INOVASI IDENTITAS DIGITAL

Pemanfaatan e-KTP Online

Platform verifikasi identitas berbasis chip e-KTP melalui ekosistem mobile dan web — tanpa fotokopi, tanpa card reader fisik.



Agenda

1. **Tentang Kami** — profil & kapabilitas
2. **Latar Belakang** — masalah & urgensi
3. **Teknologi & Solusi** — *arsitektur sistem SAM Online*
4. **Cara Integrasi** — REST API untuk sistem client
5. **Keamanan & Kepatuhan** — *regulasi & compliance*
6. **Kasus Penggunaan** — *use case per sektor*
7. **Prasyarat & Onboarding** — *langkah mulai*



TENTANG KAMI

Identitas Digital Indonesia

Perusahaan teknologi yang fokus di infrastruktur identitas digital berbasis standar Dukcapil. Tim kami terdiri dari insinyur berpengalaman di domain smart card, kriptografi, dan integrasi pemerintah.

Kapabilitas Inti

- Implementasi protokol ISO/IEC 14443 & 7816
- Integrasi SAM (Secure Access Module) & HSM
- Kepatuhan Permendagri 72/2022 & UU PDP
- Platform multi-channel: mobile, web, kiosk
- Pengalaman integrasi dengan sistem Dukcapil



Keunggulan: Satu-satunya platform yang mengimplementasikan arsitektur SAM Online — SAM terpusat di server, bukan fisik di setiap loket — sesuai Permendagri 76/2020 Lampiran hal. 53.

Latar Belakang & Masalah

Risiko Fotokopi KTP Fisik

Proses fotokopi e-KTP masih digunakan secara konvensional. Metode ini rentan terhadap:

- Kebocoran data pribadi (pelanggaran UU PDP No. 27/2022)
- Pemalsuan identitas visual
- Data tidak terverifikasi ke sumber — Dukcapil
- Tidak dapat mendeteksi KTP palsu secara otomatis



Solusi Integrasi Digital

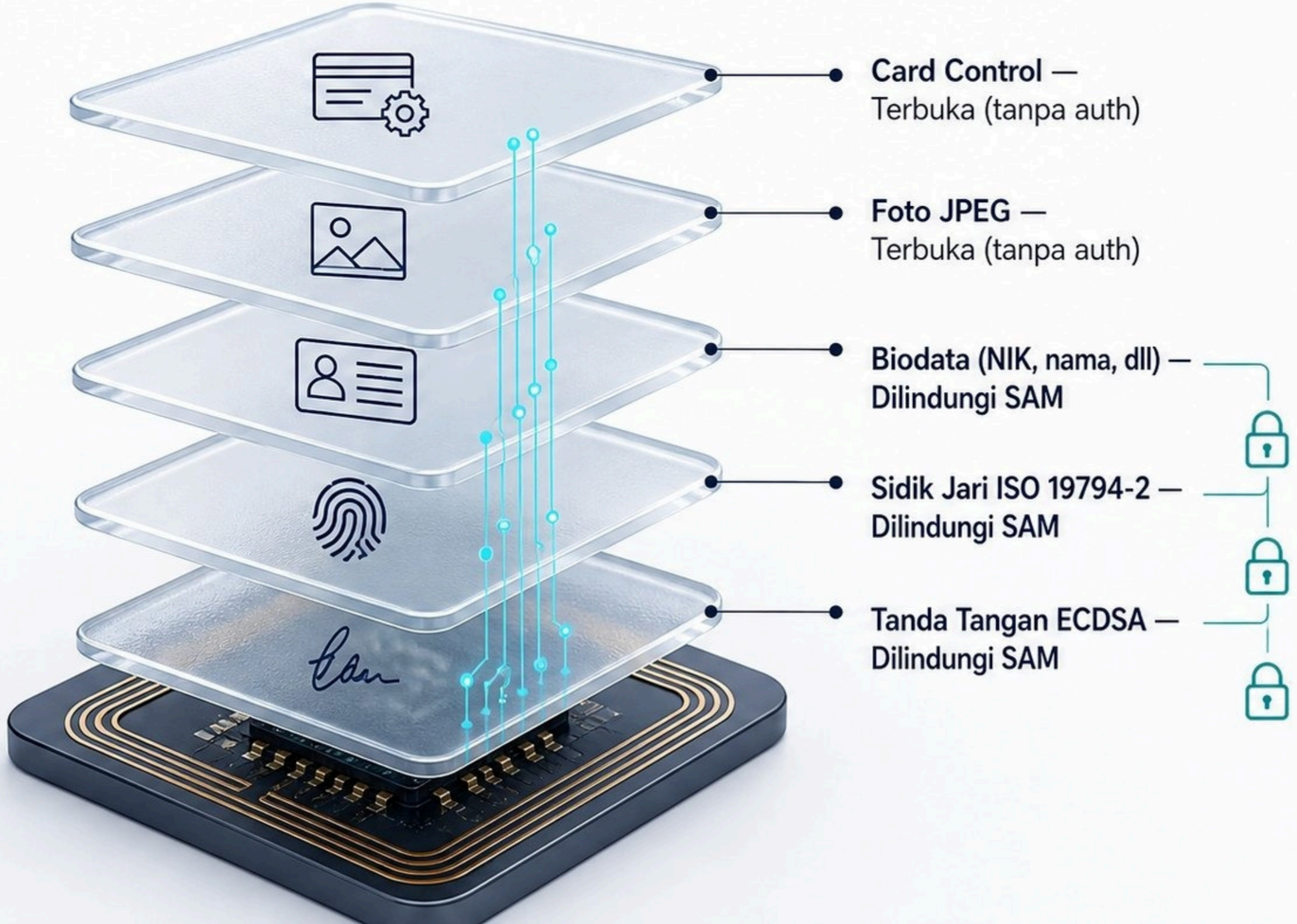
Memanfaatkan chip kriptografi internal e-KTP secara langsung melalui pembaca online:

