Towards Interoperable Vaccination Certificate Services

ANDREEA ANCUTA CORICI, Fraunhofer FOKUS Institute, Germany
TINA HÜHNLEIN, ecsec GmbH, Germany
DETLEF HÜHNLEIN, ecsec GmbH, Germany
OLAF RODE, Fraunhofer FOKUS Institute, Germany

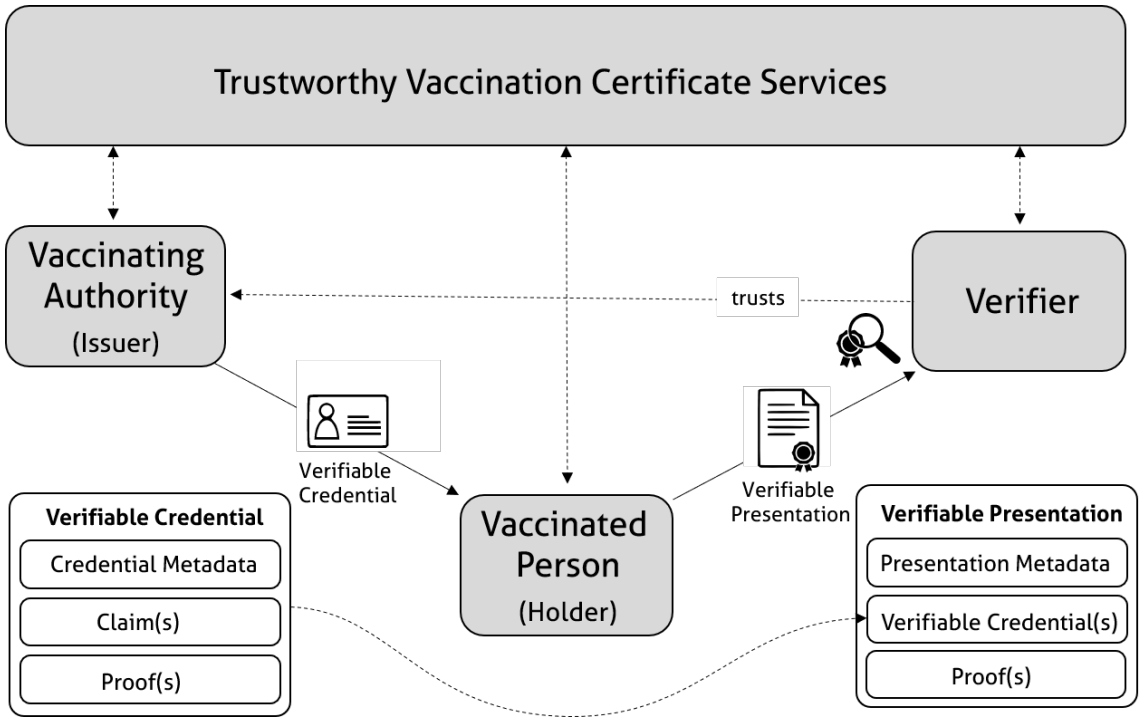

Fig. 1. Trustworthy Vaccination Certificate Service System

Against the background of the new corona virus and its far reaching impact on our everyday life there have been numerous initiatives around the globe, which work on the design and implementation of services related to certificates containing information about the vaccination, testing and/or recovery status of citizen ("Vaccination Certificates"). Due to the distributed and largely independent development under high time pressure there is a risk that the resulting services for the creation, presentation and verification of the aforementioned Vaccination Certificates, will in the end not be interoperable and hence finally turn out to be of limited interoperability. To contribute to the mitigation of this risk, the present paper aims at creating a compact overview with respect to the relevant underlying technologies and an up to date survey with respect to the most relevant initiatives around the globe, before elucidating the

Manuscript submitted to ACM

system requirements for Vaccination Certificate Services and then outline a technical reference architecture accordingly. This reference architecture, which is as far as possible based on open standards, seeks to integrate all relevant currently existing and emerging approaches and hence may facilitate well-grounded discussions and the exchange of ideas between the different communities and the harmonization of specifications and related schema artifacts in this area. The present contribution concludes with an outlook towards future developments, which includes a long term perspective towards the integration of the Vaccination Services with electronic health records and data exchange infrastructures supporting the International Patient Summary.

CCS Concepts: • **Security and privacy → Usability in security and privacy**.

Additional Key Words and Phrases: eHealth, Vaccination, Verifiable Credentials

ACM Reference Format:
Andreea Ancuta Corici, Tina Hühnlein, Detlef Hühnlein, and Olaf Rode. 2021. Towards Interoperable Vaccination Certificate Services. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3465481.3470035

1 INTRODUCTION

In the recent months coronavirus vaccination campaigns have brought to light the idea of trustworthy and verifiable vaccination certificates, for allowing activities like tourism to relaunch. The governance policies for creating, storing and validating vaccination certificates are often not yet defined and there are no formal technical standards or governance policies as well. At the same time, it seems that the various initiatives around the globe (see Section 3) are revolving around the concepts of Verifiable Credentials, defined by W3C [66], Self-Sovereign Identity, in the sense of [2] and related technologies summarized in Section 2. In the setting depicted in Fig. 1, a Vaccinating Authority (Issuer) is issuing a Verifiable Credential to the Vaccinated Person (Holder), who obtains or derives one or more Verifiable Presentations, that are handed over to the Verifier in order to be validated with the support of Trustworthy Vaccination Certificate Services.

Against this background, we introduce a set of seemingly meaningful system requirements in Section 4 and introduce more detailed technical reference architecture in Section 5. This aims at facilitating well-grounded discussions about interoperability aspects related to the minimum dataset, the verification of certificates and the implemented trust framework. Section 6 concludes with an outlook on possibly upcoming developments and future work in this area.

