SANDI DATA

Layanan Kriptografi untuk Keamanan Data



v.7.1 2026

1. **UU 27 / 2022**
   Pelindungan Data Pribadi
   (keamanan data)
2. **PP 71 / 2019**
   PP PSTE
   (keamanan sistem elektronik)
3. **Perpres 95 / 2018**
   SPBE
   (keamanan data pemerintahan)
4. **Perpres 82 / 2022**
   Pelindungan IIV
   (keamanan data sektor IIV)
5. **Perpres 47 / 2023**
   SKSN & Manajemen Krisis Siber
   (kemandirian kriptografi nasional)
6. **Perpres 82 / 2023**
   Percepatan Transformasi Digital
   (keamanan data)
7. **Perpres 12 / 2025**
   RPJMN Nasional 2025-2029
   (indeks pemerintah digital)
8. **Peraturan BSSN 4 / 2021**
   Standar Keamanan SPBE
   (kriptografi untuk kerahasiaan data)
9. **Peraturan BSSN 11 / 2024**
   Penyelenggaraan Algoritma Kriptografi Indonesia
   (kriteria penggunaan algoritma kriptografi)

NIST CSF 2.0
Cyber Security Framework 2.0
(aspek proteksi data *at-rest*, *in-transit*, *in-use*)

SNI ISO/IEC 19790 : 2015
Keamanan Modul Kriptografi
(standar algoritma dan manajemen kunci kriptografi)

1 UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI

BAB V Pasal 16 Ayat 2 (e)

Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari **pengaksesan yang tidak sah**, **pengungkapan yang tidak sah**, **pengubahan yang tidak sah**, penyalahgunaan, **perusakan**, dan/atau **penghilangan** Data Pribadi;

BAB VI Pasal 35

Pengendali Data Pribadi **wajib melindungi dan memastikan keamanan** Data Pribadi yang diprosesnya, dengan melakukan:

a. penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan
b. Penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.

BAB VI Pasal 39 Ayat 1 dan 2

(1) Pengendali Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah.
(2) Pencegahan sebagaimana dimaksud pada ayat (1) dilakukan dengan menggunakan sistem keamanan terhadap Data Pribadi yang diproses dan/atau memproses Data Pribadi menggunakan sistem elektronik secara andal, aman, dan bertanggung jawab.

PENJELASAN Pasal 46 Ayat 1

Yang dimaksud dengan "kegagalan Pelindungan Data Pribadi" adalah kegagalan melindungi Data Pribadi *seseorang* dalam hal **kerahasiaan**, **integritas** dan **ketersediaan** Data Pribadi, termasuk pelanggaran keamanan, baik yang disengaja maupun tidak disengaja, yang mengarah pada **perusakan**, **kehilangan**, **perubahan**, **pengungkapan**, atau **akses yang tidak sah** terhadap Data Pribadi yang **dikirim**, **disimpan**, atau **diproses**.

Subjek Data Pribadi

- orang perseorangan yang pemilik data pribadi

Pengendali Data Pribadi

- setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atas bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi

Prosesor Data Pribadi

- setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama pengendali data pribadi

- Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau penghilangan Data Pribadi
- Pelindungan terhadap Data Pribadi melalui mekanisme enkripsi dan/atau penyamaran data

3

PERATURAN PRESIDEN REPUBLIK INDONESIA
NOMOR 95 TAHUN 2018
TENTANG SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)

BAB I
Pasal 2 Ayat 8

Keamanan sebagaimana dimaksud pada ayat (1) huruf g merupakan **kerahasiaan**, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya yang mendukung SPBE.

ayat (1) huruf g, SPBE dilaksanakan dengan prinsip efektivitas, keterpaduan, kesinambungan, efisiensi, akuntabilitas, interoperabilitas dan **keamanan**

BAB II
Pasal 40 Ayat 1

Keamanan SPBE mencakup penjaminan **kerahasiaan**, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait **data** dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.

BAB II
Pasal 40 Ayat 2

Penjaminan kerahasiaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penetapan **klasifikasi keamanan**, **pembatasan akses**, dan **pengendalian keamanan** lainnya.

