National Applied R&D Centre

MIMOS

Vaccine Management and Certification Ecosystem

Vaccine Management and Certification Ecosystem consists of high-assurance systems that track and trace the vaccine supply chain, generate digital vaccination certificates and verify the authenticity of digital health certificates, with tamper-proof record-keeping and privacy protection.

MIMOS in Healthcare

MIMOS is Malaysia's national applied research and development centre focussing on generating technology solutions that enable the government to provide better services. In the field of healthcare and medical technologies, MIMOS develops need-based, consumer-centric solutions that have supported the consistent and quality delivery of medical and healthcare services.

Delivered and ongoing projects include applications for the Ministry of Health; namely the Vaccine Management and Certification Ecosystem, Teleprimary Care and Oral Health Clinical Information System, the Malaysian Health Data Warehouse, Medical Treatment Information System, Patient Registry Information System, and Food Safety System of Malaysia.

Backed by strong capabilities in Artificial Intelligence, Data Analytics and Integration; along with other cutting-edge technologies such as photonics, smart sensors and Internet of Things, MIMOS is committed to driving continuous improvement in healthcare for Malaysia.

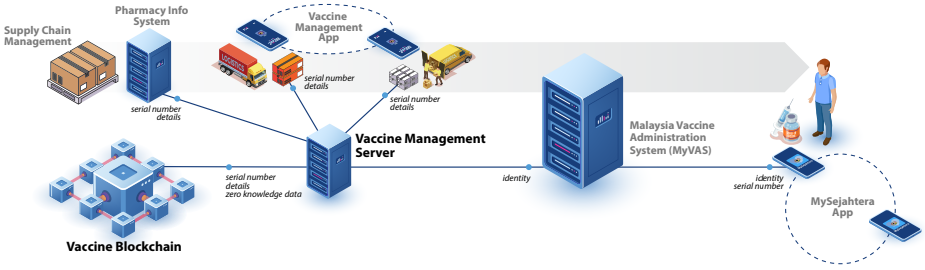
The vaccine information ecosystem in Malaysia comprises:-

- Pharmacy Information System (PHIS)
- Vaccine Administration System (VAS)
- Vaccination Certification System (VCS)
- Vaccination Certificate Verifier Application (VCV)
- Vaccine Management System (VMS)
- MySejahtera Application

Vaccine Management System (VMS)

The basic concept of the VMS is that vaccine allotments, at various levels of aggregation and each with a unique serial number, are tracked through every step of the supply chain process, with data thereof written to:

- **Blockchain:** in the event that all book-keeping rules have been adhered to, or
- **Quarantine database:** otherwise, as indicative of irregularity of fraud.



Blockchain record-keeping is used here as a "trustless" source of truth; with the "chain" providing tamper protection on records previously committed, and each new "block" subject to scrutiny by independent assessment by multiple nodes prior to commitment. Quarantine elements are periodically assessed, and written to the blockchain if deemed legitimate.

The terminal phase of vaccine movement is into the vaccine recipient. MYSJ capture of the vaccine barcode at this point enables binding to user identity information, as then transmitted to the MyVAS and henceforth to the VMS.

VMS protects identity information by means of zero knowledge cryptographic association of vaccine recipient identities to their corresponding vaccination records on the blockchain. This anonymisation prevents any vaccination record from being traced back to any identity. On the other hand, the legitimate vaccine recipient is able to straightforwardly assert an irrefutable claim to one or more vaccination records.

The VMS design objective is to implement a "hard" separation of identity and injection information, so as to be privacy protective even if the blockchain record-keep is openly accessible. The integration of such information would then occur only in the singular circumstance of the vaccination certificate, with presentment thereof under the exclusive control of the legitimate claimant.

Uniqueness

The MIMOS contributions are specifically designed to ensure the following unique value propositions: -

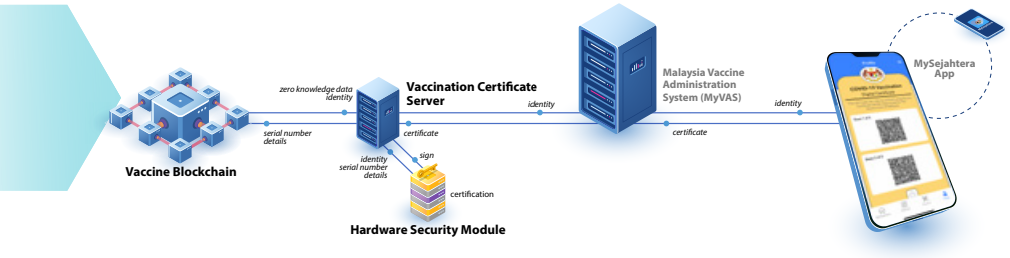
- **Maximum assurance of processes and outcomes;**
- **Maximum utility of outcomes; and**
- **Maximum security and privacy of vaccine recipient information.**

To our knowledge, and particularly so at the time of system conceptualisation and design, our system was the first attempt at population-scale blockchain-based tracking of vaccine movement from inception to injection. The obvious value proposition is to ensure the highest possible degree of trustworthiness in the vaccine supply chain process; as then literally signed, sealed and then delivered to the prescribed user-personalised client system which submits an identity claim of sufficient assurance.