2 BACKGROUND ON RELATED TECHNOLOGIES

2.1 Medical Data Exchange

Since its first release by HL7 in 2014, the "Fast Healthcare Interoperable Resources" (FHIR) [34] framework has been used in multiple healthcare domains like for the definition of the "International Patient Summary" (IPS) (cf. [38], [13] and [36]), in clinical studies data storage and processing [49] and even bioresearch apps [56]. The reason why it has achieved such wide acceptance is that compared to the old set of standards from HL7, which only standardized the messages related to events, the FHIR standard introduced multiple long needed features: a reference data model of linked resources together with a RESTful API for creating, updating and deleting these resources. These features help minimizing the effort of interoperability and compatibility and contribute towards ending the era of vendor lock-in in the area of ICT for healthcare.

By modelling the messages using HTTP, another advantage of using this standard includes the ability to be seamlessly integrated with web authentication mechanisms like OAuth 2.0 [32] and JSON Web Tokens [44]. The serialization of

the resources in requests and replies can be either XML or JSON, based on the format stated in the messages. Another aspect worth mentioning is that HL7 FHIR also introduced a Service-oriented Architecture (SOA) based Common Terminology Service in order to be able to cope within a dynamic world of communications in medicine, in which procedures and unfortunately diseases are evolving matters. This introduced the terminology server for being able to encode and resolve codes from well-known code systems, like Logical Observation Identifiers Names and Codes (LOINC) [52] and SNOMED [64], for items like materials, diseases and types of laboratory analysis parameters (e.g. glycaemia).

2.2 Compact Encoding and Compression of Data

As the Vaccination Certificate is meant to be usable without technical equipment of the holder and conveyed in a 2D barcode, it is essential to have a very compact representation of its content. A data encoding standard, which is geared towards reasonable compact encodings is the Concise Binary Object Representation (CBOR) according to RFC 8949 [7], which can be converted to or created from JSON, as explained in clause 6 of [7].

For the additional compression of rather large data sets, such as the "International Patient Summary" according to [38], [13] and [36] for example, one could imagine to use additional compression algorithms, such as ZIP [59] or DEFLATE [17] before encoding the data in CBOR and, for the compact encoding of X.509 certificates, one may use the C509 encoding [58].

2.3 Digital signatures for CBOR encoded data

While CBOR encoded data could be signed with any binary digital signature format, the use of CBOR Object Signing and Encryption (COSE) according to RFC 8152 [63] seems to be the canonical choice for digitally signing CBOR encoded data and there is a corresponding CBOR Web Token (CWT) format defined RFC 8392 [45]. Among the additional alternatives would be to use the ASN.1 based Cryptographic Message Syntax according to RFC 5652 [37] or CBOR-LD [65] in combination with linked data signatures (cf. [5], [67] and [53]), as has been done for signing vaccination certificates as outlined in [69].

2.4 Verifiable Credentials and Presentations

The W3C Recommendation [66] outlines a generic data model for "Verifiable Credentials" and "Verifiable Presentations". As outlined in Fig. 1 and clause 3.2 of [66], a Verifiable Credential contains "Credential Metadata", a set of "Claim(s)" and a set of "Proof(s)" applied to the claims. The proof types mentioned in clause 1.4 of [66] comprise JSON Web Tokens (JWT) according to RFC 7519 [44] with JSON Web Signatures (JWS) according to RFC 7515 [43], Linked Data Signatures [53] for which a set of verification method types can be found in clause 5.1 of [68], and Camenisch-Lysyanskaya (CL) Zero-Knowledge Proofs [9], which are known to be used in Hyperledger Indy [51] and the Sovrin system [47] based on this technology. An easy to read overview of the different credential flavors is available in [72].

A Verifiable Presentation as outlined in clauses 3.3 and 4.10 of [66], contains "Presentation Metadata", a set of "Verifiable Credential(s)" and a set of corresponding "Proof(s)".

2.5 APIs for managing Verifiable Credentials

Among the potentially relevant Application Programming Interfaces (API) for the management of Verifiable Credentials are the "VC HTTP API" [60] and the generic OASIS DSS-X [48].

2.6 Pseudonymisation and Selective Disclosure

To distinguish between Verifiable Credentials and Verifiable Presentations is mainly motivated by the privacy requirement for "data minimization" according to Art. 5 par. 1 (c) GDPR, which should already be considered during the design of a system (cf. Art. 25 GDPR) and which can be implemented with a combination of different technical and organizational measures and a variety of cryptographic techniques for pseudonymisation and selective disclosure. The bandwidth of possible pseudonymisation techniques ranges from the straight forward application of a (keyed) hash function to sophisticated cryptographic techniques based on zero-knowledge proofs, for example (cf. [31] and [30]).

Among the well-known zero-knowledge techniques, which enable selective disclosure for verifiable credentials, is the already mentioned "CL-Signature" [9] based on the "Strong RSA Assumption" and the "BBS+ JSON-LD Signature" (cf. [50] and [3]), which goes back to [6] and [10] and utilises bilinear pairings in rather specific elliptic curves introduced in [62]. Unfortunately both approaches are not in line with conservative cryptographic requirements, such as [61] or [16] for example. As a pragmatic alternative, which even turns out to be more efficient in practice, one may use the selective disclosure technique [4] based on Merkle hash-trees.

2.7 2D Bar Code Formats

Among the widely used 2D bar code formats are the "Aztec" code according to ISO/IEC 24778 [40], the "Data Matrix" code according to ISO/IEC 16022 [39] and the "QR Code" according to ISO/IEC 18004 [41].