- Menghilangkan proses fotokopi sepenuhnya
- Data biodata dibaca langsung dari chip, bukan OCR
- Mutual authentication — kartu memverifikasi sistem, sistem memverifikasi kartu
- Mencegah pemalsuan secara kriptografis



Teknologi Chip e-KTP

e-KTP Indonesia dirancang sebagai Smart Card berbasis contactless yang mendukung protokol internasional **ISO/IEC 14443-4** (frekuensi 13,56 MHz). Di dalam kartu tertanam chip aman (**NXP SmartMX2** atau **Infineon SLE 97**) yang menyimpan:



Card Control — Terbuka (tanpa auth)

Foto JPEG — Terbuka (tanpa auth)

Biodata (NIK, nama, dll) — **Dilindungi SAM**

Sidik Jari ISO 19794-2 — **Dilindungi SAM**

Tanda Tangan ECDSA — **Dilindungi SAM**

Tier Akses Data

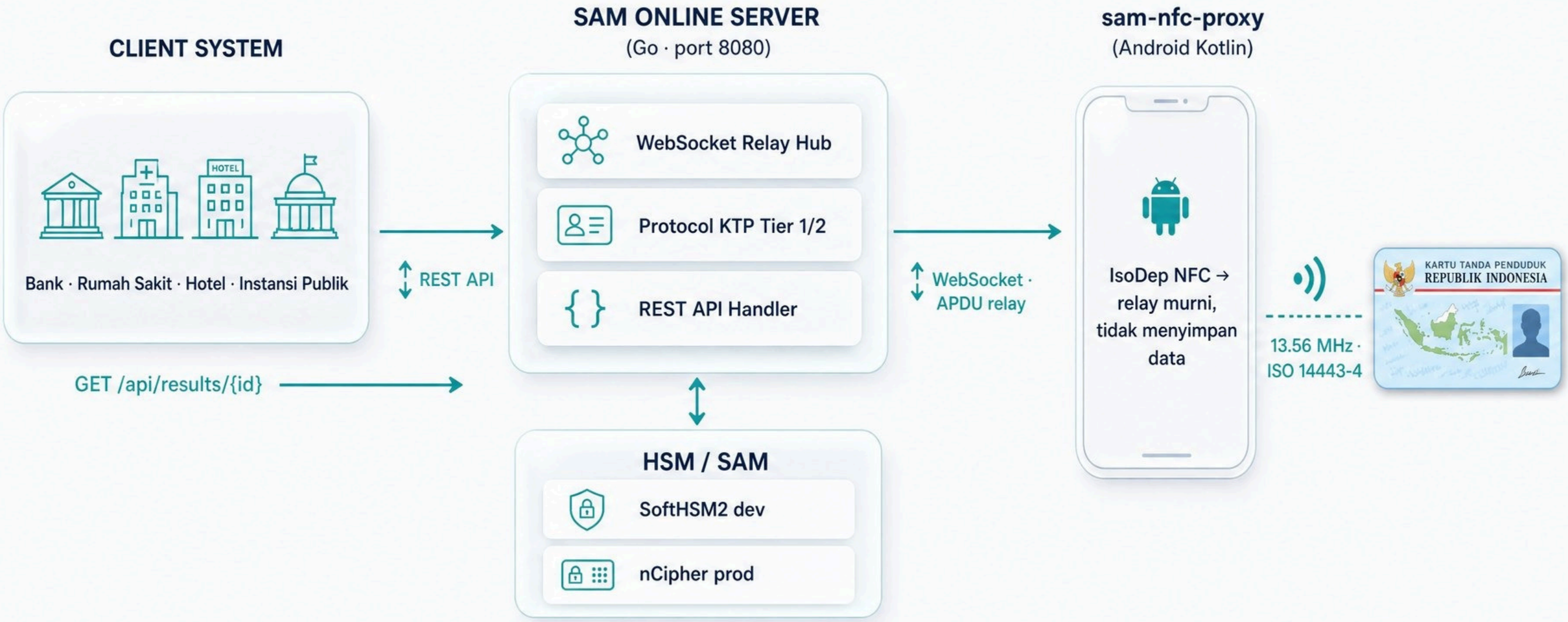
Tier 1 — Tanpa SAM (PoC)

