SMART AFRICA TRUST SDK

Baseline Concept Architecture & Integration Model

Three-Part Architecture Baseline

Document purpose	Baseline for proposed TRUST SDK architecture, integration, institutional operations and governance
Prepared by	Cibernetica Ltd
Principal author	Patrick G. Ngabonziza — Chief Executive Officer / Team Leader / Intelligent Systems Architect
Version	1.0
Date	16 September 2026
Status	Concept baseline for EOI/RFP architecture development; subject to Smart Africa validation

Baseline status

This document consolidates the requirements already reflected in the Smart Africa TRUST SDK EOI material with additional architectural conclusions derived from the design review. Where the EOI/TOR does not explicitly prescribe an element, the document labels it as a proposed architectural completion rather than an existing Smart Africa requirement.

Document Control and Reading Guide

Classification	Meaning
TOR / EOI aligned	Requirement or design principle already reflected in the Smart Africa EOI/TOR material or the submitted technical concept.
Proposed architectural completion	A component or control identified as necessary to make the end-to-end operating model complete, but not yet specified in sufficient detail by the EOI.
RFP validation item	A point that must be confirmed with Smart Africa and pilot institutions during requirements validation before production design is frozen.

Contents

Executive Baseline

The TRUST SDK should be designed as a pan-African, cross-system trust-assessment layer for digital payments. Its primary value is not to replace domestic fraud engines, core banking platforms or payment switches. Its purpose is to provide a common, explainable trust assessment when a payment or user context crosses institutional, system or operator boundaries, with cross-border interoperability as the strategic priority.

The architecture therefore separates four concerns: the financial institution's transaction systems, a distributed TRUST processing plane, an institutional operations environment for human oversight, and a Smart Africa governance/control plane. This separation preserves institutional sovereignty while enabling common scoring, conformance, lifecycle governance and continental interoperability.

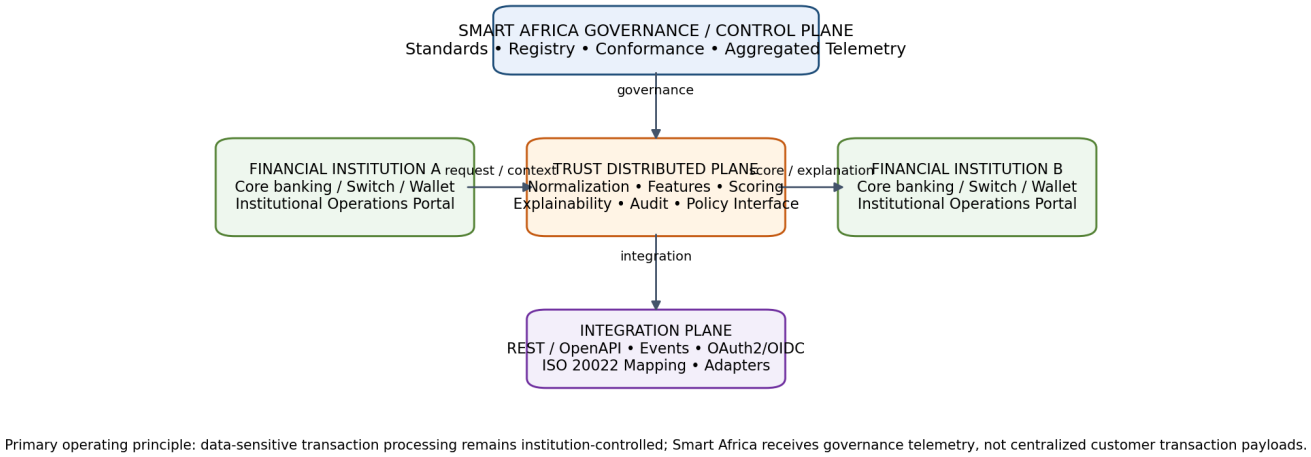

Figure 1. Proposed TRUST SDK target operating model.

Central architectural principle

Cibernetica builds and industrializes the TRUST technology; participating institutions execute payments and retain final decision authority; Smart Africa governs standards, conformance and ecosystem oversight.

PART I

Strategic Concept and Target Architecture

1. Purpose, Scope and Architecture Principles

1.1 Strategic objective

The final objective is to establish a reusable trust infrastructure that reduces uncertainty in interoperable digital payments across heterogeneous African payment ecosystems. TRUST should allow a participating institution to receive a consistent trust score, risk classification, confidence level, reason codes, contributing factors and a human-readable recommendation without surrendering its authority over the transaction or exposing unnecessary customer information.