3 OVERVIEW OF SELECTED SCHEMES

3.1 European Union (EU)

The European Union eHealth Network consulted with multiple organizations, including World Health Organization (WHO), resulting in a series of guidelines on proof of vaccination for medical purposes (see [26], [25]), a trust framework [28] and a set of detailed technical specifications [20–24] regarding corona virus with the intention to be extended to other pathogens as well. These guidelines and specifications include simplicity, by supporting both paper and digital format, flexibility and compatibility with existing national standards and rigorous protection of personal data with the goal to bring interoperability between the national EU Member States initiatives. The basic interoperability requirements foresee: (i) a minimum dataset with the essential information to be included in the vaccination certificate and (ii) a Unique Vaccination Certificate/Assertion Identifier (UVCI) that is globally unique and verifiable. From the semantic point of view, English will be the compulsory language, with other display languages also supported.

The corresponding trust framework [28] will have the role to establish the authenticity and validity of the certificate based on public key technology, similar to International Civil Aviation Organization (ICAO)'s Public Key Directory (PKD), to enable machine readable travel documents as also pushed forward by the WHO (see Section 3.4). The Vaccination Certificates are planned to be encoded using the CBOR [7] format, are signed according to COSE [42] [63], wrapped in a CWT [45] and conveyed in 2D codes using QR code symbols [41]. The European Commission proposed regulation [15] for the "Digital Green Certificate" (DGC) also covers "Test certificates" and "Certificates of recovery" in addition to the "Vaccination certificates". While the European Commission is providing basic gateway services according to the specifications [20–24], it is envisioned that the EU Member States build their own digital infrastructures for issuing and verifying the certificates of vaccination, test and recovery.

3.2 Germany

In Germany, one of the Member States of EU, there have been recently different activities around Vaccination Certificate services, which include the specification of an electronic vaccination passport ("Impfpass") [46], a Vaccination Certificate pilot followed by a national project for developing and running the necessary infrastructure for vaccination certificates. The Universal Non Infectious Verifier for Arbitrary Credential Schemas (UniVacs) [1] project strives to deliver a building block for proving the immunization status of a user by employing W3C verifiable credentials technology. The vaccination passport is specified using the FHIR-based International Patient Summary [36], which contains vaccination information, and at the same time is covering multiple types of vaccine standard codes, enabling extensibility and globally semantic interoperability. With respect to privacy, the format of the "Impfpass" includes the vaccinated person's health insurance identifier, passport number, name, name at birth, gender, date of birth, as well as information regarding the practitioner who administered the vaccination. As this kind of information is not necessary in travel and leisure scenarios for example, there is the need for selective disclosure mechanisms as outlined in Section 2.5.

3.3 United States of America (USA)

Within the USA there are various more or less independent initiatives. Among the noteworthy ones are initiatives like the Linux Foundation's COVID-19 Credentials Initiative (CCI) [33], the Vaccination Credential Initiative (VCI) [70] and the Good Health Pass Collaborative [14], which aims to be interoperable with as many user vaccination wallets as possible.

3.4 World Health Organization (WHO)

The World Health Organization (WHO) issued an "Interim guidance for developing a Smart Vaccination Certificate" [27] containing a "Recommended core data set". The data set is compared in Annex A with the corresponding data sets from other initiatives mentioned in the present Section.

Furthermore the WHO guidance outlines a trust framework, which contains a Public-Key Infrastructure (PKI) rooted in the WHO Public Key Directory (WHO PKD), which is similar to the trust framework employed by the International Civil Aviation Organization (ICAO) and similarly envisioned by the EU's trust framework [28] and proposed regulation [15]. This means that each WHO member state operates a Country Signing Certificate Authority (CSCA), which anchors the national PKI, operates a corresponding certificate revocation list (CRL) and issues certificates to one or more Document Signers (DS), which in turn sign the three types of certificates regarding: vaccination, testing and recovery. WHO in turn maintains a global Master List (ML), which contains all the public keys of the national CSCAs and corresponding CRLs.

There are some noteworthy aspects of the release candidate document [27] related to identity management. First, is the fact that the certificate on the one hand side shall contain identity attributes of the holder (i.e. name, date of birth and even a unique identifier), but on the other hand it is unambiguously stated that "the SVC is not an identity" and that it is "expected that the SVC SHALL NOT be an identity". This statement seems to stress that the vaccination certificates are no travel document, like a passport or a national ID card on its own, but would always need such a travel document for identification and passing borders. Second, there is an option for selective disclosure of a subset of the certificate, but this option does not seem to utilize any of the specific techniques outlined in Section 2.5 for achieving this, but simply foresees the issuing of additional 2D barcodes, which contain less identity information.

3.5 W3C Vaccination Certificate Vocabulary

Members of the W3C Credential Community Group (W3C CCG) have created a Vaccination Certificate Vocabulary [69], to be used to create JSON-LD [67] and CBOR-LD [65] based Vaccination Certificates. It also illustrates the different space requirements of the two encodings: whereas an example certificate in JSON-LD requires 1217 bytes, the corresponding length in CBOR-LD is 461 bytes.

4 BASIC REQUIREMENTS

Based on the main characteristics of the schemes outlined above, this Section summarizes the high-level requirements that a reasonable system for Vaccination Certificate Services should fulfil. The key words “MUST”, “SHOULD” and “MAY NOT” are to be interpreted as in RFC 2119 [8].

