



مركز إيداع الأوراق المالية
Securities Depository Center



REQUEST FOR PROPOSAL

Frontend Development & UI/UX Design

e-Portfolio Portal

Mobile & Web Applications

Issuing Authority	Securities Depository Center (SDC) — Amman, Jordan
Department	Department of Systems and Electronic Services Development
Document Reference	SDC-RFP-EPORTFOLIO-2026-01
Document Version	Final
Issue Date	October 2026
Classification	CONFIDENTIAL — FOR VENDOR USE ONLY

Securities Depository Center | Amman, Jordan | www.sdc.com.jo



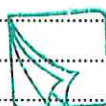
مركز إيداع الأوراق المالية
Securities Depository Center
رقم الحساب: 1/3105/39



TABLE OF CONTENTS

Table of Contents

1.	Current Backend Infrastructure	4
2.	SCOPE OF WORK	4
2.1	UI/UX Design	4
	Required Design Deliverables	4
2.2	Frontend Development	5
	Mobile Application — Flutter.....	5
	Web Application — React.js or Vue.js.....	5
2.3	API Integration.....	5
2.4	API Error Handling & Resilience	6
3.	FUNCTIONAL REQUIREMENTS	6
3.1	Authentication & Session Management	7
3.2	Investor Dashboard	7
3.3	E-Portfolio Services & Pages	8
3.4	Push Notifications.....	9
3.5	Settings, Utility & Social Features.....	9
3.6	Local Data Storage — Mobile (Offline Cache)	9
4.	NON-FUNCTIONAL REQUIREMENTS	10
4.1	Performance Standards	10
4.2	Security Requirements	10
4.3	SSO — Sanad National Identity Integration.....	11
4.4	Compliance with MODEE Digital Transformation Standards.....	11
5.	VENDOR ELIGIBILITY & QUALIFICATION REQUIREMENTS	11
5.1	Legal & Corporate Standing.....	12
6.	REQUIRED PROJECT TEAM COMPOSITION	12
7.	DELIVERABLES & PROJECT TIMELINE	12
7.1	Mandatory Deliverables	12
7.2	Training Requirements	13
8.	EVALUATION & VENDOR SCORING CRITERIA.....	14
8.1	Evaluation Criteria	14
9.	Submission Instructions	14
10.	CONTRACTUAL & LEGAL TERMS	15
10.1	Project Ownership.....	15
10.2	Confidentiality	15
10.3	Warranty & Defect Liability	15



مركز إيداع الأوراق المالية
Securities Depository Center
رقم الحساب: 1/3105/39



1- SDC Overview

The Securities Depository Center (SDC) — Jordan's official central depository for securities — is seeking a qualified and experienced technology partner to design, develop, and deliver a complete frontend solution for its E-Portfolio platform. This platform enables investors in the Jordanian capital market to monitor their securities holdings, review transaction history, access account statements, and manage their investor profiles online.

The SDC has rebuilt its backend using a modern microservices architecture. The selected vendor will be responsible solely for the frontend layer, encompassing UI/UX design, mobile applications, and web applications, all fully integrated with the backend APIs.

Engagement Summary

Component	Details
Client	Securities Depository Center (SDC) — Amman, Jordan
Platform	E-Portfolio Service
Project Type	Frontend UI/UX Design + Mobile & Web Application Development
Mobile Platform	Flutter (iOS & Android)
Web Platform	React.js or Vue.js (vendor to justify choice in proposal)
Backend Status	Fully implemented and production-ready — no backend work required
Integration Method	Secure REST APIs via API Gateway (Postman collection provided to shortlisted vendors)
Language Support	Arabic (RTL) and English (LTR) with dynamic runtime switching

Phase 1 of 2 — This engagement covers Phase 1 only: a modern rebuild of the platform's existing functionality. Phase 2, planned for a future date, will expand the service into a fully interactive digital platform. Vendors must propose an extensible architecture that accommodates this future growth.





Current Backend Infrastructure

The backend has been rebuilt from scratch using modern standards. The selected vendor must not modify or propose changes to any backend component. The infrastructure includes:

- Microservices architecture — Auth Service, Investor Service, and others — replacing the legacy monolith
- Centralized API Gateway managing all routing, access control, and performance monitoring
- JWT / OAuth2 authentication with token issuance and silent refresh
- HMAC request signing and Public/Private Key encryption for inter-service security
- Redis caching layer for reduced database load and faster response times
- Docker containerization for consistent and scalable deployment
- Session-based multi-step flows for registration, OTP verification, and password reset

⚠ No backend development is required. Vendors must not propose backend modifications, infrastructure changes, or API redesigns. The full Postman collection covering all endpoints will be provided to shortlisted vendors under NDA.

