PEMERINTAH PROVINSI
KALIMANTAN UTARA

DOKUMEN

SPESIFIKASI KEBUTUHAN PERANGKAT LUNAK

(SOFTWARE REQUIREMENT SPECIFICATIONS)

USULAN PENGEMBANGAN APLIKASI SATU PORTAL LAYANAN DAERAH

TAHUN ANGGARAN 2025

RIWAYAT DOKUMEN

RIWAYAT REVISI DOKUMEN			
TANGGAL	VERSI DOKUMEN	DESKRIPSI REVISI	INSTANSI
13/11/2024	1.0	Versi Awal	DKISP
29/07/2025	1.1	Versi Perbaikan	DKISP

DAFTAR ISI

1. PENDAHULUAN

1.1. Dasar Hukum

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

Peraturan Gubernur Kalimantan Utara Nomor 51 Tahun 2019 Tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik

Peraturan Gubernur Kalimantan Utara Nomor 3 Tahun 2023 Perubahan atas Peraturan Gubernur Kalimantan Utara Nomor 51 Tahun 2019 Tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik

Peta Rencana dan Arsitektur SPBE Kalimantan Utara

Surat Direktur Layanan Aplikasi Informatika Kementerian Komunikasi dan Informatika Nomor : B-851/DJAI.3/AI.01.01/07/2024 tentang Himbauan Pencegahan Dan Mitigasi Ransomware Pada Layanan Publik

1.2. Proses Bisnis dan Layanan

Nama Proses Bisnis :

- KLTR-DAB 09.03.01.04
- Pengelolaan e-government
- RAB.09 PEMERINTAHAN UMUM
- RAB.09.03 INFORMASI
- RAB.09.03.01 PENGELOLAAN SUMBER DAYA DAN PERANGKAT INFORMATIKA
- Dinas Komunikasi, Informatika, Statistik dan Persandian

- KLTR-DAB 09.03.01.04.02
- Penatalaksanaan dan Pengawasan E-government
- RAB.09 PEMERINTAHAN UMUM
- RAB.09.03 INFORMASI
- RAB.09.03.01 PENGELOLAAN SUMBER DAYA DAN PERANGKAT INFORMATIKA
- Dinas Komunikasi, Informatika, Statistik dan Persandian

Nama Layanan : Layanan SSO Satu Portal Daerah
Nama Data : Data Identitas dan Akses Pengguna SSO

1.3. Analisa Permasalahan

- Menindaklanjuti arahan Presiden pada SPBE Summit 2024 khususnya terkait integrasi aplikasi pada satu Portal Daerah

serta menindaklanjuti surat Direktur Layanan Aplikasi Informatika Kementerian Komunikasi dan Informatika Nomor : B-851/DJAI.3/AI.01.01/07/2024 tentang himbauan pencegahan dan mitigasi ransomware pada layanan publik, Pemerintah Daerah diminta melakukan update dan patching perangkat lunak yang digunakan pada layanan publik. Portal kaltaraprov saat ini menggunakan PHP versi 7 yang telah berakhir security supportnya pada 30 November 2020 maka perlu dilakukan peremajaan/pengembangan portal kaltaraprov

- Kondisi saat ini, Perangkat Daerah di lingkup Pemerintah Provinsi Kalimantan Utara menyediakan berbagai layanan publik yang tersebar di berbagai aplikasi atau website. Hal ini dapat menyulitkan masyarakat dalam mencari informasi dan mengakses layanan. Oleh karena itu, diperlukan satu portal terpadu yang dapat menjadi pusat layanan digital untuk masyarakat, memudahkan akses terhadap semua layanan daerah yang dibutuhkan.
- Saat ini, berbagai layanan publik yang disediakan oleh pemerintah daerah tersebar di berbagai aplikasi atau website terpisah. Hal ini menyebabkan fragmentasi yang mempersulit masyarakat untuk menemukan layanan yang mereka butuhkan secara cepat dan efisien. Beberapa permasalahan spesifik yang dihadapi adalah:
    a) Kebingungan Akses: Warga bingung mengenai aplikasi atau situs mana yang harus digunakan untuk setiap layanan, seperti layanan kesehatan, pendidikan, perizinan, atau kependudukan.
    b) Pengulangan Proses Pendaftaran: Masyarakat sering kali harus mendaftar ulang dan membuat akun berbeda untuk setiap aplikasi layanan yang terpisah.
    c) Perbedaan Standar Antar Layanan: Setiap layanan bisa memiliki antarmuka, standar pengisian data, dan proses yang berbeda, menyulitkan pengguna dalam menavigasi dan memanfaatkan layanan dengan optimal.
- Tidak semua masyarakat memiliki akses yang baik terhadap layanan digital ini karena tidak tersedianya portal terpadu:
    a) Pengguna Kurang Teknologi: Banyak masyarakat yang belum terbiasa dengan teknologi atau bahkan kesulitan menggunakan aplikasi layanan yang berbeda-beda.

b) Keterbatasan Infrastruktur: Pada daerah tertentu yang akses internetnya terbatas, layanan yang membutuhkan aplikasi terpisah dan besar bisa mempersulit pengguna dengan jaringan lemah atau kuota terbatas.

1.4. Maksud dan Tujuan

1.4.1 Maksud

Pengembangan Portal Satu Layanan Daerah dimaksudkan sebagai inisiatif strategis Pemerintah Provinsi Kalimantan Utara dalam menjawab tantangan integrasi layanan publik yang selama ini tersebar di berbagai sistem dan platform. Portal ini bertujuan menjadi titik sentral (one-stop service) untuk seluruh layanan digital pemerintah daerah, selaras dengan arahan Presiden RI dalam SPBE Summit 2024 dan kebijakan pencegahan risiko keamanan siber dari Kementerian Komunikasi dan Informatika. Portal ini juga dimaksudkan untuk mendorong transformasi digital pemerintahan yang terintegrasi, efisien, dan berorientasi pada kemudahan akses publik, serta mendukung standar keamanan layanan publik yang modern dan berkelanjutan.

