RINGKASAN DISKUSI TEKNIS

# Integrasi eKYC untuk Pendaftaran Calon Nasabah di Website Company Profile

Ringkasan pembahasan mengenai alur kerja, keamanan, dan kepatuhan regulasi untuk penerapan verifikasi identitas digital (eKYC) sebagai tahap awal sebelum tim CS melakukan pembukaan rekening reksadana.

---

Website terkait: www.trimegah-am.com

Disusun untuk: Manajemen & Tim Compliance Trimegah

Disiapkan oleh: Tim Database & Infrastruktur

Tanggal: September 2026

# 1 Apa yang Sedang Dibangun?

Gambaran umum alur pendaftaran calon nasabah baru

Calon nasabah mengisi form pendaftaran di website company profile, lalu melakukan verifikasi identitas digital (eKYC) menggunakan pihak ketiga seperti **Privy** atau **Vida**. Setelah dinyatakan terverifikasi, tim **Customer Service (CS)** yang akan melanjutkan proses pembukaan rekening secara manual ke sistem inti perusahaan.

### Konteks Pengelolaan Website

- **Pengembangan (development):** dilakukan oleh vendor eksternal (Whitespace)
- **Pengelolaan harian:** konten oleh tim Marcomm, sisi teknis oleh tim IT internal
- **Lokasi server (hosting):** on-premise di infrastruktur Trimegah, bukan cloud publik

## Alur Proses Sederhana

**1 Isi Form** — Calon nasabah mengisi data di website

→

**2 Verifikasi eKYC** — Scan KTP + foto selfie (liveness)

→

**3 Provider Proses** — Cek kecocokan wajah & data KTP

→

**4 Hasil Disimpan** — Status verified/rejected tersimpan

→

**5 CS Tindak Lanjut** — CS review & buka rekening manual

## Mengapa Prosesnya Dibuat Bertahap (Tidak Otomatis Penuh)?

### Keamanan data lebih terjaga

- Data calon nasabah masuk ke "ruang tunggu" (staging) dulu
- Tidak langsung menyentuh sistem inti perusahaan (SIAR)

### Ada lapisan pemeriksaan manusia

- CS tetap mengecek kelengkapan & kewajaran data
- Mengurangi risiko data palsu lolos begitu saja

### Mudah dilacak & diaudit

- Setiap tahap punya jejak waktu & status
- Memudahkan pelaporan ke regulator bila diperlukan

## 2 Bagaimana Data Dijaga Keamanannya?

Pemisahan area jaringan agar sistem inti tetap aman

Saat ini, website hanya terhubung ke database secara terbatas dan tanpa akses internet. Menambahkan eKYC berarti website perlu berkomunikasi dengan pihak luar (vendor) dan menyimpan data — sehingga area jaringan perlu dipisah agar risiko tidak menjalar ke sistem utama perusahaan.

### Pemisahan Area (Zona) Jaringan

**ZONA INTERNET (Publik, di luar kendali perusahaan)**

- **Calon nasabah**
  Mengisi form dari browser/HP
- **Vendor eKYC (Privy/Vida)**
  Memproses verifikasi wajah & KTP

**ZONA TERBUKA TERBATAS (Website & Data Sementara)**

- **Website & Backend**
  Menerima form, memanggil vendor, menerima hasil
- **Database "Ruang Tunggu"**
  Menyimpan data sementara, akses sangat dibatasi

**ZONA INTI PERUSAHAAN (Terlindungi, tidak terhubung internet)**

- **Tool Internal CS**
  CS mengecek data yang sudah terverifikasi
- **Sistem Inti (SIAR/IMS)**
  Data resmi nasabah & transaksi — tidak pernah diakses langsung dari internet

### Empat Risiko Utama yang Perlu Diantisipasi

**Jalur masuk data palsu**

Sistem penerima hasil verifikasi dari vendor harus dipastikan hanya menerima data asli dari vendor resmi, bukan dari pihak lain yang berpura-pura.

**Akses langsung ke sistem inti**

Website tidak boleh punya "kunci" langsung ke database utama perusahaan — hanya boleh menulis ke database sementara yang terpisah.

**Penyalahgunaan formulir**

Tanpa perlindungan, formulir bisa disalahgunakan (spam, percobaan berulang) yang berdampak pada biaya karena setiap verifikasi eKYC dikenakan biaya per-transaksi.

**Data sensitif tersimpan tanpa perlindungan**

Data seperti nomor KTP dan rekening bank perlu disamarkan/dienkripsi, bukan disimpan apa adanya.

## Catatan Tambahan Terkait Pengelolaan Website

### Keuntungan hosting on-premise

- Data tidak keluar dari infrastruktur milik Trimegah sendiri, memudahkan kontrol akses
- Tim IT internal punya visibilitas penuh terhadap lalu lintas jaringan dari/ke server

### Hal yang perlu diperjelas dengan vendor (Whitespace)

- Batasan akses vendor setelah fitur eKYC selesai dikembangkan — apakah masih ada akses jarak jauh ke server produksi
- Siapa yang bertanggung jawab atas patch keamanan & pembaruan kode setelah go-live, mengingat pengelolaan harian ada di tim IT internal
- Kredensial API vendor eKYC (Privy/Vida) sebaiknya dikelola tim IT internal, bukan tertinggal di tangan vendor pengembang

## 3 Kaitan dengan Regulasi di Indonesia

Karena melibatkan data pribadi calon nasabah keuangan

UU PDP | Komdigi | OJK

> **Catatan penting:** Ringkasan ini adalah gambaran awal untuk bahan diskusi, bukan nasihat hukum resmi. Tim Legal/Compliance perlu memverifikasi lebih lanjut sebelum implementasi.