PERATURAN MENPAN RB
NOMOR 8 TAHUN 2026
TENTANG EVALUASI KINERJA PEMERINTAHAN DIGITAL

Indikator 11. Tingkat Kematangan Penerapan Kriptografi untuk Keamanan Data

Aspek	Indikator	Bobot	Kuesioner
4	11	3%	Tingkat Kematangan Penerapan Kriptografi untuk Keamanan Data
Deskripsi Indikator:			Kemampuan/kapabilitas dari Instansi Pemerintah dalam melakukan proteksi keamanan kerahasiaan data melalui penerapan fungsi kriptografi yang bersesuaian dengan standar keamanan modul kriptografi dan penerapan kriptografi secara nasional, baik untuk posisi data ketika disimpan (*at-rest*), digunakan (*in-use*), sampai pada data dipertukarkan (*in-transit*), dalam penyelenggaraan Layanan Digital Pemerintah.
Instansi Pembina			Badan Sandi dan Siber Negara.
Peran Fungsi di Instansi Pemerintah			1. Fungsi Teknologi, Informasi, dan Komunikasi. 2. Fungsi Pengelola Layanan Digital.
Kurang (Merintis/*Initiate*) 1,00 s.d. ≤ 1,50			Kriteria: Dalam tahap penyiapan penerapan teknologi kriptografi untuk keamanan data, sesuai dengan peraturan perundang-undangan.
Cukup (Membangun/*Emerging*) > 1,50 s.d. ≤ 2,50			Kriteria: Sudah menerapkan teknologi kriptografi sesuai dengan peraturan perundang-undangan pada sebagian Layanan Digital Pemerintah.
Baik (Berkembang/*Developing*) > 2,50 s.d. ≤ 3,50			Kriteria: Teknologi kriptografi telah diterapkan pada sebagian Layanan Digital Pemerintah di 2 (dua) siklus data.
Sangat Baik (Melembaga/*Embedded*) > 3,50 s.d. ≤ 4,00			Kriteria: 1. Teknologi kriptografi telah diterapkan pada seluruh Layanan Digital Pemerintah prioritas dan/atau Layanan Digital Pemerintah tematik di 2 (dua) siklus data. 2. Telah dilakukan evaluasi pada penerapan teknologi kriptografi.
Memuaskan (Unggul/*Leading*) > 4,00 s.d. 5,00			Kriteria: 1. Penyelenggaraan Persandian telah terorganisir dan terkelola dengan baik secara menyeluruh dan berkelanjutan berdasarkan IKASANDI pada Area Kematangan Persandian. 2. Telah melakukan tindak lanjut hasil evaluasi pada penerapan teknologi kriptografi.

Services	Algoritma Kriptografi (*algorithm*)	Penggunaan (*use case*)	Keterangan
Encrypt / Seal	AES-256 RSA-3072	Enkripsi data *at-rest* & *in-transit*	- Proteksi terhadap keamanan data digital - Kepatuhan terhadap UU 27/2022 (Sektor Pemerintah ataupun Non-Pemerintah) - Kepatuhan terhadap Indeks Pemdigi (Sektor Pemerintah) - Kepatuhan terhadap penyelenggaraan kriptografi (Peraturan BSSN Nomor 11/2024) - Keamanan terhadap ancaman kebocoran data (*data-breach*)
Decrypt / Unseal	AES-256 RSA-3072	Dekripsi data *at-rest* & *in-transit*	
Tokenize / Detokenize	AES-256	Enkripsi/Dekripsi data *in-use* (*data masking*)	
HMAC	SHA-256	Kebutuhan parameter keutuhan (*integrity*)	- Mendukung keamanan dalam menjaga keutuhan data (sebagai contoh: untuk penggunaan keamanan kredensial *login*) - Kepatuhan terhadap penyelenggaraan kriptografi (Peraturan BSSN Nomor 11/2024)
TOTP	SHA-256	Otentikasi *Multi-Factor*	- Dapat dimanfaatkan sebagai parameter lain (*others factor*) dalam proses otentikasi (*authentication*) dan otorisasi (*authorization*) akses - Kepatuhan terhadap penyelenggaraan kriptografi (Peraturan BSSN Nomor 11/2024)
Random Generator (RNG)	DRBG-HMAC	Kebutuhan parameter acak (*random number*)	- Pemanfaatan dalam penggunaan parameter acak (OTP, session, uid, dan lainnya) yang dibangkitkan secara kaidah kriptografis - Kepatuhan terhadap penyelenggaraan kriptografi (Peraturan BSSN Nomor 11/2024)