1.4.2 Tujuan

a. Mewujudkan Layanan Digital Terpadu dan Terpusat
   Menyatukan seluruh aplikasi dan website layanan publik yang tersebar ke dalam satu portal daerah, sehingga masyarakat cukup mengakses satu platform untuk berbagai kebutuhan layanan.
b. Meningkatkan Aksesibilitas dan Efisiensi Layanan
   Mengurangi kebingungan masyarakat dalam mengakses layanan dan mempercepat proses pelayanan melalui pendekatan single entry point.
c. Mengimplementasikan Sistem Autentikasi Tunggal (Single Sign-On)
   Menghadirkan kemudahan bagi pengguna dengan cukup satu akun terverifikasi untuk mengakses seluruh layanan, serta mencegah duplikasi pendaftaran dan mempercepat onboarding layanan baru.
d. Memperkuat Keamanan dan Keandalan Layanan Digital
   Mengatasi risiko kerentanan sistem akibat perangkat lunak usang seperti PHP 7, melalui peremajaan infrastruktur dan penguatan sistem autentikasi yang dilengkapi fitur audit dan pengelolaan akses.
e. Meningkatkan Transparansi dan Akuntabilitas Pelayanan Publik
   Menyediakan sistem pencatatan aktivitas pengguna (audit trail), pengelolaan akses berbasis token, dan verifikasi identitas digital untuk mendukung tata kelola layanan yang transparan dan bertanggung jawab.
f. Menjangkau Seluruh Lapisan Masyarakat Secara Inklusif

Memastikan layanan dapat diakses dengan mudah oleh masyarakat umum, termasuk yang belum terbiasa dengan teknologi, dengan menghadirkan antarmuka yang ramah pengguna dan ringan untuk akses di wilayah dengan keterbatasan infrastruktur.

g. Mendukung Implementasi SPBE dan Kebijakan Nasional Digitalisasi Pemerintahan

Menjadi bagian dari upaya nasional dalam mewujudkan pemerintahan digital yang efisien dan terintegrasi sebagaimana diamanatkan dalam Perpres No. 95 Tahun 2018 tentang SPBE dan berbagai regulasi teknis lainnya

1.5. Analisa Manfaat

A. Peningkatan Aksesibilitas dan Efisiensi Layanan

Layanan Single Sign-On (SSO) sebagai Identity Provider dalam Portal Layanan Daerah memberikan kemudahan akses dan efisiensi dalam proses autentikasi pengguna untuk berbagai aplikasi layanan publik daerah. Manfaat utama yang diharapkan antara lain:

- Kemudahan Akses Satu Identitas (Single Identity Access):
  Pengguna hanya perlu memiliki satu akun terpusat untuk dapat mengakses berbagai layanan pemerintah daerah yang terintegrasi, tanpa perlu membuat akun baru untuk setiap aplikasi.
- Pengurangan Duplikasi Registrasi:
  Dengan menggunakan SSO, proses pendaftaran pengguna baru cukup dilakukan satu kali. Ini mengurangi duplikasi data akun dan mempercepat onboarding pengguna pada layanan baru.
- Efisiensi Autentikasi Lintas Aplikasi:
- Pengguna yang telah login di satu layanan, dapat langsung mengakses layanan lain yang terhubung tanpa perlu login ulang (single sign-on session), sehingga meningkatkan efisiensi penggunaan layanan.

B. Meningkatkan Transparansi dan Akuntabilitas Pelayanan Publik

Meskipun fungsi utama SSO adalah sebagai identity provider, sistem ini tetap berkontribusi dalam mendukung transparansi dan akuntabilitas melalui fitur pendukung keamanan dan pelacakan aktivitas. Manfaat yang diharapkan antara lain:

- Pencatatan Aktivitas Otentikasi (Audit Trail):

Sistem mencatat setiap aktivitas login, logout, dan perubahan data pengguna untuk keperluan audit dan keamanan. Hal ini mendukung akuntabilitas penggunaan sistem layanan publik.

- Verifikasi Identitas yang Lebih Terstandar:
  Proses verifikasi akun pengguna (email dan nomor HP) secara sistematis memastikan bahwa identitas digital yang digunakan telah diverifikasi, membantu menjaga keabsahan akses terhadap layanan.
- Integrasi Layanan yang Aman dan Terkendali:
- Melalui pengelolaan token dan izin akses per aplikasi (client ID/secret), hanya aplikasi yang resmi dan terdaftar yang dapat menggunakan identitas pengguna, mencegah penyalahgunaan dan kebocoran akses.

C. Pengembangan portal layanan SSO terpadu di daerah bukan hanya sekedar modernisasi teknologi, tetapi langkah strategis dalam meningkatkan efisiensi pelayanan, keterbukaan informasi, dan pengelolaan data yang lebih efektif. Dengan terwujudnya satu portal layanan daerah, pemerintah dapat memberikan pelayanan publik yang lebih responsif, mudah diakses, dan akuntabel, sehingga dapat meningkatkan kepuasan dan partisipasi masyarakat dalam pembangunan daerah.

1.6. Pihak-pihak Terkait Penyelenggaraan dan Pemanfaatan Aplikasi SPBE

Penyelenggaraan Aplikasi : DKISP dan Perangkat Daerah yang mengelola Layanan Publik

Pemanfaatan Aplikasi : Seluruh Masyarakat, ASN dan Perangkat Daerah

1.7. Ruang Lingkup

1.7.1. Jenis Aplikasi (Web/Mobile/Desktop/Lainnya)
Web

1.7.2. Jenis Akes Layanan (Publik/Internal)
Publik

1.7.3. Kode Sumber
Kode terbuka (opensource)

1.7.4. Lisensi Aplikasi
Tidak menggunakan lisensi

1.7.5. Jenis Bahasa Pemrograman dan Versinya

PHP 8.x

1.7.6. Jenis Framework dan Versinya
Laravel 10/11/12

1.7.7. Jenis Database dan Versinya
MySQL 5/8

1.7.8. Nama Domain yang digunakan
kaltaraprov.go.id

1.7.9. Lokasi Server, Jenisnya (Hosting/VM). Jadwal dan Retensi Backup
DKISP, VM, Backup Harian, Jumlah Retensi = 14

1.7.10. Standar minimal Keamanan Aplikasi

Sebagai layanan otentikasi terpusat (*Identity Provider*), sistem SSO harus memenuhi standar keamanan tinggi agar dapat diandalkan oleh seluruh aplikasi terintegrasi dalam ekosistem SPBE. Standar minimal yang diterapkan meliputi:

a) **Jenis Enkripsi:**
Password pengguna disimpan dalam bentuk hash menggunakan algoritma **bcrypt** (minimal), disertai *salt* untuk mencegah brute-force dan rainbow table attack.

b) Data sensitif yang disimpan (seperti client secret aplikasi) dienkripsi menggunakan algoritma modern seperti **AES-256** jika diperlukan.
Manajemen Level Akses:
Sistem mendukung pemisahan level akses: Admin Sistem, Admin Instansi, Pengguna Umum, dan peran tambahan seperti Verifier, Operator, dsb.
Setiap level memiliki hak akses dan batasan yang dikontrol secara eksplisit melalui pengelolaan peran (role-based access control / RBAC).

c) **Logging Aktivitas:**
Semua aktivitas login, logout, perubahan data akun, serta aktivitas administratif dicatat secara otomatis dalam tabel log terpisah.
Log aktivitas memuat informasi waktu, IP address, user-agent, dan tindakan yang dilakukan, serta dapat diakses oleh admin yang berwenang.

d) **Pembatasan File Upload:**
Jika aplikasi mendukung pengunggahan berkas (misalnya untuk verifikasi akun instansi), maka file yang dapat diunggah hanya terbatas pada jenis file aman seperti PDF, JPG/PNG.