Foto + Card Control — cukup untuk membuktikan kartu asli & mendapatkan UID unik.

Tier 2 — Dengan SAM/Kode Kunci

Biodata lengkap + biometrik. Memerlukan Kode Kunci dari Dukcapil (Permendagri 72/2022 Lampiran I.A.2.b.12).

Arsitektur Sistem SAM Online



Keunggulan: SAM terpusat di server — 1 SAM melayani N klien bersamaan. Tidak perlu card reader fisik di setiap lokasi.

Solusi Pembaca Kartu



MOBILE READER

Mobile Reader

Smartphone Android dengan NFC internal sebagai proxy pembacaan. Petugas lapangan dapat verifikasi di mana pun tanpa perangkat tambahan.

IDEAL UNTUK:

KYC lapangan, bantuan sosial door-to-door, verifikasi pemilih



WEB-BASED READER

Web-Based Reader

PC/laptop dengan external smart card reader via WebUSB atau middleware ringan. Langsung terintegrasi browser.

IDEAL UNTUK:

Loket RS, kantor perbankan, instansi perpajakan



KIOSK / SELF-SERVICE

Kiosk / Self-Service

Terminal mandiri dengan reader bawaan. Client melakukan verifikasi sendiri tanpa petugas.

IDEAL UNTUK:

Hotel check-in, antrian RS, loket BPJS, anjungan layanan mandiri

Alur Verifikasi e-KTP

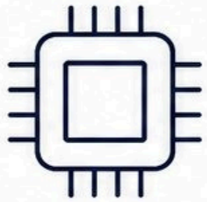
1 Tempel e-KTP

Tempelkan kartu ke sensor NFC smartphone atau desktop card reader



2 Ekstraksi Chip

Sistem baca UID + data terenkripsi via modul SAM (≤ 15 detik)



3 Relay ke Server

APDU dikirim ke SAM Online Server via WebSocket terenkripsi



Hasil Instan

Status keaslian + data muncul di aplikasi dalam < 10 detik





Tier 1 (Tanpa Kode Kunci)

Baca foto & Card Control saja. Cukup untuk:

- Membuktikan kartu fisik asli
- Mendapatkan UID unik per kartu
- Photo matching sederhana



Tier 2 (Dengan Kode Kunci Dukcapil)

Baca biodata lengkap + biometrik. Untuk:

- NIK, nama, alamat, tanggal lahir
- Sidik jari (ISO 19794-2 FMR)
- Verifikasi tanda tangan digital ECDSA

Cara Integrasi API

Client mengintegrasikan sistem mereka via REST API sederhana — tidak perlu pahami detail protokol NFC/SAM.