7

PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 4 TAHUN 2021
TENTANG PEDOMAN MANAJEMEN KEAMANAN INFORMASI DAN STANDAR TEKNIS DAN PROSEDUR KEAMANAN SPBE

BAB III Pasal 21

Terpenuhinya aspek **keaslian** sebagaimana dimaksud dalam Pasal 19 huruf b dilakukan dengan prosedur:

a. menyediakan mekanisme verifikasi;
b. menyediakan mekanisme validasi;
c. menerapkan sistem *hash function*.

BAB III Pasal 22

Terpenuhinya aspek **keutuhan** sebagaimana dimaksud dalam Pasal 19 huruf c dilakukan dengan prosedur:

a. menerapkan pendeteksian modifikasi;
b. menerapkan tanda tangan elektronik tersertifikasi.

BAB III Pasal 23

Terpenuhinya aspek **kenirsangkalan** sebagaimana dimaksud dalam Pasal 19 huruf d dilakukan dengan prosedur:

a. menerapkan tanda tangan elektronik tersertifikasi;
b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

BAB III Pasal 24

Terpenuhinya aspek **ketersediaan** sebagaimana dimaksud dalam Pasal 19 huruf e dilakukan dengan prosedur:

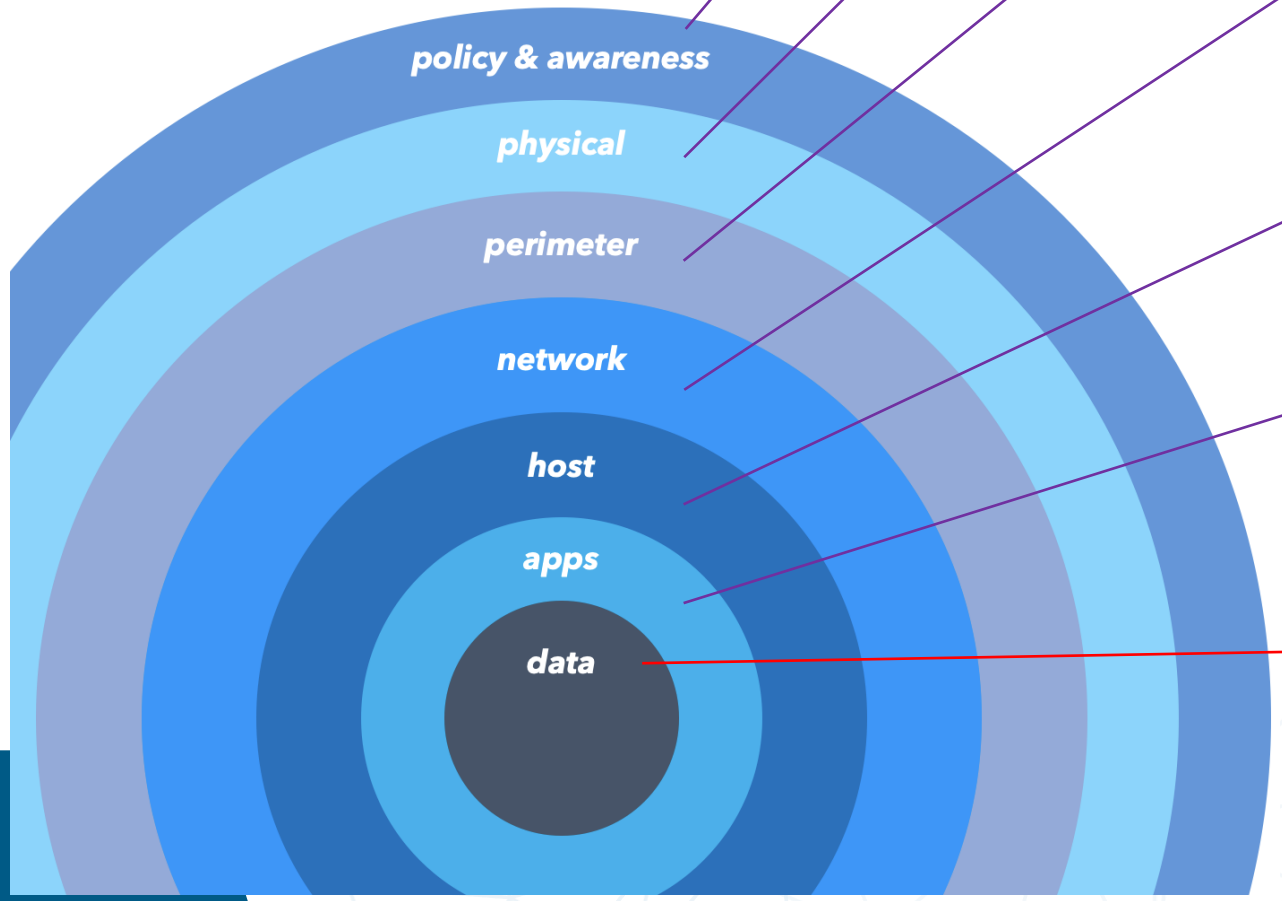
a. menerapkan sistem pencadangan secara berkala;
b. membuat perancanaan untuk menjamin data dan informasi dapat selalu diakses;
c. menerapkan sistem pemulihan.

