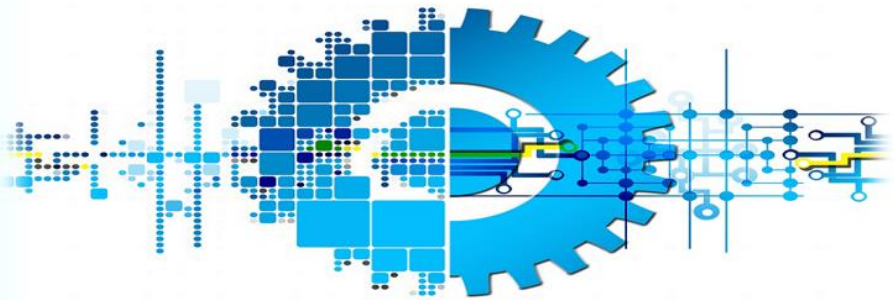
KEMENTERIAN DIGITAL
JABATAN DIGITAL NEGARA

TAKLIMAT PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN [GOVERNMENT PUBLIC KEY INFRASTRUCTURE (MyGPKI)]



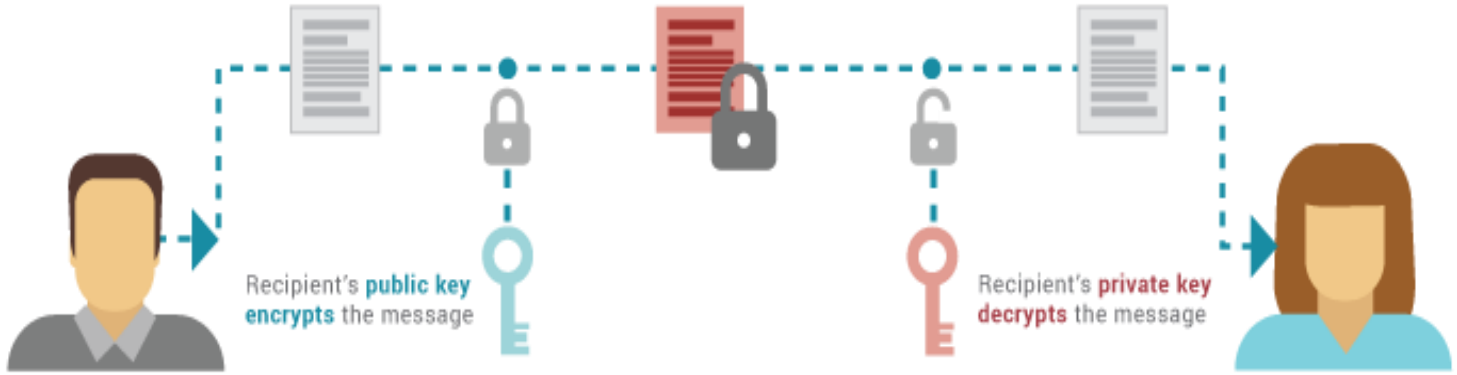
MALAYSIA MADANI

LATAR BELAKANG

- Perkhidmatan MyGPKI ialah satu perkhidmatan keselamatan ICT berasaskan teknologi *Public Key Infrastructure* (PKI) selaras dengan **Akta Aktiviti Kerajaan Elektronik 2007**, **Akta Tandatangan Digital 1997** dan **Peraturan-peraturan Tandatangan Digital 1998** serta **Arahan Teknologi Maklumat 2007.**

- Perkhidmatan MyGPKI mula dilaksanakan pada tahun 2002. Pelaksanaan Perkhidmatan MyGPKI juga melibatkan pembekalan sijil digital oleh Pihak Berkuasa Pemerakuan Berlesen - *Certification Authority* (CA) yang dilantik oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM).

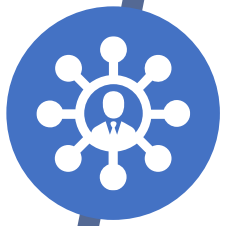
- Jabatan Digital Negara (JDN) merupakan agensi peneraju/pusat yang diberi tanggungjawab untuk melaksanakan pembekalan Perkhidmatan MyGPKI kepada agensi sektor awam.