4.1 R1. Privacy-friendly

Any Vaccination Certificate system, which is meant to be used in Europe or by European citizen, MUST be privacy-friendly and compliant to the General Data Protection Regulation (GDPR). This includes for example that the principle of data minimization according to Art. 5 (1)(c) GDPR is respected and that privacy aspects are already considered during system design (Art. 25 GDPR).

4.2 R2. Inclusive

In order to be potentially useful, a Vaccination Certificate system MUST be applicable for arbitrary citizen and hence MAY NOT impose any specific requirement with respect to the technical equipment of the Holder or network environment of the Verifier. If a system would require a citizen to possess a (specific type of) smartphone or a powerful and ubiquitous network connection for the Verifier, this would often not be acceptable.

4.3 R3. Interoperable

Closely related yet separate is the requirement that a Vaccination Certificate system MUST be interoperable in a basic sense with components from other relevant providers in order to be reasonable and acceptable. This especially means that the Vaccination Certificate system MUST be based on open standards and open interfaces and SHOULD be aligned with all relevant international standards. From a European perspective it is obvious, that a reasonable Vaccination Certificate system MUST implement the guidelines and specifications on proof of vaccination for medical purposes (see [26], [28] and [20–24]).

4.4 Trustworthy

A broadly acceptable Vaccination Certificate system MUST be trustworthy, which implies that it MUST be provided as Open Source and MUST at any time use security technology (including suitable cryptographic algorithms) and trustworthy operational environments.

5 REFERENCE ARCHITECTURE

Based on the emerging schemes mentioned in Section 3 and the set of requirements outlined in Section 4, the present section refines the high level system architecture from Fig. 1 in order to come up with a technical reference architecture depicted in Fig. 2. This reference architecture still has the three central entities (Vaccinating Authority (Issuer), Vaccinated

Person (Holder) and Verifier) and provides more details with respect to (1) the minimum dataset, the (2) issuance and verification of certificates and last but not least (3) the envisioned trust framework. As correctly stated in [55] these three areas are crucial for reaching interoperability and are therefore discussed in more details below.

5.1 Minimum data set

The minimum data set for the certificates on vaccination, testing and recovery need to be defined and specified in a suitable manner. This may involve CBOR [7] encoded data elements derived from or inspired by the FHIR JSON format [34] for example. As can be seen from the comparison of the table in Annex A, the currently available specifications are sufficiently similar, such that a harmonisation and standardisation seems to be feasible.

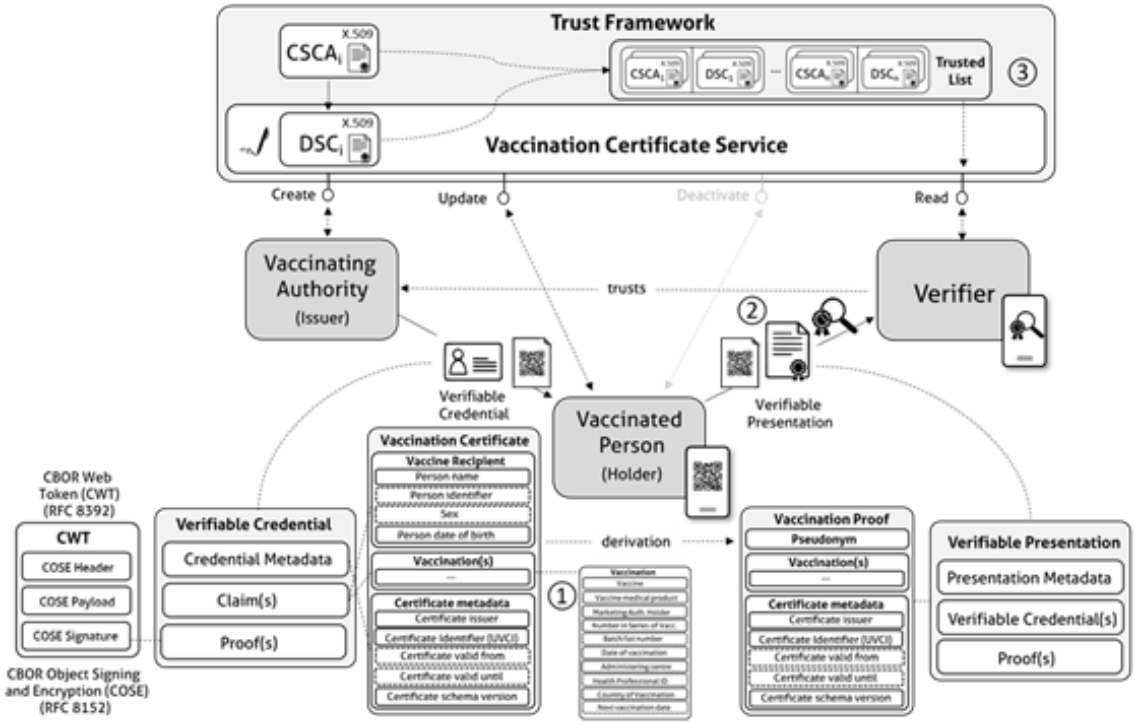

Fig. 2. Refined System Architecture with Vaccination Certificate Service

5.2 Issuance and Verification of Certificates

For the issuance and verification of certificates one may distinguish the simple case with “bearer tokens” and “trivial selective disclosure” discussed here and likely to be pursued in practice and more sophisticated and advanced system variants, based on Merkle hash trees, holder-of-key credentials and zero-knowledge proofs, which are mainly interesting from an academic perspective and therefore briefly discussed in Section 6.

In the simplest setup the holder does not have a private key, but simply obtains a more or less static, yet identity bound, signed certificate in the form of a 2D barcode (cf. Section 2.7), which can simply be printed out or captured and

maintained in a suitable smartphone application. The 2D barcode contains the CBOR encoded and signed (cf. Section 2.3) minimum data set (cf. Section 5.1 and Annex A).