Layer of Defense *(security controls)*



threats

attacks



- **Security Policies** (board commitment; privacy, audit, password, remote access, account policy, DRP, BCP, etc)
- **Training and Awareness**

- **Physical** (lock, access control, logging, alarm, fingerprint, biometric, electricity, CCTV, etc)
- **Environment** (HVAC, hot/cold aisle, fire control, etc)

- **IAM** (ACL, authentication, authorization, PIV, CAC, etc)
- **Accounts** (AD, OTP, credentials, RADIUS, Kerberos, accounting, etc)

- **Tech** (firewall, IDS/IPS, load balancer, VPN, sec.gateway, etc)
- **Design** (segmentation, DMZ, subnet, VLAN, NAT, etc)
- **Protocols** (SSH, HTTPS, SSL/TLS, SNMP, 802.11, WAP, etc)

- **Server** (logging, AV, hardening, update, backup, EDR, etc)
- **Virtual** (logging, snapshot, network conf., HCI, etc)
- **Mobile** (lock, FDE, permissions, apps & content mgmt., etc)

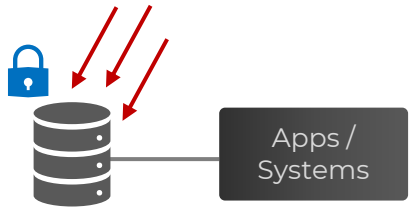
- **Development** (SDLC, dev-ops, versioning, secure coding, code testing/analysis, obfuscate, etc)
- **Operational** (auth., session, access control, input validation, error handling, logging, API security, etc)

- **At-Rest**
  (FDE, file encryption, DB encryption, IRM, DLP, etc)
- **In-Transit**
  (email encryption, MFT, security protocols, etc)
- **In-Use**
  (IAM, RBAC, IRM, etc)

Keamanan Pelindungan Kerahasiaan Data

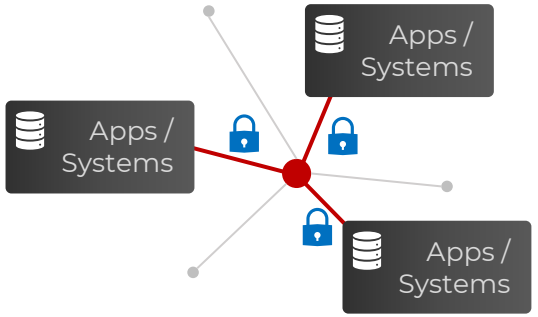
Data Disimpan (at-rest)

*mendukung keamanan data elektronik ketika data disimpan, sebagai bentuk **proteksi terhadap ancaman kebocoran data yang menyasar langsung pada penyimpanan data (database)***