FUNGSI

Menyediakan perkhidmatan *Public Key Infrastructure* (PKI) dengan **membekalkan Sijil Digital Pengguna** bagi tujuan pengesahan identiti, tandatangan digital, penyulitan dan penyahsulitan maklumat serta **Sijil Digital Pelayan** (SSL) kepada agensi-agensi Kerajaan bagi mengukuhkan keselamatan sistem ICT Kerajaan.

OBJEKTIF



Memantapkan tahap keselamatan data dan maklumat bagi sistem ICT Kerajaan.

Melindungi keselamatan data/ maklumat Kerajaan dalam talian daripada ancaman keselamatan melalui pengesahan identiti, penyulitan dan tandatangan digital.

Meningkatkan tahap kepercayaan pengguna untuk melaksanakan transaksi secara dalam talian bagi sebarang urusan Kerajaan.

TUJUAN PKI

PENGESAHAN IDENTITI

- **Kesahihan Identiti**
  Membenarkan pengguna individu, organisasi dan pengendali sistem ICT Kerajaan untuk mengesahkan identiti pengguna dan pelayan.

PENYULITAN DAN PENYAHSULITAN

- **Kerahsiaan**
  Melindungi maklumat sistem ICT kerajaan semasa transaksi dilaksanakan.

- **Integriti**
  Memastikan mesej atau dokumen tidak diubah, dimanipulasi atau rosak.

TANDATANGAN DIGITAL

- **Tanpa Sangkalan**
  Mengelakkan pengguna menyangkal sesuatu transaksi yang telah berlaku atau tindakan yang telah dilaksanakan.

AKTA AKTIVITI KERAJAAN ELEKTRONIK 2007

Tandatangan

13. (1) Jika mana-mana undang-undang menghendaki tandatangan seseorang di atas suatu dokumen, kehendak undang-undang itu dipenuhi, jika dokumen itu adalah dalam bentuk suatu mesej elektronik, oleh suatu tandatangan elektronik yang—

(a) dilampirkan kepada atau dikaitkan secara logik dengan mesej elektronik itu;

(b) mengenal pasti secukupnya orang itu dan menunjukkan secukupnya kelulusan orang itu terhadap maklumat yang berhubungan dengan tandatangan itu; dan

(c) adalah boleh dipercayai sewajarnya memberikan maksud bagi, dan hal keadaan yang tandatangan itu dikehendaki.

13. (3) Akta Tandatangan Digital 1997 [Akta 562] hendaklah terus terpakai bagi apa-apa tandatangan digital yang digunakan sebagai suatu tandatangan elektronik dalam apa-apa aktiviti Kerajaan.

ARAHAN TEKNOLOGI MAKLUMAT 2007

18.2.1. Kerahsiaan
18.2.2. Integriti
18.2.4. Kesahihan
18.2.5. Tidak Boleh Disangkal

AKTA TANDATANGAN DIGITAL 1997

Kewajipan pelanggan untuk menyimpan kunci persendirian dengan selamat

43. Dengan menerima sesuatu perakuan yang dikeluarkan oleh pihak berkuasa pemerakuan berlesen, **pelanggan yang dinamakan dalam perakuan itu menerima kewajipan untuk menjalankan jagaan yang munasabah untuk mengekalkan kawalan ke atas kunci persendirian dan mencegah pendedahannya kepada mana-mana orang yang tidak diberi kuasa** untuk menghasilkan tandatangan digital pelanggan itu.

Harta dalam kunci persendirian

44. Suatu kunci persendirian merupakan harta persendirian pelanggan yang memegangnya secara sah.

Kepuasan kehendak tandatangan

62 (2) (b). Suatu tandatangan digital yang dihasilkan mengikut Akta ini hendaklah disifatkan sebagai suatu tandatangan yang mengikat di sisi undang-undang

AKTA TANDATANGAN DIGITAL 1997

Mesej yang ditandatangani secara digital disifatkan sebagai dokumen asal

65. Suatu salinan mesej yang ditandatangani secara digital hendaklah sah, berkuat kuasa dan berkesan seperti asal mesej itu melainkan jika jelas bahawa penandatangan telah menetapkan suatu hal tertentu mesej yang ditandatangani secara digital itu sebagai asal yang unik, yang dalam hal itu hanya hal tertentu itu merupakan mesej yang sah, berkuat kuasa dan berkesan.