1.2 Primary scope

- Cross-system transactions between banks, mobile-money operators, fintechs, payment service providers and other participating payment ecosystems.
- Cross-border digital payments, which represent the strategic priority of the IDECT context.
- Interoperability scenarios in which the originating institution cannot rely only on its own internal history and needs a common trust layer.
- Pilot and conformance environments used to validate SDK integration, models, controls and interoperability.

1.3 Scope boundary

Purely intra-system local transactions processed end-to-end inside one institution are not the primary purpose of TRUST. A bank may voluntarily invoke TRUST for such a transaction if a cross-system context, external counterparty or policy reason makes the common trust layer relevant, but TRUST should not be positioned as a mandatory replacement for the bank's existing fraud, AML/CFT or transaction-monitoring controls.

1.4 Architecture principles

Principle	Baseline interpretation
Advisory, not authoritative	TRUST recommends; the participating institution makes the final payment or risk decision.
Distributed and sovereign	Sensitive transaction processing and detailed audit remain in approved institutional or sovereign environments.
Explainable by design	Every assessment exposes score, risk, confidence, reason codes and understandable evidence.
Interoperable by design	REST/OpenAPI, JSON, events and ISO 20022 mappings support heterogeneous systems.
Vendor-neutral	No core-banking, cloud or model vendor becomes a mandatory dependency.
Minimum necessary disclosure	Institutions receive only the information required for the transaction or approved operational purpose.
Auditable and reproducible	Every assessment can be reconstructed using versioned request schema, feature schema, model, policy and SDK versions.
Human-governed AI	Model approval, deployment, rollback, monitoring and bias/drift controls are governed processes.

2. Target Operating Model

The target architecture comprises four planes. These planes are logical separations; they may be deployed in different physical topologies depending on pilot institution, sovereignty requirements and Smart Africa's final operating model.

Plane	Purpose	Typical owner/operator
Institution Transaction Plane	Core banking, payment switch, mobile wallet, gateway, fraud/AML controls and final authorization.	Participating institution
TRUST Distributed Plane	Normalization, feature engineering, scoring, explainability, advisory recommendation, detailed local audit.	Institution or approved operator environment
Institutional Operations Plane	Human review, investigation, local policies, cases, local reporting, user administration and audit.	Participating institution
Smart Africa Governance / Control Plane	Registry, approved SDK/model versions, conformance, certification, aggregated telemetry, ecosystem governance.	Smart Africa or designated operator

2.1 Why the institutional operations plane is required

The EOI architecture correctly preserves the institution's final approval/rejection authority, but an end-to-end operating model also needs a defined human operational interface. Without such an interface, TRUST can generate a recommendation but the institution lacks a standardized environment to investigate, understand, audit and operationalize that recommendation. The Institutional Operations Portal is therefore a proposed architectural completion, not a claim that the EOI already defines the portal in detail.

2.2 Smart Africa's role

Smart Africa should be positioned primarily as ecosystem governor rather than a centralized payment processor. Its role includes defining common specifications, approving release/conformance policy, maintaining relevant registries, supervising ecosystem health through privacy-preserving telemetry and coordinating certification. The precise post-project 24/7 operating responsibility remains an RFP validation item.

3. Core TRUST Functional Architecture

Component	Function	Output / evidence
Integration Gateway	Authenticate institutions, validate requests, route API/event traffic, enforce schema/version policy.	Validated transaction request, API audit event

Component	Function	Output / evidence
Metadata Normalization	Convert source-system fields into the canonical TRUST metadata contract.	Canonical TransactionTrustRequest
Data Quality & Validation	Check required fields, ranges, completeness and metadata confidence.	Validation status, metadata quality score
Feature Engine	Transform normalized metadata into explainable behavioral and contextual features.	Versioned feature vector
Trust / Risk Engine	Generate trust score, risk classification and confidence.	Score, category, confidence, model version
Explainability Engine	Generate reason codes, feature contributions and human-readable explanation.	Explanation package
Policy Interface	Translate assessment into an advisory action without overriding institutional policy.	Recommendation
Audit Engine	Capture reconstructable evidence for each assessment.	Audit reference and full local trace
Telemetry Agent	Publish non-PII operational metrics to governance plane.	Volumes, latency, errors, availability, versions
Model Governance	Control model candidate, validation, approval, deployment, rollback, drift and bias monitoring.	Governed model lifecycle evidence
Conformance Suite	Verify API, security, interoperability and approved behavior.	Pass/fail evidence and certification inputs

