

TECHNOLOGY · 14 PAGES

Mobile Credentials vs Key Fobs — The Security Comparison

A side-by-side security and operational comparison of mobile credentials and physical key fobs. Includes a credential lifecycle analysis and a total cost comparison over 5 years.

14 pages · Includes fillable cost worksheet · PDF

Why the Credential Type Matters More Than the Reader

When properties evaluate access control, most of the conversation goes to the hardware at the door — the panel, the reader, the gate operator. The credential itself, the thing a resident actually carries or uses to prove they belong, tends to get treated as an afterthought. That's backwards. The credential is where most of the real-world security gaps and ongoing operational cost actually live.

Physical key fobs and mobile credentials aren't just two form factors for the same idea — they behave differently under the exact conditions that matter most: what happens when one is lost, how easily it can be duplicated, how quickly access can be revoked, and what it actually costs to manage over years, not just at initial installation.

WHAT THIS GUIDE COVERS

A factual, side-by-side look at how each credential type actually works, where each is genuinely more vulnerable, what managing each looks like over a resident's full tenancy, and a fillable worksheet to compare your real 5-year cost for either approach.

How Physical Key Fobs Actually Work

Most key fobs and proximity cards use RFID (radio-frequency identification) — a small chip inside the fob transmits an identifying number to a reader when held close enough. The reader passes that number to the access control panel, which checks it against a list of authorized credentials and unlocks the door if it matches.

Not All Fobs Are Equally Secure

There's a meaningful difference between older low-frequency (125kHz) proximity cards — widely used since the 1990s — and newer, encrypted smart cards (13.56MHz, such as HID iCLASS Seos or similar). Low-frequency fobs transmit a static, unencrypted number, which is what makes them vulnerable to cloning with inexpensive, widely available devices. Encrypted smart cards use cryptographic authentication between the card and reader, which is significantly harder to duplicate — but they cost more per credential and require compatible readers.

THE PRACTICAL QUESTION

Before comparing fobs to mobile credentials, it's worth knowing which type of fob your property actually uses. Legacy low-frequency proximity systems and modern encrypted smart cards have very different risk profiles — ask your current vendor which one is installed.

How Mobile Credentials Actually Work

A mobile credential is a digital key issued to a resident's smartphone through an app, rather than a physical object. Depending on the platform, the phone communicates with the reader over Bluetooth, NFC, or a QR code, and the credential itself is protected by cryptographic keys unique to that resident's account, tied to their specific device.

What Makes It Different From "Just an App"

The security model isn't just "the app has a key" — it's layered. Access typically requires the resident to have an authenticated session (often protected by the phone's own lock screen, PIN, or biometric), a valid, non-expired credential issued by the property's cloud platform, and in most systems, a cryptographic handshake between the phone and reader that resists simple interception or replay, unlike a static RFID number.

Because the credential is issued and managed centrally in the cloud, it can be changed, expired, or revoked the instant a property manager makes that change — no physical object needs to be recovered or reissued.

Side by Side: Where Each Credential Is Vulnerable

Risk Factor	Physical Key Fob	Mobile Credential
Cloning risk	High for low-frequency fobs; low for encrypted smart cards	Low — cryptographic, device-bound credentials resist simple duplication
Lost credential exposure window	Active until physically reported and manually deactivated	Can be revoked instantly and remotely, the moment it's reported
Unauthorized sharing / lending	Easy — a physical fob can be lent to anyone with no record	Harder — tied to an individual's authenticated account and device
Theft of the credential itself	Usable immediately by whoever holds it	Typically requires the phone's own lock (PIN/biometric) to activate
Audit trail on use	Limited to "this fob number was used" with no identity verification	Tied to an authenticated account, supporting stronger identity confidence
Vulnerability if the platform itself is compromised	Lower — no network dependency for the credential itself	Depends on the vendor's cloud security practices

Mobile credentials outperform on most day-to-day risks, but they introduce a new dependency: the security of the vendor's cloud platform and app. Ask any vendor directly about their data security and encryption practices — see our RFP Template, Section 4, for the specific requirements to check.

Managing a Key Fob, From Move-In to Move-Out

1. **Order and inventory.** Fobs must be purchased and kept in stock ahead of need — a shortage on move-in day creates a real operational problem.
2. **Programming.** Each fob must be manually programmed or registered into the access system by staff.
3. **Distribution.** A staff member hands the fob to the resident in person, typically requiring a signature or acknowledgment.
4. **Ongoing tracking.** The property must maintain a record of which fob number belongs to which resident — a spreadsheet or system that has to stay accurate over time.
5. **Loss event.** When a fob is lost, someone must report it, staff must deactivate the old credential, and a new fob must be issued — often with a replacement fee.
6. **Move-out.** Staff must physically retrieve the fob, or deactivate it if it isn't returned, and update records accordingly.

Every one of these six steps requires staff time and is a point where the record can fall out of sync with reality — a resident who moved out with an active, unretrieved fob is a common and often invisible gap.

Managing a Mobile Credential, From Move-In to Move-Out

1. **Invitation.** Staff sends a digital invitation to the resident's email or phone number — no physical inventory required.
2. **Self-service activation.** The resident downloads the app (or opens a web-based credential) and activates their own access, typically in minutes, without a staff visit.
3. **No manual tracking needed.** The system itself maintains the record of who holds which credential — there's no separate spreadsheet to keep in sync.
4. **Loss event.** If a phone is lost or stolen, the resident or staff revokes access instantly from the app or dashboard — no replacement hardware, no physical retrieval.
5. **Move-out.** Staff deactivates the credential remotely the moment the lease ends — no coordination required to physically collect anything.