Validasi dilakukan di sisi server untuk mencegah bypass dan serangan file injection (e.g., .php disguised as .jpg).

e) **Validasi & Sanitasi Input:**
Seluruh input dari pengguna divalidasi dan disanitasi baik di sisi frontend maupun backend.
Praktik keamanan standar diikuti seperti:
- Mencegah SQL Injection dengan parameterized queries/ORM
- Mencegah XSS melalui encoding output dan whitelist input
- CSRF protection di seluruh form
- Rate limiting pada endpoint login untuk mencegah brute-force

f) **Proteksi Token & Session:**
- Token akses (seperti access token / refresh token) disimpan dan dikelola dengan aman menggunakan protokol **OAuth2.0** atau **OpenID Connect**.
- Sesi login memiliki durasi terbatas dan dapat dilacak serta diakhiri secara manual oleh pengguna (logout di semua perangkat).

1.7.11. Standar minimal terkait Integrasi

Integrasi SSO dengan aplikasi layanan pemerintah daerah maupun pusat harus mengikuti standar interoperabilitas nasional, serta memastikan keamanan dan keandalan identitas digital. Standar integrasi meliputi:

a) Dukungan OAuth2.0 & OpenID Connect:

SSO bertindak sebagai Authorization Server yang mendukung protokol **OAuth2.0** dan **OpenID Connect** untuk integrasi autentikasi ke aplikasi lain.

- Setiap aplikasi wajib mendaftar untuk mendapatkan **client_id**, **client_secret**, dan **redirect URL** yang diverifikasi.

b) Registrasi API ke Sistem Pengelolaan Layanan Pertukaran (SPLP):

- Seluruh aplikasi yang ingin terhubung ke SSO wajib melakukan registrasi resmi di **SPLP Kemkominfo/Kemkomdigi**, mengikuti panduan integrasi nasional SPBE.
- Dokumentasi API, endpoint token, dan prosedur login disediakan dan dikelola dengan baik.

c) Penanganan Token dan Hak Akses:

- Token yang diberikan memiliki scope dan durasi terbatas.
- Sistem mendukung **revokasi token**, **multi-session control**, dan pemantauan aktivitas aplikasi pihak ketiga.

d) Isolasi Akses antar Aplikasi:

- Setiap aplikasi hanya dapat mengakses data identitas pengguna **yang diizinkan oleh pengguna** atau sesuai scope peranannya.
- Tidak ada akses langsung ke basis data pengguna dari aplikasi eksternal.

e) Dukungan Layanan Teknis:

- Tim pengelola SSO menyediakan dokumentasi teknis, endpoint sandbox/testing, dan dukungan integrasi untuk instansi daerah yang ingin menghubungkan aplikasinya ke layanan SSO.

1.7.12. Dokumentasi Penggunaan dan Training Pengguna
Wajib Tersedia

1.7.13. Pemeliharaan (Perbaikan bug)
Wajib Tersedia

1.8. Target Waktu
September – Oktober 2025

1.9. Pagu Anggaran
Anggaran : 100.000.000
Rincian Biaya Anggaran

No	Uraian	Vol	Intensitas	Satuan	Harga Satuan (Rp.)	Total Harga (Rp.)
Biaya Personil						
	Technical Analyst	1	2	OB		
	Fullstack Developer	2	2	OB		
	Keycloak Engineer	1	2	OB		
Total						
Biaya Non Personil						
	Dokumentasi Pelaporan	1	1	Paket		
Total						

2. RANCANGAN KEBUTUHAN

2.1. Kebutuhan Fungsional

Kebutuhan fungsional adalah fitur-fitur yang harus ada pada aplikasi yang dibangun untuk memenuhi tujuan pembangunan aplikasi ini. Berikut adalah contohnya :

ID	Deskripsi kebutuhan	keterangan
Pengelolaan Akun, Peran dan Autentikasi		
KF01	**Registrasi Pengguna**: Masyarakat dapat mendaftar dengan memasukkan informasi seperti nama, email, nomor telepon, dan identitas yang valid.	
KF02	**Single Sign-On (SSO)**: Pengguna dapat mengakses semua layanan menggunakan satu akun (SSO), sehingga tidak perlu login berulang kali untuk setiap layanan.	
KF03	**Manajemen Profil Pengguna**: Pengguna dapat mengubah informasi pribadi, seperti alamat, nomor telepon, atau kata sandi.	
KF04	**Otentikasi Dua Faktor (2FA)**: Untuk keamanan tambahan, pengguna dapat mengaktifkan 2FA dengan email atau PIN	
KF05	Sistem harus mengelola peran pengguna dan memberikan hak akses sesuai dengan peran tersebut	
Integrasi dengan Aplikasi Existing		
	Portal harus memiliki environment yang dapat diintegrasikan ke berbagai aplikasi yang sudah ada (misalnya: perizinan, kesehatan,	

	pendidikan) melalui **API Gateway** atau **middleware** serta menerapkan pemanfaatan Sistem Penghubung Layanan Pemerintah (SPLP) dan Enterprise Service Bus (ESB) yang telah disediakan oleh Kemkomdigi	
	Setiap layanan yang dipilih di portal dapat mengarahkan pengguna ke aplikasi terkait	
	Portal bisa dilengkapi dengan dashboard khusus untuk admin yang melakukan manajemen pengguna	
Pusat Informasi dan FAQ		
	Informasi Layanan: Tersedia informasi lengkap mengenai tiap layanan, persyaratan, dan waktu proses.	
	FAQ: Kumpulan FAQ yang memberikan jawaban atas pertanyaan umum seputar penggunaan portal.	
	Artikel dan Panduan: Menyediakan artikel atau panduan singkat bagi pengguna terkait layanan atau penggunaan portal.	
Fitur Pencarian dan Navigasi		
	Pencarian Layanan Terpadu: Memudahkan pengguna mencari berbagai layanan yang tersedia dengan pencarian kata kunci.	
	Kategori Layanan: Layanan dikategorikan dengan baik, sehingga pengguna dapat	

	menelusuri berdasarkan kategori, seperti kesehatan, kependudukan, pendidikan, dll.	
Notifikasi Pengguna		
	Pengguna dapat menerima notifikasi terkait informasi penting melalui notifikasi berbasis web.	
Dst…	Dst…	

2.2. Kebutuhan Non Fungsional

Kebutuhan non fungsional menggambarkan bagaimana performa sistem yang diharapkan dalam menjalankan fungsi-fungsinya.