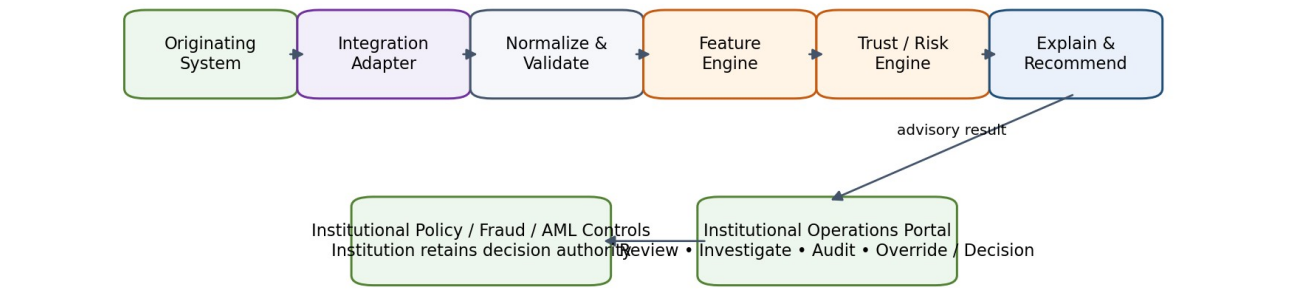

Figure 2. Transaction-scoped TRUST assessment and institutional decision flow.

PART II

Financial-Institution Integration and Operations

4. Integration Boundaries and Core-Banking Relationship

TRUST must integrate with financial institutions, but the integration should not be defined universally as a direct core-banking integration. Different institutions expose transaction context through different architectural layers. TRUST should therefore connect through the most appropriate controlled integration point.

Integration point	Typical use	Design position
Payment switch / payment hub	Real-time transaction orchestration and routing.	Preferred when it provides the required transaction context with minimal core impact.
API gateway / enterprise service bus	Standardized institutional integration and security boundary.	Preferred for governed API access.
Fraud / AML / risk platform	Existing institutional risk workflow.	Useful for policy combination and case handling.
Core banking system	Account and ledger context when required.	Supported, but avoid intrusive direct coupling unless necessary.
Mobile-money / wallet platform	Wallet-originated cross-system payment context.	Direct adapter or API integration.
Fintech / PSP platform	Digital payment or merchant ecosystem context.	REST/event integration according to approved contract.

Integration rule

TRUST should read only the minimum metadata required for trust assessment and should not post directly to the institution's ledger. The institution remains responsible for payment execution and final authorization.

4.1 Canonical integration contract

The canonical request must be stable enough to support multiple institutional systems without forcing all participants to expose the same internal data model. The baseline contract should include transaction identifiers, source/destination ecosystem, country/corridor, transaction type, amount band or permitted amount representation, device context, account/counterparty maturity, transaction velocity, authentication strength and metadata quality. Direct identifiers should be minimized, tokenized or pseudonymized where behavioral continuity requires linkage.

5. Transaction Trust Flow and APIs

1. The originating system identifies a transaction requiring cross-system TRUST assessment.

2. The institutional adapter maps source fields to the canonical metadata contract and applies data-minimization rules.
3. The TRUST gateway authenticates the caller, validates API/schema versions and performs input validation.
4. The feature engine derives versioned behavioral/contextual evidence from the permitted metadata.
5. The trust/risk model produces score, risk category and confidence.
6. The explainability engine produces reason codes, contributing factors and a human-readable explanation.
7. The policy interface returns an advisory recommendation to the institution.
8. The institution combines TRUST with its own fraud/AML/business rules and takes the final decision.
9. A detailed local audit trace is retained according to institutional and regulatory policy.
10. Only approved operational telemetry is sent to the Smart Africa governance plane.

