

ID Pulse by Touch2access Ltd

Secure Keyless Access for Everyone

Whitepaper

Mark Campbell

February 16, 2026

System Aims

ID Pulse aims to provide simple and frictionless door access for the elderly and people with disabilities. Using patented technology, ID Pulse requires only minimal intervention by a challenged user by touching or presenting their hand or face to a 12v or battery operated beacon transmitter fitted beside the door with any part of their body and with an authenticated fob carried on their person to access through a locked door. The same locking system can then be accessed by able-bodied users, with either a conventional card, fob, or smart phone device.

The ID Pulse beacon transmitter and tag credential can bolt on to any new or existing Bluetooth or NFC enabled reader, smart lock, turnstile and building control. It offers a very low cost frictionless means of access without having to replace the existing hardware. It has an open platform with OSDP or LEAF interoperability with many manufacturers hardware.

Disability legislation requires equal access and opportunities for people with disabilities [1], [2], yet conventional access credentials such as cards, fobs and mobile devices can be difficult or impossible for a profoundly disabled user to operate without assistance. When a user cannot present a card or unlock a phone, they must rely on a member of staff or family member for access. What happens when that person is not available, and who bears the cost?

Frictionless Access for Everyone

The primary aim of ID Pulse is to provide accessibility with a simple method of secure access for elderly and people with disabilities in care homes, retirement communities, multi-family units, private homes and commercial premises.

While ID Pulse was designed to solve the accessibility challenge, the same technology delivers a faster, more private experience for all users. Anyone carrying an authenticated fob can walk up to a door, present their hand and enter.

At the same time, ID Pulse solves the intention problem of near-frictionless access control: How does the system know which door the user wants to interact with and which credential should be read? In the ID Pulse system, the transmitter only tries to connect to the credential when a touch is detected, and the fobs only wake up when a valid signal is detected. Therefore, if the transmitter sees a fob, it can logically be associated.

Because the body-coupled wake requires physical contact with the transmitter surface, ID Pulse also provides a hygiene advantage: the fob stays in a pocket or on a wristband and never needs to be handled or shared, reducing contact with communal surfaces, a concern that has grown significantly since the COVID-19 pandemic [3].

Facial recognition systems are increasingly used for hands-free access, but they require the capture and storage of personally identifiable information (PII) that falls under GDPR [4] and similar legislation.

Organisations that process Personal data must meet heightened requirements for consent, storage and data protection impact assessments, leading to significant overheads.

ID Pulse achieves hands-free access *without capturing any PII*. The system identifies a credential, not a person. No biometric data is collected, stored, or transmitted. This makes GDPR compliance significantly simpler and removes the privacy concerns that make facial recognition controversial in residential, workplace, and public-facing environments.

System Overview

The system consists of a wall-mounted transmitter and a low-cost fob somewhere on the body of the user. The user only needs to touch the wall-mounted transmitter, and the fob is then activated, causing an encrypted credential to be transmitted by the fob using Bluetooth® to the transmitter. If this credential is permitted access, the transmitter will release the door. Able-bodied users can either present a physical credential, such as the fob or a card, or use a mobile app to release the door.

The protocol operates in two independent layers, illustrated in Figure 1.

