ТОВ «С.І.Т»

UAPKI

бібліотека

Настанова програміста

Версія 2.0.9

Київ, 2023

Історія версій

Дата	Версія	Опис
02.08.2021	2.0.1	Початковий реліз
16.08.2021	2.0.2	У відповіді методу додана назва методу
01.09.2021	2.0.3	Зміни у параметрах методів INIT та VERIFY_CERT
16.09.2021	2.0.4	Зміни у способах конфігурації бібліотеки. Для сертифікатів і CRL створені окремі ідентифікатори (оновлений інтерфейс методів, які використовують їх). Додана підтримка пакету сертифікатів в методі ADD_CERT
11.11.2021	2.0.5	Зміни в методах OPEN, DIGEST, SIGN, VERIFY, VERIFY_CERT
17.11.2021	2.0.6	Зміни в методу CERT_INFO
07.11.2022	2.0.7	Додані методи DECRYPT і ENCRYPT
31.01.2023	2.0.8	Додані 4 формати підписів ("CAdES-T", "CAdES-C", "CAdES-XL" і "CAdES-A") у методи SIGN і VERIFY, доданий додаток із коротким описом форматів підпису
20.03.2023	2.0.9	В метод SIGN додана підтримка додаткових опцій. В метод VERIFY додані розширені типи валідації документа

Загальні відомості

Цей документ призначено для використання розробниками додатків, які мають потреби у інтеграції механізмів електронного цифрового підпису.

До складу бібліотеки входять бінарні файли (бібліотеки), які представлені в таблиці 1 (префікси і розширення залежать від платформи/ОС) і файл конфігурації.
Таблиця 1. Перелік бінарних файлів бібліотеки

№	Базова назва бінарного файлу	Опис
1	uapki	Головна бібліотека, що реалізує основну логіку роботи
2	uapkic	Бібліотека криптографії, обов'язкова
3	uapkif	Бібліотека форматів, обов'язкова
4	cm-<storage-name> cm-pkcs12	Бібліотека провайдера сховищ ключів. Наприклад для файлового сховища це буде "cm-pkcs12". Необхідна, якщо використовуються функції, які залежать від приватних ключів (наприклад, підпис даних)

Бібліотека реалізовує свій функціонал за допомогою методів, які представлені в таблиці 2. Методи викликаються за допомогою двох експортованих функцій бібліотеки: process і json_free, інтерфейс яких описаний в таблиці 3. Вся взаємодія з методами бібліотеки базується на використання текстової строки, що складається за правилами JSON (далі JSON-строка).

Таблиця 2. Перелік методів бібліотеки

Назва методу	Короткий опис
VERSION	Версія бібліотеки
INIT	Ініціалізація бібліотеки
DEINIT	Завершення роботи бібліотеки (де-ініціалізація)
PROVIDERS	Перелік провайдерів сховищ ключів
STORAGES	Перелік сховищ ключів доступних через обраний провайдер
STORAGE_INFO	Інформація про сховище ключів
OPEN	Відкрити сховище ключів
CLOSE	Закрити сховище ключів
KEYS	Перелік ключів у відкритому сховищі
SELECT_KEY	Вибрати ключ
CREATE_KEY	Створити ключ
DELETE_KEY	Видалити ключ
GET_CSR	Отримати запит на сертифікат
CHANGE_PASSWORD	Зміна пароля (PIN коду) до сховища ключів
INIT_KEY_USAGE	Ініціалізація використання ключа
SIGN	Підпис даних
VERIFY	Перевірка підписаних даних

ENCRYPT	Шифрування даних
DECRYPT	Розшифрування даних
ADD_CERT	Додати сертифікат до кешу сертифікатів
CERT_INFO	Інформація з сертифіката
GET_CERT	Отримати сертифікат із кешу сертифікатів
LIST_CERTS	Перелік сертифікатів у кешу сертифікатів
REMOVE_CERT	Видалити сертифікат із кешу сертифікатів
VERIFY_CERT	Перевірка сертифіката
ADD_CRL	Додати CRL до кешу CRL
CRL_INFO	Інформація з CRL
DIGEST	Гешування даних
ASN1_DECODE	Декодування DER-кодованих ASN1 даних
ASN1_ENCODE	Кодування даних згідно DER-кодування ASN1

Таблиця 3. Перелік експортованих функцій бібліотеки

№	Назва функції	Короткий опис
1	process	char* process(const char* request);
2	json_free	void json_free(char* result);

Опис функції **process**:
параметр request – це вказівник на JSON-строку, яка описує параметри методу (назва методу, параметри методу);
повертає вказівник на JSON-строку, що зберігає результат виконання методу. Цей вказівник після обробки повинен завжди видаляться функцією json_free.

Опис функції **json_free**:
параметр result – це вказівник на текстовий рядок у форматі JSON, який був отриманий виконанням функції process;
нічого не повертає.

Опис методів бібліотеки

Всі запити і відповіді методів мають єдиний формат, вони розрізнюються в полях parameters й result.

Формат запиту

Назва поля	**Тип**	**Опис**
method	String	Назва методу. Обов'язковий параметр
parameters	Object	Опціональний параметр. Структура, що містить індивідуальні параметри методу

Формат відповіді

Назва поля	**Тип**	**Опис**
errorCode	Integer	Код помилки
method	String	Назва методу
result	Object	Структура, що містить результат виконання методу
error	String	Короткий текстовий опис помилки. Опціональний

Метод VERSION

Метод призначений для визначення версії бібліотеки. Параметри в запиті відсутні.

Приклад запиту:

```
{
  "method": "VERSION"
}
```

Структура поля result у відповіді

Назва поля	**Тип**	**Опис**
name	String	Ім'я бібліотеки
version	String	Номер версії бібліотеки

Приклад результату:

```
{
  "errorCode": 0,
  "method": "VERSION",
  "result": {
    "name": "UAPKI",
    "version": "2.0.9"
  }
}
```

Метод INIT

Метод призначений для ініціалізації бібліотеки. Вхідні параметри опціональні. У вихідних параметрах повертаються поточні значення статусу/параметрів підсистем бібліотеки. Якщо бібліотека була ініціалізована, то перед завершенням роботи з нею потрібно виконати метод DEINIT. Перелік методів для яких ініціалізація бібліотеки не обов’язкова: VERSION, DIGEST, ASN1_DECODE та ASN1_ENCODE.

Параметри бібліотеки можна задати двома способами: параметрами або через файл конфігурації. Параметри та файл конфігурації мають однакову структуру. Якщо використовується файл конфігурації, то необхідно в поле "configFile" вказати шлях до нього (рекомендована назва "uapki-config.json").

Якщо параметри бібліотеки не задані — будуть використанні параметри за замовченням. Для роботи із сховищем ключів необхідно задати параметри CM-провайдерів.

Структура поля parameters у запиті з використанням файлу конфігурації

Назва поля	**Тип**	**Опис**
configFile	String	Повний шлях до файлу

Приклад запиту з використанням файлу конфігурації:

```
{
  "method": "INIT",
  "parameters": {
    "configFile": "C:/uapki/uapki-config.json"
  }
}
```

Структура поля parameters у запиті

Назва поля	**Тип**	**Опис**
cmProviders	Object CMPROVIDERS_PARAMS	Параметри CM-провайдерів. Опціональний
certCache	Object CERT_CACHE_PARAMS	Параметри кешу сертифікатів. Опціональний
crlCache	Object CRL_CACHE_PARAMS	Параметри кешу CRL. Опціональний
offline	Boolean	Режим роботи “офлайн”. Опціональний
ocsp	Object OCSP_PARAMS	Параметри OCSP-сервісу. Опціональний
tsp	Object TSP_PARAMS	Параметри TSP-сервісу. Опціональний

Структура CERT_CACHE_PARAMS

Назва поля	**Тип**	**Опис**
path	String	Повний шлях до каталогу. Опціональний
trustedCerts	Base64[]	Масив довірених сертифікатів. Опціональний

Структура CRL_CACHE_PARAMS

Назва поля	Тип	Опис
path	String	Повний шлях до каталогу. Опціональний

Структура OCSP_PARAMS

Назва поля	Тип	Опис
nonceLen	Integer	Довжина одноразового випадкового числа в OCSP-запиті. Діапазон значень: 0, 8..64. Якщо значення дорівнює 0 або знаходиться не в діапазоні, то випадкове число в OCSP-запиті не використовується. Опціональний, за замовчанням дорівнює 20

Структура TSP_PARAMS

Назва поля	Тип	Опис
certReq	Boolean	Вимога повертати в TSP-відповіді сертифікат сервісу. Опціональний, за замовчанням дорівнює false
forced	Boolean	Вимога використовувати URL-адреса TSP-сервісів, які задані в полі "url", ігноруючи адреса, що вказані в сертифікаті підписувача. Опціональний, за замовчанням дорівнює false
nonceLen	Integer	Довжина одноразового випадкового числа в TSP-запиті. Діапазон значень: 0, 4..32. Якщо значення дорівнює 0 або знаходиться не в діапазоні, то випадкове число в TSP-запиті не використовується. Опціональний, за замовчанням дорівнює 8
policyId	OID	Ідентифікатор політики TSP-сервісу. Якщо поле відсутнє або в значенні пустий рядок, то параметр політики TSP-сервісу в запиті не використовується. Опціональний
url	String[] або String	масив URL-адрес TSP-сервісів. У випадку однієї адреси можна задати її як рядок. Опціональний

Структура CMPROVIDERS_PARAMS

Назва поля	Тип	Опис
dir	String	Повний шлях до каталогу з бібліотеками CM-провайдерів
allowedProviders	Object[] CMPROVIDER_PARAMS	Масив з параметрами CM-провайдерів

Структура CMPROVIDER_PARAMS

Назва поля	Тип	Опис
lib	String	Назва файлу бібліотеки CM-провайдеру
config	Object	Параметри специфічні для кожного CM-провайдеру. Опціональний

Приклад файлу конфігурації:

```
{
  "cmProviders": {
    "allowedProviders": [ {
        "lib": "cm-diamond"
      }, {
        "lib": "cm-pkcs12",
        "config": {
          "createPfx": {
            "bagCipher": "2.16.840.1.101.3.4.1.22",
            "bagKdf": "1.2.840.113549.2.10",
            "iterations": 10000,
            "macAlgo": "2.16.840.1.101.3.4.2.2"
          }
        }
      }
    ]
  },
  "certCache": {
    "path": "C:/uapki/certs/",
    "trustedCerts": ["MIIE...a2s=", ... ]
  },
  "crlCache": {
    "path": "C:/uapki/certs/crls/"
  },
  "offline": false
}
```

Приклад запиту з параметрами:

```
{
  "method": "INIT",
  "parameters": {
    "cmProviders": {
      "dir": "C:/uapki/cm-libs/",
      "allowedProviders": [ {
          "lib": "cm-diamond"
        }, {
          "lib": "cm-pkcs12",
          "config":
            "createPfx": {
              "bagCipher": "2.16.840.1.101.3.4.1.22",
              "bagKdf": "1.2.840.113549.2.10",
              "iterations": 10000,
              "macAlgo": "2.16.840.1.101.3.4.2.2"
            }
          }
        }
      ]
    },
    "certCache": {
      "path": "C:/uapki/certs/",
      "trustedCerts": ["MIIE...a2s=", ... ]
    },
    "crlCache": {
      "path": "C:/uapki/certs/crls/"
    },
    "offline": false,
```

```
    "ocsp": {
      "nonceLen": 20
    },
    "tsp": {
      "certReq": true,
      "forced": true,
      "nonceLen": 8,
      "policyId": "1.2.804.2.1.1.1.2.3.1",
      "url": "http://url_ca/services/tsp/"
    }
  }
}
```

