Towards a COVID-safe life

IOTA-enabled solutions and partnerships framework to promote adoption

Version 0.1 by IOTA Foundation - 18/02/2021

Disclaimer

Note 11.03.2021: The Federal Ministry announced the contract for the implementation of the digital vaccination card as of March 9, 2021. The solution presented here (despite matching partners) does not describe the implementation concept but was created in advance as a possible solution proposal.

The problem

With the end of 2020, tests and immunity passports have been proven to not be an effective countermeasure to limit the spread of COVID-19. A second and third wave of infections followed, with new virus variants discovered overseas, facilitated by the movement of people and difficulty to track outbreaks (following privacy concerns and difficult to enforce preventive quarantine measures without limiting people freedom). With 2021 just started, although not being able to guarantee a 100% immunity, mass scale vaccinations promise to provide a better and safer management of people movements than tests. However this needs to be combined with effective measures to track administering of vaccines.

This paper presents the solutions that the IOTA Foundation (IF) and its partners (Zebra and Ubirch) developed with the aim of creating a COVID-safe world, on which governments could rely in order to ease lockdown measures and people are allowed to go *back to a normal life*, without risking to contribute to the spread of the disease.

The developed solutions focus on the widespread adoption of vaccination programs currently undergoing in various countries and offer ways for a seamless and secure verification of the individuals who have received a vaccination and who can safely go back to their regular activities.

Beyond high-level security of information collected and shared across all the involved stakeholders, the presented solutions promote a *user-centric design*. They have at their core the *user experience* and *friendliness* of proposed tools, the *privacy-by-design* of their users' information and try to *maximise inclusion*, being available on a range of technologies, including smartphones and physical cards with barcodes and QR-codes.

The paper concludes presenting the ecosystem required for the adoption of these solutions and our call to action in order to scale up integration and deployment of the proposed tools.

What are the IOTA-enabled solutions?

IOTA Foundation is a not-for-profit organization developing and maintaining the IOTA distributed ledger and other protocols that leverage the security and immutability of data shared using the ledger itself. Among those, IOTA Identities allow to create a decentralized identity system through which identity information is fully owned by users, who also control their access from third parties, while its authenticity can be verified without need of third parties trust. IOTA ledger and protocols are free to use, does not require additional infrastructure costs and are available for integration with a range of technologies (smartphones, RFID cards, etc).

IOTA Foundation has partnered with Ubirch[1] a german company focusing on data trust, with data sealed at the source, anchored into multiple public blockchains and made verifiable through an API, and

[1] https://ubirch.de/

with Zebra Technologies[2], one of the market leaders in label & card printers, enterprise Android mobile computers and locationing technologies.

IOTA-Ubirch: Secure digital “vaccination” certificates

IOTA Foundation and Ubirch solution solves the important problem of certificate authenticity and provides a seamless user experience to those individuals equipped with smartphones, without compromising the security and authenticity of the shared information. The overall process and solution architecture is presented in the figure below.

