



A Governance-First API for Museums and Cultural Institutions

Presented By:

Louey Dridi

Supervised by:

Prof. Montassar Ben Messaoud

IT-325 Web Services

Table of Contents

- Context & Motivation
- Problem Statement
- DOCENT Vision
- Architecture
- Data Model
- API Design
- Security
- Technologies Stack
- Limitations & Future Work
- Conclusion



Context & Motivation

- Museums operate under legal, ethical, and preservation responsibilities
- Artifact care, authenticity, and inspections are continuous obligations
- Visitor access must remain meaningful even without guides
- Most digital systems focus on content, not institutional accountability

“Museums are regulated cultural institutions, not just exhibition spaces.”



Problem Statement

- Governance processes are rarely modeled digitally
- Artifact maintenance and authenticity tracking are fragmented
- Institutional roles are protected by generic security models
- Visitor access depends heavily on guide availability
- There is no single authoritative backend for museums



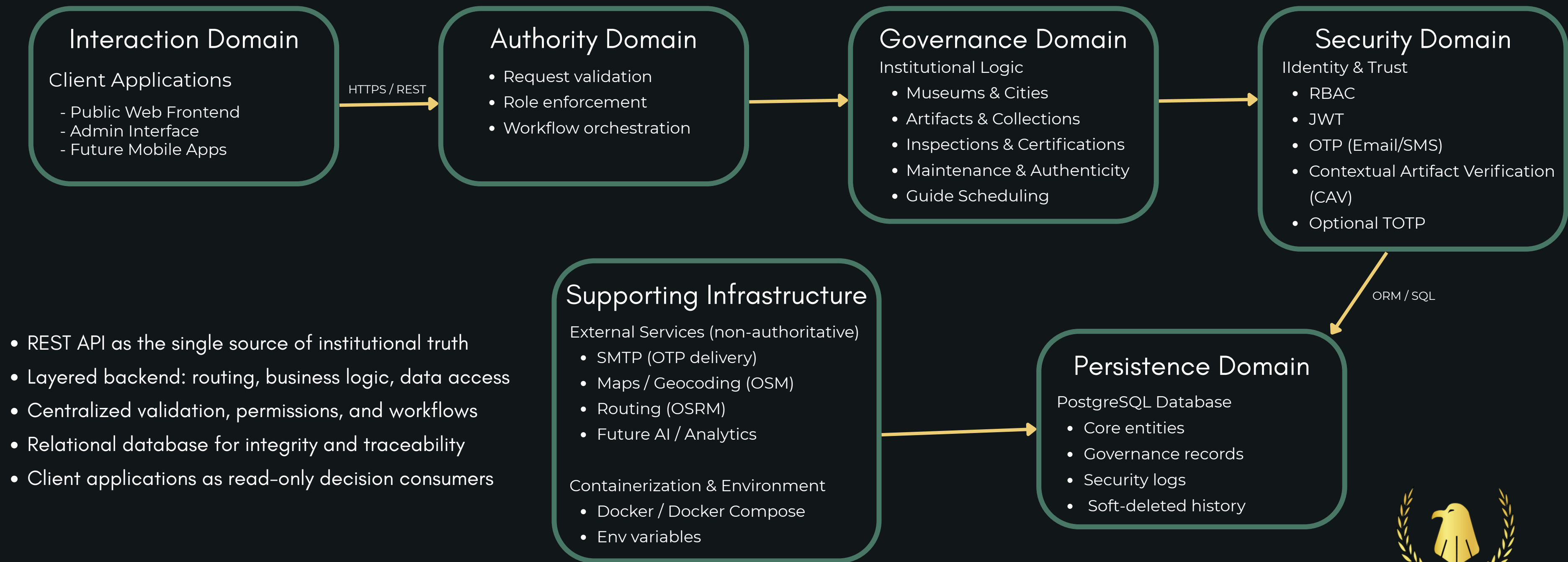
DOCENT Vision

“DOCENT is a backend-first REST API that models museums as regulated institutions.”