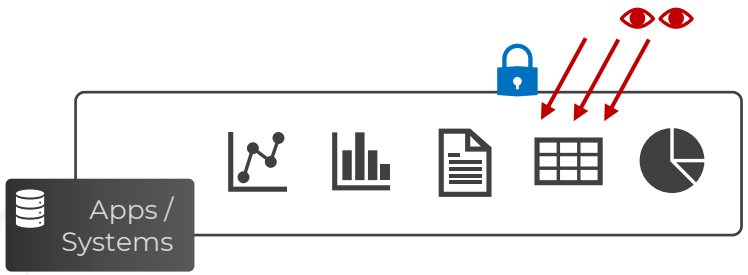
Data Dikirimkan (in-transit)

*mendukung keamanan data elektronik ketika data dikirimkan, didistribusikan ataupun dipertukarkan antara satu aplikasi dengan aplikasi lainnya, sebagai bentuk **proteksi terhadap ancaman pencurian data ketika data berada pada jalur yang tidak aman ketika dikirimkan***



Data Digunakan (in-use)

*mendukung keamanan data elektronik ketika data digunakan dan dimanfaatkan dalam interaksi aplikasi dengan penggunanya, sebagai bentuk **proteksi terhadap tersingkapnya data dan juga pembatasan akses agar data ditampilkan hanya kepada pengguna yang sah***



> ***Mendukung perwujudan keamanan penyelenggaraan Sistem Elektronik (SE) melalui penerapan fungsi kriptografi untuk pelindungan dan proteksi kerahasiaan data***

SANDI DATA

Keamanan Pertukaran Data (in-transit)

Keamanan data in-transit

Urgensi terhadap terapan keamanan data yang dikirim-terimakan dari salah satu pihak kepada pihak lainnya, untuk melindungi data akan adanya ancaman penyadapan, pencurian dan kebocoran ketika data dikirimkan.

Kemudahan pertukaran kunci

Bagaimana kunci enkripsi dapat dipertukarkan dengan aman namun tetap memberikan kemudahan dalam penggunaannya.

Enkripsi data ukuran besar

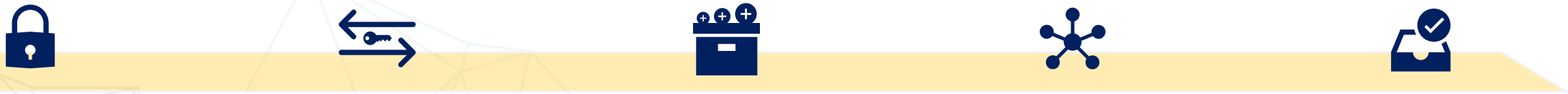
Objek data yang diamankan, bukan hanya data dalam jumlah yang banyak, namun juga ukurannya yang besar. Selain itu, berbagai macam bentuk format data juga menjadi konsideran dalam bagaimana terapan enkripsi terhadap objek data.