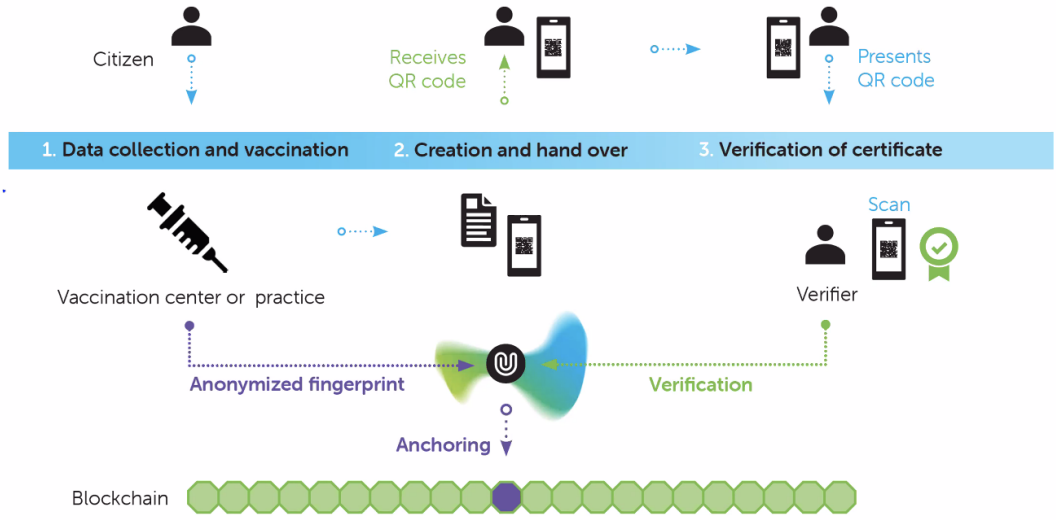


Figure 1. Secure vaccination certificates

Upon vaccination, the involved vaccination center issues a digital certificate which is collected by the given individual (i.e., in the form of an email). The email contains a unique QR-code that references a ledger transaction, where an anonymous fingerprint of the certificate (i.e., a hash of a portion of it that does not include personal information) is immutably stored.

Upon request, the certificate is presented to a verifier (i.e., airport authorities) which assesses that the certificate was issued to the given individual (i.e., through the use of other documents, such as physical IDs), computes the fingerprint and uses the QR-code to access the anonymised immutable fingerprint and confirms that the two match. Fake certificates will not have a fingerprint or the provided one won’t match with the document, thus allowing to quickly identify counterfeit certificates and malicious individuals. This is possible because of the not-tamperable nature of information stored in the IOTA ledger.

The solution is being tested in the Frankfurt Airport and 3 more German Airports as well as to the City of Altötting. Integration is simplified thanks to trusted secure APIs provided by Ubirch.

[2] https://www.zebra.com/gb/en.html

In collaboration with Zebra, the solution is currently being expanded in order to work with barcode and RFID cards issued by vaccination centers to those individuals who do not own or want to use a smartphone. Any vaccination center can be easily equipped with inexpensive commercial card printers to support this scenario.

IOTA-Zebra: Health Passport

IOTA Foundation and Zebra have worked to develop a Self-Sovereign Health Passport (SSHP) that allows individuals to collect from a vaccination center and securely store on their smartphone or barcode/RFID cards their vaccination information and allow them to be presented and securely verified by requesting authorities. Health passports use the ledger and IOTA Identities to build a secure Public Key Infrastructure that:

- Gives individuals control over their private information, in the form of digital credentials, thus including control on sensitive information, such as *having received a COVID-19 vaccination;*
- Guarantees authenticity and integrity of credentials, without requiring any third party integration, thus guaranteeing interoperability and ease of integration. The same solution can work worldwide, for any testing facility and verification authority;
- Creates a strong and verifiable link between individual identity and issued credentials, thus making more difficult to transfer or counterfeit credentials.

The IOTA Selv App[3], complemented by the Zebra Card, work as follows.

Figure 2. Self-Sovereign Health-Passports

Individuals and healthcare providers use our tool to register a digital identity, whose ownership and integrity is immutably anchored to the IOTA ledger (storing a user public key with no PII). Associated identity private key is securely stored in the user phone or card. The individual then gets vaccinated in an

[3] IOTA Selv App: https://selv.iota.org/demo/app

authorised center. After that the healthcare provider creates a digital credential, certifying the individual has been vaccinated against COVID-19 (proof of vaccination). The credential contains the unique user identifiers (public key) and it is signed with the testing facility identity. Signature is immutably anchored to the IOTA ledger. Using the Selv App or the provided electronic card, the user can download the digital credential on her device of choice; the credential stays encrypted in the device memory. The credential is linked to its signature on the IOTA ledger. Upon request the individual shows the card or opens the Selv App and presents a QR-code to a requesting authority. In case of a card the authority verifies the identity of the individual, using a 2-factor authentication, i.e., a physical ID, while in the case of a mobile device this is implicit when the user enables the phone with her biometric. The authority accesses the credential previously decrypted by the user, verifies that was issued to the given subject, and uses the decentralized PKI to verify the signature of an authorized vaccination center. The user is successfully and safely cleared for the required purpose while she retains control over her confidential information.