Contoh Response — GET /api/results/{session_id}

```
{
  "session_id": "sess-abc123",
  "uid": "04a2b3c4d5e6f7",
  "cc_hex": "001d2f8a...",
  "photo_size": 2280,
  "read_at": "2026-06-24T09:15:32Z"
}
```

Ambil foto — GET /api/results/{id}/photo

```
Content-Type: image/jpeg
← JPEG binary (foto dari chip e-KTP)
```

Alur Integrasi Client

1. **Deploy** — sam-online-server di infrastruktur client (on-premise atau cloud)
2. **Install** — sam-nfc-proxy di smartphone petugas
3. **Connect** — proxy ke server via URL WebSocket
4. **Tap** — e-KTP → server otomatis baca & simpan hasil
5. **Fetch** — hasil via REST API ke sistem core client

SDK & dokumentasi tersedia



API



CLOUD INTEGRATION



SYSTEM INTEGRATION

Keamanan & Kepatuhan Regulasi

Regulasi yang Dipenuhi

REGULASI	CAKUPAN
Permendagri 72/2022	Standar hardware/software KTP-el, kode kunci sebagai pengganti SAM fisik
Permendagri 76/2020	Arsitektur Card Reader & SAM Online
UU PDP No. 27/2022	Data kependudukan tidak disimpan di device pembaca
SNI ISO/IEC 14443	Protokol komunikasi *contactless*
SNI ISO/IEC 19794-2	Standar data sidik jari

Lapisan Keamanan



Enkripsi End-to-End

Chip ↔ SAM Server: 3-Key Triple-DES (3KTDEA) + ECDSA secp256r1



Mutual Authentication

Kartu memverifikasi sistem, sistem memverifikasi kartu — tidak bisa dipalsukan dari satu arah



Zero Persistent Storage

Data kependudukan tidak pernah disimpan di device proxy atau server. *Transient only.*



HSM-Backed Keys

Kunci kriptografi tidak pernah keluar dari HSM (SoftHSM2 dev / nCipher nShield prod)

Efisiensi Operasional

<10 dtk
durasi verifikasi
(dari tap hingga hasil)

0
fotokopi diperlukan

100%
akurasi data
(langsung dari chip)

N:1
client per SAM
(SAM terpusat di server)

Perbandingan proses manual vs SAM Online:

	MANUAL (FOTOKOPI)	SAM ONLINE
Durasi per nasabah	~5–10 menit	< 10 detik
Risiko data bocor	Tinggi (kertas beredar)	Nihil (transient)
Deteksi KTP palsu	Tidak bisa	Otomatis (kriptografis)
Typo input	Sering	Tidak ada (baca chip)

Keuntungan Implementasi

Keamanan Maksimal

Menghindari manipulasi data identitas visual. Sistem membaca langsung informasi terenkripsi dari chip fisik e-KTP. KTP palsu terdeteksi secara kriptografis.

Efisiensi Operasional

Eliminasi input manual yang lambat dan rawan typo. Antrean loket berkurang drastis. Satu operator dapat melayani lebih banyak nasabah per jam.

Compliance-Ready

Dibangun di atas regulasi Permendagri dan UU PDP. Tidak ada data kependudukan tersimpan di luar HSM. Audit trail tersedia.

Multi-Channel

Mobile, web, kiosk — satu platform, satu API, satu integrasi.

Paperless

Menghilangkan seluruh rantai fotokopi KTP di operasional layanan.

Mudah Integrasi

REST API standar. Tidak perlu ganti sistem core yang sudah ada.