- The API acts as the single authoritative source for museum data and rules
- Governance processes (inspections, maintenance, certifications) are modeled explicitly
- Security mechanisms reflect institutional responsibility, not generic access levels
- Client applications display data, but governance rules are enforced exclusively by the API



Architecture



- REST API as the single source of institutional truth
- Layered backend: routing, business logic, data access
- Centralized validation, permissions, and workflows
- Relational database for integrity and traceability
- Client applications as read-only decision consumers



Data Model: Governance-Oriented Relational Schema

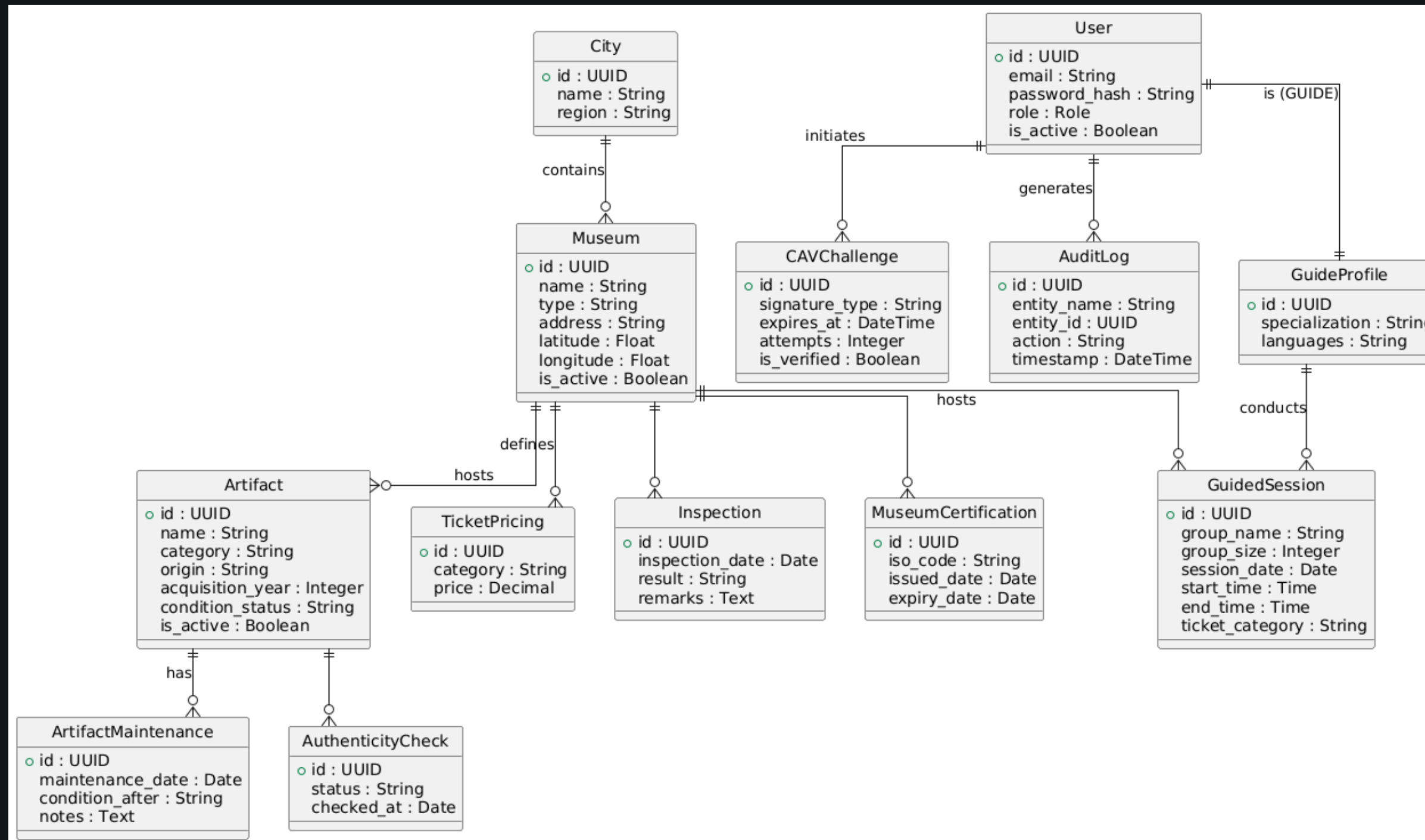


Figure: Database Structure



API Design

DOCENT API 1.0.0 [Base URL: /] /swagger.json DOCENT is a digital governance, education, and engagement platform for museums. It is designed for regions with: - limited resources - uneven tourism exposure - real operational constraints Core Domains - Cities & geography — Where museums are located - Museums & visitor rules — Core institution management - Artifacts & conservation — Cultural asset stewardship - Ticketing & fairness — Regional pricing justice - Events & engagement — Year-round cultural visibility - Guides & digital mediation — Human + AI-enabled learning - Inspections, authenticity & ISO compliance — Institutional trust DOCENT focuses on trust, transparency, and cultural sustainability.	Users User management endpoints for platform administrators cities Cities geographic management and discovery museums Museums management, discovery, and operations Ticketing Ticket pricing, categories, and regional fairness Guides Guide session management endpoints Governance Inspections, authenticity checks, and ISO compliance. Trust layer of DOCENT. CAV Contextual Artifact Verification - Domain-aware admin authentication Authentication Role-adaptive authentication operations Events Event management operations News Museum news management operations
--	--