The issuance of the 2D barcode is performed by the Vaccinating Authority after duly compiling the vaccination related data and verifying the identity of the holder by calling the Create interface of the Vaccination Certificate Service.

The verification simply consists of capturing the 2D barcode and validating the COSE based signature according to [63] for example against a set of trusted public keys rooted in the WHO Public Key Directory. The current set of public keys and revocation information, if available, can be retrieved by the Verifier via the Read interface. If it is in doubt that the holder of the "bearer token" is in fact the owner and legitimate user of the token, one may additionally ask for a proof of identity with a passport or a national ID card for example.

A very basic strategy for data minimisation and selective disclosure, as foreseen in [27] and [26], is that the holder may, during the issuing procedure or later with a smartphone app via the Update interface, obtain an additional barcode, which contains less information. As the "identity binding" requires an identification with a passport or national ID card and the presence of this kind of information in the credential, the effective utility of selective disclosure seems to be very limited – at least in the basic face-to-face scenarios implemented in practice.

On the Vaccinating Authority side, for the Create operation, one may use a suitable interface towards the Vaccination Certificate Service that allows uploading the raw form of a certificate for vaccination, test or recovery and gets back the properly signed and encoded certificate. The interface may either be based on FHIR [34] or on an API such as the "VC HTTP API" [60] or OASIS DSS-X [48]. The data set for a vaccination event may be based on the International Patient Summary (IPS) [36] and contain the personal data about the performing medical doctor, the vaccinated person, the encoded type of vaccine (COVID, influenza, others), the manufacturer of the vaccine and the date of the last shot. The interface can be secured with a mutually authenticated TLS channel, having corresponding private keys of the vaccinating personnel pre-provisioned at the Vaccination Authority, or an authentication using a suitable health professional card, if available. One of the Open Source libraries that can be used for implementing the FHIR components is HAPI FHIR [12].

The Vaccination Certificate Service receives the raw vaccination event information and can generate the Verifiable Credential and possibly one or more Verifiable Presentations from this information. When generating the presentations, different type of information may be utilized as specified in [26]. After undergoing a CBOR encoding of the payload, a COSE signature and the wrapping in a CWT, the QR code for the generated Verifiable Presentation can be generated and handed over to the vaccinated person. There are multiple Open Source CBOR and COSE implementations. One of the JAVA implementations for COSE, as defined in RFC 8152 [63], in liaison with IETF is [71], with a specific CBOR library as a dependency.

If the Vaccinated Person has a mobile wallet, which is capable of interacting with the Vaccination Certificate Service, the wallet may be linked to an eID to enable remote proofing of the vaccination status. In Germany for example, the newest generation of electronic healthcare includes a Near Field Communication (NFC) interface that can be used to establish a cryptographic connection to a backend server. The Update interface can be used to refresh the certificate in the second vaccination event or in order to obtain an alternative Verifiable Presentation.

5.3 Trust Framework

On the Verifier side, for offline validation, a periodical download of the trusted Public Keys contained in a "Trusted List" is necessary using the Read interface. Note, that the conceptually existing Deactivate interface is not necessary in the basic system setup, because issued vaccination certificates cannot be revoked for reasons of simplicity and privacy.

6 ADVANCED FEATURES AND FUTURE WORK

While the Reference Architecture outlined in Section 5 is expected to be implemented in practice soon, there are further options and advanced features, which seem to be worth to note here.

6.1 Terminology Server

When building a solution for supporting a flexible range of vaccine encoding for different diseases (or in the case of SARS-COV-2 probably also mutations of it), one can observe that there is a wide variety of codes, sometimes in different coding systems, that will have to be updated as well. Thus, for the translation and validation of the disease codes a terminology server supporting the HL7 FHIR specification [35] may turn out to be very helpful and hence could be integrated into the Vaccination Certificate Service. One of the terminology servers with an open interface is the CTS2-LE [18], successfully used in the project IOP3D [19] for translating vendor specific codes to standard codes.

6.2 Selective disclosure based on Merkle-Hashtree

Another option, which would improve the privacy of citizen would be the use of more sophisticated selective disclosure strategies based on Merkle Hash-Trees as introduced in [4]. In our special case defined in the EU guidelines on proof of vaccination [26] however there are only two scenarios (“Care” and “Travel”) and hence the implementation of the selective disclosure would boil down to an extremely simple Merkle Hash-Tree, which only consists of the root and five leaves, which consist of the not to be disclosed attributes and related random salt values. It should be noted, that the minimal dataset from the guidelines [26] requires the personally identifiable information (PII) (i.e. name, date of birth, person identifier and sex) to be present in both cases.

While it seems to be arguable whether this is fully in line with the principle of data minimisation laid down in Art. 5 (1)(c) of GDPR, it seems to reflect the currently implemented border control and airplane boarding practices, which are probably not easy to change from one day to another.

6.3 Holder-of-Key Credentials

If the verifiable credential of a vaccination passport would be used in remote electronic health scenarios, e.g. for pseudonymous authentication in order to obtain a special service, it would make sense to issue “Holder-of-Key Credentials” which integrate a public key value for which the holder controls the corresponding private key. In this case the issuing process could involve an identity proofing step before the credential is issued and the private key could be used for remote authentication and identification protocols. In this case it may also make sense to enable selective disclosure, either based on [4] or the more sophisticated techniques mentioned in Section 2.4 and Section 6.4, such that only the necessary attributes for a specific use case are conveyed to the verifier.