2. SCOPE OF WORK

This project has three required parts. One vendor must deliver all three parts together as a complete solution. The vendor may work with other companies, but they remain fully responsible for the entire delivery.

2.1 UI/UX Design

The vendor shall design a complete, fintech-grade user experience aligned with modern standards for financial applications. All designs must be delivered in Figma (or equivalent professional tool) covering both platforms under a single unified design system.

Required Design Deliverables

- Wireframes for all screens and user flows across both mobile and web
- High-fidelity UI designs with fintech-level visual quality and data clarity
- Interactive, clickable prototype demonstrating all primary end-to-end flows
- Design system and component library applicable to both mobile and web
- The application must be fully bilingual (Arabic and English), with a complete right-to-left (RTL) layout for Arabic — where the entire interface is mirrored, not just the text direction.
- Design documentation: spacing rules, typography scales, color tokens





2.2 Frontend Development

Mobile Application — Flutter

A cross-platform mobile application built with Flutter, targeting both iOS and Android from a single codebase. The app must deliver native-level performance, support biometric authentication (fingerprint and face recognition), and store authentication tokens securely using platform-native mechanisms (Keychain on iOS, Keystore on Android). The app must also be fully responsive across all screen sizes and orientations, and must respect the user's system font size settings to ensure text and layout scale correctly on all devices.

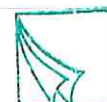
Web Application — React.js or Vue.js

A responsive, browser-based web application. The vendor must state their framework choice in the proposal and justify it based on project requirements and team expertise. The application must be fully responsive across desktop, tablet, and mobile browser viewports.

2.3 API Integration

All frontend applications must integrate with the backend APIs using the provided Postman collection. The following API service groups are in scope:

API Service Group	Estimated APIs
Auth — Login, Refresh Token, Change Password, Logout	4–5
Dashboard Charts and Statistics	3
Auth — Forgot Password (6-step flow)	6
Auth — Registration (8-step flow)	8
Auth — SSO / Sanad	2–3
Investor Info & Profile (PDF & XLSX export)	2
Accounts & Holdings (PDF & XLSX export)	4
Investor Ownership	4
Transactions & Corporate Actions (PDF & XLSX export)	4
Account Statements (PDF & XLSX export)	2
Terms & Conditions, User Manual, Concepts, Notes	5
Push Notifications	1





 The API count shown above is approximate and may increase slightly as project requirements are finalized.

2.4 API Error Handling & Resilience

The frontend applications must properly handle API errors, network failures, authentication issues, and service interruptions to ensure a secure, reliable, and consistent user experience across mobile and web platforms.

API Service Group	Estimated APIs
HTTP Error Handling	Handle HTTP 400, 401, 403, 404, 408, 409, 422, 429, and 5xx responses with appropriate application behavior.
User-Friendly Messages	Display clear and meaningful error messages in Arabic and English without exposing sensitive technical information.
Authentication Errors	Handle expired tokens, unauthorized requests, and session termination securely.
Timeout & Network Failures	Detect connectivity issues and API timeouts, providing appropriate notifications and recovery options.
Retry Mechanism	Implement controlled retries with exponential backoff for eligible requests. Never automatically retry sensitive operations unless safely supported by the backend.
API Rate Limiting	Handle HTTP 429 responses appropriately and respect the API Gateway's retry instructions, including Retry-After when provided.
Duplicate Request Prevention	Prevent duplicate submissions and unnecessary concurrent API requests.
Secure Error Logging	Record relevant technical errors for troubleshooting without exposing credentials, authentication tokens, or sensitive investor data.

3. FUNCTIONAL REQUIREMENTS

The following functional modules must be fully implemented across both mobile and web applications. All data must be sourced from live backend APIs. Hardcoded or mock data is not acceptable in any build submitted for review.





