SYMBEEO

PUBLIC

SOLUTION DESIGN DOCUMENT

Mobility design for a typical buyer: distribution-center Wi-Fi 7, yard private 5G, UEM and zero-trust endpoints, applying SRA-MOB-001

Design document (HLD + LLD)

CAPABILITY	DOCUMENT	VERSION	DATE
Mobility	SDD-MOB-001	1.1	Oct 10, 2026

WRITTEN BY

Mark Winston, Principal Network Architect

© 2026 Symbeeo. All rights reserved.

What this document is. SRA-MOB-001 applied to one client, with names, numbers, addresses, enrollment profiles and a cut-over plan, in the shape SDD-NET-001 uses. The client is the typical buyer from SRA-MOB-001 §1 [A]; every value marked [A] is replaced by the real client's during the design workshop. **No platform model is named:** each device role carries the class SRA-MOB-001 §5 defines, and the model is written in from the buyer's comparison (P4).

Document control

Document	SDD-MOB-001	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Mobility	Author	Mark Winston
Role	Principal Network Architect	Applies to	SRA-MOB-001 v1.0
Tested by	STP-MOB-001		
Credentials	CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026.		
Sign-off	"The customer's named representative signs this document before build; the practice lead signs it after."		

Contents

1 · Introduction 3
2 · Prerequisites (all must be true before build) 4
3 · Solution overview 4
4 · Logical design 5
5 · Physical design 6
6 · Services 6
7 · Migration and cut-over 7
8 · Roles and deliverables 7
9 · Security, lifecycle and handover 8

© 2026 Symbeeo. All rights reserved. · Public

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. Mark Winston remains the author.

1 · Introduction

1.1 Purpose.

Technical design for Wi-Fi 7 and private 5G at the distribution center (branch 3), the mobile SSID profile at every site, one UEM, and the device signals the SRA-SEC-001 policy engine decides on. After review, the client signs and work continues to build.

1.2 Project overview and goals.

Replace the distribution center's Wi-Fi 5 estate [A]; cover the yard with private 5G; move every corporate device to automated enrollment with a hardware-bound certificate; separate BYOD data; retire WPA2. Goals: SRA-MOB-001 R2, R6, R7, R9, R13 and R18.

1.3 Approach and phases.

Phase 1 spectrum authorization and survey. Phase 2 UEM and certificates, pilot group. Phase 3 distribution-center Wi-Fi 7, zone by zone. Phase 4 yard private 5G. Phase 5 fleet re-enrollment by device group. Phase 6 legacy SSID closed, decommission and as-built.

1.4 Change control and reporting.

- **Design changes.** Once this document is signed, any change to it — scope, site, device count, model, phase or date — is a **written change order** stating what changes, why, and its cost and schedule effect. Both parties sign it before the change is built. Nothing is built from a verbal request.
- **Operational changes.** Every change is a ticket in the client's change system citing this document's section and, where it alters the design, the change-order number; emergency changes are recorded within 24 hours.
- **Weekly status report.** Every week from signature to acceptance: % complete per deliverable (§8) and per phase (§1.3), slippage against the signed plan in days with its cause, change orders open and signed.
- **Escalation.** Contacts named by role on both sides, in §8.

1.5 Intended audience.

Client infrastructure and end-user computing teams; Symbeeo build engineers; the client's security team for §4.5–4.6.

1.6 Related documents.

SRA-MOB-001 · STP-MOB-001 · SRA-NET-001 / SDD-NET-001 (campus wireless, VLAN plan) · SRA-SEC-001 (policy engine) · sources listed in SRA-MOB-001 §9.

© 2026 Symbeeo. All rights reserved. · Public

2 · Prerequisites (all must be true before build)

Table 2. Prerequisites (all must be true before build)

#	Prerequisite	Owner	Status
P1	Spectrum authorization for the yard on file (R8); SAS or license registration complete	client	open
P2	Predictive Wi-Fi design signed for the distribution center, racking loaded (R2)	Symbeeo	open
P3	Predictive RF design signed for the yard, vehicle routes marked (R6)	Symbeeo	open
P4	Buyer's comparison closed; one model per device role written into §3.2	client	open
P5	Apple and Android enterprise enrollment accounts linked to the UEM; reseller device IDs flowing	client	open
P6	Certificate authority issuing over ACME / SCEP with attestation checking (R11)	client	open
P7	SRA-SEC-001 policy engine accepting UEM compliance and RADIUS over TLS (R19)	client	open
P8	Device-model inventory with each model's security-update end date (R17)	both	open

3 · Solution overview

3.1 Architecture.

As SRA-MOB-001 §3 Figure 1.