5.1 Baseline API services

Service	Indicative purpose
POST /trust/assessments	Submit a transaction-scoped trust assessment request.
GET /trust/assessments/{id}	Retrieve the assessment visible to the requesting institution.
GET /trust/audit/{reference}	Retrieve authorized reconstructable evidence for the institution's own case.
GET /trust/models/approved	Retrieve models/versions approved for the tenant/deployment.
GET /trust/sdk/version	Expose SDK/API compatibility state.
POST /trust/events	Optional asynchronous submission path.
GET /trust/conformance/status	Expose approved conformance/certification status to authorized parties.

Endpoint names are conceptual placeholders. Final API paths, payloads, authentication scopes and error models must be frozen during RFP requirements validation and reflected in OpenAPI documentation.

6. Institutional Operations Portal

Classification

Proposed architectural completion. The need follows from the institution retaining decision authority and requiring explainability, investigation and audit, but the EOI material does not yet prescribe the full portal in detail.

Each participating institution should have a logically isolated tenant or deployment view. The portal must never become a mechanism for one bank to browse another bank's operational data.

Module	Institutional capability
Operations Dashboard	Volumes, current alerts, risk distribution, service status and latency for the institution's own deployment.
Transaction Assessments	Search and inspect the institution's own TRUST assessments.
Risk Alerts & Cases	Queue high-risk or policy-triggered cases for investigation.
Explainability	Display score, confidence, reason codes, feature contributions and human-readable explanation.
Institutional Decision	Capture approve/review/reject/step-up or other institution-defined outcomes when the workflow requires human action.
Policies	Manage institution-specific thresholds and permitted policy mappings, subject to governance boundaries.
Models & Versions	View approved model/SDK versions deployed to the institution; local users cannot deploy unapproved versions unless governance permits.
Integration	View API credentials/scopes, adapter health, schemas and connectivity status.
Audit & Reports	Retrieve authorized audit evidence, case history and compliance reports.
Users & Roles	Institution-scoped RBAC, MFA and segregation of duties.
System Health	Deployment status, error rate, latency, availability and local operational events.

6.1 Institutional personas

Persona	Typical permissions
Fraud / Risk Analyst	Review alerts, inspect explanations, create/update cases, record disposition.
Compliance Officer	Review relevant cases and audit evidence; access

Persona	Typical permissions
	approved compliance reports.
Operations Manager	Monitor volumes, latency, errors and operational thresholds.
Institution Administrator	Manage institution users, roles, integration configuration and approved local settings.
Auditor	Read-only access to authorized audit evidence and decision history.
Technical Integrator	Manage API integration, schemas, certificates and test/conformance evidence within assigned scope.

7. Deployment and Interoperability Patterns

Pattern	Description	Use case
Operator-hosted	TRUST processing components run inside or adjacent to the institution's controlled environment.	Strongest institutional data sovereignty.
Sovereign national cloud	Approved national environment hosts components for one or more institutions under defined isolation.	National digital infrastructure model.
Regional trusted environment	Regional deployment with strict tenant isolation and data-governance controls.	Cross-border regional implementation where approved.
Smart Africa sandbox	Controlled environment for demonstrations, conformance and pilot integration; not assumed to hold production payloads.	Testing, onboarding and certification.

7.1 Interoperability stack

- REST/JSON described through OpenAPI for synchronous assessment.
- Event-driven/asynchronous integration for high-throughput or decoupled institutional workflows.
- OAuth2/OIDC-compatible patterns, mTLS or equivalent certificate-based controls as required by the final security architecture.
- ISO 20022 mapping between payment message content and the TRUST canonical metadata model where applicable.

- Versioned schemas and backward-compatibility policy to avoid coordinated “big bang” upgrades across institutions.

PART III

Governance, Data Access, Security and Lifecycle

8. Smart Africa Governance Role

Smart Africa’s baseline role should be ecosystem governance rather than centralized transaction execution. The governance plane maintains the common rules and evidence needed for interoperability while the institution remains responsible for its customers, transaction execution and final decisions.

Smart Africa capability	Baseline scope
Institution Registry	Participating institutions, identifiers, status, approved endpoints or deployment references.
SDK / API Registry	Approved SDK/API versions, compatibility and deprecation policy.
Model Registry	Approved model versions, validation state, release/rollback status and applicable deployment scope.
Conformance & Certification	Conformance results, certification state and lifecycle evidence.
Ecosystem Telemetry	Aggregated volumes, latency, availability, errors, versions and model usage without routine customer-identifiable payloads.
Governance Policy	Common security, data-governance, release, incident and interoperability requirements.
Pilot / Sandbox Governance	Controlled environments for onboarding, testing and demonstration.
Reporting & Oversight	Cross-institution operational trends and compliance status at a level that does not expose another institution’s protected internal data.