API Design

Users User management endpoints for platform administrators			^	
OPTIONS	/users	Handle CORS preflight request	✓	🔒
GET	/users	List all users (platform admin only)	✓	🔒
DELETE	/users/{user_id}	Delete a user (platform admin only)	✓	🔒
OPTIONS	/users/{user_id}	Handle CORS preflight request	✓	🔒
PUT	/users/{user_id}/role	Update a user's role (platform admin only)	✓	🔒
OPTIONS	/users/{user_id}/role	Handle CORS preflight request	✓	🔒
cities Cities geographic management and discovery				
POST	/cities	Create a new city (platform admin only)	✓	🔒
GET	/cities	List all active cities	✓	🔒
DELETE	/cities/{city_id}	Delete city - soft delete only (platform admin only)	✓	🔒
PUT	/cities/{city_id}	Update city (platform admin only)	✓	🔒
GET	/cities/{city_id}	Get a specific city	✓	🔒

museums Museums management, discovery, and operations			^	
POST	/museums	Create museum (admin only)	✓	🔒
GET	/museums	List active museums with search, filter, and pagination	✓	🔒
DELETE	/museums/{museum_id}	Delete museum - soft delete only (platform admin only)	✓	🔒
PUT	/museums/{museum_id}	Update museum (admin only)	✓	🔒
GET	/museums/{museum_id}	Get a specific museum	✓	🔒



API Design

Ticketing

Ticket pricing, categories, and regional fairness

GET

/Ticketing/museums/{museum_id}/ticketing

View ticket prices for a museum

Guides

Guide session management endpoints

GET

/guides

List all guide profiles

GET

/guides/me/schedule

Get guide's daily schedule

GET

/guides/me/sessions

Get guide's sessions

POST

/guides/sessions

Create/assign a guided session (Admin only)

GET

/guides/sessions

List all guided sessions (Admin only)

DELETE

/guides/sessions/{session_id}

Cancel a guided session (Admin only)

PUT

/guides/sessions/{session_id}

Update a guided session (Admin only)

Governance

Inspections, authenticity checks, and ISO compliance. Trust layer of DOCENT.

GET

/Governance/certifications/{museum_id}

View ISO certifications for a museum (public)

POST

/Governance/inspections

Record a museum inspection (platform admin only)

GET

/Governance/inspections

List all inspection records (public)

CAV

Contextual Artifact Verification - Domain-aware admin authentication

POST

/CAV/challenge

Generate CAV challenge for admin authentication

POST

/CAV/verify

Verify CAV challenge answer

Authentication

Role-adaptive authentication operations

POST

/auth/login

Role-adaptive login

POST

/auth/otp/verify

Verify OTP code for visitors and guides

POST

/auth/register

Register a new user

POST

/auth/totp/setup

Generate TOTP secret and QR code for admin (after CAV verification)

POST

/auth/totp/verify

Verify TOTP code from Google Authenticator



API Design

Events Event management operations			^
POST	/events	Create a new event (admin only)	✓ 🔒
OPTIONS	/events	Handle CORS preflight request	✓ 🔒
GET	/events	List all events with optional filters	✓ 🔒
DELETE	/events/{event_id}	Delete an event (admin only)	✓ 🔒
PUT	/events/{event_id}	Update an event (admin only)	✓ 🔒
OPTIONS	/events/{event_id}	Handle CORS preflight request	✓ 🔒
GET	/events/{event_id}	Get event details	✓ 🔒

News Museum news management operations			^
POST	/news	Create a new news article (admin only)	✓ 🔒
OPTIONS	/news	Handle CORS preflight request	✓ 🔒
GET	/news	List all published news articles	✓ 🔒
DELETE	/news/{news_id}	Delete a news article (admin only)	✓ 🔒
PUT	/news/{news_id}	Update a news article (admin only)	✓ 🔒
OPTIONS	/news/{news_id}	Handle CORS preflight request	✓ 🔒
GET	/news/{news_id}	Get news article details	✓ 🔒