Multi-branch

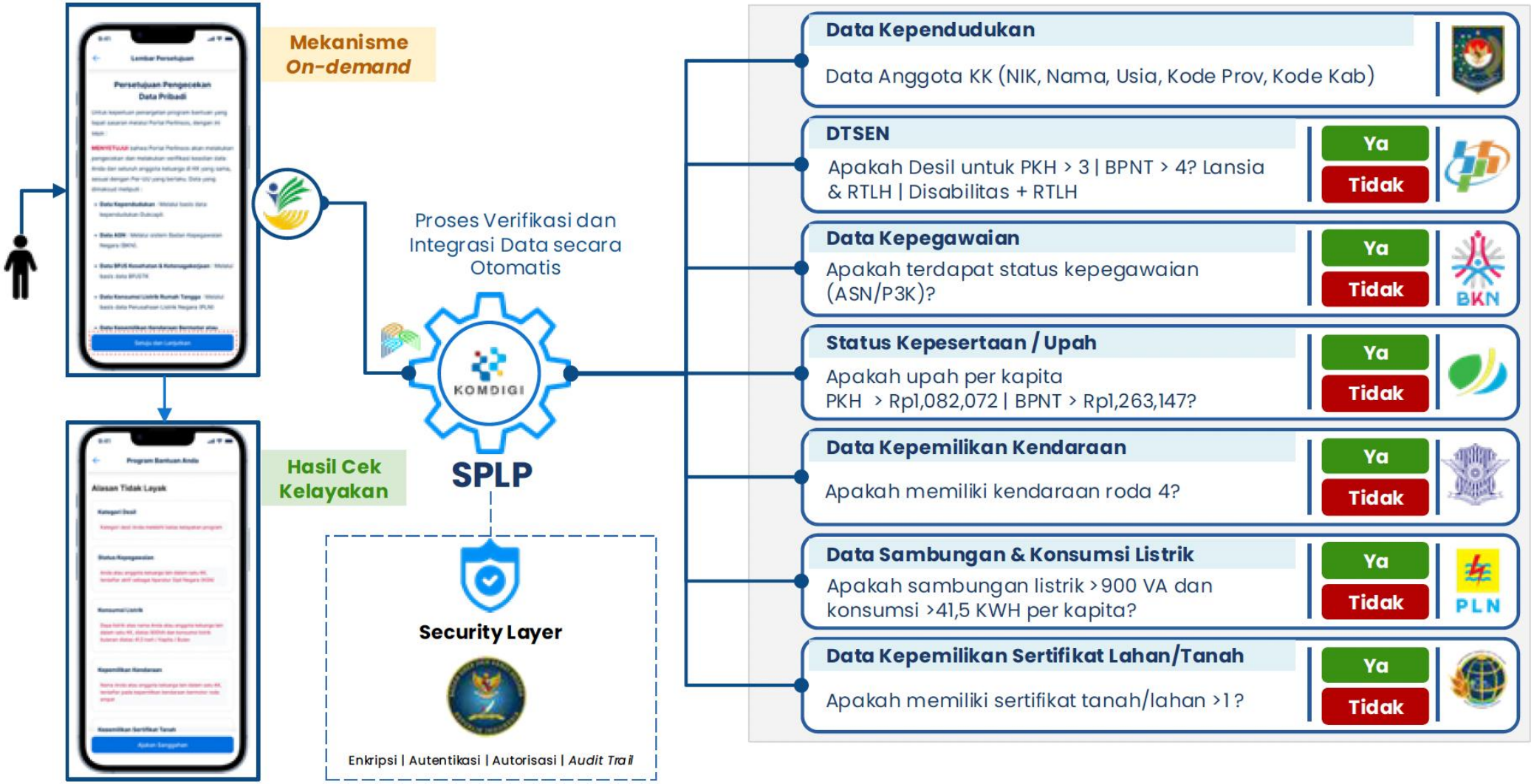
Kondisi dimana ekosistem pertukaran data melibatkan banyak pihak yang berbeda lingkungan infrastruktur dan sistem IT-nya, namun tetap membutuhkan pertukaran data yang aman dan nyaman.

