Government Public Key Infrastructure (GPKI)

Sophia binti Hashim
Datin Dr. Siti Hanom binti Marjuni
Maryani binti Che Ali
Noraida binti Aman Nor

(This article has been published in CITRA MAMPU, 2018)

INTRODUCTION

The Multimedia Super Corridor (MSC) heralded Malaysia's breakthrough into the information age since its launch by YAB Tun Mahathir Mohamad during his first tenue as Prime Minister in 1996. This monumental initiative reverberated across the region and convinced leaders and entrepreneurs from other countries to embrace the information and Communication Technology (ICT) as the new engine of economic growth. According to Jack Ma one of the richest man in Asia the establishment of the MSC is what inspired him to create Alibaba in 1999.

One of the key pillars of the MSC is the E-Government Flagship Application comprising 7 pilot projects to lead the country into the information age. To support this move, the Government of Malaysia has embarked on the project called Government Public Key Infrastructure (GPKI) in 2002 to centralize he management of digital certificate for all government agencies in order to facilitate and secure online transaction for E-Government services.

GPKI has increased the level of trust and confidence among users in using E-Government online application systems. Its main function is to secure transaction through identity has been used to secure transaction through identity verification and ensuring the privacy and integrity of data through highly secured data encryption and non-repudiation by using digital signature.

As GPKI system developed, more than 350,000 units of digital certificates have been issued and used in managing transactional high security data, information and documents for financial management and accounting system, electronic procurement system and legal related

systems. Distinct features of GPKI include of usage of multi-licensed Certification Authority and fully automated in issuance of user's digital certificate. After 15 years of implementation, GPKI has successfully elevated the confidence of users in using online application systems by an increase of 600% and the number of transactions trifold from 300 to 1200 per day. Thus GPKI has built a secure ICT foundation for Malaysia's economy.

PROJECT DETAILS

Malaysian Public Key Infrastructure (GPKI)

Public Key Infrastructure (PKI) is considerably a de-facto standard for security in a modern environment of web technologies and online services. PKI comprises od hardware, software, people, policy and procedures to uphold security which usually requires an enablement at users' end i.e laptop, desktop, mobile, etc via PKI services. PKI services csn be provided via numerous channels, usually through Application Programming Interface (API). Implementing PKI services in a very large organisation especially in government, requires proper planning, strict regulations and flexible integration mechanisms.

The PKI services have three (3) basic characteristics of security namely:

a. Identity Verification (Authentication) - guarantee the authenticity of the user
b. Data Encryption - ensuring the security and integrity of data and information in the transaction
c. Digital Signature - ensuring the data is valid and cannot be denied (non-repudiation), and to guarantee the integrity of data and information

The PKI services provided by the Government of Malaysia start with the digital certificate stored in the EG smartcard with the PKI-enabled features in 2002. During this initial period, it has been used in several EG applications, especially that involve the government's procurement and claim payment and require high security standard. Later in 2009, soft

digital certificate was introduced to support the implementation of an EG application that involve the legislative transaction in the government. At this stage, PKI services provided was considered standalone and manual process, until the introduction of the Government PKI (GPKI) system in the year 2011. Digital Certificate evolution in the government since 2002 is shown in Figure 1.