The trustworthiness of the resultant vaccination certificate enables presentment not just within the context of a mobile application, but at its most basic form as a printed-paper document with both human-readable text and machine-readable information representations. This is very much in the spirit of the WHO stipulations on process and outcome inclusiveness, and is intended to facilitate widest and most equitable use of the MOH certificates.

Picture courtesy of Ministry of Science, Technology and Innovation

Vaccination Certificate System (VCS)



Such certificates would be treated as high-assurance documents issued by a trusted authority certifying that a person has undertaken a vaccination, and details thereof. In Malaysia the Ministry of Health (MOH) is the sole authority undertaking such certification.

This certificate is presented by a claimant, to a verifier, who must possess some objective means to ascertain authenticity. To this end, screenshots and photos of certificates are not themselves certificates, due to the impossibility to establish authenticity. For casual use cases, visual inspection of the certificate within some acknowledged presentment system, i.e. the MYSJ application, is sufficient.

Use case stringency requires machine-to-machine transmission between claimant and verification systems, with optical barcodes being a suitable mechanism that naturally enforces physical proximity. Vaccination certificates worldwide generally fall into one of the following categories: -

- **Result of online query to trusted server:** which manifests as a dynamic optical code containing fixed URL and claimant identity, and also a time-constrained single-use security token to prevent replay without fresh consent. Verification systems should maintain a whitelist of such trusted servers, as subject to periodic updating; or
- **Claimant-stored document:** inclusive of digital signature from a trusted authority, which manifests as a static optical code. Verification systems should maintain a whitelist of trusted public-keys for signature verification, as likewise subject to periodic updating. Note verification of such certificates can be undertaken without online connectivity at both claimant and verification systems.

Certificate encoding formats are an evolving technical domain, with most countries and jurisdictions taking the lead from the World Health Organisation (WHO) in terms of high level objectives. The VCS design objective is for MOH certificates to be compliant to various international specifications and standards, and to be verified by the widest possible spectrum of verifier systems.

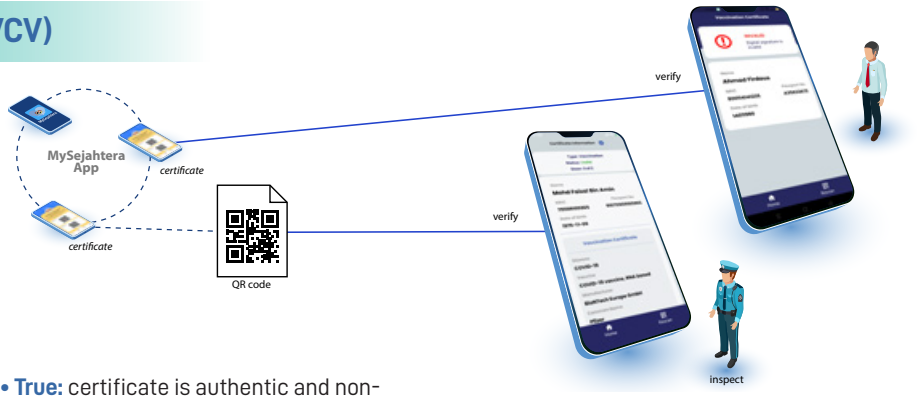
The present incarnation of the MOH certificate is of the claimant-stored category, with the signature therein computed in the interior of a hardware security module (HSM) containing the authority private-key, as furthermore located on a secure authority network. The resultant capability for offline verification is necessary for the highest possible scalability under high volume and scarcity conditions, i.e. as might occur at immigration checkpoints.

Vaccination Certificate Verifier (VCV)

The Government of Malaysia is committed to ensure the widest possible recognition of the MOH certificate for outbound travelers, and also to enable recognition of certificates presented by incoming travelers of necessity and importance to Malaysia. To this end, the Government of Malaysia will undertake upload of the MOH public-key to the relevant servers, and also download of foreign authority public-keys for subsequent VCV retrieval, as necessary on periodic basis.

VCV will attempt to be a "universal" verifier of the widest possible spectrum of vaccination certificates, and is capable of handling both live query and signature-based certificate formats.

Signature verification in VCV will return a true/false outcome, which can be interpreted as follows: -



- **True:** certificate is authentic and non-repudiable by any party inclusive of the signing authority;
- **False:** possibility of fraud; most likely from alteration, possibly unintentionally, of certificate subsequent to signing; or
- **Indeterminate:** inability to ascertain trustworthiness; due to non-possession of signing authority public-key, non-whitelisting of authority URL or non-recognition of the certificate format.

VCV will also attempt display of the barcode contents in human-readable form, perusal of which might be important for the use of case interest, ie for comparison of certificate identity information to identity as presented by the natural person claimant.

