроці 1 та повторіть крок 2.

## 3. Опціонально: Редагування CAs.json

Якщо з директорії .cer видалено всі сертифікати окремого емітента:

3.1 Завантажте актуальний CAs.json з ІІТ за [посиланням](#).

3.2 Видаліть записи вилучених емітентів, щоб уникнути некоректних посилань.

## 4. Перевірка працездатності згенерованого CACertificates.p7b

4.1 Встановіть CACertificates.p7b (та, за потреби, CAs.json) на тестовий реєстр, таким чином запустивши build-pipeline реєстру.

4.2 Pod digital-signature-ops має перейти у Running без помилок.

Якщо підписи користувачів не проходять — перевірте, чи не видалено необхідний сертифікат, та повторіть генерацію.