MAKLUMAT PALSU

73. Seseorang yang membuat, secara lisan atau bertulis, menandatangani atau memberikan apa-apa perisytiharan, penyata, perakuan atau dokumen atau maklumat lain yang dikehendaki dibawah Akta ini yang tidak benar, tidak tepat atau mengelirukan dalam apa-apa butir-butir melakukan suatu kesalahan dan boleh, apabila disabitkan, **didenda tidak melebihi lima ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi sepuluh tahun atau kedua-duanya**.

PERATURAN-PERATURAN TANDATANGAN DIGITAL 1998

Regulation 30. Storage of private keys.

*(1) The data storage medium for the private key may be **hardware based or software based**.*

*(2) If the data storage medium of the private key is **hardware based, the holder of the private key shall ensure that the token, smart card or other external device in which the private key is stored is kept in a secure place** and in a secure manner.*

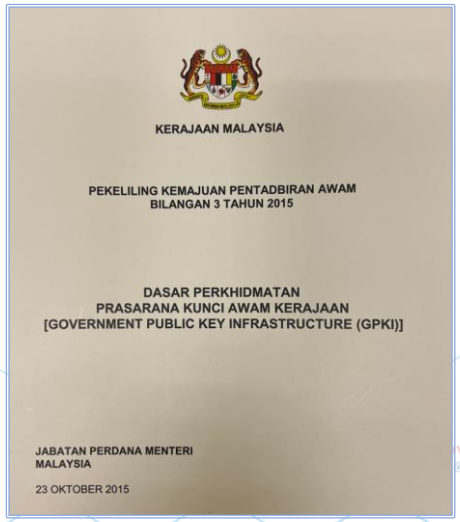
*(3) If the data storage medium of the private key is **software based, the holder of the private key shall ensure that the computer system in which the private key is stored is reasonably secure**.*

*(4) The **personal identification numbers** or other data used for the identification of the rightful holder of the private key in conjunction with the data storage medium for the private key **shall be kept secret**.*

PEKELILING KEMAJUAN PENTADBIRAN AWAM BIL. 3/2015:
DASAR PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN [GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

6. PENYATAAN DASAR

"Semua sistem ICT Kerajaan yang memerlukan kemudahan Prasarana Kunci Awam (PKI) hendaklah menggunakan Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI)"


KERAJAAN MALAYSIA

PEKELILING KEMAJUAN PENTADBIRAN AWAM
BILANGAN 3 TAHUN 2015

DASAR PERKHIDMATAN
PRASARANA KUNCI AWAM KERAJAAN
[GOVERNMENT PUBLIC KEY INFRASTRUCTURE (GPKI)]

JABATAN PERDANA MENTERI
MALAYSIA
23 OKTOBER 2015

12. PRINSIP PEGANGAN PELAKSANAAN GPKI

- Semua **penjawat awam hanya dibenarkan menggunakan satu sijil digital** sahaja.
- **Pemegang sijil digital yang mempunyai capaian kepada pelbagai aplikasi** yang mempunyai tahap kawalan keselamatan yang berbeza hendaklah **menggunakan medium sijil digital yang boleh mencapai aplikasi yang mempunyai tahap kawalan keselamatan yang tertinggi**.
- Pemegang sijil digital pengguna perlu **memaklumkan atau memulangkan medium sijil digital yang rosak, tamat tempoh, tamat perkhidmatan, bersara atau disalahgunakan kepada agensi peneraju menerusi Pegawai Diberi Kuasa (AP)**.

1 Pengurusan dan Pembekalan Sijil Digital Pengguna

- Token
- *Roaming certificate + OTP (One-Time Password)*
- *Soft certificate (SoftCert)*
- *Roaming certificate (RoamingCert)*

2 Pengurusan dan Pembekalan Sijil Digital Pelayan

- *Single domain*
- *Multi domain*
- *Wildcard*

3 Perkhidmatan Meja Bantuan dan Khidmat Sokongan Teknikal

4 Khidmat Nasihat dan Konsultasi bagi Penggunaan PKI

SIJIL DIGITAL PENGGUNA

Pengurusan Sijil Digital Pengguna meliputi proses pengesahan permohonan dan identiti pemohon, penjanaan pasangan kunci awam dan peribadi, pengeluaran dan pembatalan Sijil Digital Pengguna.

