

The Necessity Of Vaccination Passporting



Preface

TrustNet Pakistan Foundation is a nationwide industry-networked initiative focused on aid to building blockchain-based ecosystems around personal data management, based on [Self-Sovereign Digital Identity \(SSI\)](#). This TrustNet is the foundation for markets that deals with personal data, as it enables individuals and organizations to control the flow of their private data across different business sectors and industries. It establishes the fundamental building blocks for creating new personal data-centric services.

It is intended for the Pakistan business industry to gain national and international competitive advantage on blockchain-based digital identities. This fascinating new technology that has strong cross-industry potential. Still, it must be trialed to establish the market lead. TrustNet PK dedicatedly invests in arranging cross-industry trials, open-source contributing, Self-Sovereign identity community building, releasing proofs-of-concept, and educating the market about Blockchain and Self-Sovereign Identity (SSI). We believe that together we can accelerate Pakistani industry players to adopt SSI and help build interoperable decentralized ledger-based trust networks.

Our findings, suggestions, and resolutions are originally proprietary to our consortium members and conclusively released to the public in support of our mission. To find out more, please visit <https://www.trust.net.pk>.



TrustNet Pakistan Foundation, 2020

It is to be otherwise noted that this work is copyrighted 2020 by the TrustNet Pakistan Foundation and licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License. To see the copy of this license, visit creativecommons.org/licenses/by-nc-nd/4.0/legalcode.

We hope this white paper contributes to Pakistan's COVID-19 digital response, enabling blockchains and self-sovereign identity to maintain and expand its role as an attractive and competitive technology while innovation into the future. We are highly appreciative of all the valuable contributions of our initiative (Vaccify) and would like to extend a sincere thank you in this regard. We wish you a stimulating read and hope to impart interesting insights into the current challenges faced by Pakistan's digital identity and vaccination ecosystem and its prospects for the future.

The utilization of this material should be strictly under the terms of its Creative Commons license. Users may copy, distribute, or cite this document under the same license. This document may contain material (images, illustrations, and tables) used with a third party's permission or under a different Creative Commons license, and users should cite those elements separately.

To request permission for modifying, transforming, building on top of this material, or distributing any derivative of this document for any purpose. Please email TrustNet Pakistan at support@trust.net.pk. Thank you.

Overview

COVID-19 has severely affected our socioeconomic balance, way we live, do business and interact with others around us. The world is not going to be the same again, even when we recover from this pandemic. We face a stark situation whenever we interact with people, places, or things. These trust issues have become even more critical as the governments around the world have announced lockdowns to be lifted, and life progressively starts to function minimally.

With the arrival of the COVID-19 vaccination in Pakistan, there will be an immense need for rehabilitating the socioeconomic norms of society by opening offices and allowing international and domestic travel as fast as possible. As countrywide immunization can take years in Pakistan, In the phase of transition where the population is being immunized while a significant amount of people are not vaccinated a vaccination governance model will be required. The railways, airports, aviation industry and others will need to know who has been vaccinated to travel domestically or internationally. Companies will need to prevent further spread of virus once employees start returning to the office. As not knowing who is vaccinated and who isn't will make eradicating COVID-19 virus even more difficult. Informal trust is essential as a society. But it takes more than just goodwill, common sense, and manners when a life-threatening pandemic surrounds us. **Governable and digitally provable trust is required.**

Using a blockchain-based digital identity trust framework, we can enable healthcare facilities and laboratory services all across Pakistan to issue digitally-signed vaccination certificates or SarS-COV2 test result status to a person directly to their smartphones. With a quick touchless scan of a QR code either online or face-2-face, a person can prove that they are virus-free or have been vaccinated (once that is available). This special digital certificate can maintain people's data privacy and confidentiality by having only consented and limited personal information. It provides strong cryptographic proof that a certificate belongs to that person, eliminating the need for paper-based proofs. Such a digital certificate would be massively harder to fake or spoof than any paper or plastic credential. And it can be issued in seconds—and revoked in seconds if needed. Moreover, its trust interoperability would be international, meaning a digital certificate issued in Pakistan can be verified and trusted anywhere in the world.

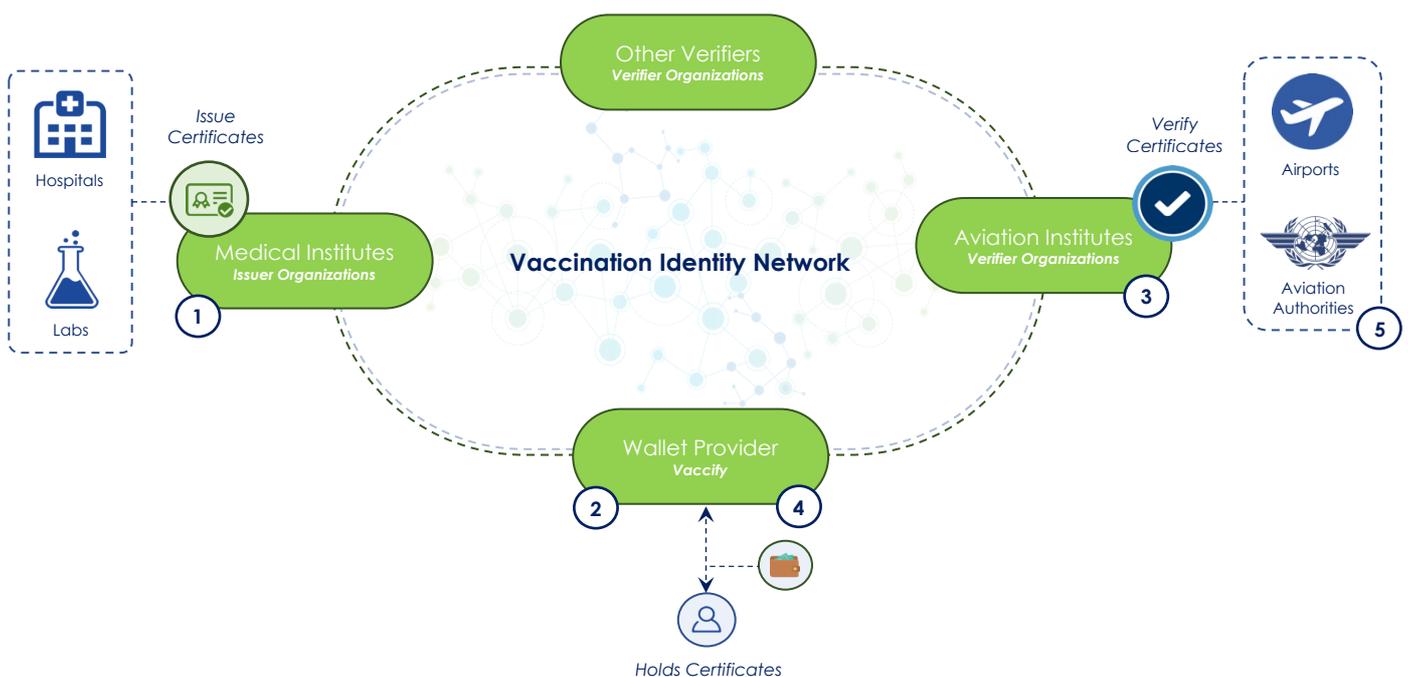


Figure 1: High-level lifecycle of a digital vaccination certificate.