3.1 Authentication & Session Management

Feature	Specification
Login	Username + password via /auth/login; reCAPTCHA validation; JWT token stored securely on success
Logout	Confirmation dialog; clean session termination; all tokens purged from secure storage
Token Lifecycle	Silent token refresh via /auth/refresh; expiry handled without user interruption; forced logout on refresh failure
Account Activation	On first login, user is prompted to change the system-issued password before accessing the service
Terms & Conditions	T&C screen presented on: first login after activation, first login after reactivation, and when T&C content is updated
Change Password	In-session password change via /auth/change-password; re-login required on success
Forgot Password (6-step)	Stateful flow: initiate → select recovery channel → verify contact → send OTP → verify OTP → reset password
Registration (8-step)	Electronic self-registration for Jordanian natural persons: start → verify identity → submit mobile → OTP → verify OTP → submit email → review summary → confirm
Biometric Login (Mobile)	Face ID and fingerprint authentication as alternative to password; graceful fallback to standard login on biometric failure
SSO — Sanad	Single sign-on via Jordan Sanad national identity platform using /auth/sso/sanad/ endpoints
Session Timeout	Automatic logout on inactivity; user redirected to login with clear notification; timeout duration configurable

3.2 Investor Dashboard

The dashboard is the primary screen after login. It provides a consolidated real-time overview of the investor's portfolio. All data must reflect the backend's last update timestamp, prominently displayed.

Dashboard Widget	Content & API Source
General Data Bar	Last data update time, last login time, ISIN lookup link, SDC members link



Last 10 Transactions	Paginated table of 10 most recent transactions with full column set
Ownership by Sector	Donut charts showing holding distribution by sector: shares count, securities count, market value (JOD)
Monthly Trading Volume	Bar chart showing monthly buy/sell volumes for trailing 12 months
Monthly Market Value	Combined bar/line chart showing monthly portfolio value for trailing 12 months
Investor Nationalities Map	World map showing nationality breakdown of all market investors
Corporate Actions Table	Recent capital actions for companies where investor holds securities; tabbed by company type
Important Links & Documents	Annual report, SDC brochure, investor services card, forms, templates

Chart Requirements: Fast rendering | Interactive | Mobile-optimized (touch-friendly, responsive) | RTL-compatible — all chart labels, legends, and axes must support Arabic direction

3.3 E-Portfolio Services & Pages

The following service pages must be fully designed and developed:

Service / Page	Description	Key Features
Investor Information	Complete investor profile and personal information management.	View profile, contact details, investor classification, PDF export, XLSX export
Investor Ownership	Consolidated portfolio holdings across all accounts.	Holdings list, sector analysis, market value summary, filtering, export
Ownership by Specific Security	Detailed ownership information for a selected security.	Quantity, market value, average cost, transaction history
Investor Accounts	Overview of all investor accounts and account details.	Multi-account management, balances, account status
Account Statement	Detailed account statement and transaction history.	Advanced filtering, pagination, PDF export, XLSX export, printing



Corporate Actions	View all corporate actions affecting investor holdings.	Dividends, rights issues, stock splits, capital increases
Portfolio Analytics	Advanced portfolio performance and valuation analysis.	Charts, trends, historical performance metrics
Documents Center	Repository for downloadable investor-related documents.	Search, download, categorization

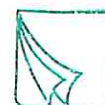
3.4 Push Notifications

Feature	Description
Mobile Push Notifications	Real-time push notifications on iOS and Android devices.
In-App Notification Center	Centralized notification inbox with read/unread status management.
Notification History	Complete history of all notifications received by the investor.

3.5 Settings, Utility & Social Features

Feature	Specification
Language Toggle	Switch Arabic (RTL) ↔ English (LTR) at runtime; no logout required; preference persists across sessions
Change Password	In-session password update; re-login required on success
Logout	Confirmation dialog; clean session termination; all tokens and cached data cleared from device
Share App (Mobile)	Native share sheet (WhatsApp, SMS, email) for app store link; message localized in Arabic and English
Contact Customer Service	Click-to-call, pre-filled email, optional WhatsApp link; contact details sourced from configurable backend value, not hardcoded
About / App Version	Current app version number and build number displayed for user reference and support diagnosis
Footer Navigation (Web)	Links to: User Guide, Concepts & Guidelines, Terms & Conditions, Disclaimer, Language Toggle

3.6 Local Data Storage — Mobile (Offline Cache)





The mobile application may utilize a local embedded NoSQL database for temporary data caching to improve user experience under intermittent connectivity. This is a frontend-only implementation and must not bypass or replicate backend business logic.

