Візуалізація електронного підпису за допомогою QR-code

Єдиний криптографічний центр. Розширення

ТОВ "Сайфер БІС": Влад Ковтун
Олександр Стокіпний
Андрій Охріменко

Intro

У зв'язку з широким впровадженням електронного документообігу та електронного підпису (ЕП), виникає необхідність в візуалізації інформації про факт наявності ЕП і про саму ЕП на паперових носіях та електронних документах (Word, PDF, ...).
З цією метою пропонується використовувати QR-code, який містить інформацію про:

- АЦСК
- Підписантів
- Мітки часу ЕП
- Мітки часу даних
- Технологічні підписи даних в QR-code (optional)

Функції

Формування і розшифровка QR-code реалізується у вигляді окремого розширення QR-sign в рамках ЄКЦ, який зобов'язаний:

- формувати QR-code
  - в процесі перевірки ЕП, на основі зв'язки документ + підпис (після того, як ЕП вже успішно перевірена)
  - в процесі формування ЕП, на основі зв'язки документ + підпис (після того, як ЕП вже сформована)
- забезпечити сумісність QR-code, що б він міг розшифровуватися і візуалізуватися за допомогою QR-code сканерів вбудованих в мобільні пристрої. Слід звернути увагу, що не всі програми дозволяють коректно візуалізувати складні QR-code. Необхідно провести пошук відповідних додатків QR-code сканерів.

Функції

Формування і розшифровка QR-code реалізується у вигляді окремого розширення QR-sign в рамках ЕКЦ, який зобов'язаний:

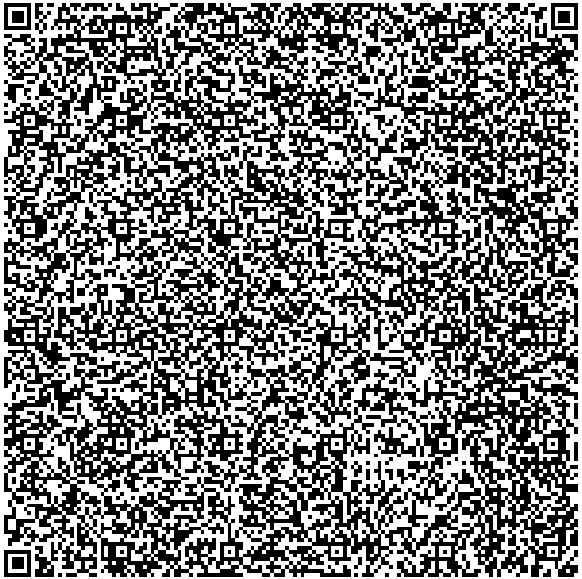
- при необхідності формувати технологічну ЕП на дані, які входять в QR-code
  - необхідно зменшити розмір конверта ЕП за рахунок стиснення за допомогою алгоритму ZIP
  - вбудовувати в QR-code посилання з технологічної ЕП для QR-code в якості параметра для ЕКЦ, для подальшої перевірки та її розшифровки

Архітектура

Архітектурно, компонент QR-signer складається з:

- мікросервіс
  - який реалізує API формування QR-code
  - який реалізує перевірку ЕП під даними в QR-code
  - візуалізує дані в QR-code, після перевірки ЕП в QR-code
- web-клієнт, по роботі з API:
  - формування QR-code
  - візуалізація QR-code і результат перевірки ЕП під QR-code

Приклад



Опис: акти Виконання робіт

Підпісувач: Бармалей Алібабайовіч Вишневий

Посада: директор

Організація: ТОВ "Роги та копита"

ІПН: 0000000033

УНЗР: 10000000000033

АЦСК / КНЕДП: ЦСК ТОВ "Сайфер БІС"

Дата підпісу: 27.03.2019, 16:22:40 GMT + 2

СН підпісанту: 63EF3F5D24764D26

ЕПЧ підпісу: дійсна; 27.03.2019, 16:22:40 GMT + 2;

СН ЕПЧ підпісу: 63EF3F5D24764D26

ЕПЧ Даних: дійсна; 27.03.2019, 16:22:40 GMT + 2

СН ЕПЧ Даних: 63EF3F5D24764D26

Технологічний підпис: Дійсний

Зауваження

Підтримувані web-браузери:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

Зауваження:

- Деякі web-браузери мають обмеження на розмір параметра в URL. Якщо розмір параметра перевищує допустимий, то параметр буде обрізатися, що в свою чергу призведе до втрати цілісності технологічної ЕП
- https://stackoverflow.com/questions/417142/what-is-the-maximum-length-of-a-url-in-different-browsers/417184#417184

Взаємодія з ЕКЦ

Взаємодія web-клієнта з підтримкою QR-sign з ЕКЦ відбувається шляхом використання затвердженого API ЕКЦ з підтримкою функцій QR-sign.