Figure 1 illustrates a high-level lifecycle of vaccination passporting in which from Step 1 the medical institutes can issue a digital vaccine certificate to people which they store at Step 2. While aviation institutes can send vaccine verification request at Step 3 to people, enabling them to give consent for their requested data at Step 4. Finally verification results can be shared with the verifier on Step 5 in a privacy preserved manner.

This whitepaper sheds light on the aftermath of the COVID-19 pandemic and the next digital steps that can be taken to reform the socioeconomic balance in the post-COVID world. It also addresses the digital identity challenges in Pakistan and the friction it creates in the innovation ecosystem. Furthermore, this whitepaper also talks about the future of digital identity and purposes a minimal-viable **vaccination passporting ecosystem** for the post-COVID world. It explains how TrustNet Pakistan's COVID initiative has not only purposed an ecosystem but also implemented a **proof-of-concept (PoC)** that can aid in tackling this digital trust vaccination passporting challenge using self-sovereign identity and blockchain technology.

Key Takeaways:

1

Post-COVID rehabilitation needs attention in advance.

Countrywide immunization could take years, In the post-COVID immunization transition phase where population is partially vaccinated an innovative ecosystem will be required for faster socio-economic recovery.

2

Blockchain-based digital vaccination certificates can help.

Mitigating the need of countless integrations among various stakeholders and saving time and funds while collaborating with existing identity infrastructure can impact post-COVID immunization phase to be faster and low-cost.

3

Self-Sovereign Identity and Blockchains can pave path for future ecosystems.

Ability to issue and verify credentials digitally can enable next generation of user-centric services. Also easy access to digitally verifiable information with Interoperability and cryptographic security can fuel new ecosystems.

4

An open-source COVID-19 initiative by the people for the people.

An innovative ecosystem can enable governance of digital vaccination certificates, allowing public-private sector to issue and verify the vaccination status of people consensually while keeping their privacy and data sovereign to users.

Aftermath of COVID-19 Pandemic

The COVID-19 outbreak has been recognized as a global threat by the **World Health Organization (WHO)**, which has directly or indirectly affected every human being on the planet. Originating from a small city in China somewhere around December 2019, it has spread rapidly across all over Asia and other continents. Many developed countries such as Italy, France, Spain, and the United States have not been fortunate enough to contain it. While the highly developed countries have struggled to contain and deal with this virus, Developing countries like Pakistan have tried to work with minimal resources while exhausting the limited funds. This catastrophe might bring us to a brink where the state has to choose between saving the economy or citizen's lives. The digital policies and actions enforced by the government play a vital role in how the future might look like for Pakistan and its economic rehabilitation.

Health Care

From educational institutes, small and medium businesses to local markets all have taken a toll. However, the system that's under the most stress is the health care sector. An outbreak at such a scale has exposed the healthcare system ruptures. These fractures in the system not only affect our ability of detection, tracking, and prevention of disease but also demonstrates the constraints of resources. Pakistan spends approximately 2% of its GDP on healthcare, where on a global average, countries spend around 10% [1].

As there is no vaccination available for this virus and due to its highly contagious nature. As illustrated in *figure 2*, as of August 2020 around 21 million people have been infected all over the globe [2]. From which more than 761k+ have died, and over 14 million have recovered. Numbers can be deceiving as the testing capacity of developing countries like Pakistan is very low. As of April 2020, there are more than 290k+ confirmed cases in Pakistan, from which around 6000 have died, and 272+ have recovered [3]. According to some experts, this is just an incubation period of the spread of the virus. This means that the

next waves of this virus is still yet to be perceived. Limiting the spread of the virus via social distancing and partial or complete lockdown are potential solutions. However, the effect of these decisions directly propagates to the livelihood of millions of people. It is a very challenging and delicate balance of containing the virus while not damaging the economy in the process. Perhaps by following certain digital footsteps of developed countries, we can achieve this delicate balance.

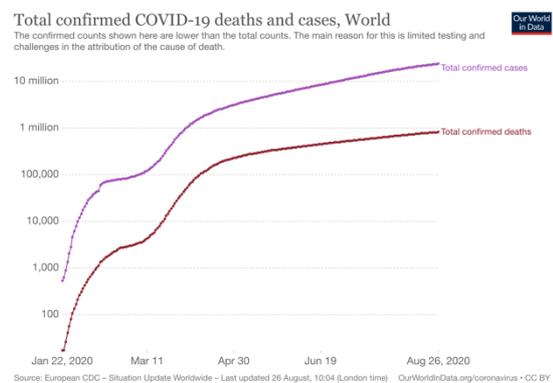


Figure 2: Total confirmed COVID-19 deaths and cases of world till August 2020 [31].

Travel

COVID-19 has significantly impacted travel industries all across the globe. Not only the domestic and international flights are halted in many countries, but the city-wide internal commute is also majorly affected. Where cities are in lockdown and self-quarantine along with social-distancing is being preached the travel industry, businesses such as airlines, hotels, and railway are suffering. People cannot use these services without the risk of getting infected, and the travel industry is trying hard to mitigate the risks of virus spread.

According to the **International Air Transport Association (IATA)** aviation industry in Pakistan is expected to have a decline of around -52% in demand as compared to previous years; Resulting in millions of dollar revenue loss and thousands of potential job losses [4]. In spite of that there are some selective flights and rails that are allowed to flow with extreme precautions and SOPs [5]. Whereas for international flights, all

passengers have to fill in the Personal Declaration of Origin and Health form [6] at the time of check-in to get their boarding passes. Passengers will hand over this form to the Health Department Staff present at the airport upon arrival. Moreover, passengers arriving in Pakistan through flights will go through established health-screening procedures and will have to comply with the Government of Pakistan's quarantine and isolation requirements [7]. As figure 3 explains according to The **World Tourism Organization (UNWTO)** the decline in international tourism is expected to be in between 58% to 78% which translated into losses of approximately between 850 Million to 1140 Million (USD) based on how travel restrictions transform globally by December 2020 [8].

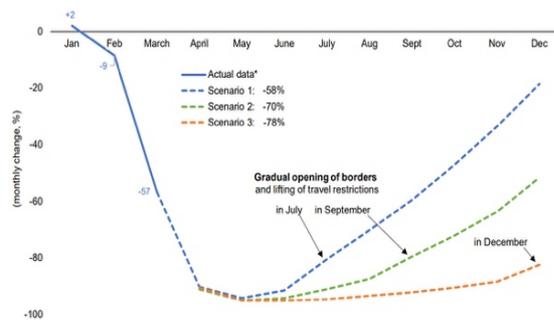


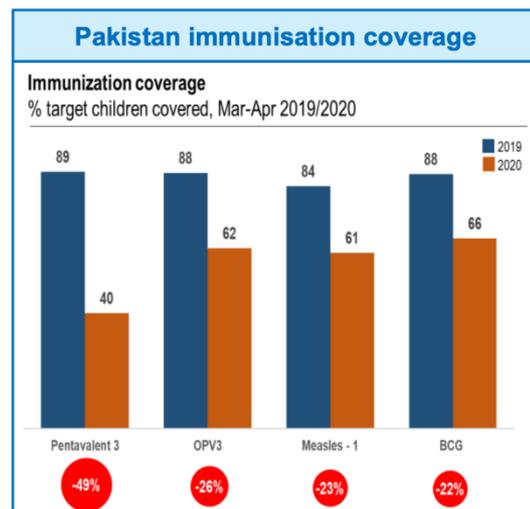
Figure 3: UNWTO estimates on global international tourist arrival in 2020: three scenarios (YoY monthly change, %).

What's Next?