4. NON-FUNCTIONAL REQUIREMENTS

4.1 Performance Standards

Metric	Requirement
API Call Optimization	Minimize redundant requests; implement request deduplication and response debouncing
Lazy Loading	Non-critical screens, large images, and heavy chart components must load on demand
Chart Rendering	All dashboard charts must render within the 3-second load budget; hardware-accelerated rendering required
Table Performance	Virtual scrolling or server-side pagination for large datasets — no DOM overload
Force App Update	Mandatory force-update mechanism with blocking prompt; soft-update option for non-mandatory releases
Connectivity Check	Active connectivity monitoring; clear offline notice; auto-retry on reconnection without manual intervention

4.2 Security Requirements

Security Requirement	Implementation Specification
Secure Token Storage	JWT tokens stored exclusively in iOS Keychain or Android EncryptedSharedPreferences.
Certificate Pinning (Mobile)	HTTPS with SSL/TLS certificate pinning to prevent MITM attacks; pinning failure must terminate the connection immediately
Two-Factor Authentication (2FA)	2FA as second authentication layer; OTP via SMS and/or email; integrated with /auth/ OTP endpoints; enforced by server-side configuration
XSS Protection (Web)	All user input sanitized before rendering; no direct DOM injection; Content Security Policy headers configured
CSRF Protection (Web)	CSRF tokens implemented for all state-modifying requests



HMAC Signed Requests	Support HMAC-signed API request headers as required by the API Gateway configuration
No Hardcoded Credentials	No API keys, tokens, passwords, or environment URLs in source code; all secrets via environment variables
Session Cleanup on Logout	All tokens, session data, cached sensitive data, and biometric session data purged on logout

4.3 SSO — Sanad National Identity Integration

The application must support single sign-on via the Jordanian government Sanad identity platform.

Requirement	Specification
Login via Sanad	Implement Sanad SSO redirect flow using GET /auth/sso/sanad/redirect; handle OAuth callback and issue local session token via POST /auth/sso/sanad/issueToken
Registration via Sanad	Users with Sanad identity must complete registration using verified Sanad data, bypassing manual identity verification steps
UI Entry Point	A clearly labeled 'Login with Sanad' button on the login screen alongside standard username/password form
Error Handling	Sanad failures (expired session, user cancellation, service unavailable) handled gracefully with clear messages and fallback to standard login

4.4 Compliance with MODEE Digital Transformation Standards

The selected vendor shall comply with all applicable digital transformation standards issued by the Jordanian Ministry of Digital Economy and Entrepreneurship (MODEE) within the scope of this project, including UI/UX design, accessibility, user experience, mobile application standards, and Sanad integration requirements.

5. VENDOR ELIGIBILITY & QUALIFICATION REQUIREMENTS

Only vendors meeting all mandatory eligibility criteria will be considered for shortlisting. Proposals from vendors who fail to demonstrate compliance with the requirements in this section will be rejected without further evaluation.





5.1 Legal & Corporate Standing

#	Criterion	Evidence Required
1	Relevant Experience	Minimum three (3) similar projects completed within the last five (5) years, preferably in capital markets, financial services, investment platforms, or government digital services.
2	Company Experience	Minimum five (5) years of continuous operation in software development.
3	Technical Capability	Proven experience in web applications, mobile applications, API integrations, and secure digital platforms.
4	Support & Maintenance	The vendor must provide support during JST business hours, with 24/7 availability for critical issues.

6. REQUIRED PROJECT TEAM COMPOSITION

The vendor must assign a dedicated and experienced project team with named individuals for each role, including (but not limited to) a Project Manager, Flutter Developer, Frontend Developer, UI/UX Designer, QA Engineer, and DevOps Engineer.

CVs for all team members must be submitted as part of the technical proposal, covering employment history, project history, certifications, and measurable achievements. Subcontracting any of these roles requires prior written approval from SDC.

7. DELIVERABLES & PROJECT TIMELINE

7.1 Mandatory Deliverables

The following deliverables are not required at the time of proposal submission. They represent the full set of outputs that the selected vendor must produce and deliver to SDC throughout the project lifecycle, in alignment with the phases defined below.