3.2 Sites and device inventory [A].

Table 3. Sites and device inventory [A]

Site	Role	Devices (class per SRA-MOB-001 §5; model from P4)	Naming
Branch 3 indoor	Wi-Fi 7 access	46 × omni AP, 24 × directional high-bay AP	br3-ap-z1-01 … br3-ap-z6-12
Branch 3 indoor	AP power and uplink	2 × 48-port 10G mGig, 802.3bt Class 6 switch	br3-acc-ap-01/02
Branch 3 yard	5G radio	6 × outdoor radio unit on 3 masts	br3-5gru-01 … 06
Branch 3 core room	5G core	1 × on-site standalone core, redundant pair	br3-5gc-01/02
Branch 3 core room	timing	1 × GNSS receiver + PTP grandmaster for TDD radios	br3-gm-01
All sites	endpoints	1,200 corporate phones · 600 BYOD · 300 rugged handhelds · 60 vehicle tablets · 150 RedCap sensors	asset tag = UEM name
Cloud	UEM tenant, CA connector	1 tenant, 2 connectors	mob-uem-prod

3.3 Locations.

Distribution center: six zones of about 3,330 m², 24 dock doors, one core room. Yard: 40,000 m², three mast positions on building corners and the gatehouse.

© 2026 Symbeeo. All rights reserved. · Public

4 · Logical design

4.1 SSID and VLAN plan [A].

VLANs extend SDD-NET-001 §4.1; site octet 4.

Table 4. SSID and VLAN plan [A]

SSID	Security	Bands	VLAN	Subnet
corp	WPA3-Enterprise, EAP-TLS, PMF required, beacon protection, FT	5 + 6 GHz, MLO	40 wifi-corp	10.4.40.0/22
legacy	WPA2-Enterprise, EAP-TLS, PMF required	5 GHz, no MLO	44 wifi-legacy	10.4.44.0/24 — closed at R5
guest	Enhanced Open, captive portal	5 GHz	50 wifi-guest	10.4.50.0/24

4.2 Private 5G data networks [A].

Table 5. Private 5G data networks [A]

Data network	Users	UE pool	Breakout	QoS
dc-ops	rugged handhelds, vehicle tablets	10.4.72.0/23	local, routed to core SVI	5QI 9 default; 5QI 1 (conversational voice) for push-to-talk
dc-sensor	RedCap sensors	10.4.74.0/24	local, to OT VLAN 60 via firewall	5QI 9
internet	none by default	—	not provisioned	—

Core: control and user plane both on site (R7). eSIM profiles issued through the UEM to phones and tablets; physical SIMs for sensors. Slices only where the device and UEM both support them [A].

4.3 IP and routing.

UE pools routed from the 5G core to the branch-3 core SVI; OSPF as SDD-NET-001 §4.3. Loopbacks 10.255.4.<device>/32.

4.4 UEM enrollment and device groups [A].

Table 6. UEM enrollment and device groups [A]

Group	Ownership	Enrollment	Management mode	Count
corp-ios	corporate	automated device enrollment	supervised, declarative	700
corp-android	corporate	zero-touch	fully managed	500
byod-ios	personal	account-driven User Enrollment	managed data only	350
byod-android	personal	user-initiated	work profile	250
rugged-shared	corporate	zero-touch	dedicated device, shared sign-in	300
vehicle	corporate	zero-touch	dedicated device, single-app	60

© 2026 Symbeeo. All rights reserved. · Public

Apple OS updates run through declarative software-update configuration only. Apple states that in all 27.0 operating systems legacy software update management no longer functions — software-update commands, queries, recommended cadence settings and software-update restrictions such as deferrals [S] (Apple Platform Deployment, WWDC26 device management updates, published June 8, 2026, read Sep 27, 2026 — https://support.apple.com/en-gb/guide/deployment/depd638aa061/web). In the Intune view, MDM-based Apple update policies are documented for iOS 10.3 – iOS 18 (supervised) and are to lose Intune support [S] (Microsoft Learn, updated Jun 22, 2026, read Sep 27, 2026 — https://learn.microsoft.com/en-us/intune/device-updates/apple/deprecated-mdm-policies-ios). No MDM update command or restriction is left in any profile (SRA-MOB-001 §4.5). Android updates through the UEM's system-update policy, 7-day freeze in peak season [A].

4.5 Compliance and certificates [A].

Non-compliant when: OS below the approved minimum; patch older than 30 days; jailbroken or rooted; mobile-threat risk high; storage unencrypted; no screen lock. State change reaches the policy engine within 5 min; access withdrawn within R13. Certificate: one per device, key generated in hardware, attestation checked by the CA, 1-year life, renewed at 30 days remaining (R11).

4.6 Security enforcement.

EAP-TLS on corp and legacy; RADIUS over TLS from the controller to the policy engine, Message-Authenticator required where TLS is not yet supported (R19); per-app access for off-site use per SRA-SEC-001 Model B; lost device: wipe and revoke from one UEM action (R18). Users sign in with passkeys (R12).

5 · Physical design

5.1 Mounting.

Omni APs at 6–8 m in open zones; directional APs at racking ends aimed down aisles; heights confirmed by post-install survey (STP-MOB-001 T2). Masts: 10–15 m, radio units sectorized over vehicle routes [A].

5.2 Cabling.

Cat6A, one run per AP; the second port is not cabled [A]; radio units on single-mode fiber to the core room, powered per the chosen model; GNSS antenna on the roof with clear sky.

5.3 Power.

Access switches and 5G core on A/B PDUs; core room UPS sized for R7's 4 hours at yard load [A].