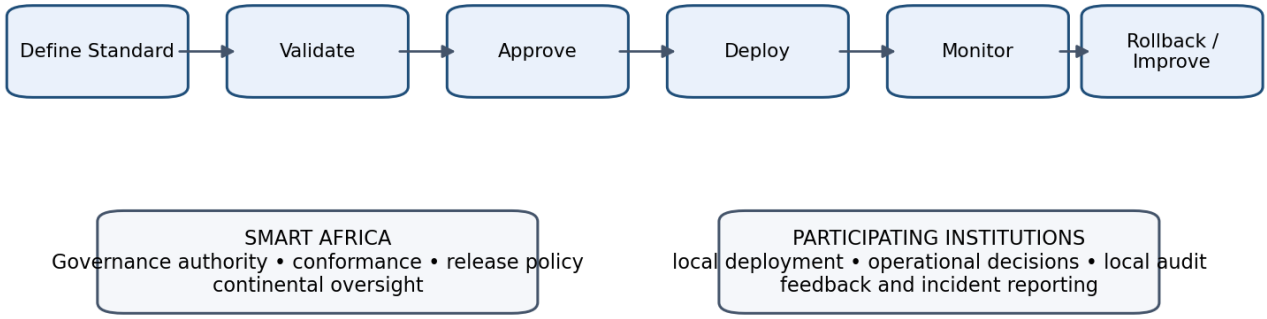

Figure 3. Governed SDK/model lifecycle shared between Smart Africa and participating institutions.

9. Institutional Data Access and Disclosure Model

The platform must distinguish three data zones: institution-private data, transaction-scoped TRUST exchange data and Smart Africa governance telemetry. This is necessary to prevent the common but unsafe assumption that a pan-African trust platform implies a pan-African centralized data lake.

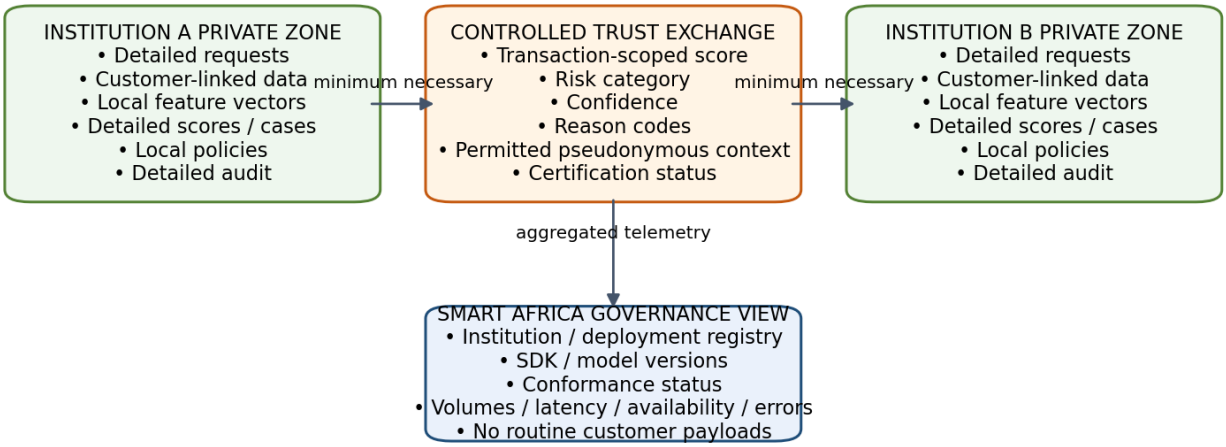

Figure 4. Proposed data-visibility and disclosure zones.

9.1 What an institution may see about its own activity

- Its own submitted assessment requests and permitted metadata.
- Its own trust scores, risk categories, confidence levels, reason codes, feature contributions and recommendations.
- Its own cases, institutional decisions, policy versions and detailed audit evidence.
- Its own deployment health, SDK/model versions, integration state, errors and performance.

9.2 What an institution may receive about another institution or counterparty

Only data required for the active cross-system trust purpose should be disclosed. Depending on the approved data-sharing policy, this may include a transaction-scoped trust signal, pseudonymous counterparty context, corridor-level indicators or a public/authorized conformance status. Any such disclosure must be purpose-bound, minimum-necessary and auditable.