#	Deliverable	Format	Phase
1	Discovery & Requirements Workshop Report	PDF document	Phase 0 — Kickoff

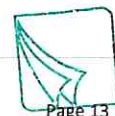


2	UI/UX Design System & Component Library	Figma file + export	Phase 1 — Design
3	Wireframes — All Screens (Mobile & Web)	Figma file	Phase 1 — Design
4	High-Fidelity Mockups (Mobile & Web)	Figma file + PDF	Phase 1 — Design
5	Interactive Prototype	Figma / InVision link	Phase 1 — Design
6	RTL Design Specification Document	PDF	Phase 1 — Design
7	Flutter Mobile Application (iOS & Android)	Source code + APK/IPA	Phase 2 — Development
8	Web Application (React.js or Vue.js)	Source code + production build	Phase 2 — Development
9	API Integration Test Report	PDF document	Phase 2 — Development
10	Security Assessment Report	PDF document	Phase 3 — Testing
11	User Acceptance Testing (UAT) Report	PDF document	Phase 3 — Testing
12	App Store Submissions (iOS & Android)	Published listings	Phase 4 — Deployment
13	Source Code Repository (Git)	Private GitHub/GitLab repo transferred to SDC	Phase 4 — Deployment
14	Technical Documentation	PDF + Markdown	Phase 4 — Deployment
15	Training Program for SDC Technical Team	Sessions + materials	Phase 5 — Handover
16	Post-Launch Support Plan (12 months)	PDF document	Phase 5 — Handover

7.2 Training Requirements

Upon project completion, the vendor is required to conduct a comprehensive training program for SDC's technical and operational teams. Training must cover:

- Full walkthrough of the delivered codebase and architecture





- Hands-on training for the mobile application (Flutter) for SDC developers
- Hands-on training for the web application for SDC developers
- API integration and troubleshooting guide
- UI/UX design system usage and extension guidelines
- Deployment, CI/CD pipeline, and app store update procedures
- Security procedures, token management, and incident response

8. EVALUATION & VENDOR SCORING CRITERIA

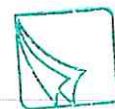
All technically compliant proposals will be evaluated using a weighted scoring model. The evaluation committee will assess each proposal against the criteria below. The total score is 100 points, distributed across technical and additional criteria. Only vendors achieving a minimum total score of 70 out of 100 will proceed the next stage of the tender evaluation.

8.1 Evaluation Criteria

#	Evaluation Criterion	Max Score
1	Technical Technical Solution & Compliance – Overall technical approach, architecture, security, UI/UX, mobile/web development, API integration, performance, scalability, and compliance with all RFP requirements.	40%
2	Technical Vendor Capability & Relevant Experience – Team qualifications, project experience, fintech expertise, and successful delivery of similar solutions.	40%
3	Additional Timeline & Value-Added Features	20%
TOTAL		100%

9. Submission Instructions

- Proposals must be submitted in English
- All documents must be submitted in both hard copy (2 sets) and digital format (USB drive or encrypted email)
- Digital copies must be in PDF format; editable files (DOCX, XLSX) are required for pricing documents





10. CONTRACTUAL & LEGAL TERMS

10.1 Project Ownership

All source code, design assets, documentation, and other deliverables developed under this engagement shall become the exclusive property of the Securities Depository Center upon full payment. The vendor shall retain no ownership, license, or usage rights to any deliverable unless otherwise agreed in writing by both parties.

10.2 Confidentiality

All vendors receiving this RFP must execute a Non-Disclosure Agreement (NDA) with SDC prior to receiving the API Postman collection or any technical specifications. Breach of confidentiality will result in immediate disqualification and may result in legal action.

10.3 Warranty & Defect Liability

The vendor must provide a minimum **24-month warranty** period covering all delivered software components. During this period, all defects must be classified by severity and resolved within the timeframes defined below.

Priority	Severity	Description	Resolution Time	Support Coverage
P1	Critical	System is completely unavailable or a core function is non-operational with no workaround	2 hours	24/7
P2	Medium	Minor feature issue with low business impact	5 business days	Business hours
P3	Low	Cosmetic issues, UI inconsistencies, or enhancement requests	Next release cycle	Business hours

Securities Depository Center

Jordan's Official Central Securities Depository

www.sdc.com.jo | Amman, Jordan



مركز إيداع الأوراق المالية
Securities Depository Center
رقم الحساب 1/3105/39
Page 15