Bil.	Perkara	SIJIL DIGITAL TOKEN	SIJIL DIGITAL ROAMING	SIJIL DIGITAL SOFTCERT
1.	**Keterangan**	Sijil digital yang disimpan di dalam peranti di mana kunci peribadi dijana secara on-board dan disimpan di dalam token yang mengandungi cip kriptografi	Fail yang mengandungi sijil digital pengguna dan kunci peribadi (private key) yang disimpan dalam pelayan di agensi peneraju	Fail yang mengandungi sijil digital pengguna dan kunci peribadi (private key) yang dimuat turun dan disimpan ke dalam komputer pengguna
2.	**Jaminan**	**TINGGI**	**SEDERHANA (TINGGI)**	**SEDERHANA (RENDAH)**
3.	**Ciri-ciri**	• Kunci peribadi (private key) disimpan dalam token • Kunci peribadi (private key) tidak boleh disalin • Kalis ubah (tamper-proof) • Pasangan kunci (key pair) dijana dalam cip (on-board key generation)	• Kunci peribadi (private key) disimpan di agensi peneraju • Kunci hanya disimpan bagi tempoh tidak melebihi dua jam dalam komputer pengguna.	• Kunci peribadi (private key) disimpan di dalam komputer pengguna • Kunci disimpan secara tetap dalam komputer pengguna sehingga ianya dihapuskan
4.	**Storan**			

PENENTUAN PENGGUNAAN JENIS MEDIUM SIJIL DIGITAL PENGGUNA

KEPERLUAN TAHAP KAWALAN KESELAMATAN SISTEM ICT KERAJAAN	MEDIUM SIJIL DIGITAL PENGGUNA YANG DIPERLUKAN			
	TOKEN	ROAMINGCERT + OTP	ROAMINGCERT	SOFTCERT
TINGGI (Klasifikasi Data : Rahsia Rasmi Risiko: Tinggi, Sederhana dan Rendah)	✓	✓	✗	✗
SEDERHANA (Klasifikasi Data : Data Terkawal/ Sensitif Risiko: Tinggi dan Sederhana)	+	+	✓	✗
SEDERHANA (Klasifikasi Data : Data Terkawal/ Sensitif Risiko: Rendah)	+	+	+	✓
RENDAH (Klasifikasi Data : Data Terbuka Risiko: Tinggi, Sederhana dan Rendah)	✗	✗	✗	✗

✓ **DIPERLUKAN** + **PERLU SOKONG** ✗ **TIADA KEPERLUAN**

Nota:

- Ditanggung oleh JDN berdasarkan kriteria dan syarat ditetapkan
- Tidak ditanggung oleh JDN. Agensi perlu melaksanakan perolehan sendiri daripada CA

EV — LENGKAP

Extended Validation

1. Menyediakan keselamatan *session* dan privasi
2. Maklumat organisasi dipapar secara automatik di alamat pelayar dengan perbezaan warna yang kontra

OV — PERTENGAHAN

Organization Validation

1. Menyediakan keselamatan *session* dan privasi
2. Maklumat organisasi hanya dipaparkan apabila diperiksa oleh pelawat

DV — ASAS

Domain Validated

1. Menyediakan keselamatan *session* dan privasi
2. Tidak memaparkan jenama/ organisasi

Private Trust — PERSENDIRIAN

1. URL dan Top Level Domain (TLD) tidak didaftarkan
2. IP local 127.0.0.1

INTERNET | **INTRANET**

Tinggi — **TAHAP KESELAMATAN** — Rendah

TRANSFORMASI SISTEM & EVOLUSI MEDIUM SIJIL DIGITAL

2002

Kad Pintar

Sijil digital disimpan di dalam kad pintar. Key Lenght:1024 bit

ivest client

ivest client diperkenalkan bagi membolehkan kad pintar yang dibekalkan dibaca oleh Sistem ICT

2009

Soft Certificate

Sijil digital disimpan di dalam medium storan pengguna

RA Portal

RA Portal diperkenalkan bagi pengurusan sijil digital *soft certificate*

2011

Sistem GPKI 1.0

Sistem GPKI 1.0 dan MAMPU GPKI Agent 1.0 diperkenalkan bagi pengurusan perkhidmatan GPKI

2012

Roaming Certificate

Sijil digital disimpan di dalam pelayan perayauan dan akan dimuat turun ke komputer pengguna jika digunakan.