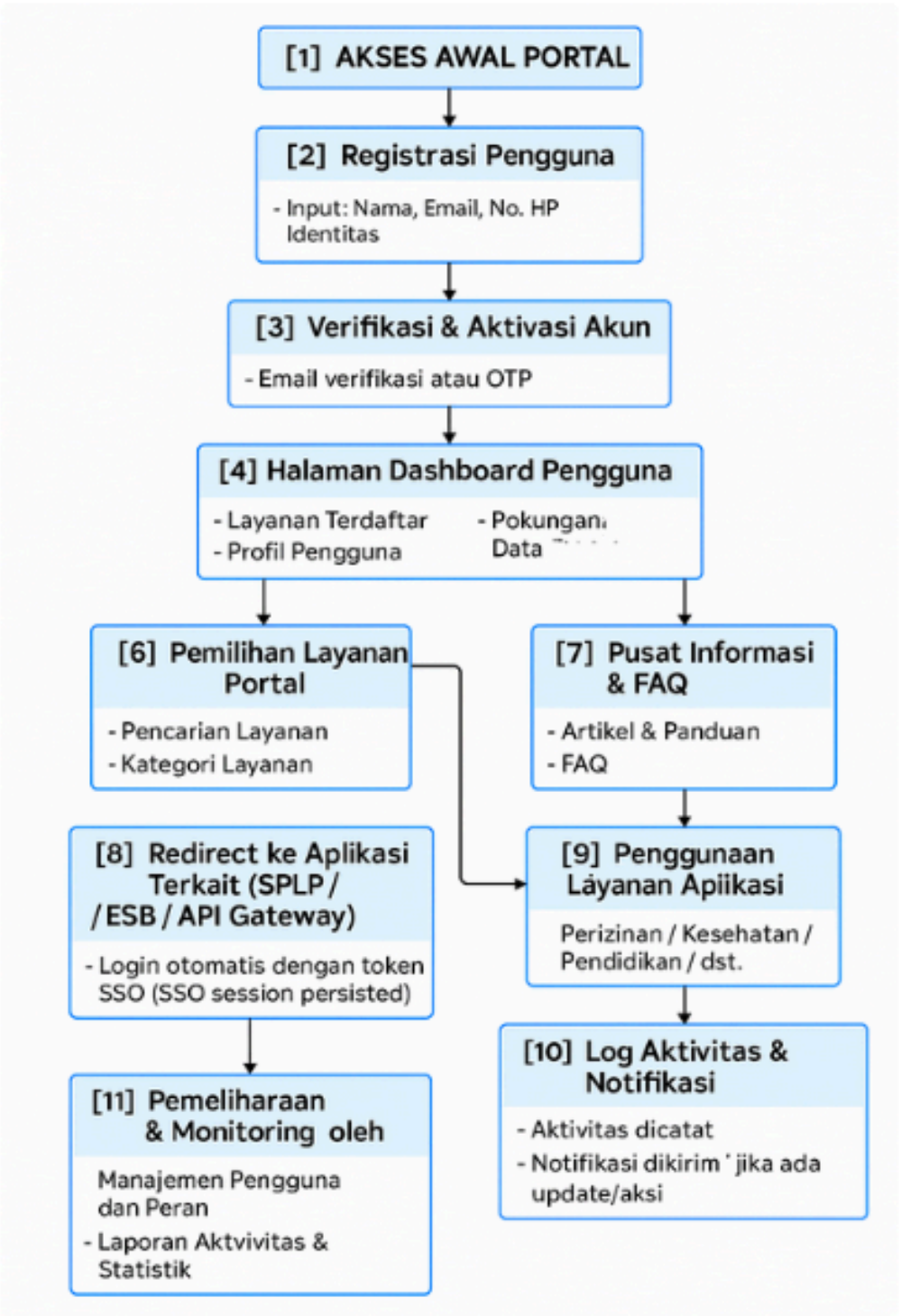
ID	Deskripsi kebutuhan	keterangan
Keamanan Data		
KNF01	Semua data yang ditransmisikan melalui portal dan aplikasi yang terhubung harus dienkripsi menggunakan protokol HTTPS/SSL untuk melindungi data pribadi dan sensitif.	
KNF02	Sistem harus memastikan bahwa data pengguna dan permohonan dilindungi dengan kebijakan keamanan yang ketat.	
KNF03	Semua API yang digunakan untuk integrasi antar aplikasi harus aman dan dilindungi dengan autentikasi berbasis token atau OAuth.	
KNF04	API yang digunakan untuk mengakses data layanan harus dilindungi dari akses yang tidak sah dan serangan keamanan	

	seperti SQL injection atau DDoS.	
Kinerja dan Responsivitas		
	Portal harus memberikan waktu respons yang cepat, dengan waktu load halaman tidak lebih dari 10 detik.	
	Sistem harus mampu menangani volume pengguna yang tinggi, terutama selama jam sibuk atau saat layanan besar dibutuhkan.	
	Harus ada kemampuan untuk menambah kapasitas secara horizontal (menambahkan server) sesuai dengan jumlah pengguna yang meningkat.	
Keandalan dan Ketersediaan		
	Sistem portal harus tersedia 24/7 dengan downtime minimal. Harus ada rencana pemulihan bencana dan cadangan data untuk menjamin ketersediaan layanan.	
	Sistem harus memiliki mekanisme log error yang efektif dan mampu memberikan peringatan jika terjadi kesalahan.	
Pengalaman Pengguna (User Experience)		
	Portal harus memiliki antarmuka yang responsif dan dapat diakses dengan nyaman di berbagai perangkat, termasuk desktop, tablet, dan ponsel.	
	UI/UX harus intuitif, mudah digunakan oleh pengguna dari	

	berbagai latar belakang dan tingkat pemahaman teknologi.	
	Portal harus memenuhi standar aksesibilitas (misalnya WCAG) untuk memastikan bahwa pengguna dengan disabilitas dapat mengakses dan menggunakan layanan	
Pemeliharaan dan Pengelolaan		
	Sistem harus memungkinkan pembaruan aplikasi secara berkala tanpa menyebabkan gangguan pada layanan pengguna.	
	Admin harus dapat melakukan pemeliharaan dan pembaruan sistem secara terpusat melalui antarmuka yang ramah pengguna.	
	Sistem harus menyediakan laporan analitik bagi admin untuk mengevaluasi kinerja layanan dan kebutuhan pengguna.	