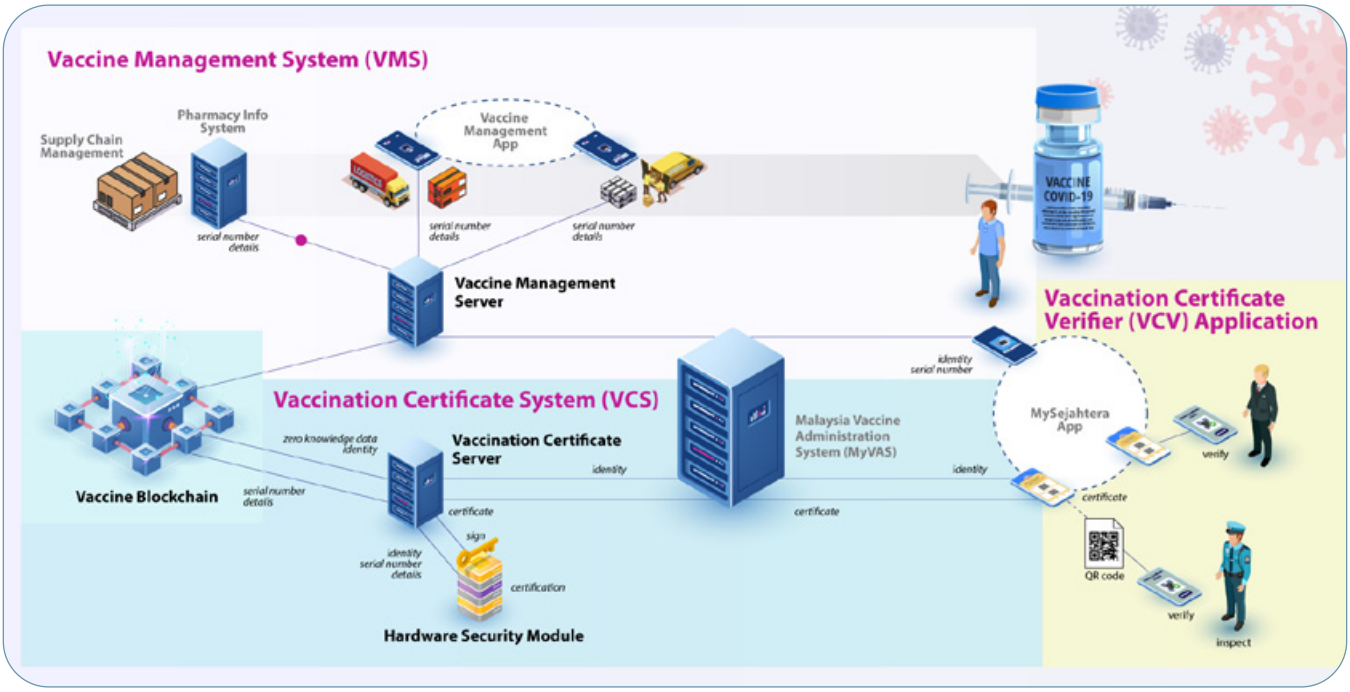
Information Trustworthiness and Assurance

Vaccine information should lend itself to third-party verification and validation; with maximum support for receiver-side use cases, minimum assumptions on the operational circumstances, and no compromises of trustworthiness and assurance. To this end, the basic concept is to undertake:-

- **Harvest of identity-specific vaccination information from the blockchain,**
- **Assembly of vaccination certificate with such constituent information,**
- **Computation of digital signature for affixation to such certificate.**

The particular form of the VCS certificate specifically designed to be "universal" is compliant to EU and WHO specifications, as ensures the widest possible recognition and acceptance.

Vaccine Management and Certification Ecosystem



Privacy Protection

Vaccine Management System (VMS) undertakes privacy protection by means of:-

- **Zero knowledge tablespace separation and traversal in database storage,**
- **Zero knowledge representations of user identity information in blockchain storage,**
- **Zero knowledge queries for blockchain search and certificate assembly.**

This architecture dispenses with no direct association of personally identifiable information (PII) to sensitive vaccination information; and ensures that VMS, and its constituent storage elements, has strong privacy and security characteristics, even if the system is in a "passive" state. This level of protection is furthermore not jeopardised by administrator access, at the system or even underlying platform level.

The form and client-side safe-keeping of the vaccination certificate also lends itself maximum privacy protection; in that certificate instances, in either electronic or paper form, are only issued on submission of a high-assurance identity claim; and further that no retention thereof is undertaken server-side. User consent is also implicit in the certificate presentation process. Note both privacy and informed consent are cited as design and operational imperatives in the WHO and EU specifications. The basic concept is that the vaccination certificate is medical information which needs respectful handling, and that presentation thereof is for a single purpose only ie assessment immediately prior to passage through a physical checkpoint, with limitation of the information processing to only serve that purpose.

The verifier-side VC2 process is likewise privacy protective, and is specifically designed not to retain certificate information subsequent to the action. The non-necessity for VC2-side online connectivity also allows minimisation of information leakage.

National Applied R&D Centre
MIMOS

MIMOS Berhad (336183-H)
Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia
Tel: +603 8995 5000 | Fax: +603 8996 2755
www.mimos.my

mimosmalaysia