The lifecycle is shorter and removes the two steps most likely to fail on a physical system: manual tracking accuracy and physical retrieval at move-out.

Lifecycle Comparison at a Glance

Lifecycle Stage	Key Fob	Mobile Credential
Initial issuance	Requires physical inventory and staff programming	Digital invitation, self-service activation
Staff time per issuance	Moderate — in-person handoff required	Minimal — automated invitation
Tracking accuracy over time	Manual, prone to drift	System of record is automatic
Response time to a lost credential	Depends on when it's reported and staff availability	Instant, resident or staff can revoke immediately
Move-out process	Requires physical retrieval or manual deactivation	Remote deactivation, no coordination needed

WHERE THIS SHOWS UP IN YOUR BUDGET

Every stage where a fob requires staff time or physical coordination is a recurring labor cost that a mobile credential largely removes. The next three pages walk through how to quantify that difference for your specific property.

Methodology and Assumptions

To fairly compare the two approaches over a 5-year period, this worksheet accounts for the costs that are easy to overlook in a simple per-unit price comparison: replacement due to loss, staff time, and turnover-driven reissuance.

For Key Fobs, You'll Need

- ✓ Cost per fob (typically \$3–\$15 depending on whether it's a basic low-frequency fob or an encrypted smart credential)
- ✓ Number of residents / units requiring a credential
- ✓ Estimated annual loss/replacement rate (many properties see 10–20% of fobs replaced annually due to loss, damage, or non-return at move-out)
- ✓ Staff time per issuance or replacement event, and the associated hourly cost

For Mobile Credentials, You'll Need

- ✓ Whether mobile credentialing is included in your platform's software subscription or billed separately per credential
- ✓ Staff time per issuance (typically minimal, since activation is self-service)

Fillable Worksheet

Key Fob — Initial Issuance Cost

Number of units: _____ × Cost per fob: \$ _____ = \$ _____

Key Fob — Annual Replacement Cost

Number of units: _____ × Annual loss rate: _____ % × Cost per fob: \$ _____ =
\$ _____ /year

× 5 years = \$ _____

Key Fob — Staff Time Cost

Issuance/replacement events per year: _____ × Hours per event: _____ × Hourly wage:
\$ _____ = \$ _____ /year

× 5 years = \$ _____

TOTAL 5-YEAR KEY FOB COST = \$ _____

Fillable Worksheet, Continued

Mobile Credential — Software Cost

If included in your platform subscription, use \$0 here and rely on your platform's monthly cost instead. If billed per credential:

Number of units: _____ × Annual cost per credential: \$ _____ × 5 years = \$ _____

Mobile Credential — Staff Time Cost

Issuance events per year: _____ × Hours per event: _____ × Hourly wage: \$ _____ =
\$ _____ /year

× 5 years = \$ _____

TOTAL 5-YEAR MOBILE CREDENTIAL COST = \$ _____

Total 5-Year Key Fob Cost (from page 10): \$ _____

Total 5-Year Mobile Credential Cost (from above): \$ _____

Estimated 5-Year Savings = \$ _____

Common Vulnerabilities Worth Knowing About

- ✓ **Fob cloning devices are inexpensive and widely available online** for low-frequency proximity cards — this is a documented, real-world risk for legacy fob systems, not a theoretical one.
- ✓ **Fobs get lent out informally** — a resident lending their fob to a family member, dog walker, or contractor creates untracked access that the system has no way of flagging.
- ✓ **Move-out retrieval is inconsistent.** Properties with high turnover frequently have a population of "orphaned" active fobs from residents who never returned them.
- ✓ **Mobile credentials shift the risk to phone security** — a resident with no lock screen or PIN on their phone reduces the practical security benefit, so device-level hygiene matters.
- ✓ **Mobile credential security is only as strong as the vendor's implementation** — ask directly about encryption standards and whether credentials are device-bound or transferable, per Section 4 of our RFP Template.

What to Look For, and Key Takeaways

- ✓ Confirm whether your existing fobs are low-frequency (higher cloning risk) or encrypted smart credentials, before assuming your current system is secure.
- ✓ Mobile credentials generally outperform fobs on revocation speed, cloning resistance, and audit trail quality — but their security depends on the vendor's cloud and app implementation.
- ✓ The lifecycle cost of key fobs is driven by loss/replacement rate and staff time, not just the unit price — both are usually underestimated.
- ✓ Run the 5-year worksheet in this guide with your property's real numbers before assuming either approach is cheaper.
- ✓ A hybrid approach — mobile credentials for most residents, physical fobs available for those who prefer them — is common and reasonable, as long as both credential types are tracked and revoked from the same platform.

VIVO CONTROL

Mobile Credentials, Managed From One Platform

Vivo Control issues and revokes resident access instantly from the cloud — no fob inventory, no manual tracking, and no coordination required at move-out.

Book a Free Demo →

www.vivocontrol.com/en/demo/ · hello@vivocontrol.com · This guide is for general informational purposes and does not constitute security engineering advice for your specific property.