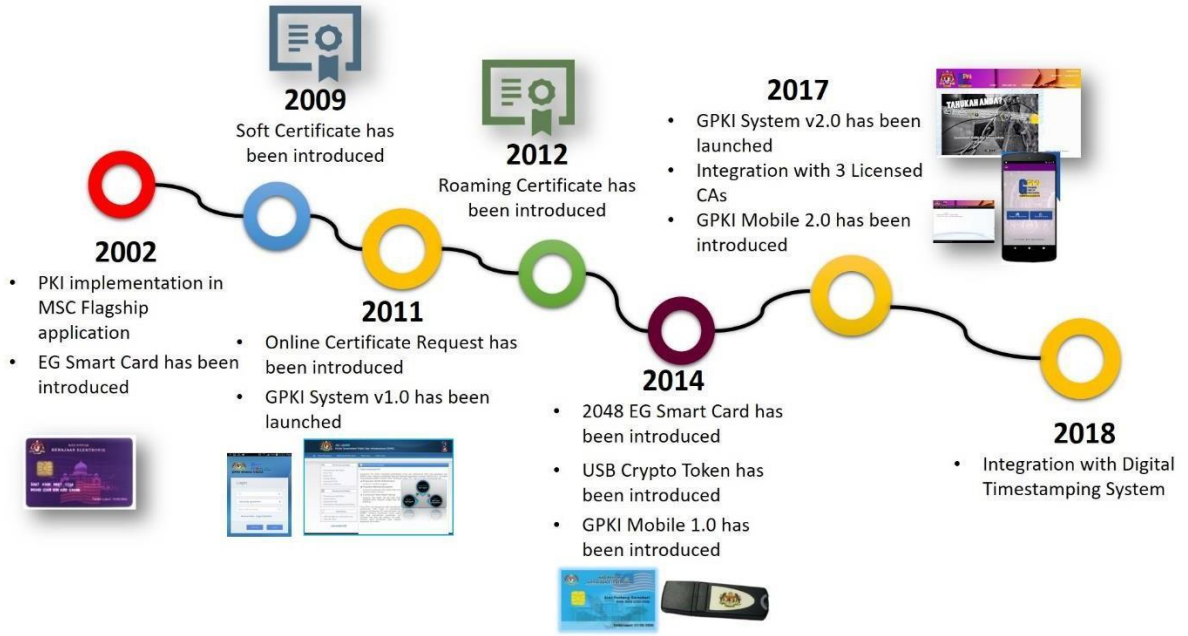

Figure 1: GPKI Evolution

MAMPU introduced GPKI 1.0 which provided a centralised digital identity request application, verification and approval for government personnel. Within 6 years, it has evolved to manage ten (10) government ICT applications servicing almost 70,000 government personnel, with various digital identity access medium including digital token, soft certificate and roaming certificate. Recently, it also includes Secure Socket Layer digital certificate request and approval application.

The GPKI system supports the transformation of government services by facilitating the transfer “from the counter to the automated online system” to drastically improve government service delivery and operational efficiently. Government services demand a very high requirement in terms of accountability, integrity and confidentiality. PKI is one of the crucial media to enable services that require a highly secured system capable of managing security risk. It is also able to offer more electronic government services and increases the workflow efficiency.

In a nutshell, GPKI objectives are:

a) To deliver a centralized PKI service by providing individual digital certificates and SSL digital certificates to agencies for the implementation of ICT systems in Government; and
b) To offer ICT Security consultancy services to advise the use of digital certificates in order to verify identities, digital signatures and encryption information.

The implementation of GPKI covers various PKI services which include:

a) To develop and implement GPKI Portal and Systems;
b) Appointment and registration of the Sub Admin and Authorized Personnel from the Implementation Agency;
c) Individual Digital Certificate Management;
d) Server Digital Certificate Management; and
e) ICT Security Advisories and consultancies.

GPKI starts with the implementation of GPKI Portal that offers all PKI services to the applications users in the Government agencies. Among PKI services provided in the GPKI Portal are digital certificate application, individual PIN management, profile and status update and medium acceptance confirmation. The portal also provides various information related to GPKI such as user manuals, supporting software and drivers, frequently asked questions and helpdesk and support information.

There are three (3) level of administration involves in the GPKI Portal implementation, namely Admin, Sub Admin and Authorized Personnel. MAMPU as central agency is the Admin that responsible for coordinating and monitoring the implementation of the overall GPKI implementation and provide advice for the use of PKI technology for Government ICT systems. The second level is the Implementation Agencies as the Sub Admin that responsible in managing the application, coordinates and administer the system application that uses and integrates with GPKI Service. The third and final layer comprise of Authorized Personnel from the Public Agencies that include Ministries, Departments, federal and state agencies as well as statutory bodies which use ICT systems of the Federal Government.

The ICT Security advisories and consultancies in the GPKI scope are targeted to the Government Lead Agencies, particularly those involved in the development of government ICT systems or the provision of ICT infrastructure. The advisories and consultancy services include:

a) Assessment of risk level Government ICT systems to identify appropriate security controls for GPKI service requirements;

b) To define the usage of digital certificates either to verify the identity, digital signature and/or encryption information;

c) Outlines the technical requirements in terms of standards, integration requirements and specific requirements for digital certificate usage.

GPKI is one of the ICT Security Services that enhance the data and information security level for the Government ICT Applications which align with the Data Signature Act 1997 (DSA 1997) and Digital Signature Regulations 1998 (DSR 1998). The Government of Malaysia has outlined that all ICT Applications that requires PKI services must subscribe to the GPKI Services administered under MAMPU. GPKI Portal provides a centralized digital certificate application and management for the Government personnel that requires GPKI Services.

ENHANCING THE GPKI SERVICES THROUGH INNOVATION

GPKI has built a secure and resilient ICT foundation and significantly increase access to information and communications technology and strive to provide universal and affordable access to the internet with high level of security. Until February 2018, 115,127 of users have registered and utilized the GPKI services from which 53.9% of them are using it for Financial and Accounting application system followed by E-Procurement application system which stands at 36.6%. Other frequently accessed are E-Judicial-Syariah (1.6%), E-Court (3.3%), E-Pension (0.1%), E-
Sovereignty (0.4%), E-Tax (0.1%), E-Vetting (0.1%), E-Land (0.1%) and others (3.8%).

In order to meet public demand for secured government services and enhance GPKI services, strategic partnership were established with the following parties:

- **Partnership with Licensed Certification Authorities (CA)**

  Licensed CA namely POS Digicert Sdn. Bhd, MSCTrustgate Sdn. Bhd. and TM Applied Business Sdn. Bhd. provide a service for digital certificate issuance. The CA will initiate digital certificate issuance and revocation, starts with the verification process of the applicant and validate the application of the certificate issuance. Then, the certificate is issued by the CA. The chain of trust in the verification process must be established and maintained by the CA along this process to ensure the process is trusted. Furthermore, the integration between GPKI system and CA system contributes an effective, trusted and secured verification and digital certificate issuance process.

