

Electronic Vaccination Proof

- Proposal for encoding and signing



Prerequisites

- **Several initiatives for an electronic proof of vaccination (EVP) have been launched, but none so far seem to have addressed the large-scale requirements of such an electronic document.**
- **An EVP should be machine readable for automatic validation (offline), and it should be possible to apply a set of rules/conditions for the check to be positive.**
- **It must not be possible for forge or tamper with an EVP.**
- **In order for it to work with all types of information-carrying media (including paper), the information of the EVP needs to be encoded very compactly.**

Control of one's personal information

- **An EVP may contain sensitive personal information, and should be carried by the holder and presented as needed, not dispersing any information without the holder/subject informed consent, nor outside of what is strictly necessary.**
- **The contents of an EVP may be filtered by an Issuer to include only what is relevant for a specific purpose.**
- **A consent for (only) processing for a specific purpose may be encoded into the EVP.**
- **Any verifier should not need access to any central registers containing sensitive information, mitigating risks for intractable data breaches.**

Identity information

- It is assumed the EVP contains a reference to an identity document.
- Hence, the EVP is intended to be used in tandem with such an identity document. The EVP itself does not need to be an identity document or contain biometrical information.
- Hence, the EVP may exist in multiple identical copies. There are no risk associated with multiplying the EVP.

Security

- **The EVP must be cryptographically sealed with a key that only the issuer of the proof is in control of.**
- **Traditional (X.509) PKI should not be used due to its complexity and heavy weight. A more light-weight route should be chosen, without relaxing the security requirements.**
- **A Coordinator is required to collect and publish a set of signed metadata containing the public keys of the Issuers, and distribute this in a secure manner to all stakeholders.**
- **A key is easily revoked by withdrawing it from the metadata, and a new one can be quickly added in its place.**

Encoding and signing

- **Given choice to build on open standards, where software libraries already exists and are readily available to implementors. Modern and proven technology should be used:**
 - **CBOR (Concise Binary Object Representation) according to RFC 7049**
 - **COSE (CBOR Object Signing and Encryption) according to RFC 8152**
 - **ECDSA (Elliptic Curve Digital Signature Algorithm) according to ISO/IEC 14888-3:2006 with the parameters for P-256**

Representation format

- **Compression according to RFC 1950 (zlib)**
- **Optical encoding according to ISO/IEC 24778:2008 (Aztec)**
 - **Aztec-code can accommodate up to about 1500 bytes**
 - **More robust reading than its sibling ISO/IEC 18004:2015 (QR)**
 - **Robustness important in these diverse environments for handling challenging lighting conditions, cracked mobile screens and folded paper**
- **Raw data format for contactless transfer (NFC/RFID)**

Proven technology

- **Similar technology already used in public transport environments in Sweden.**
- **Proven on a large scale for a few years.**
- **Most public transport companies in Sweden have already implemented this type of technology, the rest are in the implementation stages.**