Структура поля result у відповіді

Назва поля	**Тип**	**Опис**
certCache	Object CERT_CACHE_INFO	Інформація про стан кешу сертифікатів
crlCache	Object CRL_CACHE_INFO	Інформація про стан кешу CRL
countCmProviders	Integer	Кількість підключених CM-провайдерів
offline	Boolean	Режим роботи “офлайн”
ocsp	Object OCSP_INFO	Інформація о параметрах OCSP-сервісу
tsp	Object TSP_INFO	Інформація о параметрах TSP-сервісу

Структура CERT_CACHE_INFO

Назва поля	**Тип**	**Опис**
countTrustedCerts	Integer	Кількість довірених сертифікатів у кешу сертифікатів
countCerts	Integer	Загальна кількість сертифікатів у кешу сертифікатів

Структура CRL_CACHE_INFO

Назва поля	**Тип**	**Опис**
countCrls	Integer	Кількість CRL у кешу CRL

Структура OCSP_INFO

Назва поля	**Тип**	**Опис**
nonceLen	Integer	Довжина одноразового випадкового числа в OCSP-запиті. Якщо значення дорівнює 0, то випадкове число в OCSP-запиті не використовується

Структура TSP_INFO

Назва поля	**Тип**	**Опис**
certReq	Boolean	Вимога повертати в TSP-відповіді сертифікат сервісу
forced	Boolean	Вимога використовувати URL-адреса TSP-сервісів, які задані в полі "url", ігноруючи адреса, що вказані в сертифікаті підписувача

nonceLen	Integer	Довжина одноразового випадкового числа в TSP-запиті. Якщо значення дорівнює 0, то випадкове число в запиті не використовується
policyId	OID	Ідентифікатор політики TSP-сервісу
url	String	URL-адреса TSP-сервісу. Масив URL-адрес повертається у вигляді рядка з роздільником ";"

Приклад результату:


```
{
  "errorCode": 0,
  "method": "INIT",
  "result": {
    "certCache": {
      "countCerts": 29,
      "countTrustedCerts": 5
    },
    "crlCache": {
      "countCrls": 4
    },
    "countCmProviders": 2,
    "offline": false,
    "ocsp": {
      "nonceLen": 20
    },
    "tsp": {
      "certReq": true,
      "forced": true,
      "nonceLen": 8,
      "policyId": "1.2.804.2.1.1.1.2.3.1",
      "url": "http://url_ca/services/tsp/"
    }
  }
}
```

Метод DEINIT

Метод призначений для звільнення ресурсів бібліотеки які були ініціалізовані в методі INIT. Параметри в запиті відсутні. Результат — пуста структура.

Приклад запиту:

```
{
  "method": "DEINIT"
}
```

Приклад результату:

```
{
  "errorCode": 0,
  "method": "DEINIT",
  "result": {}
}
```

Метод PROVIDERS

Метод призначений для отримання переліку провайдерів. Параметри в запиті відсутні.

Приклад запиту:

```
{
  "method": "PROVIDERS"
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
providers	Object[] PROVIDER_INFO[]	Масив інформації про провайдер

Структура PROVIDER_INFO

Назва поля	Тип	Опис
id	String	Ідентифікатор провайдеру. Унікальне значення, наприклад: "CLOUD", "PKCS12", "TOKEN"
apiVersion	String	Версія API провайдеру в форматі major.minor.build
libVersion	String	Версія бібліотеки провайдеру в форматі major.minor.build
description	String	Короткий опис провайдеру
manufacturer	String	Назва виробника провайдеру
supportListStorages	Boolean	Позначка підтримки методу "STORAGES"

Приклад результату:

```
{
  "errorCode": 0,
  "method": "PROVIDERS",
  "result": {
    "providers": [{
      "id": "DIAMOND",
      "apiVersion": "1.0.0",
      "libVersion": "1.0.0",
      "description": "DIAMOND-provider",
      "manufacturer": "2021 SPECINFOSYSTEMS LLC",
      "supportListStorages": true
    }, {
      "id": "PKCS12",
      "apiVersion": "1.0.0",
      "libVersion": "1.0.0",
      "description": "PKCS12-provider",
      "manufacturer": "2021 SPECINFOSYSTEMS LLC",
      "supportListStorages": false
    }]
  }
}
```

Метод STORAGES

Метод призначений для отримання переліку сховищ провайдера.
Провайдери можуть не підтримувати даний метод: PKCS12- та CLOUD-провайдер не надають перелік доступних сховищ.

Структура поля parameters у запиті

Назва поля	Тип	Опис
provider	String	Ідентифікатор провайдера

Приклад запиту:

```
{
  "method": "STORAGES",
  "parameters": {
    "provider": "TOKEN"
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
storages	Object[]	Масив структур з описом сховища

Приклад результату, якщо метод підтримується:

```
{
  "errorCode": 0,
  "method": "STORAGES",
  "storages": [
    {
      "id": "000001",
      "manufacturer": "SPECINFOSYSTEMS LLC",
      "description": "DIAMOND 1000 token",
      "serial": "000001",
      "label": "User 1"
    }, {
      ...
    }
  ]
}
```

Приклад результату, якщо метод не підтримується:

```
{
  "errorCode": 258,
  "method": "STORAGES",
  "result": {
    "message": "PKCS12-provider not supported API
      'provider_storage_info'."
  }
}
```

Метод STORAGE_INFO

Метод призначений для отримання інформації про сховище провайдеру.
Провайдери можуть не підтримувати даний метод: PKCS12- та CLOUD-провайдер не надають перелік доступних сховищ.

Структура поля parameters у запиті

Назва поля	Тип	Опис
provider	String	Ідентифікатор провайдера
storage	String	Ідентифікатор сховища. Наприклад, це може бути ім'я файлу чи URL-адресою

Приклад запиту:

```
{
  "method": "STORAGE_INFO",
  "parameters": {
    "provider": "PKCS12",
    "storage": "storage-id"
  }
}
```

Приклад результату, якщо метод не підтримується:

```
{
  "errorCode": 258,
  "method": "STORAGE_INFO",
  "result": {
    "message": "PKCS12-provider not supported API
               'provider_storage_info'."
  }
}
```

Метод OPEN

Відкриття сховища здійснюється за допомогою методу OPEN. Має три обов'язкових параметра ("provider", "storage" й "mode") та специфічні параметри, які залежать від типу провайдера сховища.

Режими роботи із сховищем ("mode")

Значення	Тип
"RW"	Доступні всі методи для роботи з ключами
"RO"	Доступні методи для роботи з ключами, які не змінюють сховище (аналогія режиму "тільки на читання" для звичайних файлів)
"CREATE"	Створення нового сховища, доступні всі методи для роботи з ключами

Структура поля parameters у запиті до CLOUD-провайдера

Назва поля	Тип	Опис
provider	String	Ідентифікатор CLOUD-провайдера
storage	String	URL-адреса сховища
mode	String	Режим роботи із сховищем. Опціональний (значення за замовчанням: "RW")
username	String	Ім'я облікового запису користувача
password	String	Пароль до облікового запису користувача

Приклад запиту до CLOUD-провайдера (відкриття сховища в режимі тільки на читання):

```
{
  "method": "OPEN",
  "parameters": {
    "provider": "CLOUD",
    "storage": "http://url-storage",
    "mode": "RO",
    "username": "username",
    "password": "password"
  }
}
```

Структура поля parameters у запиті до PKCS12-провайдера

Назва поля	Тип	Опис
provider	String	Ідентифікатор PKCS12-провайдера
storage	String	Ім'я файлу сховища
mode	String	Режим роботи із сховищем. Опціональний (значення за замовчанням: "RW")
password	String	Пароль до файлового сховища
openParams	Object	Параметри для створення нового файлового сховища

Приклад запиту до PKCS12-провайдера (створення нового файлового сховища):

```
{
  "method": "OPEN",
  "parameters": {
    "provider": "PKCS12",
    "storage": "file.p12",
    "mode": "CREATE",
    "password": "password",
    "openParams": {
      "bagCipher": "2.16.840.1.101.3.4.1.42",
      "bagKdf": "1.2.840.113549.2.9",
      "iterations": 10000,
      "macAlgo": "2.16.840.1.101.3.4.2.1"
    }
  }
}
```

Структура поля result у відповіді

Назва поля	**Тип**	**Опис**
mechanisms	Object[]	Масив структур з описом механізмів, які доступні для використання
userPresense	Boolean	Опціональний

Приклад результату:

```
{
  "errorCode": 0,
  "method": "OPEN",
  "result": {
    "description": "PKCS12",
    "manufacturer": "2021 SPECINFOSYSTEMS LLC",
    "label": "file.p12",
    "model": "PKCS12",
    "serial": "file.p12",
    "mechanisms": [
      {
        "id": "1.2.804.2.1.1.1.1.3.6",
        "name": "DSTU-4145",
        "keyParam": ["1.2.804.2.1.1.1.1.3.1.1.2.6", ... ],
        "signAlgo": ["1.2.804.2.1.1.1.1.3.6.1", ... ]
      }, {
        "id": "1.2.840.10045.2.1",
        "name": "ECDSA",
        "keyParam": ["1.2.840.10045.3.1.7", ... ],
        "signAlgo": ["1.2.840.10045.4.3.2", ... ]
      }, {
        ...
      }
    ]
  }
}
```

Метод CLOSE

Закриття сховища здійснюється за допомогою методу CLOSE. Параметри в запиті відсутні. Результат — пуста структура.

Приклад запиту:

```
{
  "method": "CLOSE"
}
```

Приклад результату:

```
{
  "errorCode": 0,
  "method": "CLOSE",
  "result": {}
}
```

Метод KEYS

Метод призначений для отримання переліку ключів на відкритому сховищі. Параметри в запиті відсутні.

Приклад запиту:

```
{
  "method": "KEYS"
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
keys	Object[] KEY_INFO[]	Масив інформації про ключі

Структура KEY_INFO

Назва поля	Тип	Опис
id	String	Ідентифікатор ключа. Унікальне значення
mechanismId	OID	Ідентифікатор алгоритму ключа
parameterId	OID	Ідентифікатор параметра ключа
signAlgo	OID[]	Ідентифікатори алгоритмів підпису, що підтримуються ключем
label	String	Текстове позначення ключа. Опціональний

Приклад результату:

```
{
  "errorCode": 0,
  "method": "KEYS",
  "result": {
    "keys": [
      {
        "id": "112233445566...DDEEFF00",
        "mechanismId": "1.2.804.2.1.1.1.1.3.1",
        "parameterId": "1.2.804.2.1.1.1.1.3.1.1.2.6",
        "signAlgo": ["1.2.804.2.1.1.1.1.3.1.1", ... ],
        "label": "DSTU-4145, M257_PB"
      }, {
        "id": "CAFE8A8E1234...00000001",
        "mechanismId": "1.2.840.10045.2.1",
        "parameterId": "1.2.840.10045.3.1.7",
        "signAlgo": ["1.2.840.10045.4.3.2", ... ],
        "label": "ECDSA, prime256v1"
      }
    ]
  }
}
```

Метод SELECT_KEY

Метод призначений для вибору поточного ключа у відкритому сховищі.

Структура поля parameters у запиті

Назва поля	Тип	Опис
id	String	Ідентифікатор ключа. Унікальний

Приклад запиту:

```
{
  "method": "SELECT_KEY",
  "parameters": {
    "id": "112233445566...DDEEFF00"
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
signAlgo	OID[]	Ідентифікатори алгоритмів підпису, що підтримуються ключем
certId	Base64	Ідентифікатор сертифікату в кеші сертифікатів. Опціональний
certificate	Base64	Сертифікат ключа (за стандартом x.509) у форматі base64. Опціональний
exportable	Boolean	Можливість експортування ключа із сховища. Опціональний
extAuth	String	Параметри додаткової автентифікації. Опціональний

Приклад результату:

```
{
  "errorCode": 0,
  "method": "SELECT_KEY",
  "result": {
    "signAlgo": ["1.2.804.2.1.1.1.1.3.1.1", ... ],
    "certId": "MIH+MIHlMQsw ... NQAAAFwAAAA=",
    "cert": "MIIErjCCBFagAwIBAgIUFXeRu ... NcYCFp23iPeya2s="
  }
}
```

Метод CREATE_KEY

Метод призначений для створення нового ключа у відкритому сховищі. Параметри за якими може бути створений ключ визначаються при відкритті сховища. Якщо параметри не вказані, то буде створений ключ з параметрами за замовчанням: алгоритм ECDSA, параметр P256. Коли метод виконаний успішно, то новий ключ стає поточним ключем у сховищі.