9.3 What an institution should not see about another institution

- Detailed transaction-by-transaction scores unrelated to the requesting institution's authorized transaction or case.
- Other institutions' internal test datasets, detailed validation results or non-public security findings.
- Other institutions' customer identities, account numbers, balances, transaction histories or internal case notes.
- Other institutions' proprietary thresholds, detection rules, feature configurations or internal policy logic unless explicitly designated as common TRUST policy.
- Detailed performance or incident data that Smart Africa has not approved for ecosystem-wide disclosure.

Data item	Owning institution	Counterparty institution	Smart Africa
Own transaction request detail	Full, policy-controlled	No, except minimum transaction-scoped fields if required	No routine access
Own TRUST score / explanation	Full	Only if transaction-scoped disclosure policy requires it	Aggregated/telemetry only unless authorized
Detailed audit trace	Full	No	Exceptional governed access only if contract/regulation permits
SDK/model version	Full	May be visible for compatibility	Yes
Conformance status	Full	Yes if designated shareable	Yes
Customer identity / account data	Full under local rules	No	No routine access
Aggregated latency / availability	Full local view	No detailed peer view	Yes, governance telemetry
Internal test data / vulnerability detail	Full local/authorized	No	Restricted governed access where required

10. Security, Model Governance and Conformance

10.1 Security baseline

- Least-privilege identity and access management with institution-scoped RBAC and administrative MFA.
- TLS in transit and encryption at rest; secure key, secret and certificate lifecycle management.
- Strong tenant isolation across institutions and environments.
- Data minimization, pseudonymization/tokenization and retention controls.
- Tamper-evident or tamper-resistant audit event capture appropriate to the final environment.
- Secure SDLC, dependency management, vulnerability scanning, penetration testing and remediation evidence.
- Backup, recovery, high availability and resilience appropriate to production criticality.

10.2 Model governance baseline

11. Register a candidate model and its feature schema/version.
12. Validate accuracy, explainability, stability and data-quality sensitivity using approved pilot datasets.
13. Perform bias/fairness and security/robustness checks appropriate to the available data and use case.
14. Approve the model through the defined governance authority.
15. Deploy only to authorized environments and record the exact model/SDK/API versions.
16. Monitor drift, performance, confidence distribution, errors and operational health.
17. Rollback to a previously approved model when safety or performance criteria are violated.

10.3 Conformance and certification

Conformance should test more than whether an API returns HTTP 200. It should verify schema correctness, authentication, authorization, data minimization, score/explanation contract, model/version evidence, audit completeness, interoperability mappings, error behavior, performance, observability and prohibited-data leakage. Certification should be based on reproducible evidence and tied to a specific SDK/API/model/deployment combination.

11. Operating Model, Responsibilities and Handover

Responsibility	Smart Africa	Participating institution	Technology implementer / support
Define common TRUST standard	A/R	C	C
Operate transaction system	I	A/R	C
Final transaction decision	I	A/R	I
Maintain institution data sovereignty	C	A/R	C

Responsibility	Smart Africa	Participating institution	Technology implementer / support
Approve common SDK/model releases	A/R	C	R for technical evidence
Operate local TRUST deployment	Governance oversight	A/R or designated operator	R/C depending contract
Institutional cases and decisions	I	A/R	Support only as authorized
Aggregated ecosystem telemetry	A/R	R for local telemetry agent	R for platform implementation
Conformance and certification	A/R	R for evidence	R for suite/tooling
Incident response	A for ecosystem coordination	A/R locally	R for technical support under SLA
Documentation and knowledge transfer	A for acceptance	R for operational adoption	A/R for technical handover

Legend: A = Accountable, R = Responsible, C = Consulted, I = Informed. Final allocation must be contractually confirmed; this table is a baseline operating model rather than a substitute for the eventual service-management agreement.

