Cryptographic digital signature is the solution to deter forgery of MySejahtera Covid19 vaccination certificates

By: Prof. Dr. Muhammad Rezal Kamel Ariffin, Director Institute for Mathematical Research, UPM & President Malaysian Society for Cryptology Research

On August 10, 2021 the then Deputy Minister for the Ministry of Health (MOH) Dr Noor Azmi Ghazali informed that the MOH enforcers together with other government agencies will take stern actions upon parties that forge the MySejahtera Covid19 vaccination certificate.

On August 25, 2021 The Star rolled out an exclusive regarding anti-vaxxers willing to fork out at least RM1000 in order to obtain forged MySejahtera Covid19 vaccination certificates to enjoy current privileges by those who have had their vaccinations. Furthermore, The Star reported that Bukit Aman CID Director Comm Datuk Seri Abd Jalil Hassan warned the public that forging the MySejahtera Covid19 vaccination certificate is a serious offence.

The Star also reported that there is a verification application that can be used to scan a QR code within the MySejahtera Covid19 vaccination certificates. The methodology to ensure some level of security is via an automated refreshing process of an individual’s QR code in some predetermined interval. The Star also reports that the application does not prevent people form stealing, duplicating or misusing vaccination details.

It is an established principle that a digital document can be determined its authenticity by utilizing a cryptographic element known as digital signature. In contrast with public interpretation that equates digital signature with the digital image of a signature, the digital signature has its technological foundation via mathematical cryptography which is installed upon a digital application using a programming language chosen by the developer.

A developer can refer to the National Trusted Cryptographic Algorithm List (MySEAL) developed by CyberSecurity Malaysia (CSM) together with local cryptographic experts between the years 2016-2020 during the 11th Malaysian Plan for suitable cryptographic digital signature algorithms.

The digital signature is an electronic signature that is enables one to verify the identity of a sender/signatory of a message and is used to ensure the transmitted information is correct and legitimate within an electronic transaction. The digital signature enables a recipient to confirm the integrity, authenticity of a message without hesitation. At the same time, the digital signature disallows repudiation by a sender of a message.

The enforcement of digital signatures in Malaysia is governed by the Digital Signature Act 1997 (DSA1997). The DSA1997 has provisions to regulate the use of digital signatures and related matters. In Malaysia, digital signatures are supplied through a digital certificate provided by Certificate Authorities mandated by DSA1997.

Without the use of cryptographic digital signatures, a digital application provider cannot reliably determine the authenticity of a digital information transaction. Furthermore, DSA1997 only mandates the cryptographic digital signature process as a mechanism with legal provisions in terms of ensuring the integrity and authenticity of a digital information transaction.

Thus, to ensure that the transmission of Covid-19 can be curbed by using the MySejahtera Covid19 vaccination certificate, the administrator of this application needs to review the development framework of this application in terms of its compliance with DSA1997.

Only by incorporating a cryptographic digital signature mechanism into the MySejahtera application, authorities checking Covid-19 vaccination certificates can confidently give way to those intending to cross-state at this point.