Структура поля parameters у запиті

Назва поля	**Тип**	**Опис**
mechanismId	String	Ідентифікатор алгоритму ключа. Опціональний
parameterId	String	Ідентифікатор параметру ключа. Опціональний
label	String	Текстове позначення ключа. Опціональний

Приклад запиту:

```
{
  "method": "CREATE_KEY",
  "parameters": {
    "mechanismId": "1.2.804.2.1.1.1.1.3.1",
    "parameterId": "1.2.804.2.1.1.1.1.3.1.1.2.6",
    "label": "new DSTU4145-key, M257_PB"
  }
}
```

Структура поля result у відповіді

Назва поля	**Тип**	**Опис**
id	Hex	Ідентифікатор ключа. Унікальний

Приклад результату:

```
{
  "errorCode": 0,
  "method": "CREATE_KEY",
  "result": {
    "id": "112233445566...DDEEFF00"
  }
}
```

Метод DELETE_KEY

Метод призначений для видалення ключа у відкритому сховищі. Результат — пуста структура.

Структура поля parameters у запиті

Назва поля	Тип	Опис
id	Hex	Ідентифікатор ключа. Унікальний

Приклад запиту:

```
{
  "method": "DELETE_KEY",
  "parameters": {
    "id": "112233445566...DDEEFF00"
  }
}
```

Приклад результату:

```
{
  "errorCode": 0,
  "method": "DELETE_KEY",
  "result": {}
}
```

Метод GET_CSR

Метод призначений для отримання запиту на формування сертифікату для поточного ключа. Якщо алгоритм підпису не вказаний, то використовується перший алгоритм підпису із списку signAlgo для ключа.

Структура поля parameters у запиті

Назва поля	Тип	Опис
signAlgo	String	Алгоритм підпису. Опціональний

Приклад запиту:

```
{
  "method": "GET_CSR",
  "parameters": {
    "signAlgo": "1.2.804.2.1.1.1.1.3.1.1"
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
bytes	Base64	Запит на формування сертифікату (за стандартом x.509)

Приклад результату:

```
{
  "errorCode": 0,
  "method": "GET_CSR",
  "result": {
    "bytes": "MIIBJTCBzgIBADAAMIGIMGA ... xV235n6GixwS"
  }
}
```

Метод CHANGE_PASSWORD

Метод призначений для зміни пароля у відкритому сховищі. Результат — пуста структура.

Структура поля parameters у запиті

Назва поля	Тип	Опис
password	String	Старий пароль
newPassword	String	Новий пароль

Приклад запиту:

```
{
  "method": "CHANGE_PASSWORD",
  "parameters": {
    "password": "123pass",
    "newPassword": "newpass"
  }
}
```

Приклад результату:

```
{
  "errorCode": 0,
  "method": "CHANGE_PASSWORD",
  "result": {}
}
```

Метод INIT_KEY_USAGE

Метод призначений для ініціалізації використання ключа. Параметри запиту і результату залежать від сховища.

Приклад запиту:

```
{
  "method": "INIT_KEY_USAGE",
  "parameters": {
    ...
  }
}
```

Приклад результату:

```
{
  "errorCode": 0,
  "method": "INIT_KEY_USAGE",
  "result": {}
}
```

Метод SIGN

Метод призначений для підпису даних.
В офлайновому стані бібліотека може зробити підпис у форматі CAdES-BES - перевірка статусу сертифіката власника буде виконуватися із застосуванням CRL, не використовуючи OCSP.
В опціях (поле "options") можна вказати додаткові параметри підпису.
Коли прапор "ignoreCertStatus" має значення true, то під час підпису не буде перевірятися статус сертифіката власника ключа. Опція доступна для використання лише для форматів підпису CAdES-BES та CAdES-T, для інших форматів підпису вона буде ігноруватися.
Опис форматів підпису дано в додатку 2.

Структура поля parameters у запиті

Назва поля	**Тип**	**Опис**
signParams	Object, SIGN_PARAMS	Набір параметрів підпису
dataTbs	Object[], DATA_TBS_PARAMS[]	Масив структур, що містять дані для підпису
keyParams	Object, KEY_PARAMS	Набір параметрів сховища ключа. Опціональний
options	Object, OPTION_PARAMS	Набір додаткових параметрів. Опціональний

Структура SIGN_PARAMS

Назва поля	**Тип**	**Опис**
signatureFormat	String	Формат підпису: "RAW", "CMS", "CAdES-BES", "CAdES-T", "CAdES-C", "CAdES-XL", "CAdES-A"
signAlgo	OID	Ідентифікатор алгоритму підпису. Опціональний
digestAlgo	OID	Ідентифікатор алгоритму гешування. Опціональний
detachedData	Boolean	Зовнішній підпис (дані не інкапсулюються). Опціональний, за замовченням true
includeCert	Boolean	Додати до підпису сертифікат власника ключа. Опціональний, за замовченням false
includeTime	Boolean	Додати до підпису час хосту (недовірений). Опціональний, за замовченням false
includeContentTS	Boolean	Додати до підпису позначку часу від даних. Опціональний, за замовченням false
certs	[]	Масив сертифікатів. Опціональний. (зарезервовано для майбутнього використання)

Структура DATA_TBS_PARAMS

Назва поля	**Тип**	**Опис**
id	String	Ідентифікатор даних
bytes	Base64	Дані для підпису
type	OID	Ідентифікатор тип даних. Опціональний, за замовчанням має "1.2.840.113549.1.7.1" (дані)

isDigest	Boolean	Тип даних для підпису. Якщо true, то поле bytes містить геш, інакше оригінальні дані. Опціональний, за замовчанням false
signedAttributes	Object[], ATTRIBUTE_PARAMS[]	Масив структур, що містять дані атрибутів для підписаної частини підпису. Опціональний
unsignedAttributes	Object[], ATTRIBUTE_PARAMS[]	Масив структур, що містять дані атрибутів для непідписаної частини підпису. Опціональний

Структура ATTRIBUTE_PARAMS

Назва поля	**Тип**	**Опис**
type	OID	Ідентифікатор типу атрибута
bytes	Base64	Дані атрибуту

Структура KEY_PARAMS

Назва поля	**Тип**	**Опис**
permission	Base64	* Дозвіл на використання. Опціональний
provider	String	Ідентифікатор провайдера. Опціональний
storage	String	Ідентифікатор сховища. Опціональний
keyId	Hex	Ідентифікатор ключа. Опціональний
username	String	Ім'я облікового запису користувача хмарного сховища. Опціональний
password	String	Пароль до сховища ключа. Опціональний
PIN	String	PIN-код доступу до ключа. Опціональний
OTP	String	Одноразовий код для доступу до віддаленого ключа. Опціональний
serial	String	Серійний номер пристрою. Опціональний (зарезервовано для майбутнього використання)
tokenLabel	String	Зарезервовано для майбутнього використання
keyLabel	String	Зарезервовано для майбутнього використання

Структура OPTION_PARAMS

Назва поля	**Тип**	**Опис**
ignoreCertStatus	Boolean	Не перевіряти статус сертифіката власника ключа. Опціональний, за замовчанням false

Приклад запиту:

```
{
  "method": "SIGN",
  "parameters": {
    "signParams": {
      "signatureFormat": "CAdES-BES",
      "signAlgo": "1.2.804.2.1.1.1.1.3.1.1",
      "detachedData": true,
      "includeCert": false,
      "includeTime": true
    },
    "dataTbs": [
      {
        "id": "doc-0",
        "bytes": "VGhlIHF1aWNrIGJyb ... p5IGRvZw=="
      }, {
        "id": "doc-1",
        "bytes": "VHJpcGxlIENyb3duIG9mIE1vdG9yc3BvcnQ="
      }
    ]
  }
}
```

Структура поля result у відповіді

Назва поля	**Тип**	**Опис**
signatures	Object[], SIGNATURE_PARAMS[]	Масив структур SIGNATURE_PARAMS, що містять підписані дані

Структура SIGNATURE_PARAMS

Назва поля	**Тип**	**Опис**
id	String	Ідентифікатор даних
bytes	Base64	Дані підпису

Приклад результату:

```
{
  "errorCode": 0,
  "method": "SIGN",
  "result": {
    "signatures": [
      {
        "id": "doc-0",
        "bytes": "MIISxQYJKoZIhvcNAQcCo...y26i8X+13kQ/l6"
      }, {
        "id": "doc-1",
        "bytes": "MIIHcgYJKoZIhvcNAQcCo...C719o6rNlQUrTOsBx8="
      }
    ]
  }
}
```

Метод VERIFY

Метод призначений для верифікації підписаних даних у CMS/CAdES-форматі або в криптографічному виді ("RAW"). Опис форматів підпису дано в додатку 2. Поле "signature" є обов'язковим — в ньому підписані дані зберігаються в полі "signature.bytes".
Для верифікації CMS/CAdES-формату підпису як зовнішнього підпису додатково вказують оригінальні дані в полі "signature.content". Якщо CMS/CAdES-формату підпис має інкапсульовані дані, то поле "signature.content" не використовується.

Метод підтримує три типа валідації підпису CMS/CAdES-формату (поле "options.validationType"):
1) "STRUCT" — валідація структури підпису (за замовчанням), перевіряється структура даних підпису, цифровий підпис підписаних атрибутів та позначок часу (за їх наявності);
2) "CHAIN" — валідація структури підпису та ланцюжка сертифікатів, включає до себе пункт 1 і створення ланцюжка сертифікатів підписувача та позначок часу (за їх наявності) за якими можна перевірити дійсність ланцюжка сертифікатів;
3) "FULL" — повна валідація підпису, включає до себе пункт 2 і валідацію дійсності всіх сертифікатів у ланцюжку на момент створення підпису.
Для спрощення аналізу результатів валідації підпису можна використовувати поля результату "validSignatures", "validDigests" й "bestSignatureTime". Поле "bestSignatureTime" містить найкращий довірений час підпису (в порядку пріоритету: "signingTime", "contentTS.genTime" та "signatureTS.genTime").
Коли використовується тип валідації "CHAIN" або "FULL" в поле "certificateChain" зберігається інформація про ланцюжок сертифікатів (масив записів CERT_CHAIN_INFO).
Якщо для валідації не вистачає сертифіката, то інформація для його пошуку зберігаються в полі "expectedCerts" (масив записів EXPECTED_CERT_INFO).
Якщо для визначення статусу сертифіката не вистачає CRL, то інформація для його пошуку зберігаються в полі "expectedCerts" (масив записів EXPECTED_CRL_INFO).
Поле "warnings" містить зауваження до результату валідації підпису (масив текстових рядків).
Під час повної валідації підпису для визначення статусу сертифіката використовується CRL. У випадку коли неможливо отримати CRL буде використовуватися OCSP-запит (онлайн). Щоб заборонити використання OCSP-сервісу необхідно встановити параметр "options.onlyCrl" в значення true (за замовчанням — false).

Для верифікації RAW-формату підпису необхідно більше параметрів:
1) поле "signParams" містить параметри підпису ("signAlgo" - обов'язково);
2) поле "signer" містить параметри публічного ключа підписувача;
3) поле "signature.content" містить оригінальні дані.

Структура поля parameters у запиті

Назва поля	**Тип**	**Опис**
signature	Object SIGNATURE_DATA	Структура SIGNATURE_DATA, що містять підписані дані
signParams	Object SIGN_PARAMS	Набір параметрів підпису. Умовно-опціональний
signer	Object SIGNER_PUBKEY	Набір параметрів підписувача. Умовно-опціональний
options	Object OPTION_PARAMS	Набір додаткових параметрів. Опціональний

Структура SIGNATURE_DATA

Назва поля	Тип	Опис
bytes	Base64	Підписані дані
content	Base64	Оригінальні дані. Умовно-опціональний
isDigest	Boolean	Якщо встановлений в true, то поле content містить геш від даних. За замовченням false

Структура SIGN_PARAMS

Назва поля	Тип	Опис
signAlgo	OID	Ідентифікатор алгоритму підпису

Структура SIGNER_PUBKEY

Назва поля	Тип	Опис
certificate	Base64	Сертифікат підписувача. Опціональний
certId	Base64	Ідентифікатор сертифіката підписувача. Опціональний
spki	Base64	Відкритий ключ підписувача з параметрами ключа, структура SubjectPublicKeyInfo за стандартом “x.509”. Опціональний

Структура OPTION_PARAMS

Назва поля	Тип	Опис
validationType	String	Тип валідації підпису: "STRUCT", "CHAIN", "FULL". Опціональний, за замовченням має "STRUCT"
onlyCrl	Boolean	Використовувати виключно CRL. Опціональний, за замовченням false

Приклад запиту для верифікації підписаних даних у “RAW”-форматі:

```
{
  "method": "VERIFY",
  "parameters": {
    "signature": {
      "bytes": "MEYCIQCpNEQQ...b0Icmdl+yPst",
      "content": "MWkwGAYJKoZI...AgUj+NmRJtw="
    },
    "signParams": {
      "signAlgo": "1.2.840.10045.4.3.2"
    },
    "signer": {
      "certId": "MIH+MIHlMQsw ... NQAAAFwAAAA="
    }
  }
}
```

Приклад запиту для верифікації підписаних даних у “CMS/CAdES”-форматі:

```
{
  "method": "VERIFY",
  "parameters": {
    "signature": {
      "bytes": "MIIHkQYJKoZI...ZNcGXe57GF5j"
    }
  }
}
```

В залежності від формату підписаних даних структура поля result відповіді відрізняються.

Структура поля result у відповіді верифікації підписаних даних у “CMS/CAdES”-форматі

Назва поля	**Тип**	**Опис**
content	Object CONTENT_INFO	Структура CONTENT_INFO
certIds	Base64[]	Масив ідентифікаторів сертифікатів, які присутні в підписаних даних
signatureInfos	Object[] SIGNATURE_INFO[]	Масив інформації по кожному підпису

Структура поля result у відповіді верифікації підписаних даних у “RAW”-форматі

Назва поля	**Тип**	**Опис**
statusSignature	String	Статус цифрового підпису: "VALID", "INVALID", "FAILED"

Структура CONTENT_INFO

Назва поля	**Тип**	**Опис**
type	OID	Ідентифікатор типу даних
bytes	Base64	Інкапсульовані дані. Опціональний

Структура SIGNATURE_INFO

Назва поля	**Тип**	**Опис**
signerCertId	Base64	Ідентифікатор сертифіката підписувача. Опціональний
signatureFormat	String	Формат CMS/CAdES-підпису: "CMS", "CAdES-BES", "CAdES-T", "CAdES-C", "CAdES-XL", "CAdES-A"
status	String	Статус підписаних даних: "UNDEFINED", "INDETERMINATE", "TOTAL-FAILED", "TOTAL-VALID"
validSignatures	Boolean	Всі криптографічні підписи, що відносяться до структури формату підпису, валідні
validDigests	Boolean	Всі геши, що відносяться до структури формату підпису, валідні
bestSignatureTime	Time	Найкращий час підпису

statusSignature	String	Статус цифрового підпису: "UNDEFINED", "INDETERMINATE", "FAILED", "INVALID", "VALID WITHOUT KEYUSAGE", "VALID"
statusMessageDigest	String	Статус цифрового дайджесту даних: "UNDEFINED", "INDETERMINATE", "FAILED", "INVALID", "VALID"
signingTime	Time	Локальний час підпису. Опціональний — присутній, якщо підписані дані мають відповідний атрибут
signaturePolicy	Object SIGN_POLICY_INFO	Політика підпису. Опціональний — присутній, якщо підписані дані мають відповідний атрибут
statusEssCert	String	Статус ідентифікації сертифіката підписника (опціональний): "UNDEFINED", "NOT PRESENT", "INDETERMINATE", "FAILED", "INVALID", "VALID"
contentTS	Object TIMESTAMP_INFO	Позначка часу від даних. Опціональний — присутній, якщо підписані дані мають відповідний атрибут
signatureTS	Object TIMESTAMP_INFO	Позначка часу від підпису. Опціональний — присутній, якщо підписані дані мають відповідний атрибут
statusCertificateRefs	String	Статус посилань на всі сертифікати в атрибуті certificateRefs (присутній у форматі підпису "CAdES-C", "CAdES-XL" та "CAdES-A"): "UNDEFINED", "NOT PRESENT", "INDETERMINATE", "FAILED", "INVALID", "VALID"
certificateRefs	Object[] CERT_REF_INFO[]	Масив посилань на всі сертифікати в атрибуті certificateRefs. Опціональний — присутній, якщо підпис має відповідний атрибут
certValues	Base64[]	Масив ідентифікаторів сертифікатів, які присутні в атрибуті certValues (присутній у форматі підпису "CAdES-XL" та "CAdES-A"). Опціональний
revocationRefs	Object[] REVOCATION_REF_INFO[]	Масив посилань на всі елементи відклику в атрибуті revocationRefs (присутній у форматі підпису "CAdES-C", "CAdES-XL" та "CAdES-A"). Опціональний
archiveTS	Object TIMESTAMP_INFO	Архівна позначка часу. Опціональний — присутній, якщо підписані дані мають відповідний атрибут
signedAttributes	Object[] ATTRIBUTE_PARAMS[]	Масив атрибутів, що зберігаються у полі signedAttributes
unsignedAttributes	Object[] ATTRIBUTE_PARAMS[]	Масив атрибутів, що зберігаються у полі unsignedAttributes. Опціональний
certificateChain	Object[] CERT_CHAIN_INFO[]	Масив результатів верифікації ланцюжків сертифікатів. Опціональний — присутній коли тип валідації підпису "CHAIN" або "FULL"
expectedCerts	Object[] EXPECTED_CERT_INFO[]	Масив інформації по сертифікату, який необхідний для верифікації підпису. Опціональний

expectedCrls	Object[] EXPECTED_CRL_INFO[]	Масив інформації по файлу CRL, який необхідний для верифікації підпису. Опціональний
warnings	String[]	Масив зауважень до результату перевірки. Опціональний

Структура поля SIGN_POLICY_INFO

Назва поля	**Тип**	**Опис**
sigPolicyId	OID	Ідентифікатор політики підпису

Структура TIMESTAMP_INFO

Назва поля	**Тип**	**Опис**
genTime	Time	Значення позначки часу
policyId	OID	Ідентифікатор політики TSP
hashAlgo	OID	Ідентифікатор алгоритму гешування
hashedMessage	Base64	Значення гешу
statusDigest	String	Статус значення позначки часу: "UNDEFINED", "NOT PRESENT", "INDETERMINATE", "FAILED", "INVALID", "VALID"
statusSignature	String	Статус перевірки підпису в позначці часу: "UNDEFINED", "NOT PRESENT", "INDETERMINATE", "FAILED", "INVALID", "VALID"
signerCertId	Base64	Ідентифікатор сертифіката підписувача позначки часу. Опціональний — присутній, якщо сертифікат знайдено в кеші сертифікатів

Структура поля CERT_REF_INFO

Назва поля	**Тип**	**Опис**
certHash	Object HASH_INFO	Інформація про геш сертифіката
issuer	Object RDNAME_INFO	Опис сертифіката. Перелік елементів опису сертифіката дано в додатку 5. Опціональний
serialNumber	Hex	Серійний номер сертифіката. Опціональний
status	String	Статус відповідності гешу сертифіката і сертифіката

Структура поля HASH_INFO

Назва поля	**Тип**	**Опис**
hashAlgo	OID	Ідентифікатор алгоритму гешування
hashAlgoParams	Base64	Параметри алгоритму гешування (DER-кодування ASN1). Опціональний
hashValue	Base64	Значення гешування

Структура поля REVOCATION_REF_INFO

Назва поля	Тип	Опис
crlIds	Object CRLID_INFO	Масив посилань на CRL. Опціональний
ocspIds	Object[] OCSPID_INFO	Масив посилань на OCSP-відповіді. Опціональний
otherRev	Object ATTRIBUTE_PARAMS	Альтернативна інформація про відкликання. Опціональний

Структура поля CRLID_INFO

Назва поля	Тип	Опис
crlHash	Object HASH_INFO	Інформація про геш CRL
crlIdentifier	Object CRLIDENTIFIER_INFO	Ідентифікатор CRL. Опціональний

Структура поля CRLIDENTIFIER_INFO

Назва поля	Тип	Опис
crlIssuer	Object RDNAME_INFO	Опис CRL. Перелік елементів опису CRL дано в додатку 5. Опціональний
crlIssuedTime	Time	Час видання CRL
crlNumber	Hex	Номер CRL. Опціональний

Структура поля OCSPID_INFO

Назва поля	Тип	Опис
ocspIdentifier	Object OCSPIDENTIFIER_INFO	Ідентифікатор OCSP-відповіді
ocspHash	Object HASH_INFO	Інформація про геш OCSP-відповіді. Опціональний

Структура поля OCSPIDENTIFIER_INFO

Назва поля	Тип	Опис
responderId	Object RDNAME_INFO або Hex	Опис сертифіката або ідентифікатор ключа OCSP-сервісу. Опціональний. Перелік елементів опису сертифіката дано в додатку 5
producedAt	Time	Час створення OCSP-відповіді

Структура CERT_CHAIN_INFO

Назва поля	Тип	Опис
subjectCertId	Base64	Ідентифікатор сертифіката
CN	String	Назва власника сертифіката (commonName)
entity	String	Призначення: "UNDEFINED", "SIGNER", "INTERMEDIATE", "CRL", "OCSP", "TSP", "CA", "ROOT"

source	String	Джерело: "UNDEFINED", "SIGNATURE", "STORE"
validity	Object CERT_VALIDITY	Період дії сертифіката
expired	Boolean	Ознака, що закінчився термін дії сертифіката
selfSigned	Boolean	Ознака, що сертифікат самопідписаний
trusted	Boolean	Ознака, що сертифікат довірений
issuerCertId	Base64	Ідентифікатор сертифіката видавця. Опціональний
statusSignature	String	Статус цифрового підпису сертифіката: "UNDEFINED", "INDETERMINATE", "FAILED", "INVALID", "VALID WITHOUT KEYUSAGE", "VALID"
validateByCRL	Object VALIDATE_BY_CRL_INFO	Результат перевірки сертифіката користувача з використанням CRL. Опціональний
validateByOCSP	Object VALIDATE_BY_OCSP_INFO	Результат перевірки сертифіката користувача з використанням OCSP. Опціональний
statusValidation	String	Статус валідації сертифіката: "UNDEFINED", "NONE", "VALID", "INVALID", "EXPIRED"

Структура поля CERT_VALIDITY

Назва поля	**Тип**	**Опис**
notBefore	Time	Дата з якої сертифікат починає бути дійсним
notAfter	Time	Дата з якої сертифікат перестає бути дійсним

Структура VALIDATE_BY_CRL_INFO

Назва поля	**Тип**	**Опис**
crlId	Base64	Ідентифікатор CRL в CRL-кеші
CN	String	Назва власника видавця CRL (commonName)
thisUpdate	Time	Час створення поточного CRL
nextUpdate	Time	Час створення наступного CRL
crlNumber	Hex	Порядковий номер випуску CRL
deltaCrlIndicator	Hex	Номер повного випуску CRL. Опціональний
issuerCertId	Base64	Ідентифікатор сертифіката видавця. Опціональний
statusSignature	String	Статус цифрового підпису CRL: "UNDEFINED", "INDETERMINATE", "FAILED", "INVALID", "VALID WITHOUT KEYUSAGE", "VALID"
status	String	Статус сертифіката: "UNDEFINED", "GOOD", "REVOKED", "UNKNOWN"
revocationReason	String	Підстава відкликання. Можливі наступні значення: "UNSPECIFIED", "KEY_COMPROMISE", "CA_COMPROMISE", "AFFILIATION_CHANGED", "SUPERSEDED", "CESSATION_OF_OPERATION", "CERTIFICATE_HOLD", "REMOVE_FROM_CRL", "PRIVILEGE_WITHDRAWN", "AA_COMPROMISE". Опціональний

revocationTime	Time	Час відкликання. Опціональний

Структура VALIDATE_BY_OCSP_INFO

Назва поля	**Тип**	**Опис**
source	String	Джерело: "UNDEFINED", "SIGNATURE", "STORE"
responseStatus	String	Статус OCSP-відповіді: "UNDEFINED", "SUCCESSFUL", "MALFORMED_REQUEST", "INTERNAL_ERROR", "TRY_LATER", "SIG_REQUIRED", "UNAUTHORIZED"
producedAt	Time	Час створення OCSP-відповіді
statusSignature	String	Статус цифрового підпису OCSP-відповіді: "UNDEFINED", "NOT PRESENT", "INDETERMINATE", "FAILED", "INVALID", "VALID"
signerCertId	Base64	Ідентифікатор сертифіката підписувача OCSP-відповіді. Опціональний
status	String	Статус сертифіката: "UNDEFINED", "GOOD", "REVOKED", "UNKNOWN"
thisUpdate	Time	Час створення поточного запису OCSP
nextUpdate	Time	Час створення наступного запису OCSP. Опціональний
revocationReason	String	Підстава відкликання. Можливі наступні значення: "UNSPECIFIED", "KEY_COMPROMISE", "CA_COMPROMISE", "AFFILIATION_CHANGED", "SUPERSEDED", "CESSATION_OF_OPERATION", "CERTIFICATE_HOLD", "REMOVE_FROM_CRL", "PRIVILEGE_WITHDRAWN", "AA_COMPROMISE". Опціональний
revocationTime	Time	Час відкликання. Опціональний

Структура EXPECTED_CERT_INFO

Назва поля	**Тип**	**Опис**
entity	String	Призначення: "UNDEFINED", "SIGNER", "INTERMEDIATE", "CRL", "OCSP", "TSP", "CA", "ROOT"
issuer	Object RDNAME_INFO	Опис сертифіката. Перелік елементів опису сертифіката дано в додатку 5. Опціональний
serialNumber	Hex	Серійний номер сертифіката. Опціональний
keyId	Hex	Ідентифікатор ключа. Опціональний
responderId	Object RDNAME_INFO або Hex	Опис сертифіката або ідентифікатор ключа OCSP-сервісу. Опціональний. Перелік елементів опису сертифіката дано в додатку 5

Структура EXPECTED_CRL_INFO

Назва поля	Тип	Опис
authorityKeyId	Hex	Ідентифікатор ключа видавця
issuer	Object RDNAME_INFO	Опис CRL. Перелік елементів опису CRL дано в додатку 5. Опціональний
url	String	URL зберігання CRL. Опціональний
full	Object CRL_FULL_INFO	Інформація про повний CRL. Опціональний

Структура поля CRL_FULL_INFO

Назва поля	Тип	Опис
thisUpdate	Time	Час створення поточного CRL
nextUpdate	Time	Час створення наступного CRL
crlNumber	Hex	Порядковий номер випуску CRL

Приклад результату верифікації підписаних даних у "CMS/CAdES"-форматі:


```
{
  "errorCode": 0,
  "method": "VERIFY",
  "result": {
    "content": {
      "type": "1.2.840.113549.1.7.1",
      "bytes": "QWxpY2UgYW5k...ZV9hbmRfQm9i"
    },
    "certIds": [ "MGwwVDELMAkG ... CwAAAD0AAAA=", ... ],
    "signatureInfos": [{
      "signerCertId": "MGwwVDELMAkG ... CwAAAD0AAAA=",
      "signatureFormat": "CAdES-T",
      "status": "TOTAL-VALID",
      "validSignatures": true,
      "validDigests": true,
      "bestSignatureTime": "2021-07-08 12:32:41",
      "statusSignature": "VALID",
      "statusMessageDigest": "VALID",
      "signingTime": "2021-07-08 12:32:39",
      "statusEssCert": "VALID",
      "contentTS": {
        "genTime": "2021-07-08 12:32:40",
        "policyId": "1.2.804.2.1.1.1.2.3.1",
        "hashAlgo": "1.2.804.2.1.1.1.1.2.1",
        "hashedMessage": "DxNVEwtKggoeT ... le3BwYCYMrIzM=",
        "statusDigest": "VALID",
        "statusSignature": "VALID",
        "signerCertId": "MIIBMTCCARcx ... EAAADkAAAA"
      },
      "signatureTS": {
        "genTime": "2021-07-08 12:32:41",
        "policyId": "1.2.804.2.1.1.1.2.3.1",
        "hashAlgo": "1.2.804.2.1.1.1.1.2.1",
        "hashedMessage": "cgdf4po1UowRj ... 4QmGX3iyPAMFg=",
        ...
      },
```

```
      "signedAttributes": [{
        "type": "1.2.840.113549.1.9.3",
        "bytes": "BgkqhkiG9w0BBwE="
      }, {
        "type": "1.2.840.113549.1.9.5",
        "bytes": "Fw0yMzAyMTUxNTI1MDda"
      }, {
        "type": "1.2.840.113549.1.9.4",
        "bytes": "BCAPE1UTC0qCC ... 7cHBgJgysjMw=="
      },
      ...
      ]
    }]
  }
}
```

Приклад результату верифікації підписаних даних у "RAW"-форматі:

```
{
  "errorCode": 0,
  "method": "VERIFY",
  "result": {
    "statusSignature": "VALID"
  }
}
```

Метод ENCRYPT

Метод призначений для шифрування даних.

Структура поля parameters у запиті

Назва поля	Тип	Опис
content	Object CONTENT_PARAMS	Структура з даними і параметрами шифрування
originatorCertIds	Base64[]	Масив ідентифікаторів сертифікатів відправника. Опціональний.
recipientInfos	Object[], RECIPINFO_PARAMS	Масив структур, що містять параметри отримувачів
unprotectedAttrs	Object[], ATTRIBUTE_PARAMS[]	Масив структур, що містять дані атрибутів для незашифрованої частини даних. Опціональний

Структура CONTENT_PARAMS

Назва поля	Тип	Опис
bytes	Base64	Дані для шифрування
encryptionAlgo	OID	Ідентифікатор алгоритму шифрування
type	OID	Ідентифікатор типу даних. За замовченням "1.2.840.113549.1.7.1" (pkcs7-data)

Структура RECIPINFO_PARAMS

Назва поля	Тип	Опис
certId	Base64	Ідентифікатор сертифіката отримувача
kdfAlgo	OID	Ідентифікатор алгоритму функції формування ключа
keyWrapAlgo	OID	Ідентифікатор алгоритму обгортання ключа. Опціональний, залежить від kdfAlgo

Структура ATTRIBUTE_PARAMS

Назва поля	Тип	Опис
type	OID	Ідентифікатор типу атрибуту
bytes	Base64	Дані атрибуту

Рекомендовані схеми шифрування даних

№	encryptionAlgo	kdfAlgo	keyWrapAlgo
1	"1.2.804.2.1.1.1.1.1.3.3.2"	"1.2.804.2.1.1.1.1.3.7"	"1.2.804.2.1.1.1.1.1.3.11"
2	"1.2.804.2.1.1.1.1.1.3.3.2"	"1.2.804.2.1.1.1.1.3.8"	"1.2.804.2.1.1.1.1.1.3.11"
3	"1.2.804.2.1.1.1.1.1.1.3"	"1.2.804.2.1.1.1.1.3.4"	"1.2.804.2.1.1.1.1.1.1.5"
4	"1.2.804.2.1.1.1.1.1.1.3"	"1.2.804.2.1.1.1.1.3.5"	"1.2.804.2.1.1.1.1.1.1.5"

Приклад запиту:

```
{
  "method": "ENCRYPT",
  "parameters": {
    "content": {
      "bytes": "VGhlIHF1aWNrIGJyb ... p5IGRvZw==",
      "encryptionAlgo": "1.2.804.2.1.1.1.1.1.1.3"
      },
    "recipientInfos": [
      {
        "certId": "MIH6MIHhMRYw ... HgYAdKV2AA==",
        "kdfAlgo": "1.2.804.2.1.1.1.1.3.4"
      }
    ]
  }
}
```

Структура поля result у відповіді

Назва поля	**Тип**	**Опис**
bytes	Base64	Зашифровані дані

Приклад результату:

```
{
  "errorCode": 0,
  "method": "ENCRYPT",
  "result": {
    "bytes": "MIIBSAYJKoZIhvcNAQcDo ... srvSh3rZYugDU="
  }
}
```

Метод DECRYPT

Метод призначений для розшифрування даних.

Структура поля parameters у запиті

Назва поля	Тип	Опис
bytes	Base64	Зашифровані дані

Приклад запиту:

```
{
  "method": "DECRYPT",
  "parameters": {
    "bytes": "MIIBSAYJKoZIhvcNAQcDo ... srvSh3rZYugDU="
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
content	Object CONTENT_INFO	Структура CONTENT_INFO, що містить розшифровані дані
originatorCertId	Base64	Ідентифікатор сертифіката відправника
unprotectedAttrs	Object[]	Масив атрибутів у структурі ATTRIBUTE_PARAMS, що зберігаються у полі unprotectedAttrs. Опціональний

Структура CONTENT_INFO

Назва поля	Тип	Опис
bytes	Base64	Розшифровані дані
type	OID	Ідентифікатор типу даних

Приклад результату:

```
{
  "errorCode": 0,
  "method": "DECRYPT",
  "result": {
    "content": {
      "bytes": "VGhlIHF1aWNrIGJyb ... p5IGRvZw==",
      "type": "1.2.840.113549.1.7.1"
    },
    "originatorCertId": "MIH6MIHhMRYw ... HgYAdKV2AA=="
  }
}
```

Метод ADD_CERT

Метод призначений для додавання сертифікатів до кешу сертифікатів. Сертифікати додаються двома способами: масивом сертифікатів або (одним) пакетом сертифікатів (p7b-файл). Якщо сертифікат, що додається до кешу сертифікатів вже зберігається в кеші, то він не буде доданий — у відповіді буде повернутий ідентифікатор існуючого сертифікату (ознака isUnique буде мати значення false).