Although with limited resources, Pakistan has responded to this pandemic with unconventional approaches. While the on-ground COVID-19 relief force has been created to facilitate citizens, information technology (IT) is being explored to mitigate the risks and to promote public knowledge. As research and innovation projects are funded to tackle the novel coronavirus, various information technology (IT) initiatives have been brought into the light [9].

However, the situation Pakistan is facing is stark and needs an unconventional strategy. Because were world-leading countries are failing, the least Pakistan needs to do is to survive. As the situation unfolds, social and economic challenges are expected to increase. Circumstances are changing rapidly. As if now, several pharmaceutical companies are racing for a COVID-19

vaccine from which a few are in phase 3 trial [10]. Soon we are expected to have a SARS-CoV2 approved vaccination that works. According to figure 4 from **Global Alliance for Vaccines and Immunization (GAVI)** July 2020 Situation report In April and May (2020), large parts of Punjab faced vaccine stock-out (for pentavalent, measles and BCG), triggered by COVID-19-related flight disruptions [11]. Various questions regarding vaccination's access, pricing, and governance arise in such a scenario, which puts all eyes on the GAVI [12].



Source: Pakistan EPI Management Information Systems

Figure 4: GAVI's report stats on Pakistan immunisation coverage Mar-Apr 2019/2020.

Although vaccination will be available in the near future, there is still a high chance that transition to a normalized society can be chaotic. The transition phase needs to be strategized when people gradually start getting vaccinated, and society operations such as commuting, working in offices, and travel, will be rehabilitated to restore the economy. As there will a considerable number of vaccinated and non-vaccinated people available at the same time, the socio-economic restoration by opening societies cannot be hastened without the risk of spreading the virus and infecting more people. This transition will not be a short-term process as it could take even years to immunize the whole country, which is a challenge of its own. In such an unprecedented phase, there is a need to distinguish between vaccinated and non-vaccinated people so society can function to its maximum potential, and citizens and businesses can be facilitated safely toward the transition.

Pakistan Identity Challenges

Pakistan's Paper Identities

Pakistan's identity ecosystem majorly functions on paper-based credentials i.e. National Identity Card (NIC) and is slowly moving towards digitalization. Physical identity cards and paper certificates are considered convenient more than any digital solutions, and the reason behind that is the lack of inexpensive, reliable and interoperable digital identity solutions. The downsides of the paper-based identity models are far more than its benefits, lack of accessibility and digital data verification are just the tip of the iceberg. Approach of people and businesses toward identity is not wrong; It is quite complex and challenging to translate real-world paper-based trust into the digital world while maintaining privacy and interoperability. That is why even significant nations have not been able to come up with a robust identity solution.

Current Digital Identity Ecosystem

A centralized authority manages the ecosystem of digital identity in Pakistan, the **National Database and Registration Authority**, also known as NADRA [13]. It is the only institute that can digitally verify a national identity and can be trusted. Every other organization in the country needs to have an integration with it to use its services, which is challenging due to its incoherent centralized nature. NADRA application programming interface (API) are not publicly available and they charge per request for verifiable data exchange, making digital reliable information difficult to access and expensive for businesses to adopt.

In demand of reliable and innovative identity services building own identity silos is the only option left for the majority of organizations. These identity silos usually have self-verified identities; if these identity silos need to be in compliance with the government regulations, then the identities are based on NADRA verification. For example, in the case of services like (Daraz, Zameen, Uber, Careem, etc.), these organizations issue digital identities based on their on-premises verification of people via some on-boarding routine. These identities can be referred as self-attested identities. Which ultimately costs respective ecosystems in millions per annum due to their

operational and service cost. Whereas in the case of institutions like banks and telcos (HBL, UBL, Jazz, Telenor, etc.), their identity silos are based on NADRA verified identities. However, this system "works" but fails to broaden the digital identity ecosystem where consumer's one identity cannot be used to create other new identities, ultimately chaining them together in the ecosystem.

For instance, in order to open a first bank account, a consumer needs a paper-based proof of identification for know your customer (KYC) checks, whereas for opening a second account in another bank should be more comfortable as the consumer had already been through the identity verification process and KYC once. However, unfortunately that's not the case, instead of utilizing the digital identity footprint of the consumer to make services better, current digital identity ecosystem repetitively asks for paper-based proof of identifications. Ultimately duplicating processes and services while making them slow and expensive. Moreover, there are repercussions like high duplication of data in identity silos, privacy issues and no consumer's control over personal data. This colossal disconnectivity of information costs in billions per annum on a countrywide scale, as organizations pay not only for the cost of storage and compute for duplicated data but also for data verification, compliance, operations cost and internal services.

On the contrary India's identity ecosystem (Aadhaar) has exponentially improved over the last decade. Aadhaar programme rolled out in 2009, most Indians relied on rudimentary physical documents, such as the "ration card" issued for food subsidies, as their primary source of identification; estimates suggest that more than 85 percent of the population had ration cards in 2011–12. Not only did 15 percent of the population not have any form of legally verifiable ID, but there was also no way to authenticate and verify the identity of ration card holders in real time at no cost. Today that has changed dramatically: more than 1.2 billion Indians have Aadhaar digital identification [14]. As seen in figure 5 In comparison India's digital identity ecosystem is more business and citizen friendly.

Digital identity in healthcare

While all of this may sound adverse, identities in the health care system of Pakistan are another enormous challenge. They are entirely disconnected from almost every identity silo out there. Patients data, lab results, medications, and treatments; all of the information is siloed and is in disconnected individual private and public hospitals all over the country and is not even in secure and easy reach of patients. With the current weak identity infrastructure, if we even try to connect these silos together and build an healthcare identity ecosystem, the whole thing will collapse. The ecosystem won't be able to scale or handle the load and complexity let alone manage privacy, because it was never designed for that purpose. Having a minimal viable ecosystem for health care identities that can provide basic support of health record management, e-prescriptions, digital lab results and vaccination governance all while connection public and private health sector is a vision yet to be conceived.

Moreover, there are immense privacy concerns when it comes to sharing patient's medical data even with other medical institutes. Pakistan is not the only country struggling with the health care digital identity and data privacy crisis in this pandemic. A lot of countries are in hot-water due to legal privacy issues as sharing any type of medical data requires the patient's consent. **South China Morning Post** wrote that Beijing, China rolled out a citizen tracking application that is being concerned for its privacy invasion [15]. According to **The Guardian**, the UK's government is using confidential patient data in coronavirus response, which is being condemned [16].

Vaccination identities

There is no e-governance solution for Pakistani citizens to manage and track their vaccinations or lookup to any certificate repository if need to validate them. However under the **Extended Programme of Immunization (EPI)** Pakistan issues paper-based cards to children of age 0-15 months for record maintenance of their vaccinations [17]. Moreover, there is no visible vaccination ecosystem for citizens that can enable vaccination governance on an individual level in privacy preserved manner. Such an ecosystem that enables vaccination governance and empowers data privacy and data sovereignty can be a useful instrument in post-COVID world.