API Design

Events Event management operations			^
POST	/events	Create a new event (admin only)	✓ 🔒
OPTIONS	/events	Handle CORS preflight request	✓ 🔒
GET	/events	List all events with optional filters	✓ 🔒
DELETE	/events/{event_id}	Delete an event (admin only)	✓ 🔒
PUT	/events/{event_id}	Update an event (admin only)	✓ 🔒
OPTIONS	/events/{event_id}	Handle CORS preflight request	✓ 🔒
GET	/events/{event_id}	Get event details	✓ 🔒

News Museum news management operations			^
POST	/news	Create a new news article (admin only)	✓ 🔒
OPTIONS	/news	Handle CORS preflight request	✓ 🔒
GET	/news	List all published news articles	✓ 🔒
DELETE	/news/{news_id}	Delete a news article (admin only)	✓ 🔒
PUT	/news/{news_id}	Update a news article (admin only)	✓ 🔒
OPTIONS	/news/{news_id}	Handle CORS preflight request	✓ 🔒
GET	/news/{news_id}	Get news article details	✓ 🔒



Security Architecture

- ▶ Role-Based Access Control (visitor, guide, museum admin, platform admin)
- ▶ Stateless authentication using JWT
- ▶ OTP verification for public and professional users
 - Admins may enroll a device-based authenticator
 - Adds a second factor after successful CAV
 - Strengthens security without replacing contextual verification
- ▶ Contextual Artifact Verification (CAV) for administrators
 - Admins must answer a question about an artifact from their museum
 - Verifies institutional knowledge, not just credentials
 - Attempts are time-limited and audited
- ▶ Audit logging for security-sensitive actions



Technologies Stack

Backend & API

- Python 3.11
- Flask
- Flask-RESTX (REST structure + OpenAPI/Swagger)
- SQLAlchemy (ORM)

Database

- PostgreSQL

Security

- JWT (JSON Web Tokens)
- bcrypt (password hashing)
- OTP (email-based verification)
- TOTP (optional, admin-only)

Infrastructure & DevOps

- Docker
- Docker Compose
- Environment variables for configuration

External & Supporting Services

- SMTP (Gmail) for OTP delivery
- OpenStreetMap / Nominatim (geocoding)
- OSRM (routing)

Testing & Documentation

- Swagger UI (OpenAPI)
- Insomnia
- Github Copilot LLM model: Claude 4.5 OPUS



Limitations & Future Work



- Advanced analytics and reporting are not implemented
- AI-assisted features are designed but not active
- Geolocation is limited to basic coordinates and routing support
- 3D models and VR museum experiences are not implemented
- Automated testing is limited to manual verification



- Advanced analytics on visits, artifacts, and ticket categories
- AI-assisted artifact explanations and natural-language search
- Extended geolocation (indoor routing, accessibility paths)
- 3D models and immersive VR/AR museum experiences
- Enhancing the security flow with Biometric measures for Admins



Frontend consumption already implemented



In Summary

- Museums are modeled as accountable institutions, not data catalogs
- Governance, preservation, and oversight are embedded into the API design
- Security is contextual and proportional to institutional responsibility
- The backend remains authoritative while supporting diverse client applications