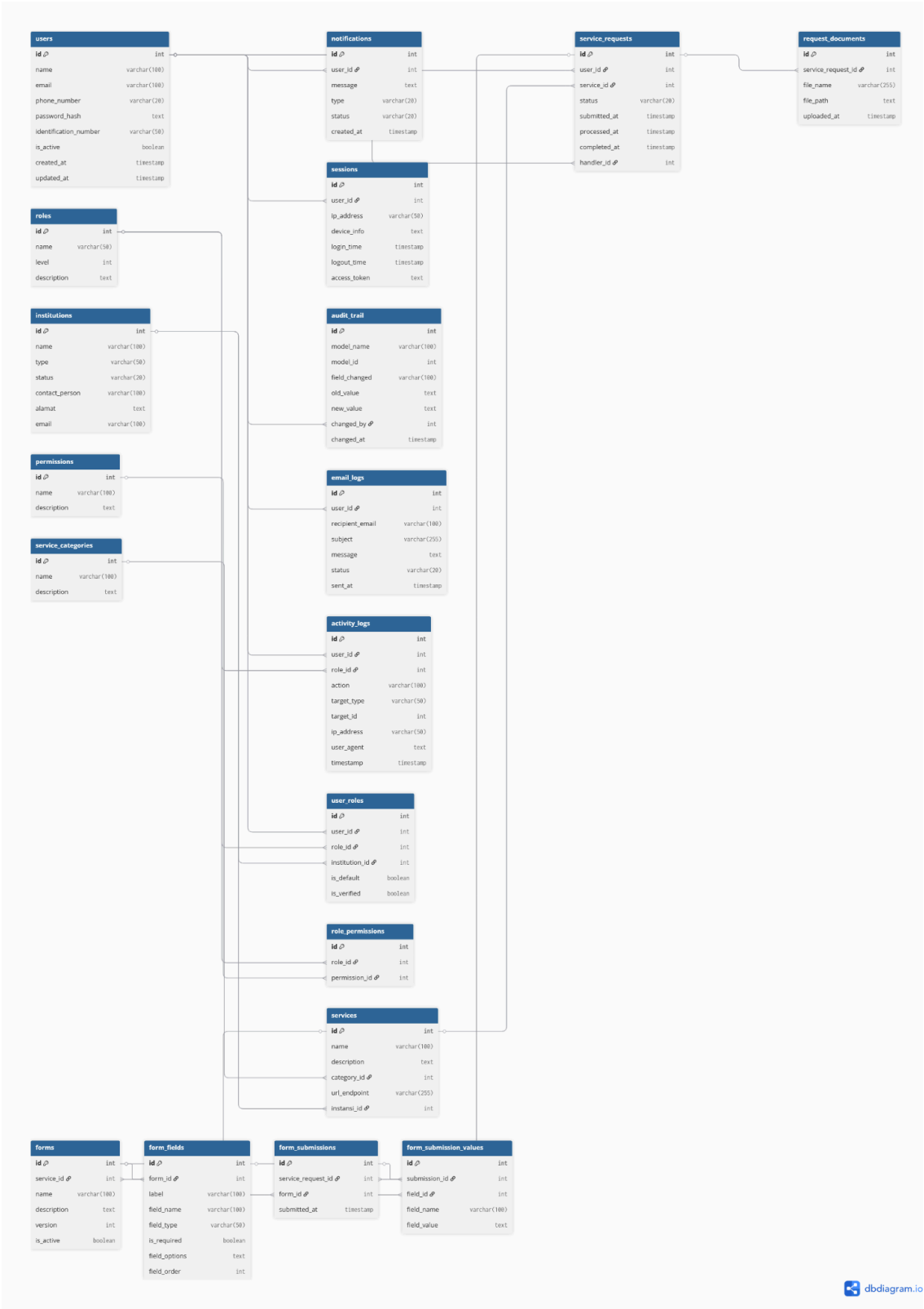
2.3. Diagram Alur (Flow Diagram)

Diisi dengan gambar flow diagram. Contohnya ada pada gambar berikut ini :


[1] AKSES AWAL PORTAL
[2] Registrasi Pengguna
- Input: Nama, Email, No. HP
Identitas
[3] Verifikasi & Aktivasi Akun
- Email verifikasi atau OTP
[4] Halaman Dashboard Pengguna
- Layanan Terdaftar
- Profil Pengguna
- Pokungan
Data
[6] Pemilihan Layanan Portal
- Pencarian Layanan
- Kategori Layanan
[7] Pusat Informasi & FAQ
- Artikel & Panduan
- FAQ
[8] Redirect ke Aplikasi Terkait (SPLP / / ESB / API Gateway)
- Login otomatis dengan token SSO (SSO session persisted)
[9] Penggunaan Layanan Apiikasi
Perizinan / Kesehatan / Pendidikan / dst.
[10] Log Aktivitas & Notifikasi
- Aktivitas dicatat
- Notifikasi dikirim ' jika ada update/aksi
[11] Pemeliharaan & Monitoring oleh
Manajemen Pengguna dan Peran
- Laporan Aktvivitas & Statistik

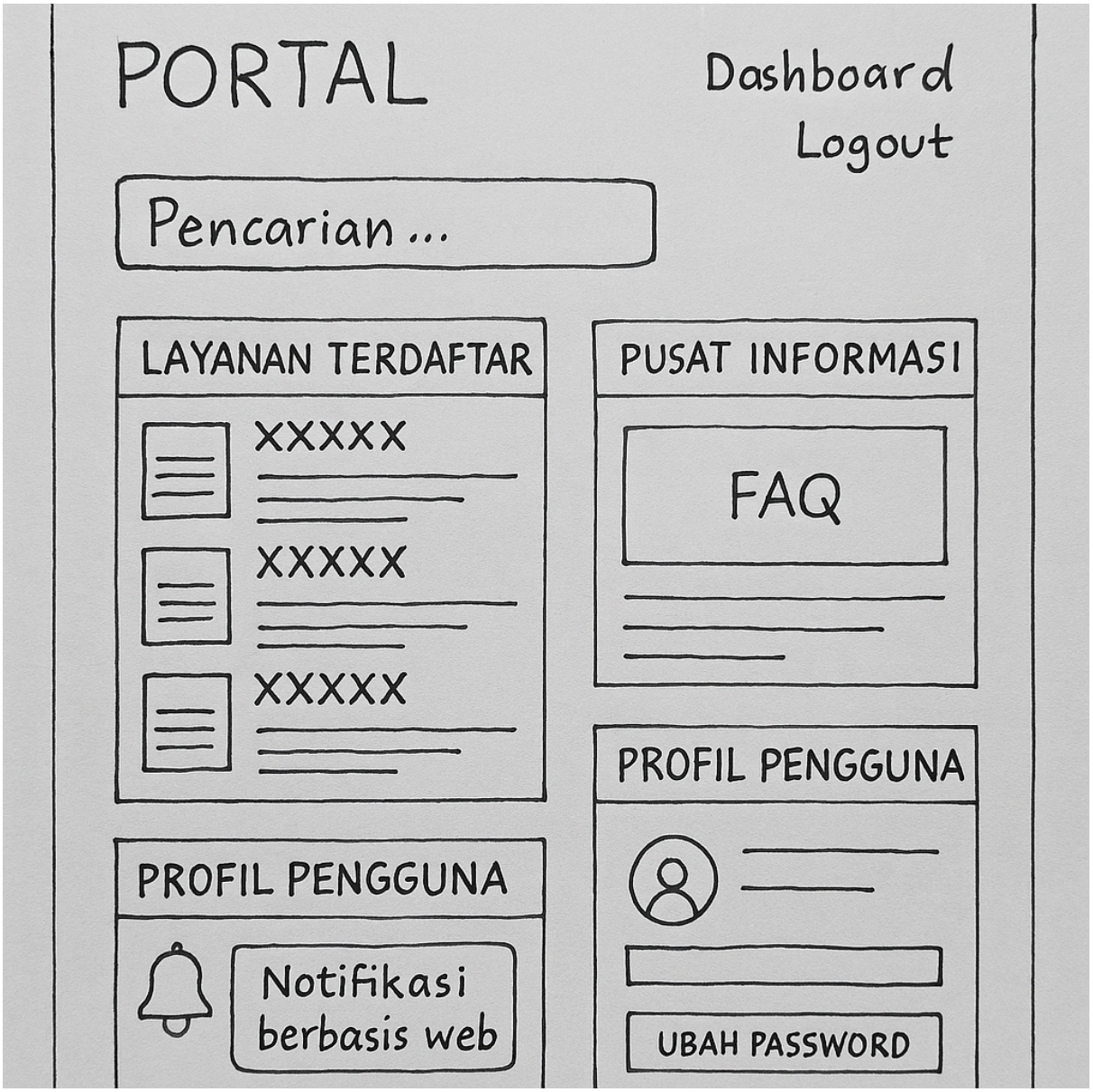
2.4. Entity Relation Diagram (ERD)