According to **Centers for Disease Control and Prevention (CDC)** you need to get certain vaccinations when traveling to Pakistan. The list includes Polio, Typhoid, Yellow Fever, Malaria, Hepatitis and more [18]. Unfortunately, it is quite common to have certain vaccination requirements when traveling to or from a developing countries. In June 2014 **World Health Organization (WHO)** imposed a pre-travel condition on Pakistani citizens to have proof of polio vaccination before traveling internationally to curb the transmission of polio virus across the

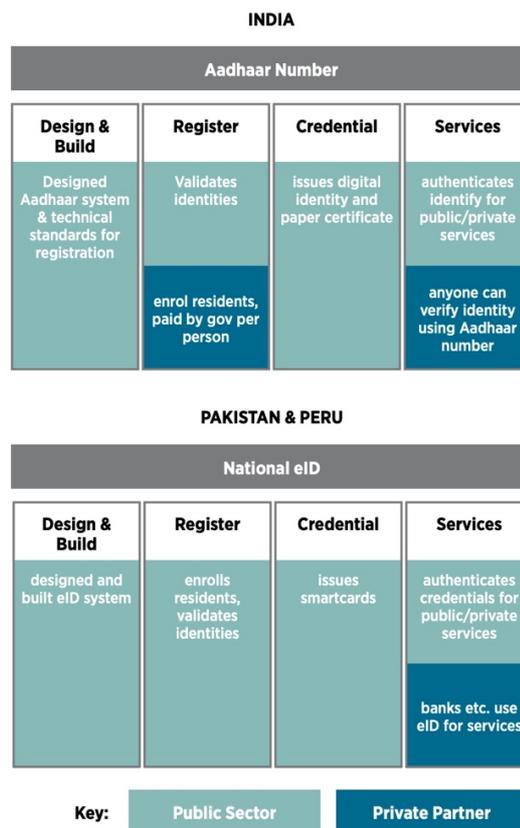


Figure 5: Private sector involvement in Pakistan's and India's digital identity ecosystems. [32]

globe [19]. Under the 18th Constitutional Amendment, the Ministry of Health was abolished, and vertical Programmes, including EPI, were devolved to provinces. Meaning each province is responsible for its own immunization efforts. With GAVI's programme and UNICEF's efforts, the provincial health sectors receive vaccination supplies, which are distributed among government hospitals and basic health units. In the case of polio immunization, teams from the basic health unit go door-to-door and vaccinate kids and mark the doors or walls with chalk for pointers and collect data on paper-based forms. Integrated disease information management system (IDIMS) provided by the world health organization (WHO) is used to convert this data later into digital records, Making this data accessible is a another challenge. Under EPI and the Health Department of Sindh Zindagi Mehfooz (ZM), [Digital Immunization Registry](#) was launching in 2017. An Android phone-based platform enables vaccinators to enroll and track their catchment population's immunization status digitally. However, it is nowhere to be seen. In a business & finance article [20] about 'How to make digital Pakistan work', a profound writer and tech entrepreneur said:

“Developing ‘Pakistan Stacks’ will allow each citizen to have their own electronic locker where their CNIC, birth certificate, academic records will be available”
 – Dawn News, Nadeem Hussain

In this article the writer is emphasizes on how a better digital identity can interact with various ecosystems flawlessly providing better digital services for everyone. In a time of such pandemic, a better digital vaccination identity ecosystem can play a vital role in enabling society to return to 'normal' in a controlled, measurable, and privacy-preserving way. In the early days of the pandemic in an interview with [TechCrunch](#) Bill Gates shared his thoughts about digital certificates for vaccination and test results.

“Eventually we will have some digital certificates to show who has recovered or been tested recently, or when we have a vaccine, who has received it.”
 – TechCrunch, Bill Gates Founder of Microsoft

India's digital identity is more developed, hence it is to leverage their digital identity ecosystem (Aadhaar) to help vaccinate the population. According to an interview article about Aadhaar model helping in vaccinating population quickly chairman of Infosys said [21]:

“The fact that we have 1.25 billion people who have a unique Aadhaar identity, we can create a massive vaccination programme. We must ensure that everybody gets a digital certificate with the date of vaccination, name of the vaccine and through which vendor and at what location.”
 – The Economics Time, Former chairman Unique Identification Authority of India

Moreover, United Kingdom [22] and Germany [23] have demonstrated in their countries that such identity systems can help in rehabilitating the society faster. *Figure 6* shows that an individual identity can be part of more than one eco-system so the digital identity of vaccination ecosystem can be interoperable with other ecosystems. In context of Pakistan's current digital identity ecosystem (NADRA), it is possible to have new generation of vaccination identities in parallel with current centralized digital identities. These vaccination identities should be interoperable, privacy oriented and sovereign to the citizens so that they can have significant autonomy over their digital data.

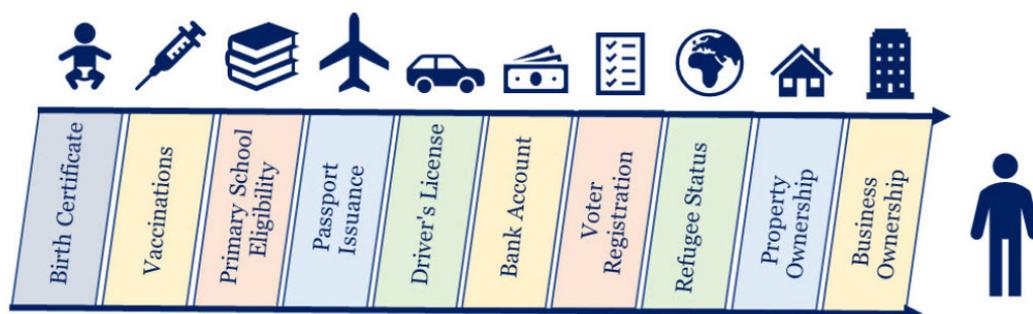


Figure 6: A single identity can be part of various ecosystems. (Based on graphics from ID2020)

Future Of Digital Identity

Evolution of Digital Identity

The Internet was built to connect machines, not people, which is why internet protocol (IP) addresses are used to identify devices over the Internet. Consequently, it was never designed with any standard or explicit way of identifying people or organizations, which has left an empty hole in the layer of internet identity. As a solution to this problem, websites started offering their local accounts with usernames and passwords, which has been the predominant solution ever since the Internet's birth [24].

As the Internet bubble exploded with time and people started using more and more online services daily. The silo-based approach in where users must manage identities for every site they interact with has become unreasonable. Being a usability disaster for individuals, it also creates an abundance of data honeypots for hackers, which exposes the digital trust vulnerable in all internet services. To solve this problem, we have tried to connect different identity silos in various federated models. However, the inadvertent side effects, such as concentrating identity control around a small number of providers, data leakage through non-consensual sharing, raise privacy concerns while not giving the identity owners individuals real control over

their data. As seen in *figure 7* the digital identity has evolved over time; this evolution has always been in effect of a need in the advancement of digital identity.

A **centralized identity** where a single entity controls and owns your data within its domain has struggled to keep up with the pace of a wide variety of online services. Hence necessitate **federated identity**, which gives a degree of portability to a centralized identity. Although federation provides a semblance of portability, the control still remains with the identity provider who sits at the federation web center. **User-centric** identity management places an administration and control of identity information directly into the hands of individuals. This means that a user may provide consent, interoperability, and power, but ultimately, an administrator has full control of their identity. This brings us to a verge where there is a dire need for a sovereign identity. A new type of digital identity that can provide control, security, and full portability on an individual level is still maintaining the governance by entities. **European Union (EU)** has already started paving its way toward this next generation of sovereign identity and is creating an **eIDAS** compatible European Self-Sovereign Identity Framework (ESSIF) [25].