**Thank You
for your attention!**



Appendix

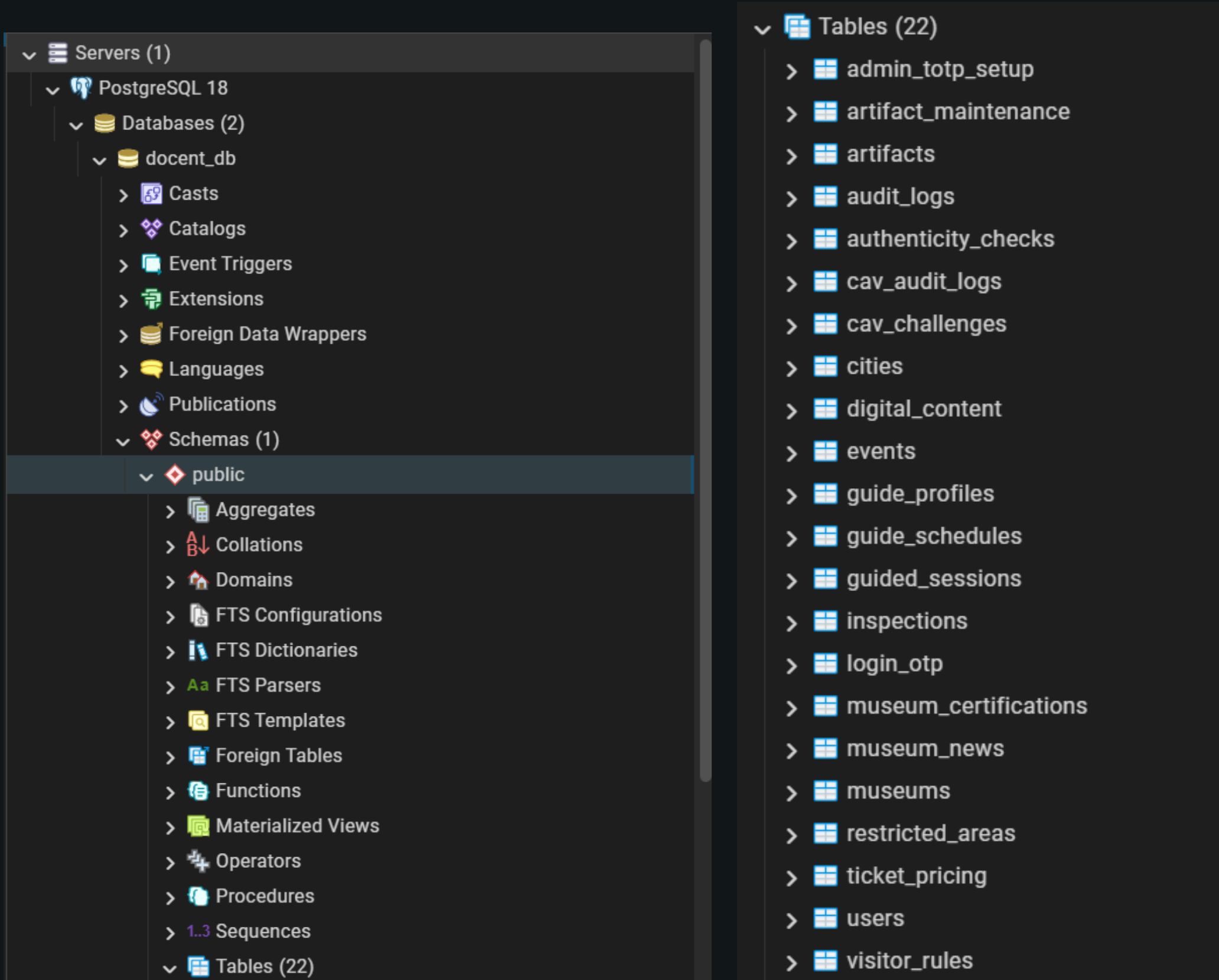