6.4 Zero-Knowledge Proofs Selective Disclosure

Instead of using Merkle-Hashtrees as suggested in [4] to implement selective disclosure, one may use zero-knowledge proofs based on the “CL-Signature” [9] or the “BBS+ JSON-LD Signature” [50] for example. In this case the credential scheme utilizes specific mathematical constructions and related signature techniques, which allow to prove ownership of attributes without disclosing the credential itself. While [9] is based on the so called “Strong RSA” assumption, [50] uses bilinear pairings in specific elliptic curves.

7 SUMMARY AND OUTLOOK

The present paper has provided a compact survey with respect to relevant technologies in Section 2 and emerging systems for certificates for vaccination, test and recovery in Section 3. It has specified basic requirements in Section 4 and highlights the differences in the used data models in Annex A in the hope to stimulate further harmonisation and standardization. The reference architecture presented in Section 5 demonstrates that the general concept of Verifiable Credentials according to the W3C Recommendation [66] can be combined with a classical PKI-based trust framework (see [28] and [27]) as well as modern CBOR based encodings (see [63] and [45]) and standardized 2D barcode formats (see [40], [39] and [41]) in order to yield a GDPR-compliant and inclusive overall Vaccination Certificate Service. This reference architecture has been developed in parallel to the gradually released guidelines and by now has turned out to be a summary of the recently published specifications [20–24], of the EU eHealth Network. Therefore one may expect that many European Member States will sooner or later implement systems similar to the outlined reference architecture. The fact that there are multiple Open Source projects (see [29] and [57]), which work on implementing the specifications fuels hope that the resulting systems in Europe will end up being trustworthy and interoperable. Whether and when other regions of the world will implement systems may become clearer during the further course of activities in this domain.

ACKNOWLEDGMENTS

The work on the present paper has been conducted within the EU Horizon 2020 framework mGov4EU project [54] and has greatly profited from the fruitful discussions with a variety of subject matter experts in the “Vaccination Certificate Services Interoperability” (VACCSI) “Cross Community Working Group” [11]. The project was granted the funding on the call for projects H2020-SC6-GOVERNANCE-2018-2019-2020/H2020-SC6-GOVERNANCE-2020 with Grant number 959072.

REFERENCES

[1] Stefan Adolf. 2021. *Universal Non Infectious Verifier for Arbitrary Credential Schemas (UniVacs).* https://github.com/elmariachi111/ultimate-non-infectious-verifier/blob/main/README.md
[2] Christopher Allen. [n.d.]. The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[3] Man Ho Au, Willy Susilo, and Yi Mu. [n.d.]. Constant-size dynamic k-TAA. In *Proceedings of the 5rd International Conference on Security and Cryptography for Networks, Springer, LNCS 4116* (2006). 111–125.
[4] David Bauer, Douglas M. Blough, and David Cash. 2008. Minimal Information Disclosure with Efficiently Verifiable Credentials. In *Proceedings of the 4th ACM Workshop on Digital Identity Management* (Alexandria, Virginia, USA) *(DIM '08)*. Association for Computing Machinery, New York, NY, USA, 15–24. https://doi.org/10.1145/1456424.1456428
[5] Tim Berners-Lee. [n.d.]. https://www.w3.org/DesignIssues/
[6] Dan Boneh, Xavier Boyen, and Hovav Shacham. [n.d.]. *Short group signatures2.* CRYPTO'04, Springer, LNCS 3152. 41–55 pages.
[7] Carsten Bormann and Paul Hoffmann. [n.d.]. Concise Binary Object Representation (CBOR).
[8] Scott O. Bradner. 1997. Key words for use in RFCs to Indicate Requirement Levels. RFC 2119. https://doi.org/10.17487/RFC2119
[9] Jan Camenisch and Anna Lysyanskaya. [n.d.]. *Lysyanskaya: A signature scheme with efficient protocols, International Conference on Security in Communication Networks.* Springer, Berlin, Heidelberg. http://cs.brown.edu/research/pubs/pdfs/2002/Camenisch-2002-SSE.pdf
[10] Jan Camenisch and Anna Lysyanskaya. [n.d.]. *Signature schemes and anonymous credentials from bilinear maps.* CRYPTO'04, Springer, LNCS 3152. 56–72 pages.
[11] Cross Community Working Group (CCWG). [n.d.]. *Contribution to Vaccination Credential Service Interoperability (VACCSI).* Retrieved June, 2021 from https://vaccsi.org/
[12] Smile CDR. 2003. *HAPI FHIR project.* Smile CDR. https://hapifhir.io/
[13] CEN. [n.d.]. Health informatics – The International Patient Summary, EN 17269.
[14] Good Health Pass Collaborative. [n.d.]. *Good Health Pass Interoperability Blueprint Draft.* Retrieved April, 2021 from https://www.goodhealthpass.org/
[15] European Commission. [n.d.]. *2021: Proposal for a Regulation of the European Parliament and the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital*

Green Certificate), 2021/0068 (COD). Retrieved April, 2021 from https://ec.europa.eu/info/sites/info/files/en_green_certif_just_reg130_final.pdf

[16] Lily Chen (NIST) Dustin Moody (NIST) Andrew Regenscheid (NIST) Karen Randall (Randall Consulting). 2019. *Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters, Draft NIST Special Publication 800-186.* Technical Report NIST.SP.800-186-draft.

[17] L.Peter Deutsch. [n.d.]. DEFLATE Compressed Data Format Specification version 1.3.