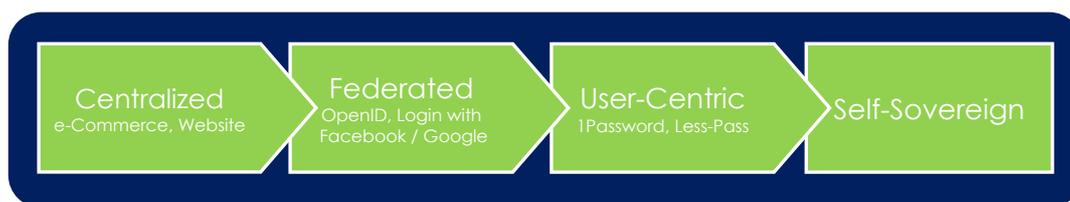


Figure 7: The evolution of digital identity

Self-Sovereign Identity (SSI)

Self-sovereign identity (SSI) is the next step beyond user-centric identity. The user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy [26]. A self-sovereign identity must allow individuals or organizations to make claims and proofs of specific facts about their identity aspects.

"Self-sovereign identity is a lifetime portable identity for any person, organization, or thing that does not depend on any centralized authority and can never be taken away."

– Drummond Reed

Any self-sovereign identity must also meet a series of **guiding principles** — and these principles attempt to ensure the user control that's at the heart of self-sovereign identity. SSI can make use of **Decentralized Identifiers (DIDs)** and **Verifiable Credentials (VCs)** in a way that give users

autonomy and freedom from intervening administrative authorities. Ultimately, which can help achieve SSI guiding principles for autonomous identity.

Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) represent an exciting new breakthrough in the field of identity management. These identifiers are to be used in the next generation of identity management and provide globally unique identifiers (URI) that do not require a centralized registration authority [27]. Control of such identifiers can be proved using **cryptography and public key infrastructure (PKI)**. Think of it as one of the identifiers such as a domain name or a phone number—without a central registrar like ICANN or Pakistan Telecommunication Authority (PTA). These decentralized identifiers prevent correlation and preserve privacy; people can have hundreds or thousands of DIDs representing all of the various digital relationships to which they are connected. These relationships might be with organizations they do business with, friends they interact with, or things they own.

Ultimately, *it eliminates the need for entities to have direct integrations with each other*, allowing them to save a vast amount of time and funds. For example, in a healthcare ecosystem, all hospitals would be able to digitally communicate and transfer sensitive information with each other in an encrypted manner without having to integrate with each other directly. In the past, to make such ecosystems functional, either a central control repository or combinational integration. It is infeasible to make every entity integrate with every other entity in the ecosystem, making it a combination nightmare.

Verifiable Credentials (VCs)

Verifiable credentials (VCs) are the digital equivalent of the physical credentials [28] that we all possess today, such as plastic cards, passports, driving licenses, qualifications, awards, etc. But while digital records are nothing new, these verifiable credentials come with certain cryptographic superpowers that make them **tamperproof, secure, and verifiable**. Whereas a simple digital copy of a university degree record can easily be edited or duplicated, A verifiable digital credential is one that has been issued by a trusted authority for, and only for, its holder. It allows the translation of real-world trust to the digital world. Verifiable claims can be combined with **zero-knowledge proofs** for minimal disclosure, enabling them to remarkably user-privacy oriented.

The data model for verifiable credentials is a **World Wide Web Consortium (W3C)** Recommendation. It allows the translation of real-world trust to the digital world. For instance, using VCs, the legitimacy of a university degree can be digitally proven without asking the university to validate or see the actual physical document. Using ZKPs, it can also be proven that someone is a registered voter and has not yet cast a ballot, without revealing their name or national ID number. The applications of verifiable credentials are simple yet powerful and can translate any real-world trust scenario into a digital. As illustrated in *figure 8*, issuers can create credentials and send them to holders, where holders can store them, and verifiers can ask for proof based upon them.

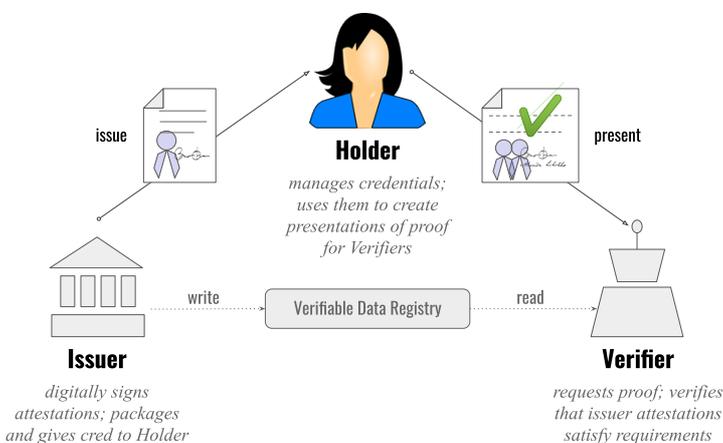


Figure 8: An illustration of triangle of trust where an issuer issues a credential to holder and verifier verifies credentials presented by holder.

Vaccination Passporting Ecosystem

The Need of Vaccination Passporting

As mentioned in the previous chapters, the current status of the digital ecosystem is utterly challenging in Pakistan, which has created a high-friction environment in the innovation ecosystem. Verifiable digital data has become a scarce entity, while the governance model required to achieve these data verifications are profoundly cumbersome. Privacy is often the first pillar that is sacrificed to make integrations, and still solutions stay non-interoperable due to either lack of standardization or inadequate security.

Healthcare services are far more affected by this weak digital trust ecosystem as compared to other services. Digital vaccination services are no stranger to this incompetence and are currently suffering. Vaccination data verification and secure low-cost, interoperable integrations are just hoped as developing nation struggles to deal with data collection governance. Due to all this friction, the overall citizen vaccination e-governance ecosystem is missing in the first place. It results in poor vaccination data governance of people and scattered unconnected silos of data that are inaccessible and unusable by governing authorities and consumers.

With the advent of the SARS-CoV2 (Novel Coronavirus) vaccine, the post-COVID world will demand that societies slowly move toward rehabilitation by governing vaccinations. It will be essential to distinguish between vaccinated and non-vaccinated people to maintain safety and smoothly transit toward an immunized society while avoiding chaos. Digitally verifiable vaccination data can play a critical role in the restoration of the post-pandemic world. A private-public digital trust ecosystem to enable vaccination data governance can facilitate low-cost interoperability and empower data privacy and autonomy. This vaccination passporting ecosystem can induce digital trust among organizations to issue and verify digital vaccination certificates. It can allow them to bypass the costly integrations and share data in a privacy preserved manner and ensure

consumer data autonomy for more trustworthy customer services. All of this and along with a lot more can be achieved by using **self-sovereign digital identity (SSI)** and **blockchain technology**.

The Purposed Ecosystem

To make such a vaccination passporting ecosystem an actuality, various stakeholders need to join hands and build a consortium that will not only benefit people but exponentially benefit the consortium members over a long-term period. **This ecosystem can work standalone and in harmony with existing immunization programme.** As illustrated by *figure 9*, four key players are required to achieve this minimal viable ecosystem, and each player may take a concrete role based on their capability and service needs.

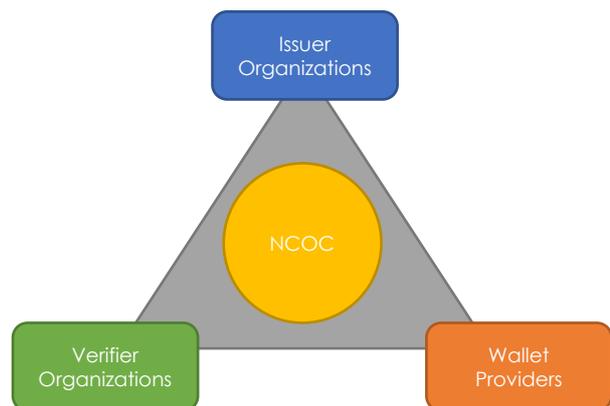


Figure 9: The minimal viable ecosystem illustration.