5.4 Software baseline [A].

AP, controller, 5G core and radio: the maker's recommended release on the day of staging; UEM: vendor-hosted current; device OS: the approved minimum per model. All recorded in the as-built with checksums.

6 · Services

6.1 DHCP and DNS.

Client's servers; relay from the core SVIs; UE addresses from the 5G core. **6.2 Time.** NTP as SDD-NET-001 §6.2; PTP from br3-gm-01 for TDD radio synchronization. **6.3 QoS.** Wi-Fi voice in the voice access category, mapped to EF at the

© 2026 Symbeeo. All rights reserved. · Public

AP; 5G push-to-talk on 5QI 1; markings preserved to the WAN per SDD-NET-001 §6.3. **6.4 Management.** As SDD-NET-001 §6.4; UEM admin roles split between end-user computing and security; audit log to the SIEM.

7 · Migration and cut-over

Table 7. Migration and cut-over

Step	Action	Rollback
1	Spectrum registered, radios staged and burned in at Symbeeo (P1)	—
2	UEM and certificates live; pilot of 20 devices per group (STP-MOB-001 T9–T13)	unenroll pilot; old management stays
3	Wi-Fi 7 installed zone by zone beside the old APs; corp and legacy SSIDs per zone	old SSID stays one week per zone
4	Yard 5G lit; 10 pilot vehicles for one week (T5–T6)	vehicles stay on Wi-Fi and public 5G
5	Fleet moved group by group, one group per week	device re-enrolls to old management within 30 days
6	Every group on corp; legacy closed (R5)	re-open legacy for one named device group
7	Decommission, as-built, acceptance (STP-MOB-001 §4)	—

8 · Roles and deliverables

Table 8. Roles and deliverables

Role	Symbeeo	Client
Design authority	practice lead (signs)	infrastructure manager (signs)
Build	build engineers	change approver, end-user computing lead
Acceptance	test lead	named acceptor

Escalation contacts [A]. Names are written in at signature; roles are fixed here.

Table 9. Roles and deliverables

Level	When	Symbeeo	Client
1	day-to-day issue, a test case blocked	build lead	change approver or end-user computing lead
2	slippage over 5 business days [A], a change order disputed, a spectrum grant at risk	practice lead	infrastructure manager
3	unresolved at level 2 after 5 business days [A], a security incident (§9)	the Founder	the client's sponsoring executive

Deliverables. This document · weekly status reports (§1.4) · signed change orders · STP-MOB-001 with results · the handover pack (§9.5).

© 2026 Symbeeo. All rights reserved. · Public

9 · Security, lifecycle and handover

9.1 Security incidents.

A security incident affecting the client's data or systems — a compromised UEM tenant or admin account, a mis-issued device certificate, a rogue AP or radio, a lost device holding enterprise data during the build — is reported to the client's level-2 escalation contact (§8) **within 24 hours of discovery**, with what is known, what is contained and the next report time.

9.2 Media sanitization.

Any device or storage medium that has held client data and leaves the client's control — a returned or replaced phone, handheld or tablet, a failed 5G core disk, a pilot device, a radio or AP staged at Symbeeo — is sanitized to **NIST SP 800-88 Rev. 2** (Guidelines for Media Sanitization, final September 2025, superseding Rev. 1) [S], technique per IEEE 2883 [S], with **a certificate per device**: serial, device type, method, date, operator and verification result [A]. A UEM remote wipe alone does not close the record [A]. Media may instead stay with the client under a non-return service; media holding PHI or other regulated personal data are never taken back unsanitized.

9.3 Lifecycle on the quote.

No AP, switch, radio unit, 5G core, handset or license is quoted past its vendor's end-of-sale date. Every quoted item shows its **end-of-sale date and end-of-support date** in the vendor's own terms — for example Cisco's End of Sale date and Last Date of Support [S] — and every endpoint model also shows its security-update end date (R17, P8). An item with no published end-of-support date is marked so on the quote.

9.4 Vendor support by severity.

Every quote states, for each vendor support contract (wireless, 5G core and radio, UEM, rugged-device service), the response time for severity 1, 2, 3 and 4 as the vendor's contract defines them. Values come from the vendor's quote at bid time; none is assumed here.

9.5 Handover pack.

At the end of Phase 6: as-built drawings (AP and radio map, mast positions, cabling); SSID, data-network and IP tables; configurations and software with checksums; UEM profiles exported; device list with serials and security-update end dates; spectrum authorizations and grants; credentials and admin roles transferred to the client and Symbeeo's revoked; licenses; support contracts with their severity terms; the signed STP-MOB-001; the acceptance certificate; open items with owner and date.

Sources for §9, read Sep 24, 2026. NIST SP 800-88 Rev. 2 `https://csrc.nist.gov/pubs/sp/800/88/r2/final` · IEEE 2883-2022, Standard for Sanitizing Storage [S] `https://standards.ieee.org/ieee/2883/10277/` · Cisco end-of-life milestones `https://www.cisco.com/c/en/us/products/eos-eol-policy.html`.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SDD-MOB-001 · Version 1.1 · Oct 10, 2026