[18] Fraunhofer FOKUS eHealth Group. [n.d.]. *CTS2 Linked Data Edition Terminology Server (CTS2-LE) wiki page.* Retrieved March, 2021 from https://publicwiki-01.fraunhofer.de/CTS2-LE/index.php/Hauptseite

[19] Fraunhofer FOKUS eHealth Group. [n.d.]. *IOP3D Project Demonstration (in german).* Retrieved March, 2021 from https://iop3d.fokus.fraunhofer.de/demo/

[20] EU eHealth Network. [n.d.]. *2021: Detailed technical specifications for Digital Green Certificates - - Value sets for Digital Green Certificates.* Retrieved April, 2021 from https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_dt-specifications_en.pdf

[21] EU eHealth Network. [n.d.]. *2021: Detailed technical specifications for Digital Green Certificates - 2D Barcode Specifications.* Retrieved April, 2021 from https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_v3_en.pdf

[22] EU eHealth Network. [n.d.]. *2021: Detailed technical specifications for Digital Green Certificates - Digital Green Certificate Applications.* Retrieved April, 2021 from https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_v4_en.pdf

[23] EU eHealth Network. [n.d.]. *2021: Detailed technical specifications for Digital Green Certificates - Volume 1: formats and trust management.* Retrieved April, 2021 from https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_v1_en.pdf

[24] EU eHealth Network. [n.d.]. *2021: Detailed technical specifications for Digital Green Certificates - Volume 2: Digital Green Certificate Gateway.* Retrieved April, 2021 from https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_v2_en.pdf

[25] EU eHealth Network. [n.d.]. *Guidelines on COVID-19 citizen recovery interoperability certificates – minimum dataset, Release 1.* Retrieved March, 2021 from GuidelinesonCOVID-19citizenrecoveryinteroperabilitycertificates\T1\textendashminimumdataset,Release1,(March15th2021)https://ec.europa.eu/health/sites/health/files/ehealth/docs/citizen_recovery-interoperable-certificates_en.pdf

[26] EU eHealth Network. [n.d.]. *Guidelines on proof of vaccination for medical purposes – basic interoperability elements, Release 2.* Retrieved March, 2021 from https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

[27] EU eHealth Network. [n.d.]. *Interim guidance for developing a Smart Vaccination Certificate.* Retrieved March, 2021 from https://www.who.int/publications/m/item/interim-guidance-for-developing-a-smart-vaccination-certificate

[28] EU eHealth Network. [n.d.]. *Interoperability of health certificates Trust framework, V.1.0, OUTLINE.* Retrieved March, 2021 from https://ec.europa.eu/health/sites/health/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf

[29] European eHealth network. 2021. *Digital covid certificate coordination.* EU Commission. https://github.com/ehn-dcc-development

[30] ENISA. [n.d.]. Data Pseudonymisation: Advanced Techniques and Use Cases. https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/at_download/fullReport

[31] ENISA. [n.d.]. Pseudonymisation techniques and best practices. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/at_download/fullReport

[32] Dick Hardt. [n.d.]. *The OAuth 2.0 Authorization Framework.* IETF RFC 6749.

[33] Linux Foundation Public Health. [n.d.]. *COVID-19 Credentials Initiative.* Retrieved April, 2021 from https://www.covidcreds.org/

[34] HL7. [n.d.]. Fast Healthcare Interoperability Resources (FHIR®). https://www.hl7.org/fhir/

[35] HL7. [n.d.]. *FHIR terminology service.* Retrieved March, 2021 from https://www.hl7.org/fhir/terminology-service.html

[36] HL7. [n.d.]. International Patient Summary Implementation Guide, HL7 FHIR® profile definition. http://hl7.org/fhir/uv/ips/

[37] Russell Housley. [n.d.]. Cryptographic Message Syntax.

[38] ISO. [n.d.]. Health informatics – The international patient summary, ISO/DIS 27269.

[39] ISO/IEC. 2006. *Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification.* Technical Report 16022.

[40] ISO/IEC. 2008. *Information technology — Information technology — Automatic identification and data capture techniques — Aztec Code bar code symbology specification.* Technical Report 24778.

[41] ISO/IEC. 2015. *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification.* Technical Report 18004.

[42] Michael Jones. 2017. Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages. RFC 8230. https://doi.org/10.17487/RFC8230

[43] Michael B. Jones, John Bradley, and Nat Sakimura. [n.d.]. JSON Web Signature (JWS), IETF RFC 7515.

[44] Michael B. Jones, John Bradley, and Nat Sakimura. [n.d.]. JSON Web Token (JWT).

[45] Michael B. Jones, Erik Wahlstroem, Samuel Erdtman, and Hannes Tschofenig. [n.d.]. CBOR Web Token (CWT).

[46] Kassenärztliche Bundesvereinigung (KBV). [n.d.]. *Impfpass, 1.1.0 (in german).* Retrieved April, 2021 from https://mio.kbv.de/display/IM1X1X0

[47] Dmitry Khovratovich and Jason Law. [n.d.]. Sovrin: digital identities in the blockchain era. https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf

[48] Andreas Kuehne and Ernst Jan van Nigtevecht. [n.d.]. Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0. *Committee Specification* 2 ([n. d.]). https://docs.oasis-open.org/dss-x/dss-core/v2.0/dss-core-v2.0.html

[49] Hugo Leroux, Alejandro Metke-Jimenez, and Michael J. Lawley. [n.d.]. Towards achieving semantic interoperability of clinical study data with FHIR. In *Journal of Biomedical Semantics.* https://jbiomedsem.biomedcentral.com/articles/10.1186/