Issuer organizations play the role of digital verifiable information producers and create digital credentials for their service users. In light of vaccination verification use-case, these issuer organizations will belong to the healthcare domain and can be private or public hospitals, laboratories and basic health units. These consortium members can issue digital vaccination certificates to people on their smartphone or even GSM phones and revoke existing credentials if needed. Eventually improving patient value experience while providing low-cost innovative e-health services.

Users would need a wallet provider service to hold and manage such digital certificates, which induce the need for another key player in the ecosystem, wallet provider. The role of a wallet provider is to render a service that can enable people with the seamless experience of managing their certificates via a digital wallet, allowing them to receive, store, and prove their vaccination credentials. This role can also be taken by the government or any of other consortium members if they desire to provide direct consumer services. A wallet provider service can be provided by any vendor public or private as long as they comply with the **W3C digital credential standards** [29]; this will enable consumers and organizations to avoid vendor locking as they will be allowed to pick any compliant wallet provider while being globally interoperable.

With verifier organizations, the ecosystem triangle completes, as they are the institutions that act as digital data validators for their consumer services. Verifier organizations can verify digital certificates issued by the issuer organizations without having any integration with the issuer organizations, ultimately saving a tremendous amount of time and funds. In line with the digital vaccination certificate use case, the potential verifier organizations can be logistic and aviation companies that want to validate their customer safety. Furthermore, civil aviation authorities can also be part of this consortium to regulate immunized traveling.

Moreover, the verifier organizations can be exposed to only relevant data based on consent requests towards their consumers. This allows verifier consortium members to be highly vigilant with data and privacy issues while bypassing the complexity of the traditional integration crisis.

At the heart of the vaccination passporting ecosystem, the 4th and final key consortium member is the **National Command and Operation Center (NOCO)** that acts as an ecosystem orchestrator. Their role revolves around engaging in creating Standards of Procedure (SOPs) and enforcing the regulations in collaboration with relevant ministries. The NOCO needs to actively support its consortium members with the adoption of this innovative solution and its

associated risks. The vaccination passporting ecosystem falls under the chicken-egg paradox, where issuers depend on verifiers to validate the issued certificates, and verifiers need issuers to issue certificates in order to be validated. Both of the stakeholders cannot function without each other, while the wallet service provider depends on both the issuer and verifier to be functional. The whole ecosystem falls apart without the orchestrator, making its engagement as a leader a necessity.

Such an ecosystem proposes a value proposition that can yield by collaboration and be beneficial for all involved stakeholders. The consortium members can explore new avenues of monetizing verifiable digital data offerings while innovating existing consumer services. It enables them to engage in offering innovative user-centric and privacy-preserved consumer services. In the context of vaccination passporting use-case, issuer organizations (Medical institutes) can operate with a subsidy or have a tariff for issuing digital vaccination certificate per user that would be viable for traveling. On the other hand, verifier organizations (Aviation institutes) can also have a per vaccination verification tariff for passengers or airlines, depending on how they want to design the cost model. Wallet service providers in the ecosystem may rely on a commission-based model in relationship with issuers and verifiers for maintaining their services. This ecosystem's commercial aspect is necessary to keep the private stakeholders motivated and responsible for their services; moreover, it can also help stakeholders to sustain the expense of their cloud infrastructure services.

Need of a governance model

An initial governance model needs to be developed to make such an ecosystem victorious. As the governance model entirely depends on the consortium members, they can propose value creation (rules of collaboration to co-create value as an ecosystem) and value sharing (rules and processes for splitting the value among ecosystem players). Certain important questions need to be answered vividly in this governance model before taking this ecosystem to pilot. Such as:

- Which initial individual partners will be allowed to participate in the ecosystem?
- What requirements do they have to fulfill in order to get access to the platform and its resources?
- To what extent are ecosystem partners invited to shape the ecosystem?
- What is the scope, detail, and strictness of the rules governing this ecosystem?
- Who decides how the value created is distributed among partners?
- What level of ecosystem-specific investments and co-specialization is required?

Only when these questions are answered, this proposed ecosystem can attempt to flourish without any bottlenecks.

Why should Pakistan Innovate?

Of course traditional technologies can get the job done. However, they defy the evolvability and long-term viability. It is precisely how things have been done in the past, where a traditional standalone solution is built without any consideration of future expansion vision or interoperability with other ecosystem services. Following traditional technologies may lead to a temporary solution to deal with the current pandemic; however, it will considerably limit the ecosystem's ability to scale and grow. Not only will it kill the overall interoperability, but it will also halt its ability to produce more beneficial e-governance and consumer services and will close avenues for future revenue growth of involved consortium members. Building this ecosystem on top of self-sovereign digital identity (SSI) and blockchain technology can open untapped horizons not only for governments but also for businesses. Undoubtedly, pursuing such an ecosystem is an opportunity to move

gradually toward the future of an interoperable digital identity at low cost and scalable high returns.

This self-sovereign identity (SSI) and blockchain based ecosystem can work in collaboration with NADRA identities leveraging Pakistan's centralized identity repository to decentrally provide vaccination identities for all without any need for integrations between entities.

The future of digital identity for developed nations and businesses is looking forward to such small interoperable ecosystems from various industries where smaller SSI based ecosystems will connect to build an ecosystem of ecosystems. Within the healthcare domain, SSI based ecosystems can be scaled with various new privacy and data-centric health services such as e-prescription, digital medical test reports, and more. All while providing digitally verifiable data points along with being fully interoperable and highly secure. Moreover, the data will be governed by the ecosystem stakeholders however, it still stays under full sovereignty of its users. Where SSI based health ecosystem has tremendous room to evolve and scale, it will also be able to flawlessly interact with other SSI ecosystems such as logistics, finance, etc. All while preserving the privacy of customers and keeping them as the focal point of the digital services. This whitepaper also illustrates a preliminary value blueprint in figure 10 of the digital vaccination ecosystem, which can be used to assess **co-innovation risks** and **adoption chain risks** of this ecosystem when establishing it.

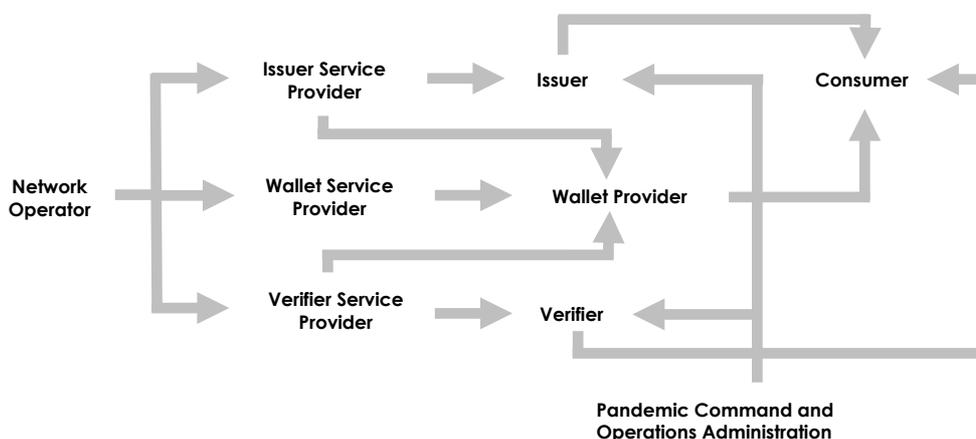


Figure 10: Ecosystem Preliminary Value Blueprint

Vaccify – A COVID-19 Initiative

In April 2020, **TrustNet Pakistan** kicked off an **open-source**¹ COVID-19 initiative **Vaccify**² to tackle the pandemic's digital trust challenges in Pakistan. The vision behind this initiative was to purpose a *Self-Sovereign Identity* and *Blockchain-based* digital vaccination ecosystem. This proposed ecosystem will enable the public-private sector to work in collaboration to provide digital vaccination identities to people who are vaccinated (once the vaccine is available for SARS-CoV2) and verify them on demand.