12. Baseline Decisions and RFP Validation Register

ID	Baseline decision	Status
BAD-01	TRUST is an advisory cross-system trust layer; it does not replace institutional payment authorization.	Baseline
BAD-02	Cross-border and cross-system transactions are the primary scope; purely intra-system local transactions are not the primary target.	Baseline
BAD-03	Integration is through the appropriate institutional transaction/integration layer; direct core-banking coupling is supported	Baseline

ID	Baseline decision	Status
	only when necessary.	
BAD-04	Detailed transaction data and detailed audit remain institution-controlled; Smart Africa receives privacy-preserving governance telemetry by default.	Baseline
BAD-05	Each institution requires an operational interface for review, explainability, cases, local audit and administration.	Proposed completion
BAD-06	No institution may browse another institution's detailed scoring, tests, customer data, internal policies or security findings.	Proposed control
BAD-07	Cross-institution disclosure is transaction-scoped, minimum-necessary, purpose-bound and auditable.	Proposed control
BAD-08	Smart Africa maintains governance registries, conformance/certification and lifecycle oversight; exact 24/7 operator model is to be confirmed.	RFP validation
BAD-09	Model and SDK lifecycle must support approval, versioning, deployment, monitoring and rollback.	Baseline
BAD-10	The production design must preserve vendor neutrality, versioned interoperability and independent maintainability.	Baseline

12.1 RFP validation questions

- Who operates the Smart Africa governance/control plane after project acceptance, and under what SLA?
- Which institutions and transaction corridors will participate in the contractual pilot?
- What exact transaction metadata may be exchanged across institutions and jurisdictions?
- Which party is the controller/processor for each data class and deployment pattern?

- Which cross-institution trust indicators are permitted to be disclosed to a counterparty institution?
- What is the required latency, throughput and availability target for real-time assessment?
- What are the required retention periods for detailed local audit and aggregated governance telemetry?
- What certification status and test evidence may be visible to peer institutions?
- What exact Smart Africa approval authority applies to model, SDK, API and policy versions?
- What regulatory, data-residency and cross-border-transfer constraints apply to each pilot country?
- What support model is required after handover: Smart Africa internal team, managed service, or hybrid?
- What pre-existing Cibernetica components remain background IP versus project-specific deliverables under the final contract?

Annex A — Requirements-to-Architecture Traceability

Requirement / concern	Architecture response	Evidence / deliverable
Cross-system trust scoring	Canonical request + feature engine + trust/risk engine	API contract, feature schema, model evidence
Explainability	Separate explainability service/module	Reason codes, factor contributions, human-readable explanation
Institution retains decision authority	Policy interface + institutional decision workflow	Decision trace and audit reference
No centralized production transaction store	Distributed deployment + local detailed audit	Deployment architecture and data-flow evidence
Interoperability	Adapters, REST/OpenAPI, events, ISO 20022 mapping	Integration specifications and conformance tests
Security	IAM, MFA, TLS, encryption, secrets, audit, secure SDLC	Security architecture and test evidence
Model lifecycle	Registry, approval, deployment, monitoring, rollback	Model governance records
Operational oversight	Institution portal + Smart Africa control plane	Dashboards, telemetry and role model
Conformance	Automated conformance suite and certification framework	Repeatable test results and certification state
Handover	Versioned source, deployment packages, docs, training and test evidence	Technical handover package

Annex B — Reference Architecture Data Objects

B.1 Canonical TransactionTrustRequest

Indicative fields: transaction reference, source system, destination system, origin country, destination country, transaction type, currency, permitted amount representation or amount band, account age, device status, transaction velocity, counterparty age, corridor frequency, authentication strength, metadata quality, schema version and request timestamp. Identifiers must follow the approved tokenization/pseudonymization policy.

B.2 TrustAssessmentResult

Indicative fields: trust score, risk category, confidence, recommendation, reason codes, feature contributions, human-readable explanation, model version, SDK version, API version, feature-schema version, policy version, processing latency and audit reference.

B.3 GovernanceTelemetryEvent

Indicative fields: pseudonymous operator/deployment identifier, SDK version, model version, transaction-assessment count, average/percentile latency, availability, error count/rate, model usage and timestamp. Customer identity, account number and payment payload are excluded by default.

Source Basis

This baseline consolidates the Smart Africa TRUST SDK EOI submission, the preliminary technical concept and demonstration material, the demonstrator user manual, and the architecture decisions developed during the associated design review. It intentionally distinguishes documented EOI/TOR principles from proposed architectural completions that require Smart Africa validation at RFP/inception stage.

Baseline Acceptance

This document should be used as the starting architecture baseline for the next detailed design stage. No production interface, data-sharing rule, model, deployment topology or operating responsibility should be treated as frozen until validated against the final Smart Africa RFP, participating-institution requirements, pilot-country regulations and approved security/data-governance requirements.