Integration does not require any system to system direct integration and is simplified thanks to the shared PKI infrastructure and available Business to Business tools (i.e., card printers) and APIs provided by Zebra and Ubirch.

This solution provides maximum outreach thanks to the combination of smartphones and card technologies.

How do IOTA solutions help?

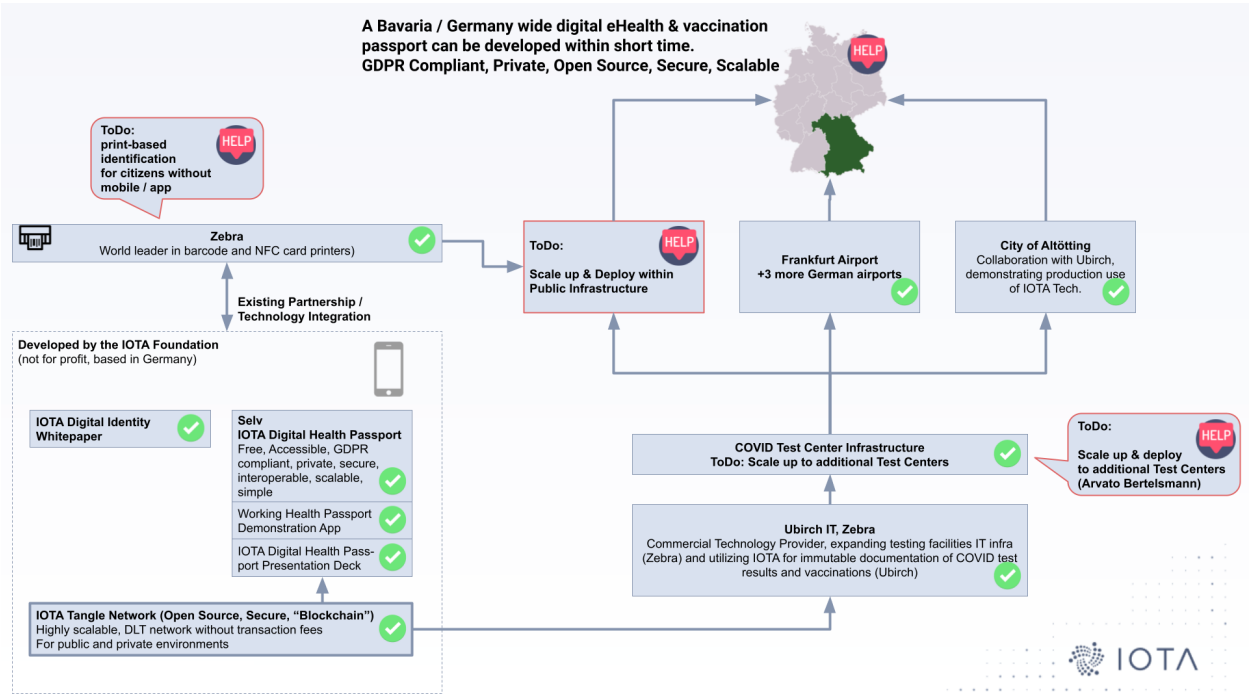
Our solutions have a number of benefits for 1) Individuals who can go back to a COVID-safe life; 2) Health authorities who handle and administer vaccines; and 3) various industry stakeholders who can ensure safe management of people.