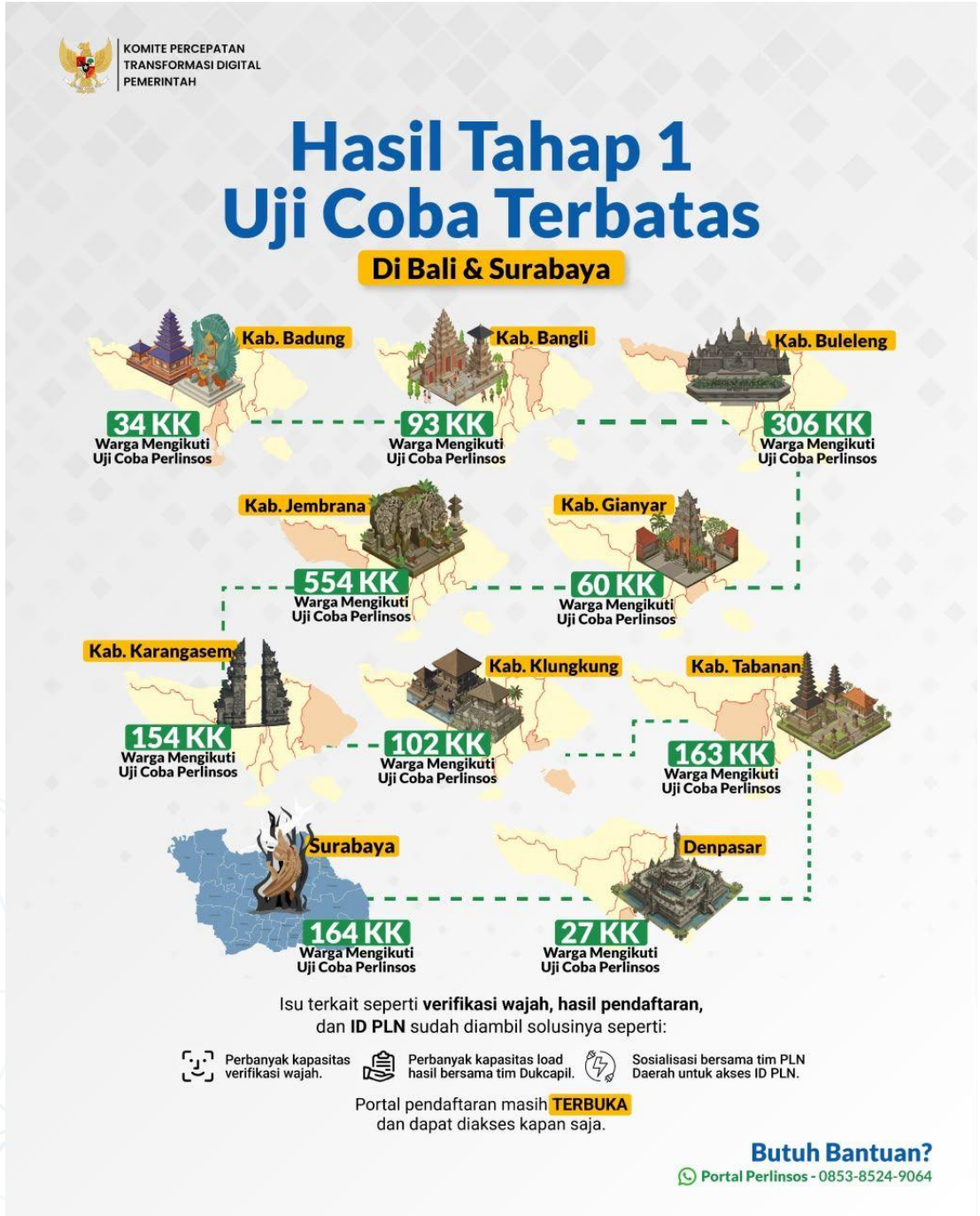
Kemudahan Penggunaan

Perilaku masing-masing pengelola dan pengguna data yang berbeda-beda, terkhusus pada tingkat kesadaran keamanannya, membutuhkan solusi yang mudah untuk dipahami dan digunakan.



Keamanan Pertukaran Data *(best-practice)*




KOMITE PERCEPATAN
TRANSFORMASI DIGITAL
PEMERINTAH
Hasil Tahap 1
Uji Coba Terbatas
Di Bali & Surabaya
Kab. Badung
34 KK
Warga Mengikuti
Uji Coba Perlinsos
Kab. Bangli
93 KK
Warga Mengikuti
Uji Coba Perlinsos
Kab. Buleleng
306 KK
Warga Mengikuti
Uji Coba Perlinsos
Kab. Jembrana
554 KK
Warga Mengikuti
Uji Coba Perlinsos
Kab. Gianyar
60 KK
Warga Mengikuti
Uji Coba Perlinsos
Kab. Karangasem
154 KK
Warga Mengikuti
Uji Coba Perlinsos
Kab. Klungkung
102 KK
Warga Mengikuti
Uji Coba Perlinsos
Kab. Tabanan
163 KK
Warga Mengikuti
Uji Coba Perlinsos
Surabaya
164 KK
Warga Mengikuti
Uji Coba Perlinsos
Denpasar
27 KK
Warga Mengikuti
Uji Coba Perlinsos
Isu terkait seperti verifikasi wajah, hasil pendaftaran,
dan ID PLN sudah diambil solusinya seperti:
Perbanyak kapasitas verifikasi wajah.
Perbanyak kapasitas load hasil bersama tim Dukcapil.
Sosialisasi bersama tim PLN Daerah untuk akses ID PLN.
Portal pendaftaran masih TERBUKA
dan dapat diakses kapan saja.
Butuh Bantuan?
Portal Perlinsos - 0853-8524-9064

“Kechilafan satu orang sahaja tjukup sudah menjebabkan keruntuhan negara”

Mayjen TNI Dr. Roebiono Kertopati (1914-1984)
Bapak Persandian Republik Indonesia

contact us

TERIMA KASIH