Структура поля parameters у запиті

Назва поля	Тип	Опис
certificates	Base64[]	Масив сертифікатів. Взаємовиключний до поля bundle
bundle	Base64	Пакет сертифікатів. Взаємовиключний до поля certificates
permanent	Boolean	Ознака зберегти сертифікат у кешу сертифікатів

Приклад запиту:

```
{
  "method": "ADD_CERT",
  "parameters": {
    "certificates": [ "MIIErjCCBFag...Fp23iPeya2s=", ... ],
    "permanent": true
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
added	Object[] CERT_ADDED[]	Масив інформації про додані сертифікатів

Структура CERT_ADDED

Назва поля	Тип	Опис
certId	Base64	Ідентифікатор сертифікату в кеші сертифікатів
isUnique	Boolean	Ознака унікальності сертифікату

Приклад результату:

```
{
  "errorCode": 0,
  "method": "ADD_CERT",
  "result": {
    "added": [
      {
        "certId": "MIH+MIHlMQsw ... NQAAAFwAAAA=",
        "isUnique": true
      }, {
        "certId": "MIGFMG0xCzAJ ... AAAAhAAAAA==",
        "isUnique": false
      },
      ...
    ]
  }
}
```

Метод CERT_INFO

Метод призначений для отримання інформації, яка зберігається в сертифікаті. Сертифікат повинен бути відповідним стандарту x.509 та мати мінімальну версію 3.
Метод повертає масив розширень сертифікату в тому порядку в якому вони зберігаються в сертифікаті. Якщо розширення сертифікату відомо бібліотеці, то воно буде декодоване. Перелік розширень сертифікату, які можуть бути декодованими в CERT_INFO дано в додатку 3.

Структура поля parameters у запиті

Назва поля	Тип	Опис
bytes	Base64	Сертифікат. Взаємовиключний до поля certId
certId	Base64	Ідентифікатор сертифікату. Взаємовиключний до поля bytes

Приклад запиту:

```
{
  "method": "CERT_INFO",
  "parameters": {
    "bytes": "MIIErjCCBFagAwIBAgIUFXeRu...NcYCFp23iPeya2s="
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
bytes	Base64	Сертифікат в DER-кодуванні ASN1
version	Integer	Версія сертифікату
serialNumber	Hex	Унікальний номер сертифікату в ЦСК
issuer	Object	Опис видавця сертифікату
validity	Object CERT_VALIDITY	Період дії сертифікату
subject	Object	Опис власника сертифікату
subjectPublicKeyInfo	Object SUBJECT_PUBLICKEY_INFO	Публічний ключ власника сертифікату
extensions	Object[], EXTENSION_INFO[]	Масив розширеній які має сертифікат
signatureInfo	Object SIGNATURE_INFO	Цифровий підпис сертифікату
selfSigned	Boolean	Ознака, що сертифікат самопідписаний

Структура SUBJECT_PUBLICKEY_INFO

Назва поля	Тип	Опис
bytes	Base64	DER-кодоване поле subjectPublicKeyInfo
algorithm	String	Ідентифікатор алгоритму публічного ключа
parameters	Base64	Параметри алгоритму публічного ключа
publicKey	Base64	Значення публічного ключа

Структура EXTENSION_INFO

Назва поля	Тип	Опис
extnId	String	Ідентифікатор розширення
critical	Boolean	Ознака, що розширення критичне. Опціональний
extnValue	Base64	Закодоване значення розширення
decoded	Object DECODED_EXTENSION_INFO	Декодоване значення розширення. Опціональний

Структура DECODED_EXTENSION_INFO

Назва поля	Тип	Опис
id	String	Найменування розширення
value	Object	Значення розширення.

Структура SIGNATURE_INFO

Назва поля	Тип	Опис
algorithm	String	Ідентифікатор алгоритму підпису
parameters	Base64	Параметри алгоритму підпису. Опціональний
signature	Base64	Значення підпису

Приклад результату:


```
{
  "errorCode": 0,
  "method": "CERT_INFO",
  "result": {
    "bytes": "MIIErjCCBFagAwIBAg...cYCFp23iPeya2s=",
    "version": 3,
    "serialNumber": "157791B9508857ED04000000...0000",
    "issuer": {
      "C": "UA",
      "SERIALNUMBER": "UA-12345678-0001",
      "CN": "Центр сертифікації ключів",
      "O": "ТОВ Магія",
      "OU": "ЦСК",
      "L": "Київ"
    },
    "validity": {
      "notBefore": "2020-08-26 12:34:56",
      "notAfter": "2022-08-26 12:34:56"
    },
    "subject": {
      "C": "UA",
      "CN": "Серпень Аугусто",
      "L": "Марсополіс",
      "SN": "Серпень",
      "G": "Аугусто"
    },
    "subjectPublicKeyInfo": {
      "bytes": "MFkwEwYHKoZIzj0CAQY...nZOCZhbZMl3XsA==",
      "algorithm": "1.2.804.2.1.1.1.1.3.1.1",
      "parameters": "MFEGDSqGJAIBAQEBAwEB...uPrFeQQ=",
      "publicKey": "BCEhu7U+dG5kWwuTfPV30tf...8SjmlDitQE="
```

```
    },
    "extensions": [
      {
        "extnId": "2.5.29.14",
        "extnValue": "BCAzM/MjlbJMdildTG...98Wazw8wPoj+g==",
        "decoded": {
          "id": "subjectKeyIdentifier",
          "value": {
            "keyIdentifier": "BCB3BE7274D075DD...1370"
          }
        }
      },
      {
        "extnId": "2.5.29.35",
        "extnValue": "BCC8s75ydNB13VIlK2...PPVx/adALwTcA==",
        "decoded": {
          "id": "authorityKeyIdentifier",
          "value": {
            "keyIdentifier": "D0069AA0A8DF7D707A...28CC7"
          }
        }
      },
      {
        "extnId": "2.5.29.15",
        "critical": true,
        "extnValue": "AwIGwA==",
        "decoded": {
          "id": "keyUsage",
          "value": {
            "digitalSignature": true,
            "contentCommitment": true
          }
        }
      },
      ...
    ],
    "signatureInfo": {
      "algorithm": "1.2.804.2.1.1.1.1.3.1.1",
      "signature": "MIIErjCCBFagAwIBAg...cYCFp23iPeya2s="
    },
    "selfSigned": false
  }
}
```

Метод GET_CERT

Метод призначений для отримання сертифікату (в DER-кодуванні) із кешу сертифікатів. Метод повертає сертифікат якщо він є в кеші сертифікатів, інакше повертається помилка - сертифікат не знайден ("CERT_NOT_FOUND").

Структура поля parameters у запиті

Назва поля	Тип	Опис
certId	Base64	Ідентифікатор сертифікату

Приклад запиту:

```
{
  "method": "GET_CERT",
  "parameters": {
    "certId": "MIH+MIHlMQsw ... NQAAAFwAAAA="
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
bytes	Base64	Сертифікат

Приклад результату:

```
{
  "errorCode": 0,
  "method": "GET_CERT",
  "result": {
    "bytes": "MIIErjCCBFag...Fp23iPeya2s="
  }
}
```

Метод LIST_CERTS

Метод призначений для отримання переліку ідентифікаторів сертифікатів із кешу сертифікатів. Підтримує пагінацію.

Структура поля parameters у запиті

Назва поля	Тип	Опис
offset	Integer	Індекс першого сертифікату. Опціональний (значення за замовчанням: 0)
pageSize	Integer	Максимальна кількість сертифікатів. Опціональний

Приклад запиту:

```
{
  "method": "LIST_CERTS",
  "parameters": {
    "offset": 10,
    "pageSize": 10
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
certIds	Base64[]	Масив ідентифікаторів сертифікатів
count	Integer	Кількість сертифікатів
offset	Integer	Індекс першого сертифікату
pageSize	Integer	Максимальна кількість сертифікатів

Приклад результату:

```
{
  "errorCode": 0,
  "method": "LIST_CERTS",
  "result": {
    "certIds": [ "MIGWMH4xCzAJ ... AAQAAAALAAAA", ... ],
    "count": 29,
    "offset": 10,
    "pageSize": 10
  }
}
```

Метод REMOVE_CERT

Метод видаляє сертифікат якщо він є в кеші сертифікатів, інакше повертається помилка - сертифікат не знайдено ("CERT_NOT_FOUND"). Результат — пуста структура.

Структура поля parameters у запиті

Назва поля	Тип	Опис
bytes	Base64	Сертифікат. Взаємовиключний до поля certId
certId	Base64	Ідентифікатор сертифікату. Взаємовиключний до поля bytes

Приклад запиту:

```
{
  "method": "REMOVE_CERT",
  "parameters": {
    "certId": "MIH+MIHlMQsw ... NQAAAFwAAAA="
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис

Приклад результату:

```
{
  "errorCode": 0,
  "method": "REMOVE_CERT",
  "result": {}
}
```

Метод VERIFY_CERT

Метод призначений для верифікації сертифікату. Якщо сертифікат самопідписаний, то поле issuerCertId у відповіді відсутнє.
Поле validateTime встановлює значення часу за який треба визначити валідність сертифікату за CRL. Якщо це поле відсутнє, то використовується поточний час хосту.

Структура поля parameters у запиті

Назва поля	Тип	Опис
bytes	Base64	Сертифікат. Взаємовиключний до поля certId
certId	Base64	Ідентифікатор ключа. Взаємовиключний до поля certificate
validationType	String	Типи валідації сертифікату за статусом відкликання. Має наступні значення: "CRL" та "OCSP". Опціональний
validateTime	Time	Значення часу валідації. Опціональний, використовується при використанні CRL

Приклад запиту:

```
{
  "method": "VERIFY_CERT",
  "parameters": {
    "bytes": "MIIErjCCBFag...Fp23iPeya2s="
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
validateTime	Time	Значення часу перевірки валідації
subjectCertId	Base64	Ідентифікатор сертифіката користувача
validity	Object CERT_VALIDITY	Період дії сертифіката користувача
expired	Boolean	Ознака, що закінчився термін дії сертифіката
selfSigned	Boolean	Ознака, що сертифікат самопідписаний
trusted	Boolean	Ознака, що сертифікат довірений
statusSignature	String	Статус цифрового підпису сертифіката: "VALID", "INVALID", "FAILED"
issuerCertId	Base64	Ідентифікатор сертифікату видавця. Опціональний
validateByCRL	Object VALIDATE_BY_CRL	Результат перевірки сертифіката користувача з використанням CRL. Опціональний
validateByOCSP	Object VALIDATE_BY_OCSP	Результат перевірки сертифіката користувача з використанням OCSP. Опціональний