Diisi dengan diagram relasi antar hubungan. Contohnya ada pada gambar berikut ini :



2.5. Sketsa Aplikasi (App Sketch)

Diisi dengan sketsa aplikasi pertampilan antarmuka. Contohnya pada gambar berikut ini :




REGISTRASI
NAMA
EMAIL
NO. HP
IDENTITAS
Saya setuju dengan syarat & ketentuan
DAFTAR

2.6. Autentifikasi login

Diisi dengan penjelasan bagaimana autentifikasi aplikasi yang diperlukan dalam sistem. Autentifikasi yang dimaksud contohnya seperti. Silahkan diisi sesuai kebutuhan :

a. Kata sandi untuk login minimal 8 digit dan dengan kombinasi angka, huruf besar, huruf kecil dan simbol.
b. Kode OTP lewat SMS/Email/WA
c. Login Captcha
d. PIN

2.7. Otorisasi

Diisi dengan penjelasan bagaimana otorisasi atau penentuan kontrol akses (pemetaan hak akses) yang berlaku didalam sistem.

Jawab: Telah tertera pada KF

2.8. Data, Transaksi, Laporan, Integrasi dan Interoperabilitas (Silahkan dijawab sesuai pertanyaan berikut)

a. **Standar Data**. Apakah perangkat daerah telah memiliki standar data yang harus dipatuhi? Jika ya, bisa diberikan contoh standar tersebut atau siapa instansi pembina datanya?

Jawab :

Ya, perangkat daerah telah memiliki standar data yang harus dipatuhi. Standar tersebut mengacu pada standar interoperabilitas nasional dan ketentuan Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagaimana diamanatkan oleh Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE dan regulasi teknis turunannya. Contohnya, pada integrasi SSO diatur penggunaan protokol OAuth 2.0 dan OpenID Connect sebagai standar autentikasi, serta kewajiban registrasi aplikasi di Sistem Pengelolaan Layanan Pertukaran (SPLP) Kemkominfo/Kemkomdigi.

Instansi pembina data untuk standar ini adalah Kementerian Dalam Negeri , Badan Kepegawaian Negara.

Contoh Standar Data:

- **Format Nama Lengkap** → huruf alfabet tanpa angka/simbol, maksimal 100 karakter.
- **Nomor HP** → format internasional (+62...), tanpa spasi atau tanda baca lain.
- **Email** → format valid email (`nama@domain`), huruf kecil semua.
- **NIK/NIP** → wajib 16 digit angka (untuk NIK) atau sesuai format NIP BKN.

- **Tanggal Lahir** → format `YYYY-MM-DD` (ISO 8601).
  Semua layanan yang terhubung SSO wajib mengikuti format ini agar data bisa dibaca dan diolah oleh sistem lain tanpa error.

b. **Meta Data dan Daftar Data**. Apakah perangkat daerah memiliki metadata khusus yang harus dicatat untuk setiap entri data? Apakah ada persyaratan khusus seperti sumber data atau otoritas yang bertanggung jawab yang perlu disertakan dalam metadata ini?

Jawab :

Metadata:

1. Sumber Data: pendaftaran mandiri atau impor dari sistem lain
   - Menunjukkan asal-usul data
   - Penanggung jawab: DKISP
2. Otoritas Penanggung Jawab: OPD pengelola atau DKISP
   - Menunjukkan pihak yang bertanggung jawab terhadap validitas data
   - Penanggung jawab: DKISP & OPD terkait
3. Waktu Dibuat: timestamp (mis. 2025-08-14 09:45:00)
   - Mencatat kapan akun atau data dibuat
   - Penanggung jawab: DKISP
4. Waktu Diubah Terakhir: timestamp terakhir update
   - Untuk audit dan riwayat perubahan
   - Penanggung jawab: DKISP
5. Status Verifikasi: belum / email verified / HP verified
   - Menentukan kelengkapan proses verifikasi identitas digital
   - Penanggung jawab: DKISP
6. ID Pencatat: user ID atau admin ID yang membuat/mengubah
   - Untuk keperluan audit trail dan keamanan
   - Penanggung jawab: DKISP

Daftar Data

1. Data Identitas Pengguna

- NIK / NIP → untuk identitas resmi (wajib sesuai Dukcapil atau BKN)
- Nama Lengkap
- Tempat Lahir
- Tanggal Lahir
- Jenis Kelamin
- Alamat Lengkap

- Nomor HP
- Alamat Email

2. Data Akun & Akses

- Username
- Password (hashed bcrypt)
- Status Verifikasi (email verified, phone verified, belum verifikasi)
- Role / Hak Akses (Admin Sistem, Admin Instansi, User Umum, Verifier, Operator)
- Tanggal Pembuatan Akun
- Tanggal Terakhir Login
- Status Akun (aktif, nonaktif, suspend)

3. Data Aktivitas

- Log Login / Logout (waktu, IP, user-agent)
- Log Perubahan Profil
- Riwayat Aktivitas di Aplikasi Terintegrasi

4. Data Integrasi

- client_id dan client_secret (untuk integrasi aplikasi)
- redirect_url yang terdaftar di SPLP
- Scope Akses (data apa saja yang bisa diambil aplikasi)
- Token OAuth / OpenID Connect (access token, refresh token)

c. **Integrasi dan Interoperabilitas**. Apakah ada data tertentu yang perlu diinteroperabilitaskan dengan sistem lain? Jika ya, data apa saja yang diinginkan untuk diakses oleh pihak ketiga, seperti layanan publik lain atau antarinstansi?