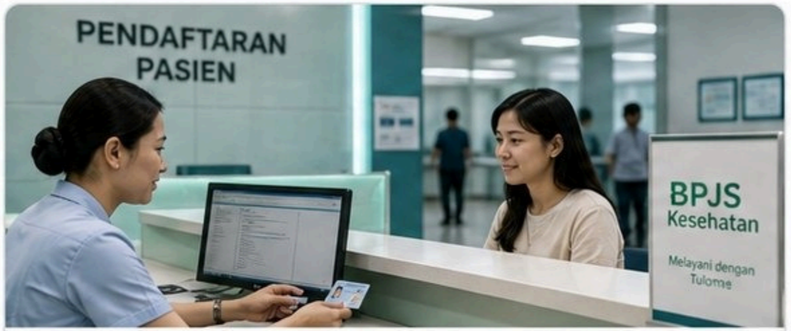
Kasus Penggunaan Utama



PERBANKAN & FINTECH

Pembukaan rekening mandiri (E-KYC), persetujuan kredit

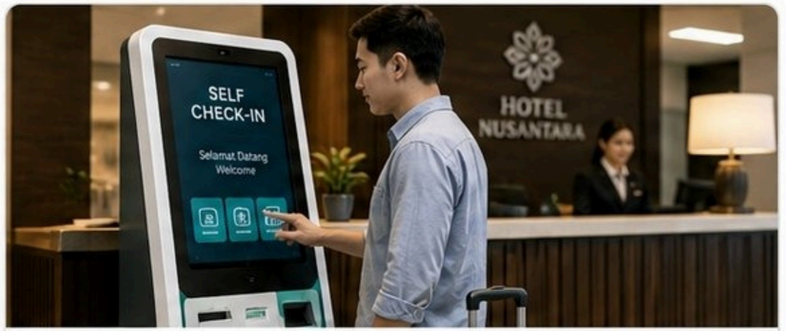
Akurasi data 100%, tekan risiko fraud identitas, comply POJK.



LAYANAN KESEHATAN

Registrasi pasien baru di RS, verifikasi kepesertaan BPJS

Hilangkan antrean loket, cegah penyalahgunaan kartu orang lain.



PERHOTELAN

Check-in mandiri (Self Check-in Kiosk)

Proses reservasi instan tanpa fotokopi KTP fisik.



ADMINISTRASI PUBLIK

Verifikasi penerima bantuan sosial, PTSP, layanan kependudukan

Penyaluran tepat sasaran, cegah data ganda/ ghost recipient.



LOGISTIK & EKSPEDISI

Verifikasi identitas pengirim/penerima paket

Kurangi risiko penipuan pengiriman.



PENDIDIKAN

Registrasi ujian, verifikasi peserta PPDB/SNBT

Cegah joki ujian, data peserta akurat.

Integrasi Mobile App



Portable NFC Scanning

Dengan memanfaatkan NFC internal pada ponsel pintar, petugas di lapangan dapat melakukan proses KYC di mana pun tanpa membutuhkan device besar.

Cocok untuk:

- Pendaftaran nasabah baru bank nirkantor
- Verifikasi pemilih di TPS
- Pembagian bantuan sosial door-to-door
- Ekspedisi logistik — verifikasi penerima

Persyaratan:

- Android 7+ dengan NFC IsoDep (ISO 14443-4)
- Koneksi ke SAM Online Server (WiFi/4G)

