SYMBEEO

PUBLIC

DESIGN STUDY

Zero-trust phones for a retail bank: 10,000 devices, device-bound passkeys, 15-minute cut-off

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Mobility	Financial Services	EU retail bank
DOCUMENT	**VERSION**	**DATE**
MOB-004	1.1	Oct 10, 2026

WRITTEN BY

Mark Winston, Principal Network Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	MOB-004	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Mobility	Industry	Financial Services
Author	Mark Winston	Role	Principal Network Architect
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. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 5
3 · Architecture overview 6
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's or regulator's own current page on Sep 24, 2026, or on Sep 27, 2026 where the text says so · [S*] figure from a page summary or trade press where the page could not be opened or was not read in full · [A] design assumption, to be confirmed by the signing engineer · [T] design target: the record's outcome figure and anything derived from it. No figure comes from any engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

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 · Scope

Who it is for. The chief information security officer of a retail bank whose phones still sign in with passwords and one-time codes, whose Apple update policies still use MDM software-update commands that Apple's 27.0 operating systems no longer run, and who must show a supervisor how a lost phone loses access to customer data within minutes.

Typical buyer [A]. An EU retail bank, 11,000 staff, 140 branches and two head offices. 7,500 corporate phones (6,500 iPhone, 1,000 Android) and 2,500 personal phones used for mail, Teams and the branch app. Microsoft Entra ID is the identity provider; Microsoft Intune is the UEM already in service; certificates today are issued over SCEP.

What is in. Enrollment modes per ownership; the certificate and attestation path; passkey sign-in on phones; compliance rules and the hand-off to Conditional Access; Apple update policy moved to declarative management; the lost-device runbook. **What is out.** Laptops; Wi-Fi and campus network (SRA-NET-001); the policy engine's own design and the per-app gateway (SRA-SEC-001); mobile threat defense product choice.

Assumptions. The bank is in scope of DORA [A]. Intune and Entra ID stay; no platform change is in scope [A]. Every corporate iPhone is in Apple Business and every corporate Android in zero-touch [A]. Staff phones meet the OS floor in R6 [A].

Related documents, read Sep 24, 2026.

- Microsoft Learn, Intune software updates for supervised iOS/iPadOS (updated Jun 22, 2026) — https://learn.microsoft.com/en-us/intune/device-updates/apple/deprecated-mdm-policies-ios
- Microsoft Learn, passkeys in Authenticator for Microsoft Entra ID (updated Jul 6, 2026) — https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-authenticator-passkey
- Microsoft Learn, Overview of Apple Automated Device Enrollment for iOS/iPadOS in Intune (updated Jul 1, 2026, read in full Sep 27, 2026) — https://learn.microsoft.com/en-us/intune/device-enrollment/apple/overview-automated-enrollment-apple
- 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
- Regulation (EU) 2022/2554 (DORA) — https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
- SRA-MOB-001, SDD-MOB-001, STP-MOB-001 (Symbeeo), v1.0 of Sep 27, 2026

© 2026 Symbeeo. All rights reserved. · Public

1c · Public implementations this design follows

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
A Nordic bank builds Zero Trust on Microsoft Entra ID: Conditional Access, passwordless sign-in with Windows Hello, "only compliant devices can access the network", Defender for Endpoint on corporate mobile devices; 18,000 employees onboarded	Microsoft customer story · November 19, 2024 · public deployment	the design's shape — an EU bank deciding access on identity plus device compliance in Entra ID — runs at a real bank; that bank's passwordless is Windows Hello on PCs, not phone passkeys, so it does not settle R5–R7	https://www.microsoft.com/en/customers/story/19727-seb-group-microsoft-entra-id
Apple: legacy software update management no longer functions in all 27.0 operating systems — software-update commands, queries, recommended cadence settings and software-update restrictions such as deferrals; use declarative software update management	Apple Platform Deployment, WWDC26 device management updates · published June 8, 2026 · vendor documentation, used to build our own design	R10 and §4.4: the platform owner's statement of what is removed and in which release	https://support.apple.com/en-gb/guide/deployment/depd638aa061/web
Intune view of the same change: Apple has deprecated MDM-based software updates; Intune "will soon end support" for them and recommends declarative device management; MDM update policies apply to iOS 10.3 – iOS 18 (supervised)	Microsoft Learn · updated Jun 22, 2026 · vendor documentation, used to build our own design	R10 and §4.4: every Apple update policy moves to declarative management before cut-over	https://learn.microsoft.com/en-us/intune/device-updates/apple/deprecated-mdm-policies-ios
Passkeys in Microsoft Authenticator: Android 14 and later or iOS 17 and later; device-bound profile; attestation through iOS App Attest, Play Integrity or Android key attestation; attested passkeys cannot be registered cross-device	Microsoft Learn · updated Jul 6, 2026 · vendor documentation, used to build our own design	R6, R7 and §4.3: the passkey path and its OS floor	https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-authenticator-passkey
Intune Automated Device Enrollment: the management profile receives an ACME certificate at enrollment; ACME supported on iOS 16.0 or later and iPadOS 16.1 or later	Microsoft Learn · updated Jul 1, 2026 · vendor documentation, used to build our own design	R8 and §4.2: ACME-issued device identity on corporate iPhones enrolled through ADE	https://learn.microsoft.com/en-us/intune/device-enrollment/apple/overview-automated-enrollment-apple