- **Partnership with National Registration Department**

  National Registration Department provides a service for user's identity verification through MyIDENTITY system. User's identity verification is a vital process in order to ensure the applicant of the certificate is a valid user as claimed. This real time identity verification will reduce human error during user registration in GPKI system and help better user management.

  The integration of GPKI with the partnership is illustrated in Figure 2 below:

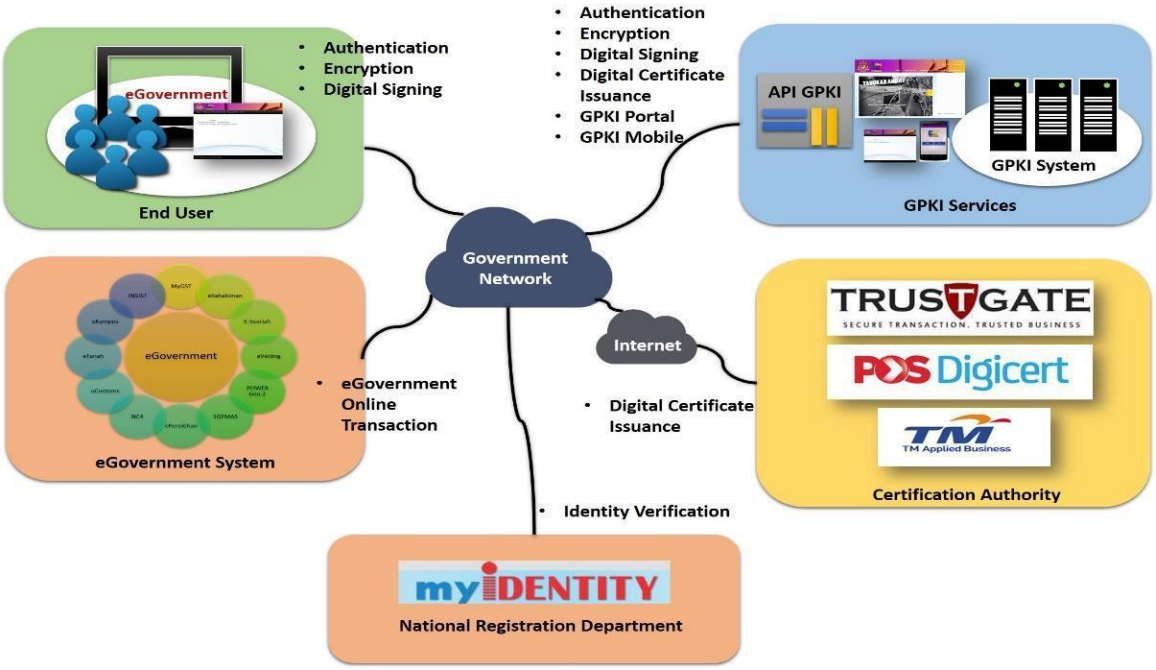

Figure 2: The integration of GPKI system with the partnership

LESSON LEARNT FROM 15 YEARS OF IMPLEMENTATION

Throughout the span of 15 years of its implementation the GPKI project development and management team encountered several challenges to note categorically:

- **Technologies** - The PKI technology is evolving which include token and digital certificate key length. The complexity of PKI solution also contributes to the challenges where the GPKI system needs to cater and applies all related changes.

- **Work Process** – Effective PKI project implementation requires a framework as a guideline. However, during the GPKI implementation since 2002 there is no framework established and lack of monitoring and coordination of the stakeholders has reduced the effectiveness of GPKI service delivery.

- **Knowledge and Awareness** - Lack of understanding in PKI implementation, especially among the ICT application system owner on how to implement the PKI technology had reduced the growth of GPKI services provided.

CHARTING THE WAY FORWARD

In future the GPKI project will be enhanced by adding the digital timestamping features. Digital timestamping (DTS) is a digital time service provided by MAMPU centrally to public sector agencies. Whereas, Time Stamping Authority (TSA) is a responsible agency that provided DTS service does not act as a licensing Authority. As set forth in the Digital Signature Act 1997, DTS service providers should provide date and time marking services recognized by the Malaysian (Communication and Multimedia Commission (MCMC). MAMPU as a DTS service provider and also responsible as a TSA should meet the following requirements for due recognition to be recognised as TSA:

i. Develop TSA policy and Practise Statement;
ii. Develop DTS system by standard; and
iii. Conduct compliance audit.

This expansion process is expected to be completed by the year 2020 with the development of policy and guideline for DTS service in the public sector which would help facilitate the wider implementation of the service through its integration with other government application systems.

Figure 3: Roadmap of DTS Services