Data structure

- **Basic Interoperability Elements according to a specification drafted within the EU eHealth Network.**
- **Expressed as a JSON Schema for automatic validation.**
- **Defines the data structure of the EVP.**

```
$schema: http://json-schema.org/schema#

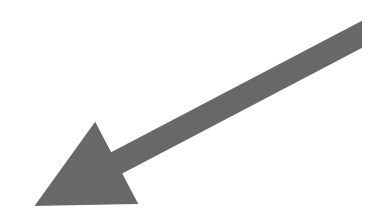
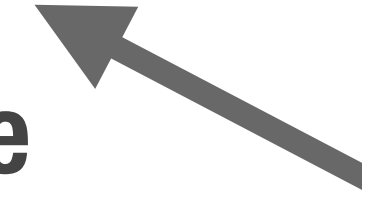
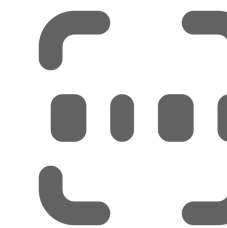
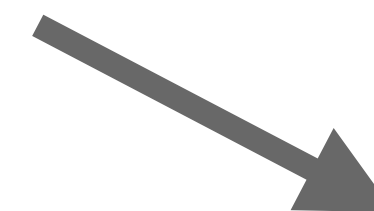
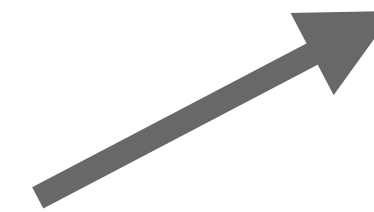
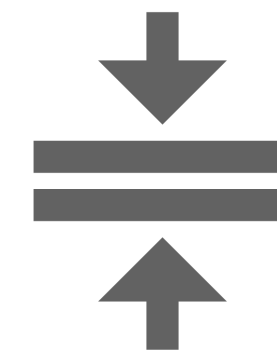
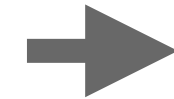
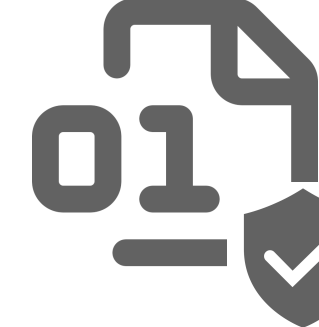
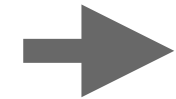
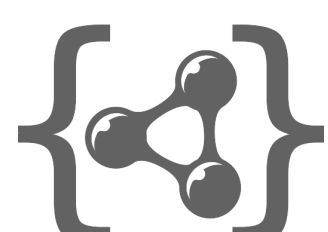
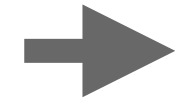
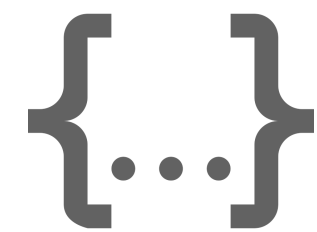
type: object
required:
  - sub
  - vac
properties:
  sub:
    description: Subject
    type: object
    required:
      - n
    properties:
      n:
        title: Person name
        description: The legal name of the vaccinated person
        type: string
        example: Tolvan Tolvansson
      id:
        title: Person identifiers
        description: Identifiers of the vaccinated person, according to
          the policies applicable in each country.
        type: array
        items:
          type: object
          required:
            - t
            - i
          properties:
            t:
              title: Identifier type
              description: The type of identifier
              pin = personal identity number
              pas = passport number
              nid = national identity card number
              example: pin
              enum:
                - pin
                - pas
                - nid
              type: string
            i:
              title: Identifier number or string
              type: string
              example: 121212-1212
      dob:
        title: Date of birth
        description: Mandatory if no Person identifier is provided.
        format: date
  vac:
    description: Vaccination/prophylaxis information
    type: array
    items:
      type: object
      required:
        - des
        - nam
        - aut
        - seq
        - tot
        - dat
        - adm
      properties:
        tar:
          title: Disease target
          description: Disease or agent that the vaccination provides protection.
            against.
          type: string
          example: SARS-CoV-2
        des:
          title: Vaccine/prophylaxis
          description: Generic description of the vaccine/prophylaxis or its
            component(s).
          type: string
          example: J07BX03
        nam:
          title: Medicinal product name
          description: Name of the medicinal product as registered in the country.
```

Evaluation of conditions

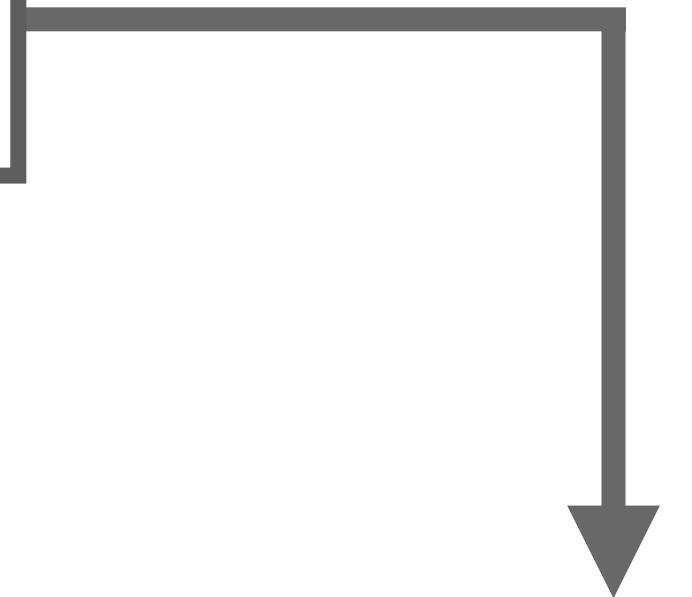
- **Exampel of conditions:**
 - **At least one vaccination against a specific decease within the last month, or**
 - **Full vaccination against the decease within the last two years.**
- **Conditions can automatically be evaluated and the result presented to the Verifier (including any failing factor).**

```
vac:
  description: Vaccination/prophylaxis information
  type: array
  items:
    type: object
    required:
      - des
      - nam
      - aut
      - seq
      - tot
      - dat
      - adm
    properties:
      tar:
        title: Disease target
        description: Disease or agent that the vaccination provides protection
          against.
        type: string
        example: SARS-CoV-2
      des:
        title: Vaccine/prophylaxis
        description: Generic description of the vaccine/prophylaxis or its
          component(s).
        type: string
        example: J07BX03
      nam:
        title: Medicinal product name
        description: Name of the medicinal product as registered in the countr
        type: string
        example: COMIRNATY
      aut:
        title: Marketing Authorisation Holder
        description: EMA's Organisations System data (SPOR).
        type: string
        example: Pfizer BioNTech
      seq:
        title: Dose sequence number
        description: The sequence number of this dose in the series of
          vaccinations.
        example: 1
      tot:
```

Vaccination registry



Metadata



JSON
Schema

JSON
Document

CBOR Binary
Document

COSE Signed
Document

ZLib
Compression

NDEF Tag

Validator
App

Example proof:

12 vaccinations
6 different substances

(2717 bytes)

(1276 bytes)

(1349 bytes)

(455 bytes)