Every row was read in full on Sep 27, 2026. The Apple and Intune rows state one change from two sides: Apple removes MDM software-update management in its 27.0 operating systems; Intune documents its legacy update policies only up to iOS 18. Microsoft's ACME page does not state that the key is held in the Secure Enclave; that point is an assumption [A] until read from Apple's own documentation.

© 2026 Symbeeo. All rights reserved. · Public

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Devices	6,500 corporate iPhone · 1,000 corporate Android · 2,500 personal = 10,000	[A]
R2	Regulation	ICT risk management and incident reporting under DORA, applicable since January 17, 2025	[S*] Regulation (EU) 2022/2554
R3	Corporate enrollment	100 % automated, no manual console step	SRA-MOB-001 R10
R4	Personal-device separation	bank data erasable without reading personal data	SRA-MOB-001 R14
R5	Sign-in method on phones	100 % passkey, device-bound, no password or one-time code	[T]; SRA-MOB-001 R12
R6	OS floor for passkeys	iOS 17 or later · Android 14 or later	[S] Entra passkeys in Authenticator
R7	Passkey attestation	enforced on every registration	[S] Entra attestation; [T] policy
R8	Device credential	one certificate per corporate device, key hardware-bound and attested	[S] Intune ACME; [A] hardware key binding; SRA-MOB-001 R11
R9	Access cut-off, non-compliant device	≤ 15 min after state change	SRA-MOB-001 R13
R10	Apple OS updates	declarative management only; no MDM update command in any policy	[S] Apple; Intune; [T]
R11	Patch compliance	95 % of devices on the latest patch within 14 days	SRA-MOB-001 R15
R12	Lost device	wiped or bank data removed, sessions revoked ≤ 15 min after report	SRA-MOB-001 R18
R13	Evidence for the supervisor	every revocation logged with actor, device, time and result in the bank's SIEM	[T]

Thirteen rows; five carry a vendor or regulator figure, one is a design assumption, two are design targets, and five restate an SRA-MOB-001 requirement for this design.

© 2026 Symbeeo. All rights reserved. · Public

3 · Architecture overview

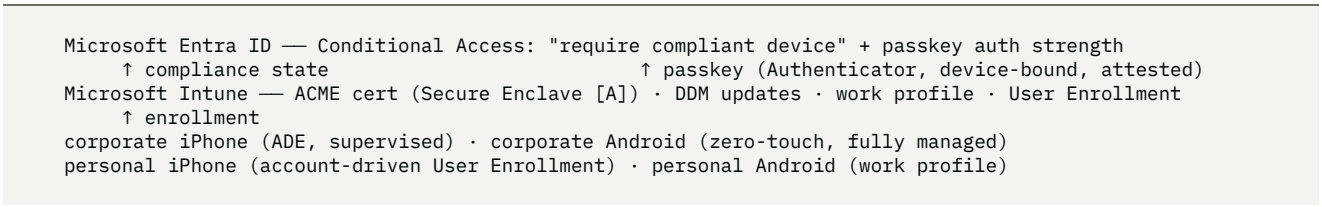


Figure 1. Phone identity and device compliance

Nothing in this design is new infrastructure. The bank already owns the identity provider and the UEM; the work is to set them so that three things hold on every phone: the device proves what it is, the user proves who they are without a shared secret, and a change in either removes access inside fifteen minutes.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
UEM	Microsoft Intune	1 tenant	10,000 devices [A]	in service; DDM for Apple updates [S]; ACME for Apple [S]
Identity and access decision	Microsoft Entra ID, Conditional Access	1 tenant	11,000 users [A]	in service; compliant-device grant control [S]
Phone authenticator	Microsoft Authenticator, device-bound passkey	1 per phone per profile	10,000+	Secure Enclave or hardware keystore [S*]; attestation [S]
Certificate authority	bank's CA behind the Intune connector	1	7,500 corporate certificates	SDD-MOB-001 P6 [A]

4 · Design by subsystem

4.1 Enrollment by ownership.

Corporate iPhone: Automated Device Enrollment, supervised. Corporate Android: zero-touch, fully managed. Personal iPhone: account-driven User Enrollment, managed data only. Personal Android: work profile [A], as SRA-MOB-001 §4.5 sets out. Existing corporate devices re-enroll by group; personal devices move when their user next signs in [A].