Структура поля VALIDATE_BY_CRL

Назва поля	Тип	Опис
status	String	Статус сертифіката: "UNDEFINED", "GOOD", "REVOKED", "UNKNOWN"
revocationReason	String	Підстава відкликання. Можливі наступні значення: "UNDEFINED", "UNSPECIFIED", "KEY_COMPROMISE", "CA_COMPROMISE", "AFFILIATION_CHANGED", "SUPERSEDED", "CESSATION_OF_OPERATION", "CERTIFICATE_HOLD", "REMOVE_FROM_CRL", "PRIVILEGE_WITHDRAWN", "AA_COMPROMISE". Опціональний
revocationTime	Time	Час відкликання. Опціональний
full	Object CRL_INFO	Інформація про повний CRL
delta	Object CRL_INFO	Інформація про частковий CRL. Опціональний

Структура поля CRL_INFO

Назва поля	Тип	Опис
url	String	URL зберігання CRL. Опціональний
crlId	Base64	Ідентифікатор CRL в CRL-кеші
statusSignature	String	Статус цифрового підпису CRL: "VALID", "INVALID", "FAILED"

Структура поля VALIDATE_BY_OCSP

Назва поля	Тип	Опис
status	String	Статус сертифіката: "UNDEFINED", "GOOD", "REVOKED", "UNKNOWN"
revocationReason	String	Підстава відкликання. Можливі наступні значення: "UNDEFINED", "UNSPECIFIED", "KEY_COMPROMISE", "CA_COMPROMISE", "AFFILIATION_CHANGED", "SUPERSEDED", "CESSATION_OF_OPERATION", "CERTIFICATE_HOLD", "REMOVE_FROM_CRL", "PRIVILEGE_WITHDRAWN", "AA_COMPROMISE". Опціональний
revocationTime	Time	Час відкликання. Опціональний
responseStatus	String	Статус OCSP-відповіді: "UNDEFINED", "SUCCESSFUL", "MALFORMED_REQUEST", "INTERNAL_ERROR", "TRY_LATER", "SIG_REQUIRED", "UNAUTHORIZED"
responderId	Object RDNAME_INFO або Hex	Опис сертифіката або ідентифікатор ключа OCSP-сервісу. Опціональний. Перелік елементів опису сертифіката дано в додатку 5
statusSignature	String	Статус цифрового підпису OCSP-відповіді: "VALID", "INVALID", "FAILED"
producedAt	Time	Час створення OCSP-відповіді
thisUpdate	Time	Час створення поточного запису OCSP

nextUpdate	Time	Час створення наступного запису OCSP. Опціональний

Приклад результату:


```
{
  "errorCode": 0,
  "method": "VERIFY_CERT",
  "result": {
    "validateTime": "2021-04-29 12:34:56",
    "subjectCertId": "MIH+MIHlMQsw ... NQAAAFwAAAA=",
    "validity": {
      "notBefore": "2020-08-26 23:13:07",
      "notAfter": "2022-08-26 23:13:07"
    },
    "expired": false,
    "selfSigned": false,
    "trusted": false,
    "statusSignature": "VALID",
    "issuerCertId": "MIH+MIHlMQsw ... AQAAAAEAAAA="
  }
}
```


Приклад результату з OCSP-відповіддю:


```
{
  "errorCode": 0,
  "method": "VERIFY_CERT",
  "result": {
    "validateTime": "2021-04-29 12:34:56",
    "subjectCertId": "MIH+MIHlMQsw ... NQAAAFwAAAA=",
    "validity": {
      "notBefore": "2020-08-26 23:13:07",
      "notAfter": "2022-08-26 23:13:07"
    },
    "expired": false,
    "selfSigned": false,
    "trusted": false,
    "statusSignature": "VALID",
    "issuerCertId": "MIH+MIHlMQsw ... AQAAAAEAAAA=",
    "validateByOCSP": {
      "status": "GOOD",
      "responseStatus": "SUCCESSFUL",
      "responderId": {
        "O": "Test CA",
        "CN": "OCSP-service",
        "C": "UA",
        "L": "Київ"
      },
      "statusSignature": "VALID",
      "producedAt": "2021-04-29 12:34:56",
      "thisUpdate": "2021-04-29 12:34:56"
    }
  }
}
```

Метод ADD_CRL

Метод призначений для додавання CRL до кешу CRL. Повертає ідентифікатор CRL у CRL-кеші.

Структура поля parameters у запиті

Назва поля	Тип	Опис
bytes	Base64	CRL
permanent	Boolean	Ознака зберегти CRL у кешу CRL

Приклад запиту:

```
{
  "method": "ADD_CRL",
  "parameters": {
    "bytes": "MIIJajCCCRIC...15Wd5gBHHCg="
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
crlId	Base64	Ідентифікатор CRL
isUnique	Boolean	Ознака унікальності сертифікату

Приклад результату:

```
{
  "errorCode": 0,
  "method": "ADD_CRL",
  "result": {
    "crlId": "MIHtMIHlMQsw ... 0ZfQsgIDAULT",
    "isUnique": true
  }
}
```

Метод CRL_INFO

Метод призначений для отримання інформації, яка зберігається в CRL (списку відкликаних сертифікатів). CRL повинен бути відповідним стандарту x.509.

Структура поля parameters у запиті

Назва поля	Тип	Опис
bytes	Base64	CRL

Приклад запиту:

```
{
  "method": "CRL_INFO",
  "parameters": {
    "bytes": "MIIJajCCCRIC...15Wd5gBHHCg="
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
issuer	Object	Опис видавця
thisUpdate	Time	Час створення поточного CRL
nextUpdate	Time	Час створення наступного CRL
countRevokedCerts	Integer	Кількість CRL записів
authorityKeyId	Hex	Ідентифікатор ключа CA. Опціональний
crlNumber	Hex	Порядковий номер випуску CRL. Опціональний
deltaCrlIndicator	Hex	Номер повного випуску CRL. Опціональний
revokedCerts	Object[] REVOKED_CERT_INFO[]	Масив записів CRL (структура REVOKED_CERT_INFO). Опціональний

Структура поля REVOKED_CERT_INFO

Назва поля	Тип	Опис
userCertificate	Hex	Серійний номер відкликаного сертифікату
revocationDate	Time	Час відкликання
crlReason	String	Підстава відкликання. Опціональний. Можливі наступні значення: "UNDEFINED", "UNSPECIFIED", "KEY_COMPROMISE", "CA_COMPROMISE", "AFFILIATION_CHANGED", "SUPERSEDED", "CESSATION_OF_OPERATION", "CERTIFICATE_HOLD", "REMOVE_FROM_CRL", "PRIVILEGE_WITHDRAWN", "AA_COMPROMISE"
invalidityDate	Time	Час недійсності

Приклад результату:


```
{
  "errorCode": 0,
  "method": "CRL_INFO",
  "result": {
    "issuer": {
      "C": "UA",
      "SERIALNUMBER": "UA-12345678-0001",
      "CN": "Центр сертифікації ключів",
      "O": "Організація",
      "OU": "ЦСК",
      "L": "Київ"
    },
    "thisUpdate": "2021-07-31 06:00:00",
    "nextUpdate": "2021-08-07 06:00:00",
    "countRevokedCerts": 25,
    "authorityKeyId": "D0069AA0...9EA28CC7",
    "crlNumber": "0142D3",
    "revokedCerts": [
      {
        "userCertificate": "157791B95088...14000000",
        "revocationDate": "2019-04-17 15:16:22",
        "crlReason": "SUPERSEDED",
        "invalidityDate": "2019-04-17 15:16:22"
      }, {
        "userCertificate": "157791B95088...35000000",
        "revocationDate": "2019-11-07 14:20:06",
        "crlReason": "CERTIFICATE_HOLD",
        "invalidityDate": "2019-11-07 14:20:06"
      },
      ...
    ]
  }
}
```

Метод DIGEST

Метод призначений для гешування даних. Для вказання алгоритму гешування використовується параметри hashAlgo або signAlgo (одночасно тільки один із двох). Дані для гешування можуть бути задані або безпосередньо у вигляді base64-кодованої строки, або вказанням імені файлу, або вказання на область пам'яті.

Структура поля parameters у запиті для верифікації цифрового підпису

Назва поля	Тип	Опис
hashAlgo	String	Алгоритм гешування. Взаємовиключний до поля signAlgo
signAlgo	String	Алгоритм підпису. Взаємовиключний до поля hashAlgo
bytes	Base64	Вхідні дані, якщо дані задані безпосередньо
file	String	Вхідні дані, що зберігаються у файлі
ptr	Hex	Покажчик на дані в оперативній пам'яті
size	Number	Довжина вхідних даних в оперативній пам'яті

Приклад запиту, дані задані безпосередньо:

```
{
  "method": "DIGEST",
  "parameters": {
    "hashAlgo": "2.16.840.1.101.3.4.2.1",
    "bytes": "VGhlIHF1aWNrIGJyb3duIGZve...IGRvZw=="
  }
}
```

Приклад запиту, дані задані що зберігаються у файлі:

```
{
  "method": "DIGEST",
  "parameters": {
    "hashAlgo": "2.16.840.1.101.3.4.2.1",
    "file": "~/docs/filename.doc"
  }
}
```

Приклад запиту, дані знаходяться в пам'яті:

```
{
  "method": "DIGEST",
  "parameters": {
    "hashAlgo": "2.16.840.1.101.3.4.2.1",
    "ptr": "000001940D2F8400",
    "size": 10000000
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
hashAlgo	String	Алгоритм гешування, який був використаний
bytes	Base64	Значення геш-функції від даних

Приклад результату:


```
{
  "errorCode": 0,
  "method": "DIGEST",
  "result": {
    "hashAlgo": "2.16.840.1.101.3.4.2.1",
    "bytes": "16j7swfXgJRpypq8sAguT41...vzfJ5ZI="
  }
}
```

Метод ASN1_DECODE

Метод призначений для декодування DER-кодованих ASN1 даних. Перелік ASN1-типів, що можуть бути декодовані дано в додатку 4.

Структура поля parameters у запиті

Назва поля	Тип	Опис
items	Object[], DECODE_ITEM[]	Масив структур, що містять дані для декодування

Структура DECODE_ITEM

Назва поля	Тип	Опис
bytes	Base64	Дані для декодування
id	String	Ідентифікатор даних. Опціональний

Приклад запиту:

```
{
  "method": "ASN1_DECODE",
  "parameters": {
    "items": [{
      "bytes": "BAowMTIzNDU2Nzg5",
      "id": "octet-10bytes"
    }, {
      "bytes": "AgEB",
      "id": "integer-1"
    }, {
      "bytes": "AgMBAAE=",
      "id": "integer-65537"
    }, {
      "bytes": "AhQ9tz578NV1sgEAAAABAAAAugAAAA==",
      "id": "integer-big"
    }, {
      "bytes": "AQH/"
    }, {
      "bytes": "BQA="
    }, {
      "bytes": "BgQqAwQF"
    }, {
      "bytes": "EwJVQQ=="
    }, {
      "bytes": "ExdFeGFtcGxlOiBBbGljZSBhbmQgQm9iLg=="
    }, {
      "bytes": "DCXQn9GA0LjQutC70LDQtDog0JDQu9GW0YHQsCDRliDQkdC+0LEu"
    }, {
      "bytes": "Fw0yMTA3MDgxMjM0NTZa"
    }, {
      "bytes": "GA8yMDIxMDcwODEyMzQ1Nlo="
    }, {
      "bytes": "AwIGwA=="
    }]
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
decoded	Object[], DECODED_ITEM[]	Масив структур, що містять декодовані дані