Figure: PostgreSQL Database Structure



Appendix

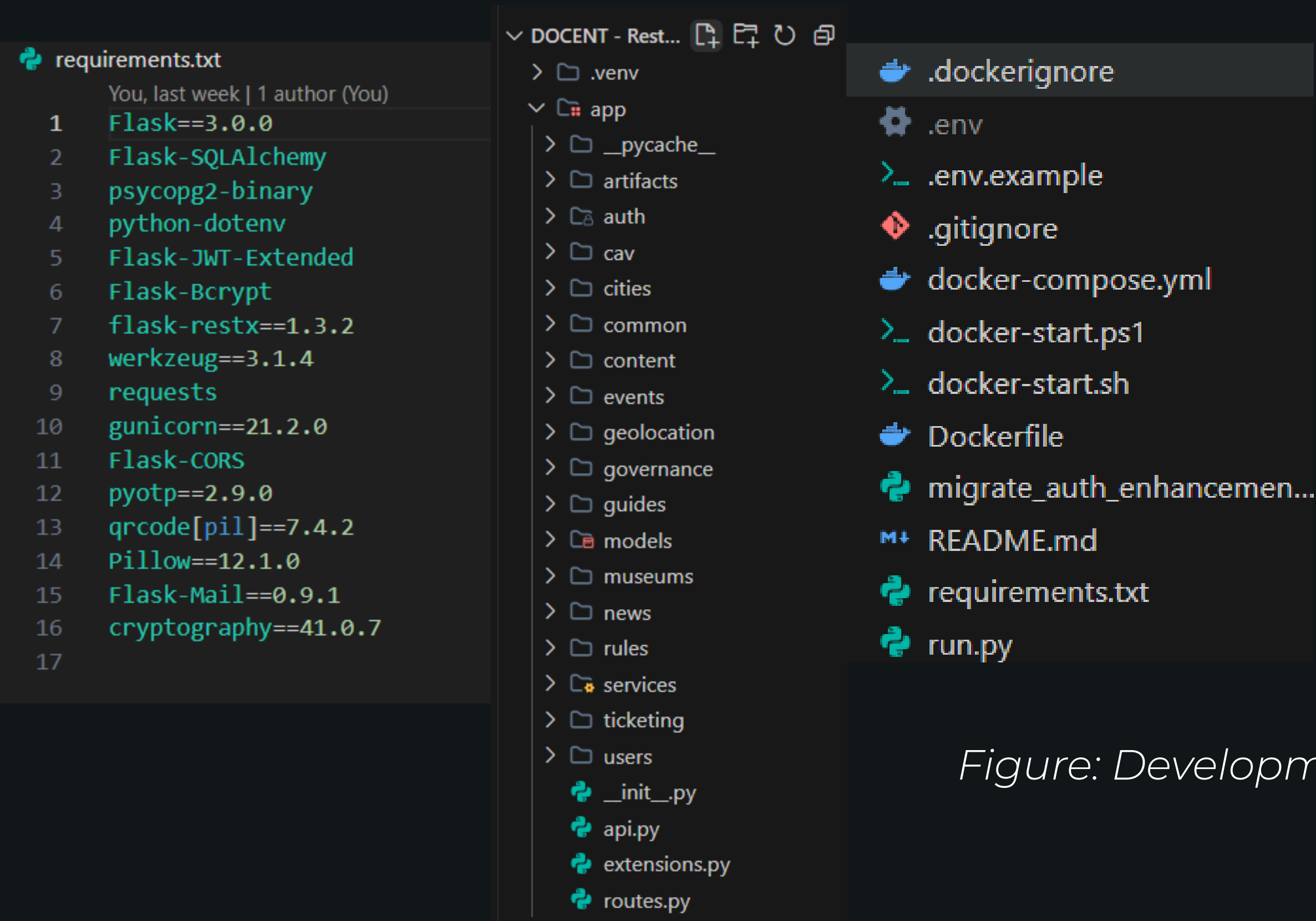


Figure: Development Structure



