SmartCampus Suite

Software Product Description (SPD)

1. Product Overview

SmartCampus Suite is a campus-wide physical access and entitlements platform. It manages badge/mobile credentials, fine-grained privileges, cafeteria access, and user information. It integrates with campus identity systems, door controllers, and point-of-sale (POS) to enforce policies in real time and provide auditable records.

Primary Users: Students, faculty, staff, visitors/contractors, security operations, HR/registrar, facilities, cafeteria managers.

Primary Hardware/Edges: Door readers & controllers, turnstiles, kiosks, POS terminals, printers/encoders.

2. Goals & Non-Goals

Goals

- Centralize identity, credentials, and access privileges across campus facilities.
- Support both card and mobile credentials (BLE/NFC) with rapid revocation (<60s).
- Handle cafeteria entitlements (meal plans, subsidies, allowances) and POS authorization.
- Provide real-time monitoring, audit trails, and compliance reporting.
- Maintain operations during network loss via edge/reader caches; sync when online.

Non-Goals

- Building automation (HVAC/lighting) beyond access events (integrations optional).
- Payment processing gateway; SmartCampus authorizes entitlements, not card settlement.

3. Success Metrics (KPIs)

- **<300 ms** average access decision at edge; **P95 < 500 ms**.
- **<60 s** credential revocation propagation to all online controllers.
- **99.95%** monthly service availability (cloud core), **>24h** offline edge operation.
- **Audit completeness 100%** (no gaps), log latency **<15 s** to central store.
- **POS authorization**: P95 decision time **<300 ms**.

4. System Context

- **Upstream Systems:** SIS/Registrar, HRIS, Directory (AD/LDAP), SSO (SAML/OIDC), Payment provider, Facilities/BMS (optional), Email/SMS providers.

- **Downstream/Devices:** Door controllers/readers (OSDP preferred, Wiegand legacy), POS terminals, Badge printers, Visitor kiosks.

5. Key Features

1. **Identity & Credentialing**: Persons, affiliations, statuses; badge lifecycle (issue, replace, suspend, revoke), mobile credentials, PINs.
2. **Access Control**: Areas/zones, schedules, rules, anti-passback, visitor passes, emergency lockdown/unlock, escort rules.
3. **Entitlements**: Meal plans, daily/weekly allowances, dietary/allergen flags, staff/subsidy policies, time-windowed offers.
4. **POS Authorization**: Online/offline authorization, wallet/balance, per-item restrictions, spend limits, exemptions.
5. **Policy Engine**: Attribute- and role-based (RBAC + ABAC) evaluation with precedence and exceptions.
6. **Audit & Reports**: Tamper-evident event logs, privilege change history, attendance, capacity, compliance (FERPA/GDPR), anomaly detection.
7. **Self-Service Portal**: Lost badge reporting, temporary QR, viewing allowances, transaction history, schedule requests.
8. **Admin Console**: Real-time door status, maps, bulk operations, rule simulation ("why denied"), approval workflows.

6. Personas & User Stories (samples)

- **Security Admin**: "As a security admin, I can create an access zone and assign it to all dorm doors; changes go live within 1 minute."
- **Cafeteria Manager**: "I can define a meal plan allowing 3 swipes/day, reset at 4am, with gluten-free restriction alerts."
- **Student**: "I can add a mobile credential, report my card lost, and receive a temporary QR valid for 48 hours."
- **Registrar/HR**: "When a student withdraws or staff is terminated, access and entitlements revoke automatically."

7. Functional Requirements

7.1 Identity & Data

- Maintain **Person** (global ID), affiliations (student, faculty, staff, contractor, visitor), program/department, status, and contact.
- Credential types: **Card** (e.g., DESFire EV3/Seos), **Mobile** (BLE/NFC), **PIN/QR (temporary)**.
- Photo capture, card printing/encoding, batch import via SCIM/CSV.

7.2 Access Privileges

- Zones, doors, schedules, holidays, anti-passback, two-person rule, muster points.
- Policy: `(role ∧ schedule ∧ zone) ∨ (exception)` with ABAC (e.g., dorm ≡ resident=true).

- Edge cache capacity: ≥100k identities, ≥10k rules per controller.

7.3 Entitlements & Cafeteria

- Plans: unlimited, N swipes/day, currency/wallet, time windows, location scopes.
- Restrictions: allergens/dietary flags, age limits, item categories.
- Wallets: pre-paid, subsidies, staff discounts; auto top-ups via provider.
- POS offline mode with deferred sync; double-spend protection via token windows.

7.4 Events & Audit

- Event types: access_granted/denied, door_forced, door_held, panic, plan_consumed, top_up, refund, privilege_changed.
- Tamper-evident hashing chain; export to SIEM (CEF/LEEF), webhooks and Kafka.

7.5 Visitor Management

- Pre-registration, host approvals, ID scan, temporary badges/QR, expiration and watchlist checks.

7.6 Emergency Operations

- One-click global lockdown/unlock, rules override by role, broadcast to controllers with confirmation fan-out.

8. Non-Functional Requirements

- **Security**: TLS 1.3, HSTS, FIPS-validated crypto where required; AES-256 at rest; PBKDF2/Argon2 for secrets; HSM/KMS for keys.
- **Privacy & Compliance**: FERPA (US), GDPR (EU), CCPA (CA) principles; consent records; data minimization; subject request workflow.
- **Reliability**: Active-active cloud core; controller offline operation ≥24h; RPO ≤ 15 min; RTO ≤ 2 h.
- **Performance**: See KPIs; controllers process >200 transactions/minute.
- **Scalability**: 100k+ active users, 2k+ doors, 50k POS tx/day.
- **Observability**: Central logs, metrics (Prometheus/OpenTelemetry), alerts (PagerDuty/Email/SMS).