Jawab :

Ya, terdapat data yang perlu diinteroperabilitaskan dengan sistem lain, terutama untuk mendukung pertukaran informasi antar layanan publik dan antarinstansi di lingkungan Pemerintah Provinsi Kalimantan Utara maupun dengan sistem nasional. Integrasi ini dilakukan melalui Sistem Pengelolaan Layanan Pertukaran (SPLP) atau Enterprise Service Bus (ESB) yang disediakan oleh Kemkomdigi, dengan standar protokol OAuth 2.0 dan OpenID Connect untuk autentikasi dan otorisasi.

Data yang dapat diakses oleh pihak ketiga (sesuai persetujuan pengguna dan scope akses):

1. **Data Identitas Dasar Pengguna**
    - NIK/NIP
    - Nama Lengkap
    - Alamat Email
    - Nomor HP
    - Tanggal Lahir
    - Jenis Kelamin
2. **Data Akun & Status Akses**
    - Role/Hak Akses (mis. Admin Sistem, Admin Instansi, User Umum)
    - Status Verifikasi (email verified, phone verified)
    - Tanggal Terakhir Login
3. **Data Integrasi Teknis**
    - client_id dan redirect_url aplikasi pihak ketiga
    - Token akses (access token, refresh token) sesuai scope yang disetujui
    - Scope Akses yang mengatur jenis data yang boleh diambil

Catatan:

- Pertukaran data hanya dilakukan dengan aplikasi/instansi yang **terdaftar resmi di SPLP** dan telah mendapatkan persetujuan dari pengguna (consent-based).
- Data sensitif seperti password, riwayat aktivitas internal, dan log keamanan **tidak dibagikan** ke pihak ketiga.
- Mekanisme integrasi memastikan isolasi data antar aplikasi dan pembatasan akses sesuai peran.

d. **Kode Referensi dan Data Induk**. Apakah perangkat daerah sudah memiliki kode referensi dan data induk yang diharuskan, misalnya kode wilayah atau kode lainnya yang penting?

Jawab :

Ya, perangkat daerah telah memiliki kode referensi dan data induk yang digunakan dalam pengelolaan identitas pengguna dan integrasi antar sistem. Kode referensi dan data induk ini mengikuti standar nasional agar data dapat saling diinteroperabilitaskan dengan aplikasi pemerintah daerah maupun pusat.

1. **Kode Wilayah**
   - Mengacu pada Kode dan Data Wilayah Administrasi Pemerintahan dari Kementerian Dalam Negeri (Permendagri Nomor 137 Tahun 2017 dan perubahannya).
   - Digunakan untuk menandai asal domisili pengguna (Provinsi, Kabupaten/Kota, Kecamatan, Kelurahan/Desa).

2. **Kode Instansi Perangkat Daerah**
   - Mengacu pada daftar resmi OPD di lingkungan Pemprov Kaltara (SK Gubernur tentang Struktur Organisasi Perangkat Daerah).
   - Digunakan untuk menentukan hak akses pengguna dalam SSO berdasarkan instansi.

3. **Kode Role/Hak Akses**
   - Standar peran di SSO seperti: `ADMIN_SYS`, `ADMIN_OPD`, `USER`, `VERIFIER`, `OPERATOR`.
   - Mengatur otorisasi pengguna di seluruh layanan terintegrasi.

4. **Kode Jenis Layanan**
   - Mengacu pada daftar jenis layanan publik yang tersedia di portal terpadu, misalnya: `PERIZINAN`, `KESEHATAN`, `PENDIDIKAN`.
   - Digunakan untuk mengelompokkan layanan dan menentukan scope akses aplikasi pihak ketiga.

5. **Kode Integrasi Aplikasi**

   - Setiap aplikasi yang terhubung ke SSO memiliki `client_id` unik yang terdaftar di **SPLP Kemkomdigi**.

- Digunakan untuk memastikan keamanan dan keterlacakan integrasi.

Pengelolaan dan pembaruan kode referensi dilakukan oleh DKISP bekerja sama dengan instansi pembina masing-masing kode (Kemendagri untuk kode wilayah, OPD terkait untuk kode instansi, Kemkomdigi untuk registrasi integrasi aplikasi).

---

e. **Format Laporan Ekspor**. Apakah perangkat daerah membutuhkan laporan dalam format khusus (PDF, XLSX, CSV)? Laporan apa saja yang perlu dapat diekspor pada sistem?
Jawab : Ya dalam bentuk PDF, XLSX dan CSV

f. **Pencatatan Transaksi.** Apakah diperlukan pencatatan lengkap setiap transaksi? Apakah ada spesifikasi tentang data yang perlu disimpan, seperti pengguna, waktu, dan jenis transaksi?
Jawab : Y
Ya, diperlukan pencatatan lengkap setiap transaksi yang terjadi di dalam sistem SSO sebagai bagian dari mekanisme **audit trail** dan pemenuhan standar keamanan SPBE. Pencatatan ini membantu memastikan keamanan, akuntabilitas, dan keterlacakan setiap aktivitas yang dilakukan oleh pengguna maupun administrator.

Spesifikasi data yang dicatat dalam setiap transaksi:

1. **Identitas Pengguna**

   - `user_id` atau NIK/NIP (jika tersedia)
   - Nama pengguna yang melakukan transaksi

2. **Waktu Transaksi**

   - Tanggal dan jam dalam format timestamp (`YYYY-MM-DD HH:MM:SS`)

3. **Jenis Transaksi**

   - Login / Logout
   - Perubahan profil pengguna
   - Reset kata sandi

- Aktivasi / nonaktifkan akun
- Pembuatan akun baru
- Permintaan token akses oleh aplikasi pihak ketiga
- Perubahan hak akses/role

4. **Detail Teknis Transaksi**

- IP address asal
- User-agent (browser, OS, perangkat)
- Lokasi akses (jika tersedia melalui geo-IP)
- Status transaksi (berhasil / gagal)

5. **Identitas Petugas/Admin (jika ada)**

- `admin_id` atau nama admin yang memproses perubahan

Catatan Teknis:

- Semua log transaksi disimpan di tabel terpisah dalam database (mis. `transaction_logs` atau `audit_logs`) dengan proteksi akses terbatas hanya untuk admin berwenang.
- Log disimpan minimal sesuai periode retensi yang ditetapkan DKISP, dan diikutkan dalam backup harian.
- Pencatatan mengikuti prinsip **non-repudiation** agar setiap aktivitas dapat dipertanggungjawabkan dan tidak dapat disangkal oleh pihak yang melakukan.

