Зміст

[Процес продовження строку чинності сертифіката в інтегрованому режимі 2](#_Toc137219699)

[1. Створення заяви на продовження строку чинності сертифіката ключа 2](#_Toc137219700)

[2. Генерація нового ключа у сховищі DepositSign або з використанням сторонніх носіїв ключової інформації та передача запитів для формування сертифікатів 2](#_Toc137219701)

[Генерація нового ключа у сховищі DepositSign 2](#_Toc137219702)

[Генерація нового ключа на сторонніх носіях та передача запитів для формування сертифікатів 3](#_Toc137219703)

[3. Підписання заяви на продовження строку чинності сертифіката 3](#_Toc137219704)

[Особистий ключ якого зберігається у сховищі DepositSign 3](#_Toc137219705)

[Особистий ключ якого зберігається на зовнішньому носії 4](#_Toc137219706)

[4. Сертифікація заяви на продовження 4](#_Toc137219707)

# Процес продовження строку чинності сертифіката в інтегрованому режимі

Для продовження строку чинності сертифіката ключа в інтегрованому режимі, необхідно виконати такі кроки:

1. Створення заяви на продовження строку чинності сертифіката ключа;

2. Генерація нового ключа або приймання зовнішніх запитів;

3. Підписання заяви на продовження строку чинності сертифіката ключа;

4. Сертифікація заяви на продовження строку чинності сертифіката ключа

1. Створення заяви на продовження строку чинності сертифіката ключа

Для створення заяви на продовження необхідно викликати метод:
POST api/v1/{clientId}/keyApplications/{keyApplicationId}/renewal/create
де keyApplicationId – ідентифікатор заяви на сертифікат котрий продовжуємо

У тілі запиту необхідно передати JSON:
{

 "ValidityPeriod": 1,

 "ApplicationType": 3

}
де:

* ApplicationType - Тип заяви:
1 - Генерація файлового ключа; //obsolete

2 - Генерація ключа на гряді; //obsolete

3 - Відкладена генерація на гряді;

4 - Відкладена генерація файлового ключа.

* ValidityPeriod – період на який буде випущений новий сертифікат

1 – один рік;

2 – два роки.

У відповідь буде отримана JSON-структура виду:
{

 "KeyApplicationId": "bb1340f4-486c-476d-a05f-4b0783d965a7",

 "Number": "1660804278235"

}

Де:

* KeyApplicationId – ідентифікатор заяви на продовження;
* Number – унікальний номер заяви.

2. Генерація нового ключа у сховищі DepositSign або з використанням сторонніх носіїв ключової інформації та передача запитів для формування сертифікатів

Новий ключ може бути згенеровано у сховищі DepositSign або бути на зовнішньому носії (файл, токен, гряда).

Генерація нового ключа у сховищі DepositSign

Потрібно викликати метод:
POST api/v1/{clientId}/keyApplications/{applicationId}/generate/key

Де keyApplicationId – ідентифікатор заяви на продовження

У тілі запиту необхідно передати JSON:
{

 "Password": "pwd",

 "CodeWord": "codeWord",

}

Де:

* Password – пароль нового ключа;
* CodeWord – кодове слово для відновлення доступу до ключа.

### Генерація нового ключа на сторонніх носіях та передача запитів для формування сертифікатів

Потрібно викликати метод:
POST api/v1/{clientId}/keyApplications/{applicationId}/key/requests

Де keyApplicationId – ідентифікатор заяви на продовження
У тілі запиту необхідно передати JSON:
{

 "Request ": "ByteArray as base64 string",

 "RequestFileName ": "file name",

 "KEPRequest": "ByteArray as base64 string",

 "KEPReqFileName": "file name",

 "KeyInfo": "ByteArray as base64 string",

}

Де:

* Request – запит на сертифікацію ключа підпису;
* RequestFileName – ім’я файлу запиту на сертифікацію ключа підпису;
* KEPRequest – запит на сертифікацію ключа шифрування;
* KEPReqFileName – ім’я файлу запиту на сертифікацію ключа шифрування
* KeyInfo – публічна частина приватного ключа.

3. Підписання заяви на продовження строку чинності сертифіката

### Особистий ключ якого зберігається у сховищі DepositSign

Потрібно викликати метод:
POST api/v1/{clientId}/sign/renewal/{applicationId}

де keyApplicationId – ідентифікатор заяви на продовження

У тілі запиту необхідно передати JSON:

{

 "Password": "pwd",

}

Де:

* Password – пароль ключа сертифікат котрого продовжують.

### Особистий ключ якого зберігається на зовнішньому носії

POST api/v1/{clientId}/sign/renewal/{applicationId}

Де keyApplicationId – ідентифікатор заяви на продовження

У тілі запиту необхідно передати JSON:
{

 "Signature": "ByteArray as base64 string"

}

Де:

* Signature – зовнішній підпис заяви (друкована форма - pdf)
Хеш цієї заяви можна взяти викликавши метод
GET api/v1/{clientId}/keyApplications/{applicationId}/pdf/hash

Де keyApplicationId – ідентифікатор заяви на продовження.

4. Сертифікація заяви на продовження
Для формування нового сертифіката (продовження) та скасування поточного необхідно викликати метод
POST api/v1/{clientId}/management/application/renewal/{applicationId}/process
Де keyApplicationId – ідентифікатор заяви на продовження.