Appendix

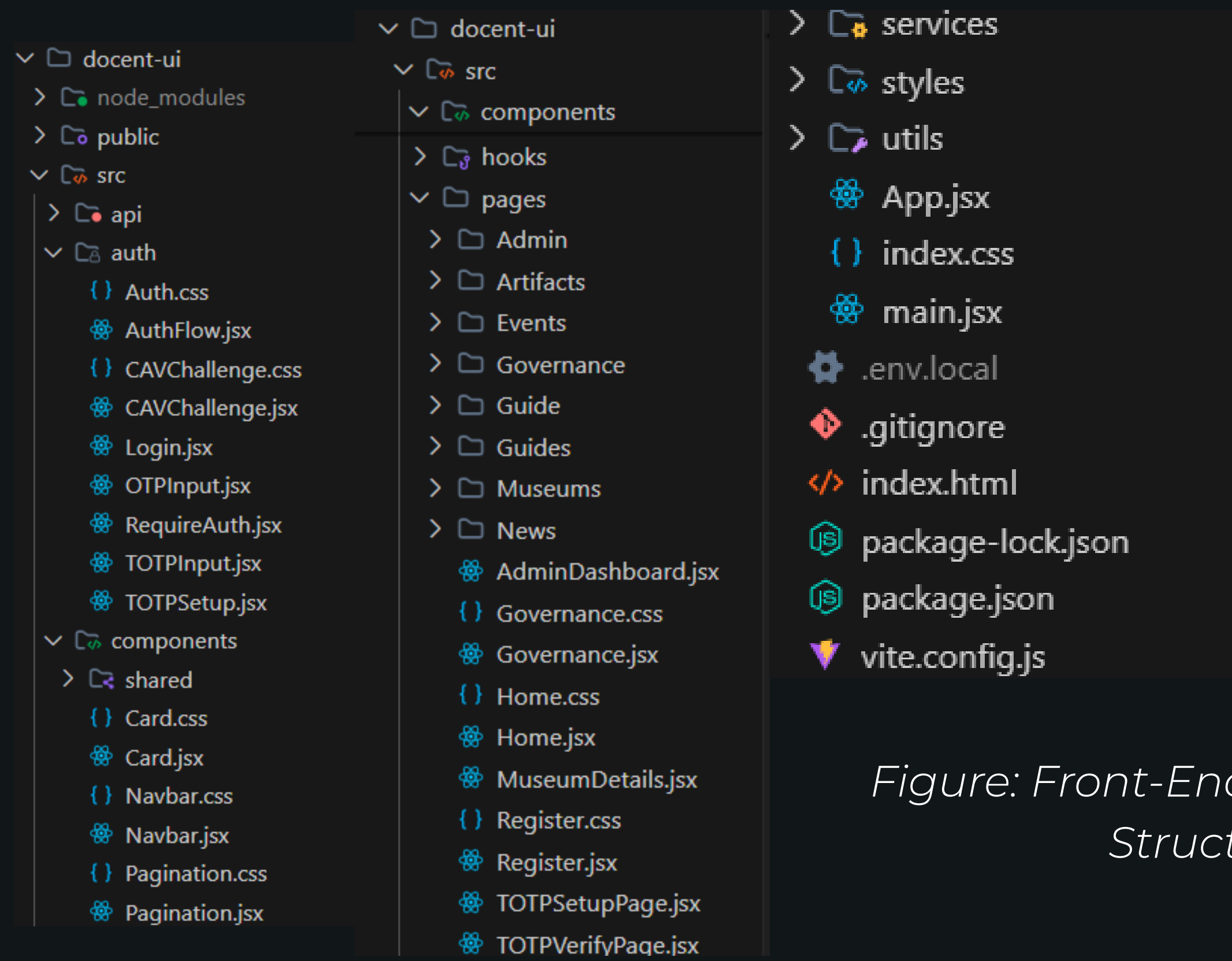
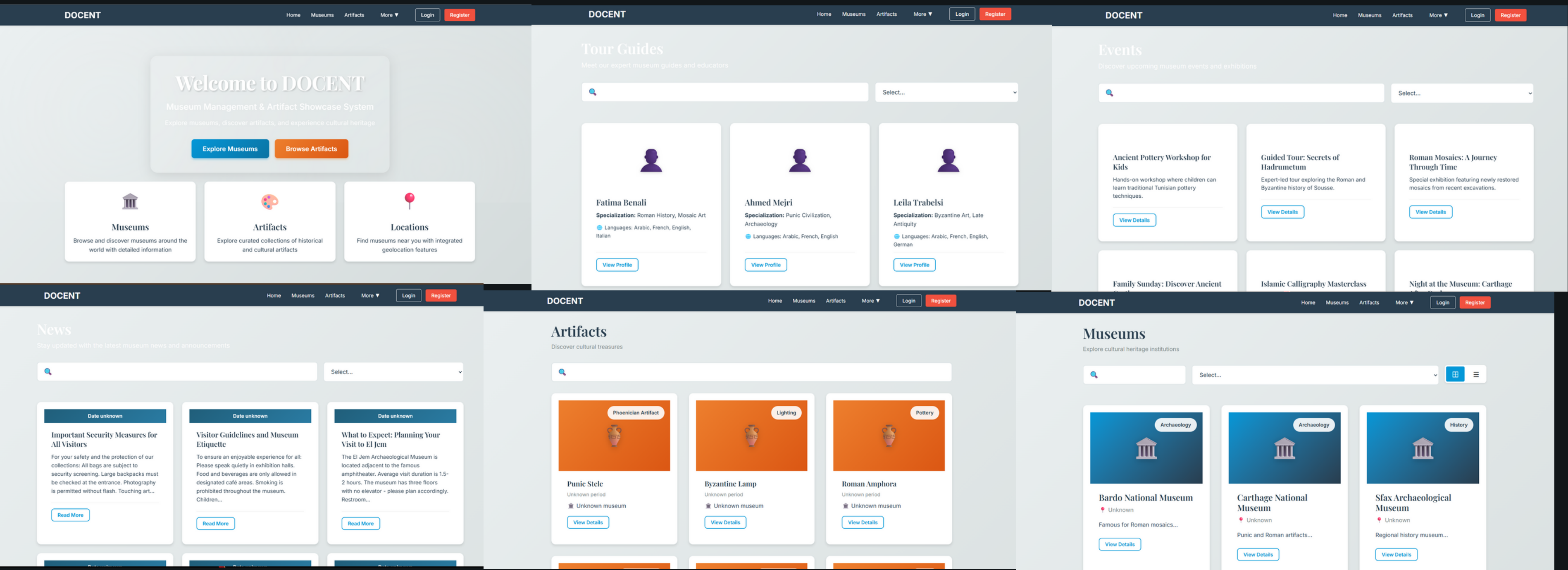