2014

Kad Pintar

Sijil digital disimpan di dalam kad pintar. Key Length:2048 bit

Token

Sijil digital disimpan di dalam kripto token

2015

GPKI Mobile Client 1.0

GPKI Mobile Client 1.0 diperkenalkan

2016

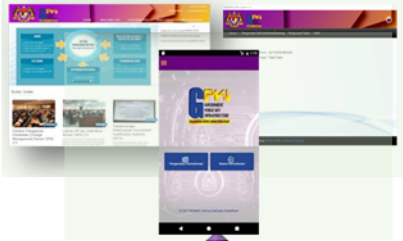
Sistem GPKI 1.1

MAMPU GPKI Agent 1.1 diperkenalkan bagi menggantikan SCAN GPKI Agent 1.0

2017

Sistem GPKI 2.0

Sistem GPKI 2.0, MAMPU GPKI Agent 2.0 dan GPKI Mobile Client 2.0 diperkenalkan bagi menggantikan Sistem GPKI 1.0



2020

Sistem GPKI 3.0

1. GPKI Agent 3.0 Release 1.0.0.0
2. Sistem GPKI Desk
3. Sistem GPKI eLearning
4. GPKI Mobile
5. Multi token:
   - Token ST3
   - Secure Token ST3 ACE
   - SafeNet eToken 5110
6. Multi Algo (RSA, ECC)

2021

Sistem GPKI 3.0

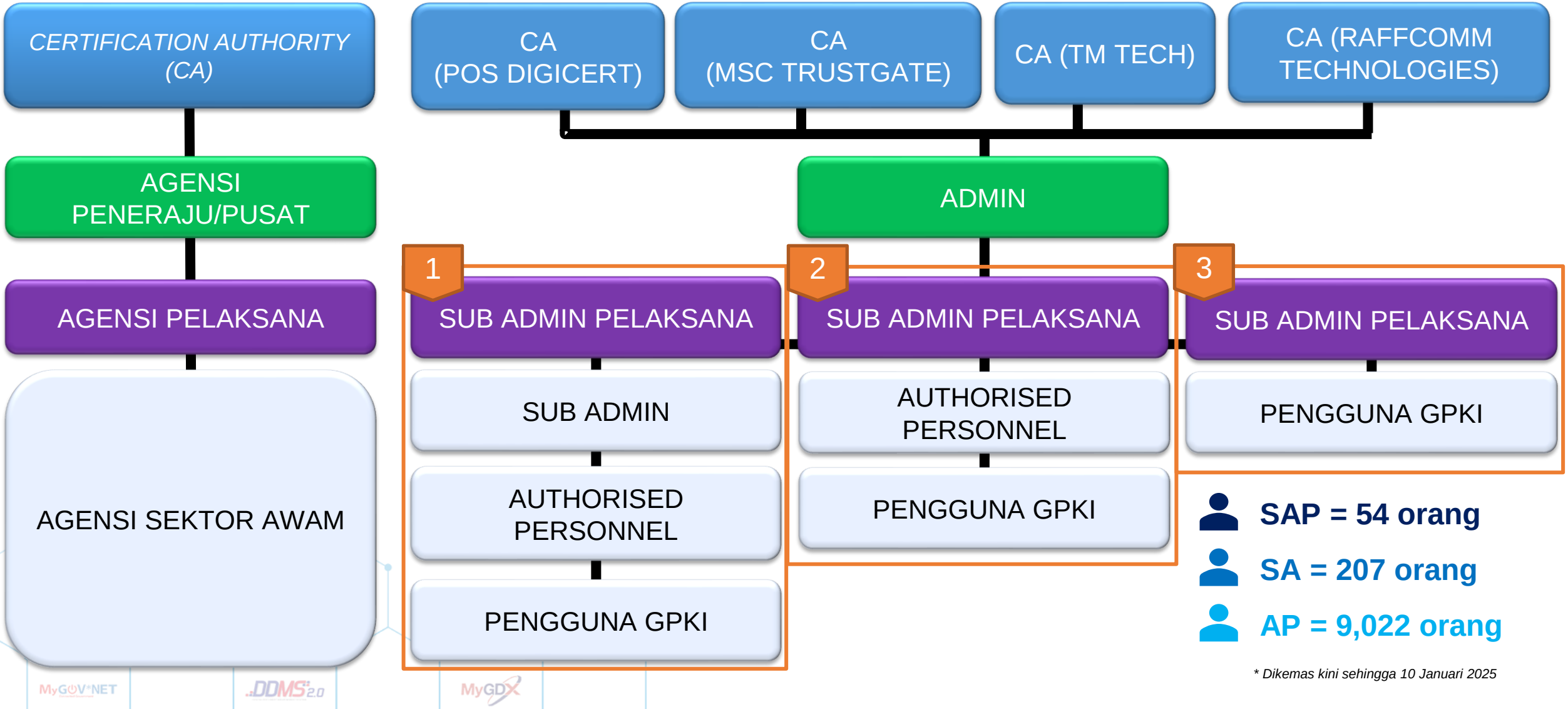
1. GPKI Agent 3.0 Release 1.0.0.1
2. Secure Token ST3 ACE mula digunakan
3. Pengenalan Roaming Certificate + OTP