It is a Blockchain-based digital identity solution for all healthcare institutes, laboratories, and testing facilities across Pakistan. Its purpose is to enable them to directly send digitally signed credentials containing people's COVID-19 vaccination status to their smartphones. It also facilitates the governance of vaccination passporting by allowing the institutions like aviation authorities or commercial airlines to verify people's vaccination status, ultimately helping society to return to the norm and function in a seamless manner. In a traditional approach such a solution would end up with thousands of integration pipelines increasing cost and performance risks.

All this is achieved without making any API integrations between involved ecosystem entities. Such a dynamic approach that doesn't require integration between information issuers and verifiers can significantly reduce cost of operations and services.

Various tech organizations³ who believe in the future of self-sovereign digital identity joined hands with TrustNet Pakistan in working on this initiative. Many professionals and tech enthusiasts from different cities of Pakistan, along with various international

contributors, volunteered⁴ with the aim to help mitigate the post-COVID challenges of society. Ultimately rehabilitation the society by providing user-privacy oriented vaccination certificates and allowing citizens to have autonomy over their personal data while giving national health ecosystem ability to govern vaccination passporting.

The solution is based on Self-Sovereign Identity (SSI) deliberately. An SSI-based digital credential surpasses a paper credentials because of obvious advantages offered by the blockchain technology. These digital credentials have the ability to maintain the data confidentiality of people innovatively. It enables users to prove specific facts about them without sharing data digitally. It would cryptographically verify their vaccination status without revealing any personal information to 3rd-party services. This kind of digital identity puts the user as the focal point of services. Providing people with more autonomy over their digital identity opens doors for new user-centric and privacy-oriented services. It can also enable prior services to be faster, secure, and portable while placing a tab on nonconsensual data harnessing.

Moreover, as it is based on Blockchain, all the records will be immutable. Unlike paper credentials, these will be issued in no time and cannot be forged. In case of false certificate issuance, it could be revoked in seconds, making SSI digital credentials a simple yet powerful concept. With a quick touchless scan of a QR code either online or face-2-face, a person can prove that he or she is virus-free or has been vaccinated. This special digital certificate can maintain the privacy and confidentiality of people by having no personal information and still providing strong cryptographic proof that the credential belongs to that person. Moreover, its trust interoperability would be international, meaning a digital credential

¹ <https://github.com/TrustNetPK>

² <https://vaccify.pk>

³ TrustNet PK Initiative (Vaccify) Partners

⁴ <https://vaccify.pk/hall-of-contributors>

issued in Pakistan can be verified and trusted anywhere in the world as they will be W3C standard compliant. The applications of these decentralized digital immunity passports are expandable and can do more than just proving vaccination status [30]. It can enable public and private organizations to translate the real world trust into digital world, which has been very challenging with the traditional technology.

Vaccify is part of a global initiative called 'COVID-19 Credential Initiative (CCI)' which supports projects that use privacy-preserving Verifiable Credentials (VCs) in order to mitigate the spread of COVID-19 and strengthen our societies and economies. More than 300 individuals from over 100 organizations from all over the world are looking to deploy and/or help to deploy privacy-preserving verifiable credential projects in order to mitigate the spread of COVID-19 and help rehabilitate economies faster using blockchains.

The international organizations across the globe including the United Nations (UN) have proven this technology and the standards we are using. Verifiable digital credential technology is already powering several vital projects, spanning government (verifiable public directories), financial services (banks, credit unions, FinTechs), healthcare (doctor onboarding), humanitarian services (portable identity for refugees, privacy-preserving HIV testing), and many other sectors.

This initiative not only aided in composing an ecosystem but also implemented and open-sourced a **proof-of-concept** to demonstrate it. This proof-of-concept shows how such an ecosystem shall work in a real-world technical setting with all the actors. The PoC demo is built using a stack of various technologies such as **Hyperledger Aries**, **Hyperledger Indy** and **React Framework**. It comprises of a cross-platform (iOS / Android) mobile application to handle digital wallets of users along with vaccine certificate issuer and verifier web-applications and backend agents. This open-source contribution provides a base-line to test such a model and validate its feasibility for e-governance.

Figure 11 shows the high-level flow for digital vaccination certificate issuance and verification. The issuance flows can be broken down into three steps. Firstly the physical identity verification, then the vaccinating process, and finally, the digital certificate's issuance. The vaccination verification process can be either face-2-face or entirely online without any human interaction. This image caters face-2-face verification in which the user needs to first prove his identity by providing a paper-based document and then later scan a QR code to provide a digital proof for his vaccination. In any use-case, face-2-face, or online such tamper-proof digital vaccination certificates can help govern immunization and mitigate digital trust challenges in the post-COVID world in a faster and privacy preserved manner.