Структура DECODED_ITEM

Назва поля	Тип	Опис
tag	String	Ідентифікатор ASN1-типу (тег)
value	Base64 Boolean String	Декодоване значення відповідно ASN1-типу
integer	Integer	Ціле число. Опціональний
bytes	Base64	Значення без декодування. Опціональний

Приклад результату:


```
{
  "errorCode": 0,
  "method": "ASN1_DECODE",
  "result": {
    "decoded": [{
      "id": "octet",
      "tag": "OCTET_STRING",
      "value": "MDEyMzQ1Njc4OQ=="
    }, {
      "id": "integer-1",
      "tag": "INTEGER",
      "value": "AQ==",
      "integer": 1
    }, {
      "id": "integer-65537",
      "tag": "INTEGER",
      "value": "AQAB",
      "integer": 65537
    }, {
      "id": "integer-big",
      "tag": "INTEGER",
      "value": "Pbc+e/DvdbIBAAAAAQAAALoAAAA="
    }, {
      "tag": "BOOLEAN",
      "value": true
    }, {
      "tag": "NULL"
    }, {
      "tag": "OID",
      "value": "1.2.3.4.5"
    }, {
      "tag": "PRINTABLE_STRING",
      "value": "UA",
      "bytes": "VUE="
    }, {
      "tag": "PRINTABLE_STRING",
      "value": "Example: Alice and Bob.",
      "bytes": "RXhhbXBsZTogQWxpY2UgYW5kIEJvYi4="
    }, {
```

```
      "tag": "UTF8_STRING",
      "value": "Приклад: Аліса і Боб.",
      "bytes": "0J/RgNC40LrQu9Cw0LQ6INCQ0LvRltGB0LAg0ZYg0JHQvtCxLg=="
    }, {
      "tag": "UTC_TIME",
      "value": "2021-07-08 12:34:56",
      "integer": 1625747696000
    }, {
      "tag": "GENERALIZED_TIME",
      "value": "2021-07-08 12:34:56",
      "integer": 1625747696000
    }, {
      "tag": "BIT_STRING",
      "value": "wA==",
      "integer": 3
    }]
  }
}
```

Метод ASN1_ENCODE

Метод призначений для кодування даних згідно DER-кодування ASN1. Перелік ASN1-типів, що можуть бути кодовані дано в додатку 4.

Структура поля parameters у запиті

Назва поля	Тип	Опис
items	Object[], ENCODE_ITEM[]	Масив структур, що містять дані для кодування

Структура ENCODE_ITEM

Назва поля	Тип	Опис
tag	String	Ідентифікатор ASN1-типу (тег)
value	Base64 Boolean String	Дані для кодування. Опціональний, залежить від типу
integer	Integer	Ціле число. Опціональний, залежить від типу
id	String	Ідентифікатор даних. Опціональний

Приклад запиту:

```
{
  "method": "ASN1_ENCODE",
  "parameters": {
    "items": [{
      "id": "octet",
      "tag": "OCTET_STRING",
      "value": "MDEyMzQ1Njc4OQ=="
    }, {
      "id": "integer-1-as-integer",
      "tag": "INTEGER",
      "integer": 1
    }, {
      "id": "integer-2-as-value",
      "tag": "INTEGER",
      "value": "Ag=="
    }, {
      "id": "integer-65537-as-integer",
      "tag": "INTEGER",
      "integer": 65537
    }, {
      "id": "integer-big",
      "tag": "INTEGER",
      "value": "Pbc+e/DVdbIBAAAAAQAAALoAAAA="
    }, {
      "id": "null",
      "tag": "NULL"
    }, {
      "id": "oid",
      "tag": "OID",
      "value": "1.2.3.4.5"
    }]
  }
}
```

Структура поля result у відповіді

Назва поля	Тип	Опис
encoded	Object[], ENCODED_ITEM[]	Масив структур, що містять кодовані дані

Структура ENCODED_ITEM

Назва поля	Тип	Опис
bytes	Base64	Кодовані дані
id	String	Ідентифікатор даних. Опціональний

Приклад результату:

```
{
  "errorCode": 0,
  "method": "ASN1_ENCODE",
  "result": {
    "encoded": [{
      "id": "octet",
      "bytes": "BAowMTIzNDU2Nzg5"
    }, {
      "id": "integer-1-as-integer",
      "bytes": "AgEB"
    }, {
      "id": "integer-2-as-value",
      "bytes": "AgEC"
    }, {
      "id": "integer-65537-as-integer",
      "bytes": "AgMBAAE="
    }, {
      "id": "integer-big",
      "bytes": "AhQ9tz578NV1sgEAAAABAAAAugAAAA=="
    }, {
      "id": "null",
      "bytes": "BQA="
    }, {
      "id": "oid",
      "bytes": "BgQqAwQF"
    }]
  }
}
```

Додаток 1. Коди помилок

Таблиця. Коди помилок

Код	Опис
RET_OK	Операція виконана успішно
RET_UAPKI_GENERAL_ERROR	Невизначена помилка
RET_UAPKI_CONNECTION_ERROR	Помилка з'єднання з сервером
RET_UAPKI_INVALID_JSON_FORMAT	Неправильний формат JSON запиту
RET_UAPKI_INVALID_METHOD	Метод не існує
RET_UAPKI_INVALID_PARAMETERS	Інвалідний параметр
RET_UAPKI_UNKNOWN_PROVIDER	Невідомий провайдер
RET_UAPKI_FILENAME_REQUIRED	Потребує ім'я файлу як ідентифікатор сховища
RET_UAPKI_LOGIN_REQUIRED	Потребує ім'я користувача як ідентифікатор сховища
RET_UAPKI_NOT_INITIALIZED	Бібліотеку не ініціалізовано
RET_UAPKI_ALREADY_INITIALIZED	Бібліотеку вже ініціалізовано
RET_UAPKI_NO_STORAGE	Сховище не відкрито
RET_UAPKI_NO_KEY	Ключ не вибрано
RET_UAPKI_INVALID_KEY_USAGE	Ключ не може бути використаний для операції не за призначенням
RET_UAPKI_NOT_ALLOWED	Операція не дозволена

Додаток 2. Перелік форматів підпису

Таблиця. Перелік форматів підпису, що підтримуються бібліотекою

Назва формату	Короткий опис
RAW	Вихідна послідовність даних ЕЦП. Має специфічний бінарний формат для кожного алгоритму цифрового підпису.
CMS	Базовий формат підпису з ідентифікацією підписувача за ідентифікатором відкритого ключа. Має два обов'язкових підписаних атрибутів: 1) contentType; 2) messageDigest.
CAdES-BES	Базовий формат підпису з ідентифікацією підписувача за ідентифікатором сертифіката підписувача. Має три обов'язкових підписаних атрибутів: 1) contentType; 2) messageDigest; 3) signingCertificateV2.
CAdES-T	Формат підпису, який є розширеним варіантом формату CAdES-BES із двома додатковими атрибутами: позначкою часу від даних (contentTimestamp) і позначкою часу від підпису (timeStampToken). Має 4 обов'язкових підписаних атрибутів: 1) contentType; 2) messageDigest; 3) signingCertificateV2; 4) contentTimestamp. Має один обов'язковий непідписаний атрибут: 1) timeStampToken.
CAdES-C	Формат підпису, який є розширеним варіантом формату CAdES-T із двома додатковими непідписаними атрибутами: certificateRefs і revocationRefs. Перелік 4 обов'язкових підписаних атрибутів збігається з CAdES-T. Має три обов'язкових непідписаних атрибутів: 1) timeStampToken; 2) certificateRefs; 3) revocationRefs. Для перевірки статусу сертифікатів використовується тільки CRL, відповідно в атрибуті revocationRefs знаходяться посилання на використані CRL.
CAdES-XL	Формат підпису, який є розширеним варіантом формату CAdES-C із двома додатковими непідписаними атрибутами: certValues і revocationValues. Перелік 4 обов'язкових підписаних атрибутів збігається з CAdES-T. Має 5 обов'язкових непідписаних атрибутів: 1) timeStampToken; 2) certificateRefs; 3) revocationRefs; 4) certValues; 5) revocationValues.

CAdES-A	Формат підпису, який є розширеним варіантом формату CAdES-XL з одним додатковим непідписаним атрибутом — архівною позначкою часу archiveTimestampV3. Перелік 4 обов'язкових підписаних атрибутів збігається з CAdES-T. Має 6 обов'язкових непідписаних атрибутів: 1) timeStampToken; 2) certificateRefs; 3) revocationRefs; 4) certValues; 5) revocationValues; 6) archiveTimestampV3.

Формати сімейства CMS/CAdES дозволяють використання необов'язкових атрибутів. Наприклад, у підписаних атрибутах використовують атрибут signingTime. В залежності від завдання можна використовувати нестандартні атрибути (в рамках стандарту CMS/CAdES).

Додаток 3. Перелік розширень сертифіката

Таблиця. Перелік розширень сертифіката, які можуть бути декодованими в CERT_INFO

Назва розширення	OID	Короткий опис
authorityInfoAccess	1.3.6.1.5.5.7.1.1	
authorityKeyIdentifier	2.5.29.35	Ідентифікатор ключа видавця сертифіката
basicConstraints	2.5.29.19	Основні обмеження
cRLDistributionPoints	2.5.29.31	Посилання на адреси зберігання повних CRL-файлів
certificatePolicies	2.5.29.32	Політики сертифіката
freshestCRL	2.5.29.46	Посилання на адреси зберігання часткових CRL-файлів
keyUsage	2.5.29.15	Призначення ключа
qcStatements	1.3.6.1.5.5.7.1.3	
subjectDirectoryAttributes	2.5.29.9	Додаткові атрибути підписувача
subjectInfoAccess	1.3.6.1.5.5.7.1.11	
subjectKeyIdentifier	2.5.29.14	Ідентифікатор ключа власника сертифіката

Додаток 4. Перелік ASN1-типів

Таблиця. Перелік ASN1-типів, що підтримуються в методах ASN1_DECODE й ASN1_ENCODE

Назва ASN1-типу	Короткий опис
INTEGER	Ціле число
OCTET_STRING	Довільна послідовність байт (октетів)
NULL	Позначка відсутності
OID	Ідентифікатор об'єкта

Додаток 5. Перелік елементів опису сертифіката

Таблиця. Перелік елементів опису сертифіката в структурі RDNAME_INFO *

Назва	OID	Distinguished name
C	2.5.4.6	country
CN	2.5.4.3	commonName
G	2.5.4.42	givenName
L	2.5.4.7	locality
O	2.5.4.10	organization
OI	2.5.4.97	organizationIdentifier
OU	2.5.4.11	organizationalUnit
S	2.5.4.8	state
SERIALNUMBER	2.5.4.5	serialNumber
SN	2.5.4.4	surname
STREET	2.5.4.9	streetAddress
TITLE	2.5.4.12	title

* якщо елемент опису сертифіката невідомий (відсутній в таблиці), то замість назви використовується значення OID.