9. Data Model (logical)

Entities

- `Person(person_id, name, dob, email, phone, affiliation, status, department, photo_id, created_at, updated_at)`
- `Credential(credential_id, person_id, type, technology, enc_key_ref, state, issued_at, revoked_at)`
- `Role(role_id, name, description)` and `PersonRole(person_id, role_id)`
- `Zone(zone_id, name, description)`; `Door(door_id, zone_id, controller_id, reader_id, state)`

- `Schedule(schedule_id, name, cron/rrule, exceptions)`
- `Policy(policy_id, expression, priority, active)`
- `Entitlement(entitlement_id, person_id, plan_id, balance, window, restrictions)`
- `Plan(plan_id, name, type, limits, reset_rule)`
- `PosTransaction(tx_id, person_id, location_id, items, amount, entitlement_used, status, ts)`
- `Event(event_id, type, subject_id, payload_json, hash, prev_hash, ts)`

Indexes: `Event(ts,type)`, `Credential(person_id,type,state)`, `Entitlement(person_id)`, `PosTransaction(person_id, ts)`.

10. APIs (v1)

Auth: OAuth2/OIDC for users; mTLS + PAT for devices/controllers; SCIM 2.0 for provisioning.

REST (examples)

- `POST /v1/persons` – create person
- `POST /v1/persons/{id}/credentials` – issue credential
- `POST /v1/access/authorize` – policy decision (door_id, person_id, ts)
- `POST /v1/entitlements/authorize` – POS decision (person_id, items, location)
- `POST /v1/events` – device event ingest
- `POST /v1/lockdown` – emergency broadcast
- `GET /v1/reports/audit?from=..&to=..`

Webhooks: `credential.revoked`, `access.denied`, `pos.entitlement.used`, `security.alert`.

Device Edge Protocols: MQTT/HTTPS for controllers; OSDP v2 (secure channel) preferred to readers.

11. Security Architecture

- **Credential Security**: MIFARE DESFire EV3/Seos or mobile credentials with mutual auth; diversified keys; anti-clone counters; rolling nonces.
- **Policy Engine**: Deterministic evaluator; signed policy bundles; simulators for "explain deny/grant".
- **Least Privilege**: RBAC with scoped admin roles (Security Admin, Entitlements Admin, POS Admin, Auditor, Operator, Helpdesk).
- **Secrets**: Central KMS, per-tenant keys, quarterly rotation; no secrets in device configs.
- **Data Protection**: PII encrypted at rest; field-level encryption for DOB, contact; PANs never stored (tokenized by payment provider).
- **Audit**: Immutable log with chain hashing; write-ahead to local edge when offline; periodic notarization.
- **Threats & Mitigations**
  - Card cloning → secure tech + diversified keys + replay protection.
  - Tailgating → anti-passback, camera/analytics integration, random audit prompts.
  - DoS on controllers → local allowlists, rate limits, watchdogs.

- Insider misuse → dual control on lockdown, segregation of duties, approval flows.

12. Deployment Architecture

- **Cloud Core (SaaS)**: API, Policy, Identity, Entitlements, Event Ingest, Reporting, Admin & Portal UIs.
- **Edge Gateway** (on-prem VM/appliance): Device broker, local cache, offline queue, secure update channel.
- **Controllers/Readers**: Vendor-agnostic via OSDP; policy & credential cache; signed firmware updates.

Environments: Dev, Test, Staging, Prod; blue/green deploys for core; ringed rollout for edges.

13. Operations

- **CI/CD**: Git + build pipelines; SAST/DAST; SBOM; signed artifacts.
- **Monitoring**: Uptime, decision latency, queue depth, sync lag, device health.
- **Backups & DR**: Daily encrypted backups, point-in-time for databases; DR runbooks; quarterly restore tests.
- **Data Retention**: Events 2 years (configurable), POS tx 7 years, access denials 2 years, PII per policy with purge workflows.

14. UI Modules (high-level)

- **Command Center**: Live map, door states, alarms, lockdown controls.
- **Identity**: Person search, credential issuance, photo capture, role & policy assignment, history.
- **Entitlements**: Plan designer, balances, bulk ops, restrictions, refunds.
- **Reports**: Audit explorer, attendance, capacity, exception reports, POS summaries.
- **Self-Service**: My ID, mobile credential, lost badge, temporary QR, meal plan view.

15. Data Privacy & Ethics

- Privacy by design, consent where applicable, clear retention policies, opt-out for analytics, DPIA templates.
- Access to PII requires elevated roles; purpose-bound data usage; regular privacy reviews.

16. Testing & Acceptance

- **Unit/Integration**: Policy evaluation, entitlement authorization, sync & offline queues.
- **Performance**: Load tests to target KPIs; chaos tests for edge offline.
- **Security**: Pen tests, red-team scenarios, reader/controller hardening checks.
- **UAT Criteria**: Sample policies, 50 doors, 5k users, POS sandbox, emergency drill.

17. Open Questions / Assumptions

- Target reader/controller vendors and protocols beyond OSDP? Any legacy Wiegand constraints?
- Payment provider(s) for wallet top-ups and settlement.
- Regional compliance scope (FERPA/GDPR/others) per tenant.
- Exact retention requirements by institution.

18. Glossary

- **ABAC**: Attribute-Based Access Control
- **RBAC**: Role-Based Access Control
- **OSDP**: Open Supervised Device Protocol
- **SIS**: Student Information System
- **POS**: Point of Sale

Version: 4.3.0.9 **Document Owner**: Product Management – Iuliia Drabik

Reviewers: Security, IT Ops, Facilities, Cafeteria Operations