Перевірка ЕП і формування QR-code

Користувач переходить на Web-сторінку (web-клієнт ЕКЦ), де йому пропонується сформувати QR-code.

Для формування QR-code має бути вказано:

- Параметри перевірки ЕП
- Ознака формування QR-code
- Параметри QR-code

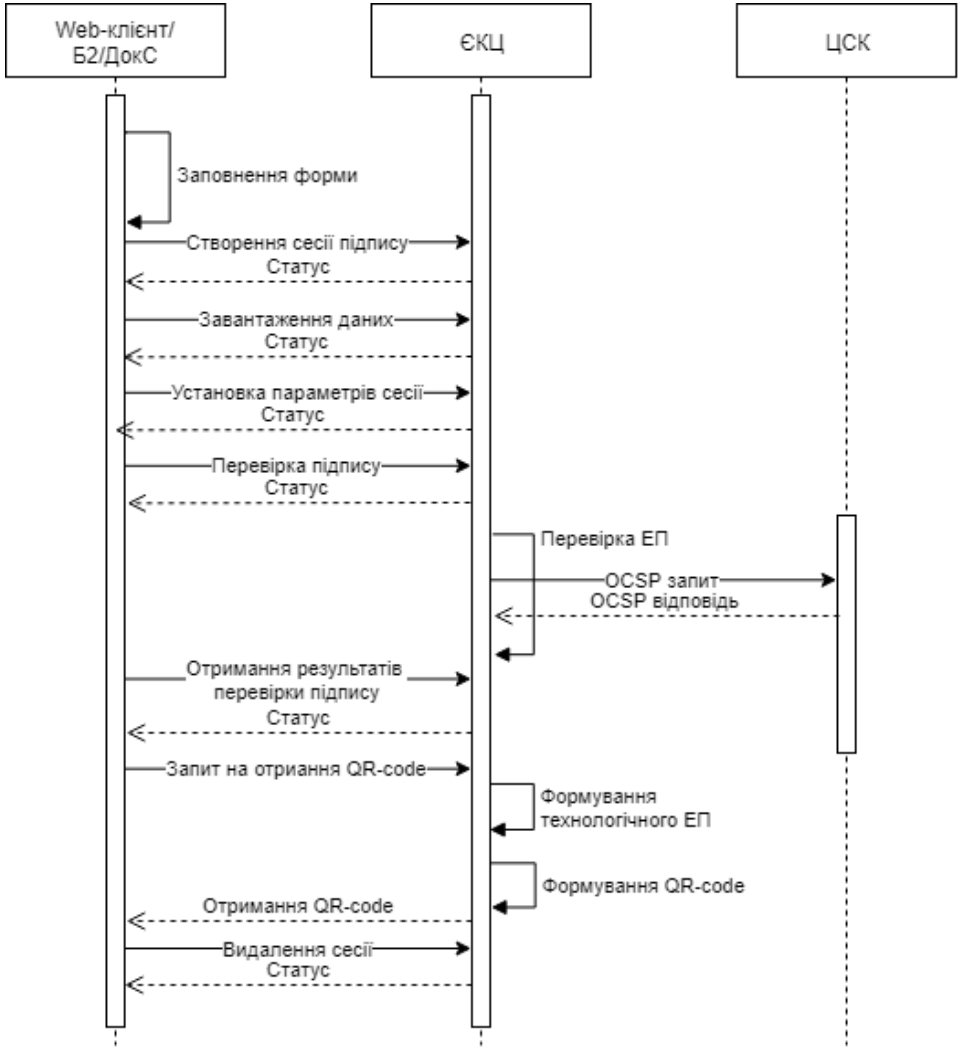
Користувачем завантажуються дані (у разі відкріплення ЕП) і відповідне ЕП (в тому числі і множинна - єдиний CMS конверт для декількох ЕП), які потім передаються на ЕКЦ.

Перевірка ЕП і формування QR-code

На стороні ЕКЦ:

1. Проводиться перевірка ЕП для завантажених даних.
2. Формуються дані, які відображають результат перевірки ЕП (однієї і більше)
3. За окремим запитом:
    a. Створюється вбудована технологічна ЕП для даних, які відображають результат перевірки ЕП і склад яких вказано раніше в цій специфікації.
    b. Формується URL, одним з параметрів якого є дані раніше створеної вбудованої ЕП.
    c. URL кодується в QR-code.
    d. У разі декількох ЕП, етапи a, b, c виконуються для кожної з ЕП, які присутні в конверті CMS.
    e. Один або кілька QR-code повертаються у вигляді JSON масиву. Дані окремого QR-code закодовані з використанням кодування Base64.

Перевірка ЕП і формування QR-code



Постановка ЕП і формування QR-code

Користувач переходить на Web-сторінку (web-клієнт ЕКЦ), де йому пропонується сформувати QR-code.