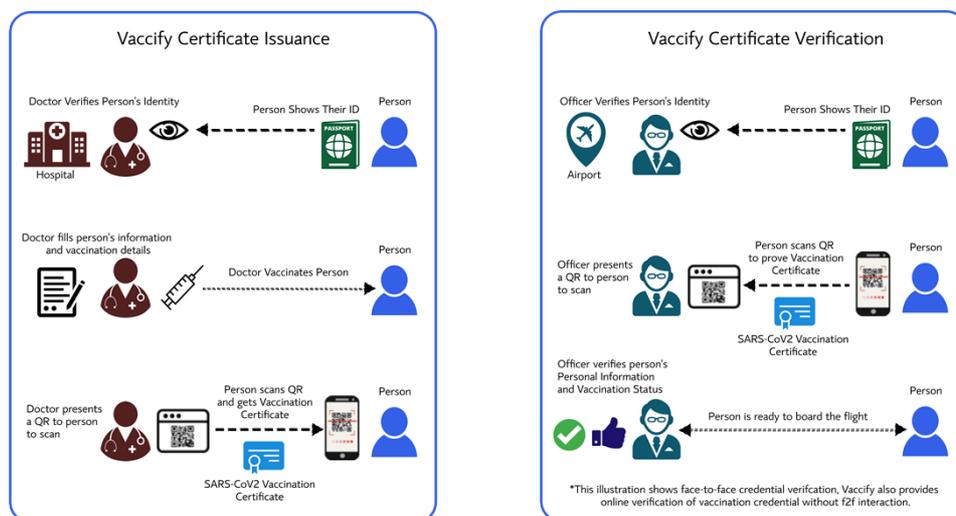


Figure 11: High-level vaccination certificate issuance and verification flow

References

- [1] World Bank, "World Health Organization Global Health Expenditure Database," 2017. [Online]. Available: <https://data.worldbank.org/indicator/SH.XPD.CHEX.GD.ZS>. [Accessed 17 4 2020].
- [2] WHO, "Coronavirus disease (COVID-19) Situation Report – 209," 16 8 2020. [Online]. Available: <https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200816-covid-19-sitrep-209.pdf>. [Accessed 21 8 2020].
- [3] Government of Pakistan, "COVID-19 Pakistan Cases Detail," 21 8 2020. [Online]. Available: <http://covid.gov.pk/stats/pakistan>. [Accessed 21 8 2020].
- [4] International Air Transport Association, "COVID-19 Impact on Asia-Pacific Aviation Worsens," IATA, 24 4 2020. [Online]. Available: <https://www.iata.org/en/pressroom/pr/2020-04-24-01/>. [Accessed 21 8 2020].
- [5] NCOC, "SOPs for travelers," NCOC, 8 2020. [Online]. Available: http://covid.gov.pk/intl_travellers/guidelines_for_travellers. [Accessed 8 2020].
- [6] Pakistan Civil Aviation Authority, "International Passenger Health Declaration Form," CCA, 2 8 2020. [Online]. Available: http://covid.gov.pk/travel_guidelines/International%20Passenger%20Health%20Declaration%20Form%20-%20English.pdf. [Accessed 8 2020].
- [7] Civil Aviation Authority Pakistan, "Precautions Document," CCA, 4 2020. [Online]. Available: <https://www.caapakistan.com.pk/images/Precautions.jpg>. [Accessed 8 2020].
- [8] UNWTO, "IMPACT ASSESSMENT OF THE COVID-19 OUTBREAK ON INTERNATIONAL TOURISM," The World Tourism Organization (UNWTO) is a specialized agency of the United Nations, 5 2020. [Online]. Available: <https://www.unwto.org/impact-assessment-of-the-covid-19-outbreak-on-international-tourism>. [Accessed 8 2020].
- [9] NOCO, "Pakistan Launches Multi- Million Rupees Research Project for COVID-19," National Command and Operation Center, 2020. [Online]. Available: <https://ncoc.gov.pk/govt-initiatives.php>. [Accessed 8 2020].
- [10] J. Corum, D. Grady, S.-L. Wee and C. Zimmer, "Coronavirus Vaccine Tracker," The New York Times, 21 8 2020. [Online]. Available: <https://www.nytimes.com/interactive/2020/science/coronavirus-vaccine-tracker.html>. [Accessed 23 8 2020].
- [11] GAVI, "Gavi COVID-19 SITUATION REPORT #14," GAVI, 28 7 2020. [Online]. Available: <https://www.gavi.org/sites/default/files/covid/Gavi-COVID-19-Situation-Report-14-20200728-1.pdf>. [Accessed 27 8 2020].
- [12] P. Patnaik, "GAVI COVAX FACILITY: Questions on access, pricing & governance," Geneva Health Files, 19 6 2020. [Online]. Available: <https://genevahealthfiles.wordpress.com/2020/06/19/gavi-covax-facility-questions-on-access-pricing-governance/>. [Accessed 23 8 2020].
- [13] Wikipedia, [Online]. Available: <https://en.wikipedia.org/wiki/Nadra>. [Accessed 5 2020].
- [14] Noshir Kaka et. al, "Digital India (Technology to transform a connected nation)," McKinsey Global Institute, 2019.
- [15] South China Morning Post, "Beijing rolls out colour-coded QR system for coronavirus tracking despite concerns over privacy," 2 3 2020. [Online]. Available: <https://www.scmp.com/tech/apps-social/article/3064574/beijing-rolls-out-colour-coded-qr-system-coronavirus-tracking>. [Accessed 15 6 2020].
- [16] The Guardian, "UK government using confidential patient data in coronavirus response," 12 4 2020. [Online]. Available: <https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response>. [Accessed 15 4 2020].
- [17] "Home-based Record Repository," Expanded Programme on Immunisation (EPI), 11 2013. [Online]. Available: <http://www.immunizationcards.org/pak-pakistan>. [Accessed 8 2020].
- [18] Centers for Disease Control and Prevention, CDC, 12 2019. [Online]. Available: <https://www.wnc.cdc.gov/travel/destinations/traveler/none/pakistan>. [Accessed 5 2020].
- [19] The Express Tribune, [Online]. Available: <https://tribune.com.pk/story/707958/for-international-travel-pakistanis-have-to-carry-polio-certificate-from-june-1/>. [Accessed 5 2020].
- [20] N. Hussain, "How to make Digital Pakistan work," Dawn News, 17 8 2020. [Online]. Available: <https://www.dawn.com/news/1574748>. [Accessed 28 8 2020].
- [21] R. K. e. al., "Aadhaar model can help in vaccinating population quickly: Infosys chairman Nandan Nilekani," The Economics Time, 26 8 2020. [Online]. Available: <https://economictimes.indiatimes.com/tech/ites/aadhaar-model-can-help-in-vaccinating-population-quickly-infosys-chairman-nandan-nilekani/articleshow/77754154.cms>. [Accessed 27 8 2020].
- [22] The Next Web, "Could biometric immunity passports get the UK back to work?," 11 5 2020. [Online]. Available: <https://thenextweb.com/neural/2020/05/11/could-biometric-immunity-passports-get-the-uk-back-to-work/>. [Accessed 16 5 2020].
- [23] The Guardian, "Immunity passports' could speed up return to work after Covid-19," 4 2020. [Online]. Available: <https://www.theguardian.com/world/2020/mar/30/immunity-passports-could-speed-up-return-to-work-after-covid-19>. [Accessed 5 2020].
- [24] A. Tobin and D. Reed, "The Inevitable Rise of Self-Sovereign Identity," 29 9 2016. [Online]. Available: <https://www.evernym.com/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>. [Accessed 8 2020].
- [25] "The European Blockchain Services Infrastructure is on its way," 10 2019. [Online]. Available: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/09/25/The+European+Blockchain+Services+Infrastructure+is+on+its+way>. [Accessed 8 2020].
- [26] W. contributors, "Self-sovereign identity," 2020. [Online]. Available: https://en.wikipedia.org/wiki/Self-sovereign_identity. [Accessed 8 2020].
- [27] D. R. e. al, "Decentralized Identifiers (DIDs) v1.0," W3C, 7 2020. [Online]. Available: <https://www.w3.org/TR/did-core/>. [Accessed 8 2020].
- [28] D. C. e. al, "Verifiable Credentials Data Model 1.0," W3C, 11 2019. [Online]. Available: <https://www.w3.org/TR/vc-data-model/>. [Accessed 2020].
- [29] M. Sporny, D. Longley and D. Chadwick, "Verifiable Credentials Data Model 1.0," W3C World Wide Web Consortium, 19 November 2019. [Online]. Available: <https://www.w3.org/TR/vc-data-model/>. [Accessed 20 August 2020].
- [30] Gartner Blogs, "Enabling Safe Worker Certificate with Decentralized Identity," 6 4 2020. [Online]. Available: <https://blogs.gartner.com/homan-farahmand/2020/04/06/enabling-safe-worker-certificate-with-decentralized-identity/?fbclid=IwAR27thmoWKeYU9LoIda9USxieNWv5nCW6jPjLMpomRD33Y7g6ZmjKGDsWx4>. [Accessed 16 5 2020].
- [31] E. CDC, "Our World in Data," European Centre for Disease Prevention and Control (ECDC), 26 8 2020. [Online]. Available: <https://ourworldindata.org/grapher/total-deaths-and-cases-covid-19?yScale=log>. [Accessed 27 8 2020].
- [32] GSMA, World Bank Group and Secure Identity Alliance, "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperati World Bank Group, 2016.