Figure: Front-End Development Structure



Appendix



Figures: Front-End UI

DOCENT

HomeMuseumsArtifactsMore▼LoginRegister



DOCENT

Digital Organization for Cultural Education

Create Account

Join DOCENT to explore cultural heritage

Email Address *

Password *

Minimum 6 characters

Confirm Password *

Account Type *

Visitor

Create Account

Already have an account? [Sign in](#)

DOCENT

Museum Management System

Email

your@email.com

Password

Enter password

Sign In

Demo Credentials:

Visitor (OTP): demo.visitor@docent.local / demo123

Admin (CAV+TOTP): admin@docent.local / admin123

💡 Visitors use email OTP, Admins use CAV + Google Authenticator

Figures: CAV & MFA

DOCENT

HomeMuseumsArtifactsMore▼LoginRegister



DOCENT

Security Verification

Prove your knowledge of the collection

Ulysses and the Sirens Mosaic

Enter the acquisition year of this artifact

01:26

remaining

Your Answer

Enter the year...

Attempts remaining: 3

Submit Answer

DOCENT

HomeMuseumsArtifactsMore▼LoginRegister

Setup Google Authenticator

Scan the QR code to enable two-factor authentication

1 Install Google Authenticator

Download from App Store or Google Play

2 Scan this QR code



3 Or enter this code manually

ERX3HPKTQYCU5GPYJNP2BZB4ATXFWB3I

DOCENT

HomeMuseumsArtifactsMore▼LoginRegister

Enter Authenticator Code

Enter the 6-digit code from Google Authenticator to confirm setup

0 0 0 0 0 0

Verify Code

💡 The code refreshes every 30 seconds in Google Authenticator

DOCENT

Home

Museums

Artifacts

More

Admin

PLATFORM_ADMIN

Logout

Events

Discover upcoming museum events and exhibitions

Select...

Ancient Pottery Workshop for Kids

Hands-on workshop where children can learn traditional Tunisian pottery techniques.

View Details

Edit

Delete

Guided Tour: Secrets of Hadrumetum

Expert-led tour exploring the Roman and Byzantine history of Sousse.

View Details

Edit

Delete

Roman Mosaics: A Journey Through Time

Special exhibition featuring newly restored mosaics from recent excavations.

View Details

Edit

Delete

Family Sunday: Discover Ancient

Islamic Calligraphy Masterclass

Night at the Museum: Carthage

Create New Museum

Add a new museum to the collection

Museum Name *

Description

Brief description of the museum...

Museum Type

Select...

Established Year

City *

Country

Address/Location

Cancel

Create Museum

Create New Museum

Add a new museum to the collection

Museum Name *

Description

Brief description of the museum...

Museum Type

Select...

Select Type

Art Museum

History Museum

Science Museum

Natural History Museum

Archaeological Museum

Cultural Museum

Military Museum

Maritime Museum

Other

Established Year

Country

Cancel

Create Museum

DOCENT

Home

Museums

Artifacts

More

Admin

PLATFORM_ADMIN

Logout

Guided Sessions

Manage guide assignments and schedules

+ Assign Session

Date	Time	Guide	Museum	Group	Size	Category	Status	Actions
No sessions found. Create your first session above.								

Tour Guides

Meet our expert museum guides and educators

Select...

Fatima Benali

Specialization: Roman History, Mosaic Art

Languages: Arabic, French, English, Italian

View Profile

Edit

Delete

Ahmed Mejri

Specialization: Punic Civilization, Archaeology

Languages: Arabic, French, English

View Profile

Edit

Delete

Laila Trabelsi

Specialization: Byzantine Art, Late Antiquity

Languages: Arabic, French, English, German

View Profile

Edit

Delete

Admin Dashboard

Manage museums and artifacts

0

TOTAL MUSEUMS

Museums in the system

0

TOTAL ARTIFACTS

Artifacts across all museums

Recent Museums

No museums found

Recent Artifacts

No artifacts found

DOCENT

Home

Museums

Artifacts

More

Admin

PLATFORM_ADMIN

Logout

Platform Governance

Manage users, roles, and system access

Filter by Role

All Roles

14

Total Users

14

Filtered

EMAIL	ROLE	REGISTERED	ACTIONS
T test@docent.local	VISITOR	Dec 30, 2025	Visitor Delete
N newadmin@docent.local	VISITOR	Dec 31, 2025	Visitor Delete
D dridilouey67@gmail.com	VISITOR	Jan 4, 2026	Visitor Delete
D demo.visitor@docent.local	VISITOR	Jan 4, 2026	Visitor Delete
T test@example.com	VISITOR	Jan 5, 2026	Visitor Delete

Figures: Admin UI