	For individuals	**For healthcare providers**	**For industry and authorities**
Secure Vaccination Certificates * can be combined with card-based Certificates	Ready and Easy to use*; reduce the risk of forgery; can go back to a safe normal life * increase inclusion if combined with card-based certificates	Easy to integrate and adopt; simplify secure exporting of information	Easy to integrate and access to verified information; reduce the risk of forgery; can safely manage people in a secure way
Health Passports	All of the above; plus increased accessibility and inclusion and guarantee privacy and user-centric control of sensitive information	All of the above; plus reduce liability and risks in handling and exporting sensitive information. *In future*: it can also include vaccines traceability and guarantee their integrity (see below)	All of the above; plus does not require third party pre-agreed collaborations. IOTA infrastructure can be used in a permissionless way and credentials can exist independently from their use

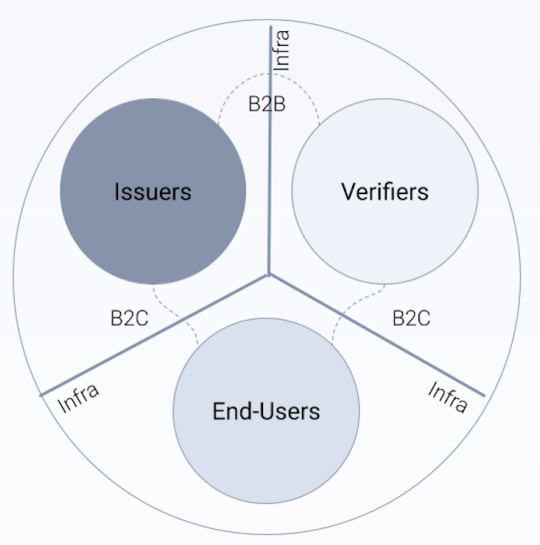
We are aware of a number of academic works and similar initiatives adopted in various countries. Differently from some of them we avoid the risks of technology recentralization[4] and to trade user privacy over convenience[5]. Intestead we leverage an *open infrastructure (IOTA)* and promote *integration, interoperability and outreach.*

How can we scale up?

IOTA Foundation and its partners are further collaborating to expand their network of solution providers in Europe and North America.



However, with technology ready and already being tested (figure above), we need to scale up our adoption ecosystem and include target stakeholders. Ultimately we want to help governments to drive design of standardised and interoperable approaches.



Our Ecosystem

On top of the solution providers, our ecosystem needs to be further developed by including:

- *Healthcare providers* issuing *Certificates and credentials* that certify individuals have been vaccinated (i.e., vaccination facilities, test centers, etc), and that will make use of the B2B side of the proposed solutions;

vaccineguard
h-Check/vaccine-diary/blob/main/Papers/misaca.pdf
1 by IOTA Foundation - 18/02/2021

- *Industry and authorities* (airports, transport authorities, etc) verifying *Certificates and credentials* to ensure individuals have been vaccinated and suitable to come back to a normal life without any risk for the still vulnerable classes of the society, and will make use of the B2B side of the proposed solutions.
- *Individuals and* customer facing organizations willing to adopt these solutions to speed up their return to normal and using the B2C side of the selected solution. This includes flight carriers, companies in the construction industry (i.e., willing to safely bring their workers on-site, with public transport), hospitality services, etc. It can be that in some circumstances Verifiers take this role directly (i.e., governments).

Let's work together

Actors	**Currently Involved stakeholders/Responsible**	**Future Stakeholders/Responsible partners**
Healthcare providers	German Testing center/Arvato Bertelsmann	tbc/Zebra Customers
Industry and authorities	Frankfurt + 3 german airport, City of Altotting/Ubirch	tbc/Zebra Customers; tbc/IOTA Foundation partners
Individuals	Germans flight operator (classified)	ISVs/Zebra; more/tbc

Table 1: Ecosystem maturity

IOTA solutions are open and available to a larger adoption ecosystem. Any other stakeholder that sees itself playing a role in the above ecosystem or helps facilitate inclusion of the above stakeholders is welcome to participate, joining us directly or our infrastructure with its own interoperable solution.

To discuss this further please reach us at: michele@iota.org