Для формування QR-code має бути вказано:

- Параметри створення ЕП
- Ознака формування QR-code
- Параметри QR-code

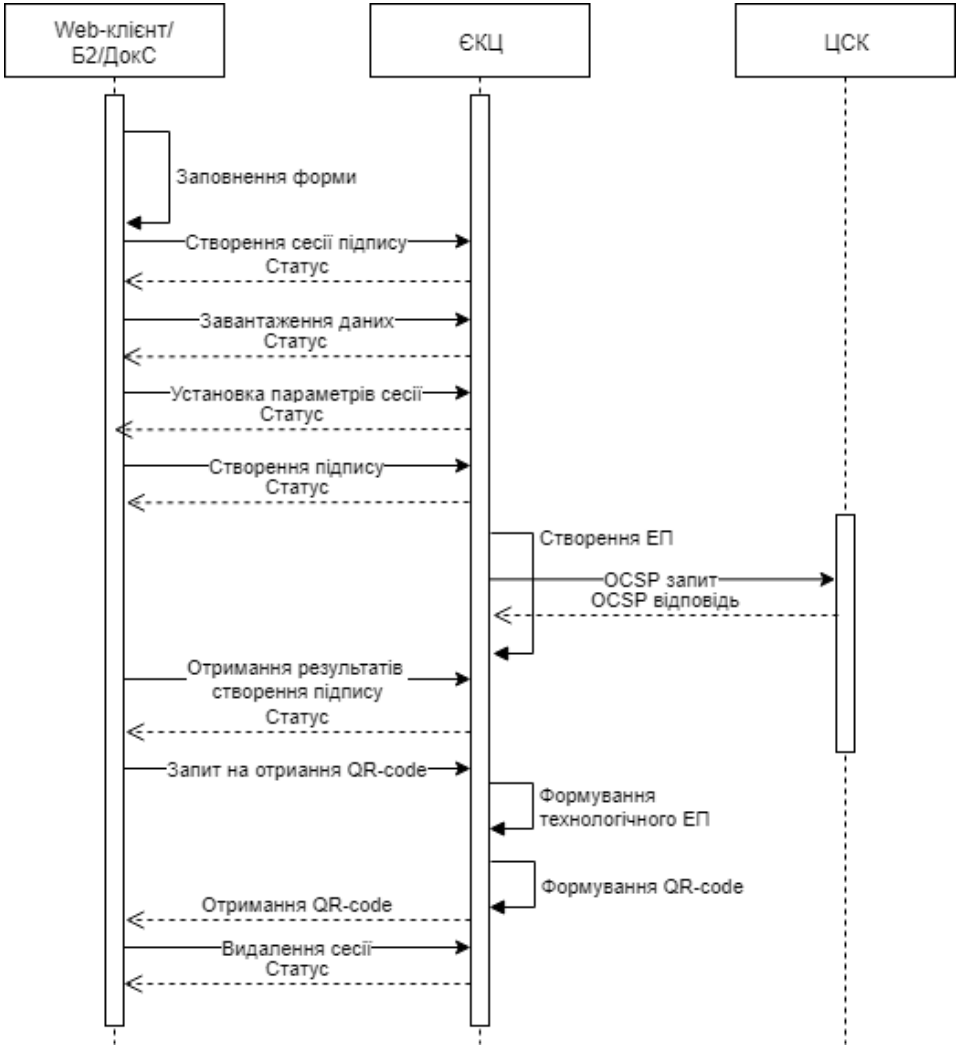
Користувачем завантажуються дані і вказується ключовий контейнер підписанта ЕП. Якщо відбувається додавання ЕП в існуючий конверт CMS, то QR-code формується тільки для ЕП поточного підписанта. Для ЕП інших підписантів, дані яких присутні в CMS конверті, QR-code не формується.

Постановка ЕП і формування QR-code

На стороні ЕКЦ:

1. Проводиться створення ЕП для завантажених даних.
2. Виконується перевірка створеної ЕП.
3. Формуються дані, які відображають результат перевірки ЕП.
4. За окремим запитом:
    a. Створюється вбудована технологічна ЕП для даних, які відображають результат перевірки ЕП і склад яких вказано раніше в цій специфікації.
    b. Формується URL, одним з параметрів якого є дані раніше створеної вбудованої ЕП.
    c. URL кодується в QR-code.
    d. QR-code повертаються у вигляді JSON масиву. Дані окремого QR-code закодовані з використанням кодування Base64.

Створення ЕП і формування QR-code



Як зроблено у інших?

У сервісі електронного документообігу https://document.online має вигляд: Акт виконан робіт №23154898-10_1 від 13.10.17.pdf

ТОВ "Сайфер БІС"

Олександр Стокіпний: as@cipher.kiev.ua

Андрій Охріменко: ao@cipher.kiev.ua

Влад Ковтун: vk@cipher.kiev.ua

www: https://cipher.com.ua