

DIGME

Biometric Digital Credentialing

WHITE PAPER

**Reimagining the ID Badge: Two-Factor Identity, Physical Access, and Real-Time
Safety Beaconing**

April 2024

U.S. Patent No. 15/733,702

www.DigAware.net

Executive Summary

The corporate identity badge has not fundamentally changed in decades, even as the risks it is meant to manage have grown far more complex. Organizations today face a workforce that is more distributed, more reliant on contractors and vendors, and more exposed to insider threats than ever before. At the same time, the badge itself typically offers little more than a photo and a proximity chip — a single factor of authentication that can be lost, shared, cloned, or stolen without immediate detection.

DigMe reimagines the ID badge as a biometric, digitally credentialed device that delivers genuine **two-factor** authentication (MFA) without requiring organizations to rip out and replace existing physical access infrastructure. This paper describes the DigMe ID Badge (with beaconing or without), the insider-threat landscape that motivates the product, and a new safety dimension: device-based beaconing that extends DigMe beyond access control into real-time occupant safety, duress signaling, and emergency accountability.

The Problem: Identity, Access, and the Human Risk Factor

Every organization issues credentials for a mix of reasons — physical security, time and attendance, compliance, branding, and professional identification among them. Yet the badge itself has remained a single-factor device: possession of the card is treated as proof of identity, regardless of who is actually holding it.

The consequences of that gap show up directly in insider-threat data. Contractors, vendors, and shared workspaces have all expanded the population of people who carry organizational credentials without a corresponding increase in the assurance that those credentials provide.

47%	57%	31%	2,500
increase in insider threat incidents over the last two years	of insider-threat actors are contractors or consultants	of companies manage in excess of 1,000 vendors	internal security breaches experienced daily across U.S. companies

Sources: Coworking Space Global Market Report 2023; Security Week, April 12, 2023; Soft Activity — 31 Insider Threat Stats, 2023. Co-working space capacity in the U.S. has also grown roughly 150% over the same period, further blurring the boundary of who holds a badge to which building.

These figures point to a simple conclusion: people, not infrastructure, are the weakest link in most security programs. The fix does not require replacing card readers, door controllers, or access-control panels. **It requires making the badge itself prove who is holding it.**

Why the ID Badge Needs to Evolve

Physical access infrastructure — readers, panels, wiring, and management software — represents a significant, multi-year capital investment for most organizations. Replacing it to gain stronger authentication is rarely practical. DigAware's premise is that the badge, not the infrastructure, is the right layer to upgrade: a **true** second factor can be added to the credential itself, leaving existing readers and access-control systems untouched.

- No rip-and-replace of door readers, panels, or head-end software
- Biometric verification happens on the credential before it presents an identity
- Existing 125kHz and 13.56MHz reader infrastructure continues to work as-is

Introducing DigMe: Biometric Digital Credentialing

DigMe brings biometric digital credentialing to physical access control through two complementary form factors.

DigMe Biometric Id Badge

A biometric identity badge with multiple radio capability, built for organizations that want to keep the familiar card form factor while adding a real second authentication factor.

- Tap and go, same footprint as a standard badge
- Supports 13.56MHz NFC and 125kHz RFID, with single- or multi-radio configurations
- ISO 14443 compliant; 2.5k bit memory across 5 sectors
- On-card fingerprint sensor with biometric lockout
- BLE 5.1 radio with persona enablement for context-aware credential presentation
- 45+days on one charge – USB C charging
- Water resistant
- Access Control only or Beacons once Id is triggered every 2secs / with Help and Emergency buttons

Beyond Access: Safety Capabilities Through Device Beacons

Access control answers the question of who may enter a space. It does not answer a different, equally important question: is everyone who should be safe, actually safe, right now? DigAware extends its biometric credential into a real-time safety layer by using the BLE 5.1 radio already present in the DigMe Id Badge to beacon status, presence, and distress signals to the organization's existing infrastructure — without any additional hardware for the wearer to carry.

How Beaconing Works

Every DigMe credential can periodically broadcast a low-energy Bluetooth beacon containing an encrypted identifier, a battery and connectivity status, and — when triggered — a distress flag. Fixed or mobile BLE receivers (including existing access-control readers where BLE-capable, dedicated gateway hardware, or even paired mobile devices) pick up these beacons and relay them to the Digital Identity Dashboard, where they are correlated against the badge holder's identity and last-known location.

- Beacons are encrypted and rotate identifiers on a schedule, so passive interception cannot be used to track an individual over time
- Beacon interval is configurable per deployment, balancing battery life against positional freshness
- Beaconing operates independently of the access-control transaction, so status is visible whether or not the holder is actively badging through a reader

Safety Capabilities This Enables

- Duress and panic signaling: a discreet, deliberate action on the card or device (such as a defined fingerprint pattern or a hidden control) transmits a distress beacon, alerting security operations and nearby responders without the wearer needing to speak, dial, or draw attention to the act
- Lone-worker safety: staff working alone in low-traffic areas, off-hours shifts, or remote facility zones are beacons on a check-in interval; a missed beacon window automatically raises a wellness alert to a supervisor or security desk
- Geofenced zone alerts: the dashboard can define safety-relevant zones — restricted areas, hazardous zones, construction sites — and flag when a badge beacons from inside a zone is not authorized or expected to be in
- Emergency mustering and evacuation accountability: during a fire alarm, lockdown, or other emergency, beacon data lets the dashboard show in real time who has reached a designated muster point and who has not yet been accounted for, replacing manual headcounts with a live roster
- Tamper and removal detection: because the biometric sensor governs credential activation, a card or device separated from its verified holder, or forced offline, can itself raise an anomaly flag rather than silently going dark

Why This Matters for the Buyer

Adding safety beacons to an identity credential turns a compliance cost center into a program with a direct, visible return: faster emergency response, verifiable duty-of-care for lone and remote workers, and hard evidence of who was where during an incident — all delivered through the same card or device already being issued for access control, with no new hardware to distribute, charge, or lose.

Because beaconing rides on the same BLE 5.1 radio and biometric lockout used for access, it inherits DigMe's core security properties: signals are tied to a verified individual, not merely a token, used to manage access rights becomes the console for real-time occupant safety.

Conclusion

The badge every employee, contractor, and vendor already carries can do more than open a door. By adding biometric verification and BLE-based beaconing to the same credential, DigMe turns a single-factor access token into a true second factor for identity — and, at the same time, into a real-time safety device that gives organizations visibility into duress, lone-worker wellbeing, restricted-zone incursions, and emergency accountability. No new hardware for the wearer, no replacement of existing access infrastructure — just a badge that finally does the job security has needed it to do all along.

For more information, visit www.digmyinfo.com or contact robin@digaware.net.