2023

Sistem GPKI 3.0

GPKI Agent 3.0 Release 1.0.0.2 dan Release 2.0.0.0

MODEL OPERASI PENTADBIR MyGPKI



AGENSI PENERAJU/ PUSAT (JDN)

- Pemilik Perkhidmatan MyGPKI
- Bertangungjawab menyelaras dan memantau pelaksanaan MyGPKI secara keseluruhan serta memberi khidmat nasihat bagi penggunaan teknologi PKI untuk sistem ICT Kerajaan.
- Mentadbir Portal MyGPKI
- Mengurus permohonan Perkhidmatan MyGPKI.
- Melantik dan mengurus Pentadbir Sub Admin Pelaksana (SAP).

AGENSI PELAKSANA (SAP)

- Pemilik Sistem ICT Kerajaan
- Bertanggungjawab mengurus, menyelaras dan mentadbir sistem aplikasi yang menggunakan Perkhidmatan MyGPKI.
- Mengenal pasti dan mengurus Sub Admin (SA).
- Melantik dan mengurus *Authorised Personnel* (AP).

AGENSI SEKTOR AWAM (SA/AP)

- Agensi merangkumi Kementerian, Jabatan Persekutuan dan Negeri, Badan Berkanun Persekutuan dan Negeri yang menggunakan sistem ICT Kerajaan Persekutuan.
- Mengenal pasti *Authorised Personnel* (AP).
- Mengurus permohonan daripada pengguna di agensi.

PEKELILING KEMAJUAN PENTADBIRAN AWAM BIL. 3/2015: DASAR PERKHIDMATAN PRASARANA KUNCI AWAM KERAJAAN [*GOVERNMENT PUBLIC KEY INFRASTRUCTURE* (GPKI)]

Bil.	Kategori Agensi	Tanggungan Kos		
		Integrasi	Sijil Digital Pelayan	Sijil Digital Pengguna
1.	Kementerian	✓	✓	✓
2.	Jabatan			
	i. Agensi Pentadbiran Persekutuan	✓	✓	✓
	ii. Agensi Pentadbiran Negeri	✗	✗	✓
3.	Badan Berkanun			
	i. Badan Berkanun Persekutuan Tidak Diasingkan Saraan	* ✓	* ✓	* ✓
	ii. Badan Berkanun Persekutuan Diasingkan Saraan	✗	✗	✓
	iii. Badan Berkanun Negeri	✗	✗	✓
4.	Pihak Berkuasa Tempatan / Penguasa Tempatan			
	i. Pihak Berkuasa Tempatan / Penguasa Tempatan Persekutuan	✗	✗	✓
	ii. Pihak Berkuasa Tempatan / Penguasa Tempatan Negeri	✗	✗	✓

* Kelulusan tambahan oleh Mesyuarat Jawatankuasa Pemandu Projek MyGPKI Bil. 7 Tahun 2018

PENGGUNA PERKHIDMATAN MyGPKI

32 Sistem ICT Kerajaan

159,888 Pengguna Aktif

4 Certification Authority (CA)

9,283 Pentadbir

3,303 Subdomain (SSL/TLS)