| Regulasi | Apa yang Diatur | Relevansi untuk Proyek Ini |
|---|---|---|
| **UU PDP (Pelindungan Data Pribadi)** | Wajib ada persetujuan (consent) jelas dari pemilik data sebelum data pribadi (termasuk data wajah/biometrik) diproses. | Form pendaftaran wajib mencantumkan persetujuan eksplisit, bukan sekadar centang standar. |
| **Komdigi (dulu Kominfo)** | Mengawasi pendaftaran sistem elektronik yang mengelola data pribadi dalam skala tertentu. | Perlu dicek apakah sistem pendaftaran ini perlu didaftarkan sebagai Penyelenggara Sistem Elektronik (PSE). |
| **OJK** | Mewajibkan proses verifikasi identitas nasabah (CDD) termasuk pengecekan daftar terlarang (anti pencucian uang). | Perlu dipastikan vendor eKYC yang dipakai sudah diakui untuk sektor jasa keuangan, dan proses CDD lengkap (tidak hanya cocokkan wajah-KTP). |

### Empat Langkah yang Disarankan untuk Kepatuhan

- [ ] **Verifikasi status vendor**
  Pastikan Privy/Vida memiliki sertifikasi resmi untuk digunakan sektor jasa keuangan, dan didokumentasikan.
- [ ] **Perjanjian kerja sama data (DPA)**
  Buat kesepakatan tertulis dengan vendor: data apa yang mereka simpan, berapa lama, dan siapa yang boleh mengakses.
- [ ] **Persetujuan (consent) yang jelas di form**
  Sebaiknya direview oleh tim compliance sebelum form dipublikasikan.
- [ ] **Kebijakan penyimpanan & penghapusan data**
  Tentukan berapa lama data calon nasabah yang batal/ditolak akan disimpan sebelum dihapus.

# 4 Pilihan Pendekatan: Video Call vs eKYC Pihak Ketiga

Perbandingan dua opsi verifikasi identitas calon nasabah

> Selain menggunakan eKYC pihak ketiga, sempat dibahas alternatif membangun fitur video call sendiri di website untuk verifikasi manual oleh CS. Berikut perbandingannya.

| Aspek | Bangun Video Call Sendiri | Pakai eKYC Pihak Ketiga |
|---|---|---|
| **Kerumitan pembangunan** | Sangat tinggi — perlu teknologi baru yang belum dikuasai tim | Rendah–menengah — sesuai dengan keahlian tim yang ada |
| **Waktu ke penerapan** | Berbulan-bulan | Hitungan minggu |
| **Kebutuhan sumber daya CS** | CS harus siap sedia real-time untuk setiap panggilan | Proses otomatis, tidak tergantung jadwal CS |
| **Deteksi kecurangan (fraud)** | Manual, bergantung ketelitian CS | Otomatis dan terus diperbarui vendor |
| **Biaya** | Investasi awal besar (infrastruktur video) | Biaya kecil di awal, berjalan per transaksi |
| **Tanggung jawab keamanan** | Ditanggung penuh oleh perusahaan | Berbagi dengan vendor yang sudah berpengalaman |

## Kelebihan & Kekurangan Tiap Opsi

### Video Call Embedded — Kelebihan

- Kontrol penuh atas proses & tampilan, tanpa ketergantungan vendor luar
- Tidak ada biaya per-transaksi ke pihak ketiga (setelah infrastruktur jadi)
- Interaksi langsung dengan CS bisa membangun kepercayaan calon nasabah
- Data tidak perlu dikirim ke server pihak luar

### Video Call Embedded — Kekurangan

- Waktu pengembangan lama, butuh keahlian teknis baru (infrastruktur video real-time)
- CS harus tersedia secara langsung (real-time), membatasi skala & jam layanan
- Deteksi kecurangan (foto/video palsu) bergantung ketelitian manusia, bukan otomatis
- Perusahaan menanggung penuh risiko keamanan & penyimpanan rekaman video
- Biaya perawatan sistem berkelanjutan (bug, kompatibilitas perangkat/browser)

### eKYC Pihak Ketiga — Kelebihan

- Lebih cepat diterapkan, hitungan minggu bukan bulan
- Deteksi kecurangan (liveness, deepfake) otomatis & terus diperbarui vendor
- Tidak bergantung ketersediaan CS — proses berjalan kapan saja
- Umumnya sudah tersertifikasi untuk kebutuhan sektor jasa keuangan
- Sesuai dengan keahlian tim teknis yang sudah ada (integrasi API & database)

### eKYC Pihak Ketiga — Kekurangan

- Biaya berjalan terus per-transaksi verifikasi, bukan biaya satu kali
- Bergantung pada layanan & keandalan pihak ketiga (ketersediaan, perubahan API)
- Data calon nasabah sempat diproses di sistem vendor luar
- Perlu perjanjian kerja sama data (DPA) & verifikasi sertifikasi vendor secara berkala

**✓ Rekomendasi**

Menggunakan **eKYC pihak ketiga (Privy/Vida)** lebih sesuai untuk kondisi saat ini — lebih cepat diterapkan, sejalan dengan keahlian tim, dan lebih andal dalam mendeteksi kecurangan. Video call dapat dipertimbangkan sebagai pelengkap di kemudian hari, misalnya untuk kasus khusus yang memerlukan pemeriksaan tambahan, bukan sebagai metode utama.