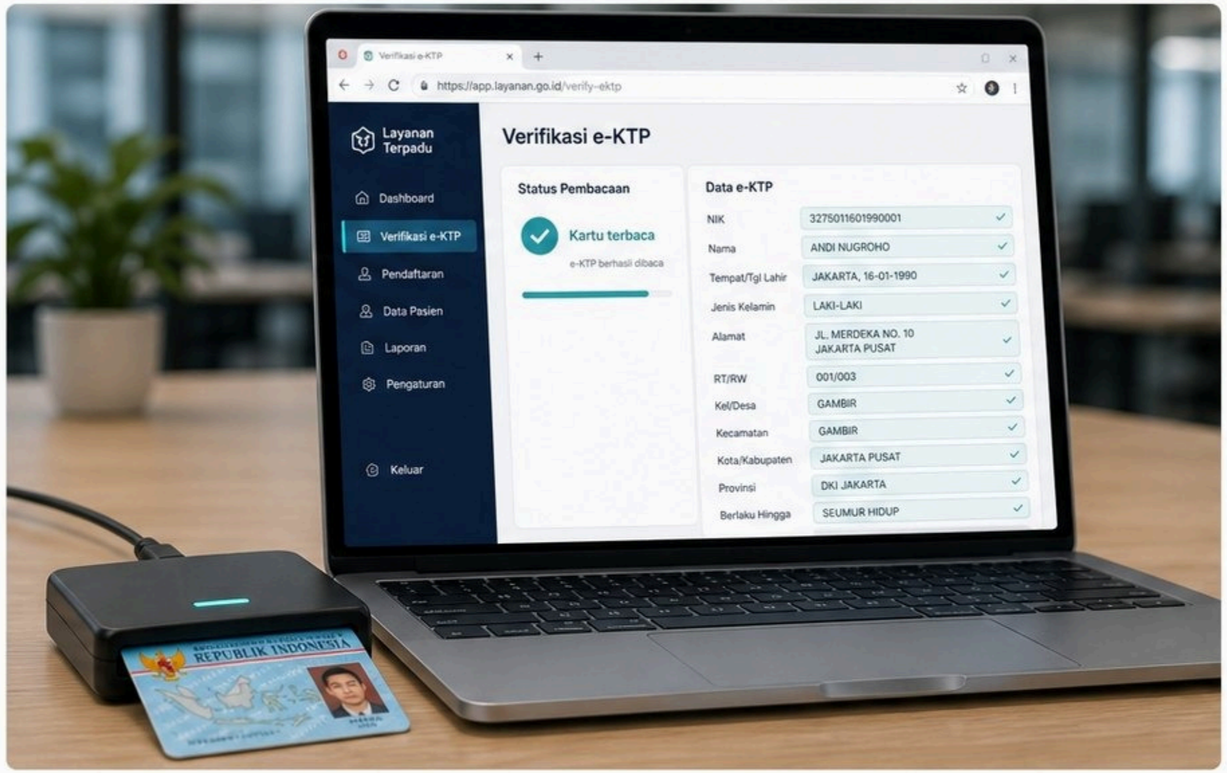
Alur di Aplikasi

1. Buka SAM NFC Proxy
2. Masukkan URL server → Connect
3. Status: "Connected — tap KTP-el"
4. Tempel kartu ke bagian belakang HP
5. Foto + data tampil otomatis di layar
6. Sistem core client menerima data via REST API

Aplikasi bersifat relay murni — tidak menyimpan, tidak mendekripsi data. Semua kriptografi di server.

Integrasi Aplikasi Web & Kiosk

Web-Based (Loket & Perkantoran)