Instansi penanggung jawab: DKISP selaku pengelola SSO, bekerja sama dengan OPD terkait untuk validasi dan audit berkala.

g. **Pembatasan Akses atau Keamanan Data.** Apakah ada data yang bersifat sensitif atau terbatas aksesnya? Jika ada, data apa saja yang hanya boleh diakses oleh pihak tertentu?
Jawab :
Jawab:
Ya, terdapat data yang bersifat sensitif dan terbatas aksesnya dalam sistem SSO. Data tersebut hanya dapat diakses oleh pihak

tertentu yang memiliki kewenangan sesuai peran/hak akses yang ditetapkan dalam sistem (Role-Based Access Control / RBAC).

Jenis data sensitif yang dilindungi:

1. Data Pribadi Pengguna
   - Nama Lengkap
   - NIK/NIP
   - Tanggal Lahir
   - Nomor HP
   - Alamat Email
   - Alamat Domisili
   - Foto Profil

2. Data Akun
   - Username
   - Password (tersimpan dalam bentuk hash bcrypt)
   - Status verifikasi akun
   - Riwayat login dan logout

3. Data Teknis Integrasi
   - client_id dan client_secret aplikasi terdaftar
   - Token akses (access token, refresh token)
   - Redirect URL aplikasi terdaftar

Pembatasan Akses:
- Admin Sistem (DKISP) → memiliki akses penuh terhadap seluruh data untuk keperluan pengelolaan dan pemeliharaan sistem.
- Admin Instansi → hanya dapat mengakses data pengguna di lingkup instansinya masing-masing.
- Verifier → hanya dapat mengakses data yang diperlukan untuk proses verifikasi (misalnya NIK, dokumen pendukung).
- Operator/Pengguna Umum → hanya dapat mengakses data milik dirinya sendiri.

Pengamanan Tambahan:
- Semua data sensitif disimpan dengan enkripsi sesuai standar keamanan (contoh: bcrypt untuk password, AES-256 untuk client_secret jika diperlukan).
- Akses ke data sensitif hanya dapat dilakukan melalui koneksi aman (HTTPS/TLS).

- Setiap akses terhadap data sensitif dicatat di log aktivitas untuk keperluan audit.

h. **Kebutuhan Penyediaan Data Real-Time atau Berkala.** Apakah data yang akan dibagikan perlu selalu diperbarui secara real-time, atau cukup disediakan dalam waktu-waktu tertentu saja?
Jawab :
Jawab:
Ya, data yang dibagikan melalui SSO perlu selalu diperbarui secara real-time, terutama data identitas dan status autentikasi pengguna. Hal ini penting untuk memastikan konsistensi informasi di seluruh layanan terintegrasi, mencegah penggunaan data lama yang sudah tidak valid, serta menjaga keamanan sistem.

Contoh data yang wajib real-time:
- Status login pengguna (aktif/nonaktif)
- Status verifikasi akun (email verified, phone verified)
- Perubahan data identitas (nama, NIK/NIP, alamat email, nomor HP)
- Perubahan hak akses/role
- Token autentikasi OAuth/OpenID Connect

Alasan kebutuhan real-time:
- Mencegah akses tidak sah akibat data yang belum diperbarui
- Menjamin pengalaman pengguna yang konsisten di semua aplikasi terintegrasi
- Memungkinkan pencabutan hak akses atau pemutusan sesi secara langsung jika ada pelanggaran

Catatan:
Untuk data non-kritis atau bersifat statistik (misalnya laporan penggunaan bulanan), pembaruan dapat dilakukan secara berkala sesuai jadwal yang ditentukan oleh DKISP.

i. **Kebutuhan Akses Tambahan (Tambah, Ubah, Hapus).** Selain melihat data, apakah ada kebutuhan untuk menambah, mengubah, atau menghapus data oleh sistem lain?
Jawab : Tidak. Belum saat ini.

2.9. Manajemen Pengetahuan

a. Apakah aplikasi yang dibangun akan menyediakan dokumentasi aplikasi yang memuat penjelasan pada source code?
   Jawab : Ya wajib tersedia
b. Apakah aplikasi yang dibangun akan menyediakan dokumentasi prosedur instalasi (pemasangan) aplikasi?
   Jawab : Ya wajib tersedia
c. Apakah aplikasi yang dibangun akan menyediakan manual penggunaan aplikasi?
   Jawab : Ya wajib tersedia
d. Apakah aplikasi yang dibangun akan menyediakan akses/fasilitas mengenai Daftar Pertanyaan Yang Sering Diajukan (Frequently Asked Question/FAQ) untuk pengguna aplikasi?
   Jawab : Ya wajib tersedia
e. Apakah aplikasi yang dibangun akan menyediakan fasilitas Helpdesk (Layanan Bantuan terkait teknis aplikasi)?
   Jawab : Ya wajib tersedia

2.10. Pencadangan dan Pemulihan

a. Apakah pencadangan data perlu dilakukan setiap hari pada waktu tertentu, misalnya pukul 24.00, atau ada jadwal lainnya yang lebih sesuai dengan kebutuhan?
   Jawab : Sudah sesuai
b. Data atau file apa saja yang perlu dicadangkan setiap hari? Apakah mencakup semua (aplikasi, database, dan file pengguna)?
   Jawab : Semua
c. Apakah ada ketentuan khusus terkait dimana cadangan data akan disimpan? Apakah harus di server lokal, cloud, atau lokasi lain yang aman?
   Jawab : Cloud
d. Apakah ada persyaratan khusus terkait dengan enkripsi atau perlindungan data cadangan untuk mencegah akses tidak sah?
   Jawab : N/A
e. Apakah waktu pemulihan data (waktu restore) dalam waktu kurang dari 2 x 24 jam sesuai dengan kebutuhan Anda, atau ada batasan waktu lain yang lebih ideal?
   Jawab : Ya

2.11. Evaluasi dan Pemantauan

Diisi dengan penjelasan bagaimana aplikasi akan direviu/dievaluasi. Misalnya :

a. Penjelasan terkait rencana/jadwal berkala reviu aplikasi.

Jawab : Rencana rapat evaluasi aplikasi minimal 1 tahun sekali pada triwulan IV dengan melibatkan seluruh OPD terkait

b. Penjelasan terkait penyusunan indikator keberhasilan aplikasi.
Jawab : Pembuatan kuesioner feeback kepuasan pengguna pada aplikasi. Feedback dibuat pada gform dan diembed linknya pada aplikasi

3. PENUTUP