[50] Mike Lodder and Tobias Looker. [n.d.]. BBS+ Signature Scheme. https://mattrglobal.github.io/bbs-signatures-spec/
[51] Mike Lodder and Brent Zundel. [n.d.]. Anonymous Credential Protocol. https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0109-anoncreds-protocol/README.html
[52] loinc.org. [n.d.]. Logical Observation Identifiers Names and Codes (LOINC) code system.
[53] Dave Longley and 2020 Manu Sporny. [n.d.]. Linked Data Proofs 1.0, Draft Community Group Report 29 December 2020. ccg.github.io/ld-proofs/
[54] mGov4EU Project. [n.d.]. *Official website.* Retrieved June, 2021 from https://www.mGov4.EU/
[55] Israeli Ministry of Health. [n.d.]. *Vaccination Certificate, Green Pass and Certificate of Recovery.* Retrieved March, 2021 from https://corona.health.gov.il/en/green-pass/
[56] Medical University of South Carolina. [n.d.]. FHIR Apps for Bioresearch. https://www.hl7.org/events/fhir/roundtable/2017/03/pdfs/D-22_Doug-Williams.pdf
[57] Official GitHub Organization of the EU Digital COVID Certificates (EUDCC) project. 2021. *EU Digital Green Certificates.* EU Commission. https://github.com/eu-digital-green-certificates
[58] Shahid Raza, Joel Hoeglund, Goeran Selander, John Preuss Mattsson, and Martin Furuhed. [n.d.]. In *CBOR Encoded X.509 Certificates (C509 Certificates), draft-mattsson-cose-cbor-cert-compress-08, IETF Internet Draft 08.* https://tools.ietf.org/html/draft-mattsson-cose-cbor-cert-compress-08
[59] Ref-14 [n.d.]. *ZIP File Format Specification, Version 6.3.3.* Technical Report. PKWARE® Inc. https://pkware.cachefly.net/webdocs/APPNOTE/APPNOTE-6.3.3.
[60] Ref-31 [n.d.]. VC HTTP API (0.0.2-unstable). ccg.github.io/vc-http-api/
[61] Ref-40 [n.d.]. BSI: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=1
[62] Yumi Sakemi, Tetsutaro Kobayashi, and Riad S. Wahby. [n.d.]. Pairing-Friendly Curves, IETF Internet Draft. https://tools.ietf.org/html/draft-irtf-cfrg-pairing-friendly-curves-09
[63] Jim Schaad. [n.d.]. CBOR Object Signing and Encryption (COSE).
[64] snomed.org. [n.d.]. SNOMED Clinical Terms (SNOMED-CT).
[65] Manu Sporny and Dave Longley. [n.d.]. CBOR-LD 1.0 – A COBR-based Serialization for Linked Data, W3C Editor's Draft 08. https://digitalbazaar.github.io/cbor-ld-spec/
[66] Manu Sporny, Dave Longley, and David Chadwick. [n.d.]. *Verifiable Credentials Data Model 1.0 – Expressing verifiable information on the Web.* Technical Report. W3C Recommendation. https://www.w3.org/TR/vc-data-model/
[67] Manu Sporny, Dave Longley, Gregg Kellog, Markus Lanthaler, Pierre-Antoine Champin, and Niklas Lindström. [n.d.]. JSON-LD 1.1 – A JSON-based Serialisation for Linked Data, W3C Recommendation. https://www.w3.org/TR/json-ld11/
[68] Orie Sporny, Manu nd Steele. [n.d.]. DID Specification Registries – The interoperability registry for Decentralized Identifiers. https://www.w3.org/TR/did-spec-registries
[69] Orie Steele Tobias Looker and Michael Prorock. [n.d.]. Vaccination Certificate Vocabulary, v0.1, W3C. ccg.github.io/vaccination-vocab/
[70] VCI. [n.d.]. *Vaccination Credential Initiative (VCI).* Retrieved April, 2021 from https://vci.org/
[71] COSE working group. 2016. *COSE Java implementation.* IETF. https://github.com/cose-wg/COSE-JAVA
[72] Kaliya Young. [n.d.]. Verifiable Credentials Flavors Explained. https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf

A DATA MODELS FOR VACCINATION AND RECOVERY CERTIFICATES (AS OF APRIL 2021)

Table 1. Selected data models

Header	WHO	EU Care	Health Travel	Network Recovery	EU Commission	W3C CCG	East Kent NHS
Name	x	x	x	x	x	x	x
Date of birth	x	x	x	x	x	x	-
Unique identifier	x	x	x	x	-	-	x
Sex	x	x	x	-	-	-	-
Name	x	x	x	x	x	x	x
Vaccination Event		x	x	-	-	x	=
Vaccine or Prophylaxis	x	x	x	-	x	x	=
Vaccine brand	x	x	x	-	x	x	x
Vaccine manufacturer	x	x	x	-	x	-	=
Vaccine market authorization holder	x	x	x	-	x	x	=
Vaccine batch number	x	x	-	-	-	x	x
Date of vaccination	x	x	x	x	x	x	x
Dose number	x	-	-	-	x	x	x
Country of vaccination	x	x	x	x	-	x	=
Country of vaccination	x	x	-	-	-	x	x
Signature of health worker	x	x	-	-	-	-	=
Health worker identification	x	x	-	-	-	x	=
Disease or agent targeted	x	x	x	x	x	x	=
Due date of next dose	x	x	-	-	-	x	=
Vaccine Certificate Metadata					-		=
Certificate issuer	in RC 2	x	x	x	x	x	x
Certificate identifier	in RC 2	x	x	x	x	x	x
Certificate valid from	in RC 2	x	x	x	-	x	x
Certificate valid until	in RC 2	x	x	x	-	x	x
Certificate schema version	in RC 2	x	-	-	-	x	x