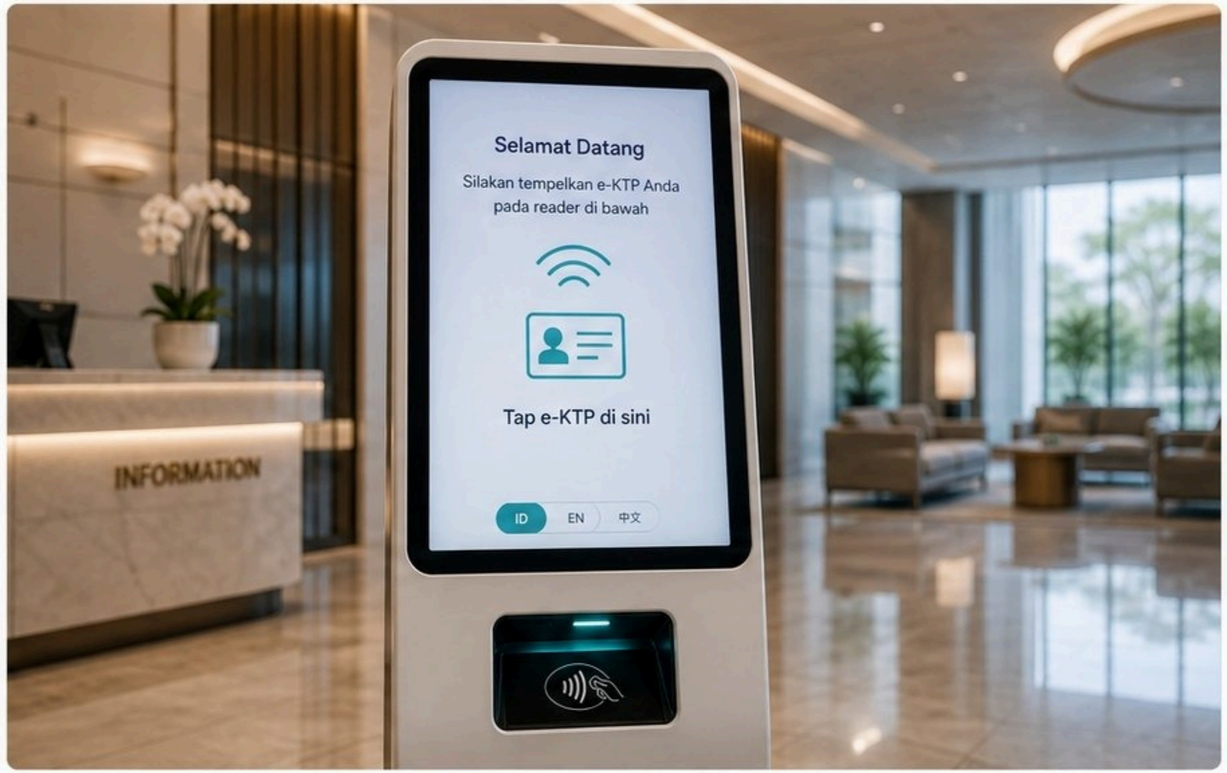


Aplikasi berbasis web mendeteksi smart card reader eksternal via WebUSB API atau middleware ringan. Tidak perlu install aplikasi besar — cukup browser modern.

Cocok untuk:

- Loket pendaftaran rumah sakit
- Kantor perbankan cabang
- Instansi perpajakan (DJP, BAPENDA)
- Meja resepsionis gedung perkantoran

Kiosk / Self-Service Terminal



Terminal mandiri dengan reader built-in. Nasabah/pasien/tamu melakukan verifikasi sendiri.

Skenario tipikal:

- Ambil nomor antrean dengan tap e-KTP
- Hotel check-in: tap → kamar otomatis di-assign
- BPJS: verifikasi kepesertaan mandiri di poli

Keuntungan vs kiosk konvensional:

- Tidak ada keyboard → tidak ada risiko skimming
- Data akurat dari chip, bukan input manual

Prasyarat Teknis & Regulasi

TECHNICAL REQUIREMENTS

Prasyarat Teknis

KOMPONEN	KEBUTUHAN
Server	Linux x86-64, min 2 core / 4 GB RAM
HSM (dev)	SoftHSM2 — gratis, open source
HSM (prod)	nCipher nShield Connect atau setara
Android	Min Android 7 (API 26), NFC IsoDep
Jaringan	HTTPS/WSS antara proxy ↔ server
Kode Kunci	Dari Dukcapil — diperlukan Tier 2



REGULATORY REQUIREMENTS

Prasyarat Regulasi

Berdasarkan Permendagri 72/2022 Lampiran I.A.2.b.12 — lembaga pengguna wajib terdaftar di Dukcapil sebelum mendapat akses Kode Kunci.

- Terdaftar sebagai Pengguna KTP-el resmi
- MoU / PKS dengan Ditjen Dukcapil
- Kode Kunci diterbitkan per lembaga pengguna
- Infrastruktur keamanan memenuhi standar Permendagri 76/2020



Tahapan Onboarding



PoC / Pilot

Deploy server + proxy, test baca foto & Card Control. Tidak perlu Kode Kunci Dukcapil.

Registrasi Dukcapil

Ajukan permohonan Kode Kunci ke Ditjen Dukcapil (kami bantu dokumen).

Integrasi Sistem Core

Hubungkan REST API ke aplikasi existing (core banking, HIS, HRIS, dll).

UAT & Go-Live

Pengujian end-to-end + pelatihan operator + sign-off keamanan.

Produksi

HSM fisik + Kode Kunci aktif. Akses biodata + biometrik penuh.

Next Steps



STEP 01

Mulai PoC (2 minggu)

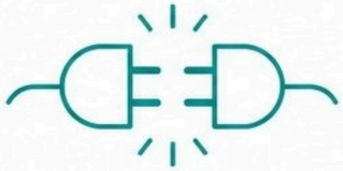
Deploy SAM Online Server di lingkungan staging client. Test end-to-end: tap KTP-el → foto muncul di sistem client. Tidak perlu Kode Kunci Dukcapil untuk tahap ini.



STEP 02

Siapkan Dokumen Regulasi

Kami bantu menyusun dokumen permohonan Kode Kunci ke Dukcapil: profil lembaga, use case, arsitektur keamanan.



STEP 03

Technical Deep-Dive

Sesi teknis dengan tim IT client untuk mapping integrasi REST API ke sistem core yang sudah ada (core banking, HIS, HRIS, dll).



Target: PoC berjalan dalam 2 minggu sejak kick-off. Tidak perlu hardware tambahan untuk tahap awal — cukup smartphone Android NFC + server cloud.

SESI DISKUSI

Masa Depan Identitas Digital

Bangun infrastruktur verifikasi identitas Indonesia yang terintegrasi, aman, dan tanpa celah kebocoran data.