4.2 Device identity.

Corporate iPhones enrolled through Automated Device Enrollment receive their management certificate over ACME, supported from iOS 16.0 and iPadOS 16.1 [S]; the key held in the Secure Enclave [A]; Android corporate devices use hardware-backed keys with key attestation [A] (SRA-MOB-001 §4.6). SCEP stays only for devices below ACME's OS floor [S] or where the ACME profile fails to install [A], and each such device is listed by name [A]. Rejected: one certificate template for all four groups — personal devices get no device certificate, only app-level trust.

4.3 Passkeys.

Entra passkey profile: device-bound, attestation enforced, Authenticator AAGUIDs allowed [S]. The key lives in the Secure Enclave on iOS and the hardware keystore on Android [S*]. OS floor iOS 17 and Android 14 [S]. On an Android phone with a work profile, the passkey is used only from the profile where it was created, so users create it in the work profile [S]. Registration is done in the Authenticator app itself, because attested passkeys cannot be registered cross-

© 2026 Symbeeo. All rights reserved. · Public

device [S]. A Temporary Access Pass bootstraps registration without a password [S]. Rejected: synced passkeys for all staff — the bank's policy wants the key bound to a managed device (R7).

4.4 Compliance and updates.

Non-compliant when: OS below floor; patch older than 14 days; jailbroken or rooted; no screen lock; storage unencrypted [A]. Intune marks the state; Conditional Access requires a compliant device and a passkey for every bank app [S]. Apple updates are declared through DDM with a version and a deadline [A]; no MDM update policy is left in the tenant (R10): Intune documents those policies only up to iOS 18 [S], and Apple states that software-update commands, queries, recommended cadence settings and restrictions no longer function in any 27.0 operating system [S] (§1c, Apple, June 8, 2026). Android updates through the system-update policy with a seven-day ring [A].

4.5 Lost device and evidence.

One service-desk action: Intune wipe (corporate) or retire (personal); Entra sessions revoked; device certificate revoked at the CA [A]. Each step writes to the SIEM with actor, device, time and result (R13), the record the supervisor asks for under DORA incident handling [A].

4.6 Rollout.

Pilot of 200 users across all four groups for four weeks; then by business unit, 1,000 users a week; passkey enforcement per unit only after 95 % of that unit has registered [A]. About 14 weeks to complete [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Intune unreachable	devices keep last policy; compliance state goes stale; new enrollments wait	SRA-MOB-001 F7
Entra ID unavailable	sign-in fails for new sessions; existing tokens run to expiry	SRA-SEC-001 F2, F3 via SRA-MOB-001 F8
Apple or Google attestation service down	attested passkey registration blocked until service returns; existing passkeys keep working	[S] Entra attestation note
CA connector down	new corporate enrollments fail; issued certificates stay valid	SRA-MOB-001 F9
Phone lost	wipe or retire, revoke sessions and certificate ≤ 15 min	[T] R12
User's only phone lost	Temporary Access Pass issued after identity check; new passkey on the replacement	[A]

6 · Limits

- Device counts and the 1,000-a-week pace are assumptions; the real mix comes from the bank's Intune inventory.
- Microsoft's page confirms ACME for Automated Device Enrollment only (iOS 16.0+, iPadOS 16.1+); Secure Enclave key binding is [A] until read from Apple's documentation, and SCEP stays a named fallback.
- The 15-minute cut-off depends on how fast Intune reports compliance to Entra; it is measured (STP-MOB-001 T12), not assumed.

© 2026 Symbeeo. All rights reserved. · Public

- Phones below iOS 17 or Android 14 cannot hold an Authenticator passkey and must be replaced before enforcement.
- DORA obligations are the bank's; this design supplies evidence, not a compliance opinion.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

Mark Winston

Principal Network Architect

CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 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.

MOB-004 · Version 1.1 · Oct 10, 2026