MyeTaPP (TOKEN)	iGFMAS (TOKEN)	ePerolehan (TOKEN)	MyCukai (TOKEN)	SisMaSS (TOKEN)
eTanah (TOKEN)	eKadaster (TOKEN)	iSPKP (TOKEN)	I-LESEN (TOKEN)	
INSIST (TOKEN)	eROSA (TOKEN)	MHPS (ROAMING)	DDMS 2.0 (ROAMING)	
MyGDX (ROAMING)	SMPPV2 (ROAMING)	MyGST (ROAMING)	eVetting (ROAMING)	
SDB (ROAMING + OTP)	iPOST (SOFTCERT)	eKSS (SOFTCERT)	POWER Gen.2 (SOFTCERT)	eKehakiman (SOFTCERT)
PsMJM (ROAMING + OTP)	E-Syariah v3 (ROAMING + OTP)	J10 (ROAMING + OTP)	eIPTS v2 (ROAMING + OTP)	e-KERETA (ROAMING + OTP)
E-ACC (ROAMING + OTP)	EQMP (ROAMING + OTP)	HIMS (ROAMING + OTP)	OSC 3.0 Plus Online (ROAMING + OTP)	eJPKA (ROAMING + OTP)

*Dikemaskini sehingga 10 Januari 2025

1 Taklimat Awal

Taklimat Awal diberikan kepada Agensi yang berhasrat untuk mengintegrasikan Sistem ICT Agensi dengan Sistem MyGPKI.

2 Penilaian Risiko & Tahap Ketersediaan Sistem

Agensi perlu membuat penilaian risiko ke atas sistem yang berintegrasi dengan Sistem MyGPKI untuk menilai tahap keselamatan yang diperlukan dan memastikan sistem agensi telah bersedia untuk berintegrasi.

3 Permohonan Rasmi

Agensi perlu memastikan agar Pembangunan Sistem (terutamanya bagi modul yang melibatkan Tandatangan Digital) telah selesai melebihi 60% hingga 70% sebelum membuat dan mengemukakan permohonan rasmi bersama Laporan Penilaian Risiko kepada pihak JDN.

4 Kelulusan Permohonan

Permohonan Agensi akan melalui Mesyuarat Jawatankuasa Teknikal (JKT) dan Mesyuarat Jawatankuasa Pemandu (JKP) Projek Perkhidmatan MyGPKI untuk kelulusan.

5 Mesyuarat Kick-Off

Mengadakan Mesyuarat Kick-Off bagi membentangkan Pelan Perancangan Integrasi dan penyerahan API sebaik sahaja mendapat kelulusan JKP.

6 Pelaksanaan Integrasi

Agensi akan melaksanakan aktiviti integrasi sehingga selesai dan mengadakan pengujian bersama pihak JDN.

JADUAL PELAKSANAAN INTEGRASI

BIL.	AKTIVITI	TINDAKAN	TEMPOH (MING-GU)	CARTA PERBATUAN (MINGGU)																			
				Bulan 1				Bulan 2				Bulan 3				Bulan 4				Bulan 5				Bulan 6			
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1.	i. Pengumpulan Maklumat Integrasi	JDN/Agensi	1																				
	ii. Taklimat mengenai MyGPKI dan keperluan integrasi																						
	iii. Taklimat Sistem ICT dan keperluan sistem																						
2.	Penilaian Risiko	Agensi	2																				
3.	Permohonan dan Kelulusan Pelaksanaan Integrasi	JDN/Agensi	4																				
4.	Pelaksanaan Integrasi: i. Perbincangan Teknikal ii. Serahan API MyGPKI iii. Serahan Medium Pengujian iv. Integrasi API MyGPKI dengan Sistem ICT	JDN/Agensi	12																				
5.	Pengujian System Integration (SIT)	JDN/Agensi	1																				
6.	Pengujian Penerimaan Pengguna (UAT)	JDN/Agensi	2																				
7.	Pengujian Penerimaan Akhir (FAT)	JDN/Agensi	1																				
8.	Latihan Pentadbir MyGPKI	JDN/Agensi	1																				
9.	Sign-off	JDN/Agensi	1																				

KEMENTERIAN DIGITAL
JABATAN DIGITAL NEGARA

TERIMA KASIH

MyGPKI
GOVERNMENT PUBLIC KEY INFRASTRUCTURE

HOTLINE: 03-88008008

pmo.gpki@jdn.gov.my

mygpki_support@posdigicert.com.my