Tandatangan digital berkriptografi merupakan penyelesaian masalah pengesahan arahan kepada aplikasi MySejahtera

Oleh: Prof. Dr. Muhammad Rezal bin Dato' Kamel Ariffin, Pengarah Institut Penyelidikan Matematik, UPM & Presiden, Persatuan Penyelidikan Kriptologi Malaysia (MSCR)

Pada 20 Oktober 2021 Kementerian Kesihatan Malaysia (KKM) mengeluarkan kenyataan media berkenaan "penghantaran emel dan SMS palsu" yang diterima oleh pengguna MySejahtera adalah "disebabkan oleh penyalahgunaan API (*Application Programming Interface*) dan bukannya kebocoran pada pangkalan data MySejahtera."

Situasi yang telah menyebabkan penyalahgunaan API ini boleh berlaku adalah kerana ketiadaan mekanisme pengesahan arahan. Dalam situasi sedia ada, permintaan pelaksanaan arahan oleh API telah dipersetujui oleh aplikasi serta-merta. Sewajarnya aplikasi perlu mengesahkan terlebih dahulu sumber arahan tersebut.

Dokumen digital (dalam kes ini arahan oleh API kepada aplikasi) boleh dipastikan kesahihannya dengan memasang elemen kriptografi yang dipanggil tandatangan digital. Berbeza dengan pengetahuan umum yang menyamakan istilah tandatangan digital dengan imej digital tandatangan, tandatangan digital didasari teknologi kriptografi bermatematik.

Tandatangan digital adalah tandatangan elektronik yang digunakan untuk mengesahkan identiti penghantar/penandatangan sesuatu mesej dan digunakan bagi memastikan sesuatu maklumat adalah betul dan sah di dalam transaksi elektronik. Ianya boleh dipasang pada aplikasi digital menggunakan bahasa pengaturcaraan pilihan pembekal aplikasi.

Pembekal aplikasi boleh merujuk kepada Senarai Algoritma Kriptografi Terpecaya Negara (MySEAL) yang dibangunkan oleh CyberSecurity Malaysia (CSM) bersama-sama pakar kriptografi negara diantara tahun 2016-2020 semasa Rancangan Malaysia ke-11.

Penguatkuasaan tandatangan digital di Malaysia terletak di bawah Akta Tandatangan Digital 1997 (ATD1997) yang mempunyai peruntukan untuk mengatur penggunaan tandatangan digital dan hal-hal yang berkaitan dengannya. Di Malaysia, tandatangan digital dibekal melalui sijil digital oleh pihak berkuasa pemerakuan (*Certificate Authority*) yang dimandat oleh ATD1997.

Tanpa penggunaan tandatangan digital berkriptografi, sesuatu pembekal aplikasi digital tidak dapat dengan pastinya untuk menentukan kesahihan suatu transaksi maklumat digital. Tambahan pula, ATD1997 hanya memandatkan proses tandatangan digital berkriptografi sebagai mekanisme yang dipayungi peruntukan undang-undang negara dalam hal memastikan kesahihan suatu transaksi maklumat digital.

Justeru, bagi memastikan aplikasi MySejahtera hanya menerima arahan dari sumber yang sahih, pentadbir aplikasi ini perlu melihat semula kerangka pembangunan aplikasi ini dari segi kepatuhannya pada ATD1997. Hanya dengan memasukkan mekanisme tandatangan digital berkriptografi ke dalam aplikasi MySejahtera, aplikasi MySejahtera boleh mengatasi masalah integriti dan kesahihan arahan yang diterima.