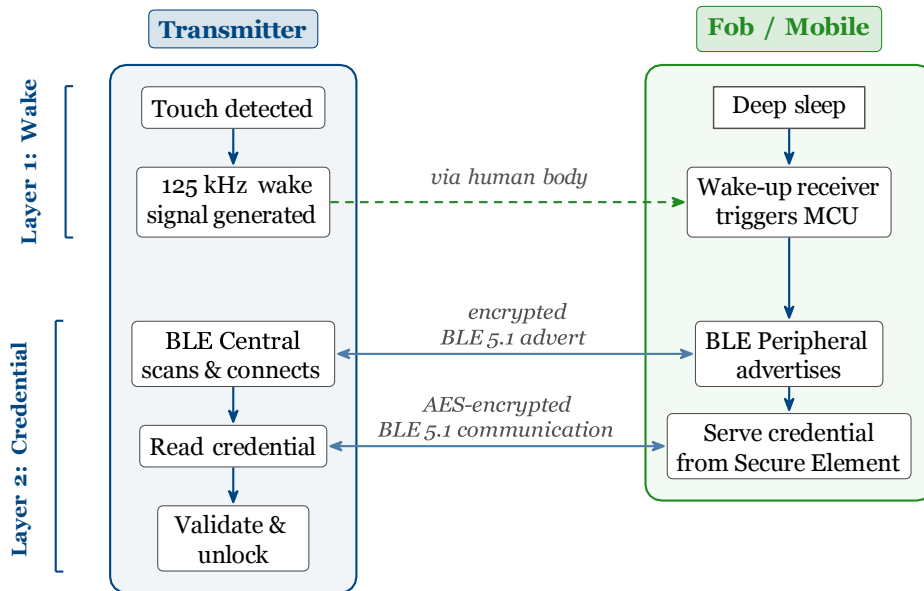


Figure 1: ID Pulse two-layer protocol: body-coupled wake followed by encrypted BLE credential exchange.

Layer 1 - Body-Coupled Wake. When a user touches the transmitter, a coded 125 kHz signal propagates through the body to the fob [5]. Until that moment, the fob draws only micro-amps in deep sleep, giving it a battery life extending into years, far beyond what conventional Bluetooth wake-up methods achieve [6]. The wake signal carries no identity data; it is purely a proximity trigger.

Layer 2 - BLE Credential Exchange. Once awake, the fob transmits an encrypted credential to the transmitter over Bluetooth Low Energy [7]. The transmitter can validate the credential locally or submit it to a central system.

Comparison with Existing Technology

Several access control products target care and assisted living. Each serves staff and visitors well, but a gap remains: what must the *resident* do to open a door independently?

Dormakaba TouchGo™ transmits identity data through the body via Resistive Capacitive Identification (RCID) [8]. The transponder can sit in a pocket or on a wheelchair; the resident grasps the handle to authenticate [9]. Staff benefit from the same hands-free workflow. This is the closest analogue to ID Pulse, but TouchGo sends credential data directly through the body-coupled channel rather than separating wake from credential, and requires a proprietary transponder and ecosystem.

ASSA ABLOY operates several care-focused brands. Phoniro [10] provides smartphone-based digital locks for *care staff* entering clients' homes; the resident does not use Phoniro to open their own door. Vigil provides RFID VingCard™ locks where residents present a card, wristband, or lanyard to a reader. Intelligent Care offers nurse-call systems oriented toward staff. The resident must still present a credential to a reader or rely on staff.

HID Global provides mobile credentials via Apple Wallet, Google Wallet, and the Seos® platform [11]. The resident taps a phone against the reader or performs a 90-degree wrist twist. Seos credentials can be loaded onto wearables, but the device must still be brought within range. HID facial recognition removes the credential dependency but requires biometric PII storage. All HID approaches use proximity detection for intent, which is ambiguous when multiple readers are nearby.

SALTO® Systems is a major European electronic locking provider deployed across care homes [12]. Residents wear an RFID wristband and present it to a reader. SALTO offers long-range readers that can open doors automatically as a wheelchair user approaches, reducing the presentation requirement. However, the system still relies on RFID proximity, and long-range detection introduces the same intent ambiguity as other proximity-based systems.

	User action	Intent	Battery	Security
Dormakaba TouchGo	Grasp handle	Touch	Years	Identity via body
ASSA ABLOY / Vigil	Present wristband	Tap	Wristband	Encrypted RFID
HID Mobile / Seos	Tap or twist phone	Proximity	Phone	Encrypted BLE
HID Facial Recognition	None (camera)	Camera	Mains	Biometric PII
SALTO Systems	Approach with wristband	Proximity	Wristband	Encrypted RFID
ID Pulse	Touch surface	Touch	Years	Wake + encrypted BLE

Applications

Although access control for doors is the primary use case, the ID Pulse transmitter is a general-purpose body-coupled trigger. A single fob and mobile app combination can operate multiple device types:

- Door access readers and smart locks
- Door operators and automatic openers
- Elevators and barrier gates
- Garages and parking systems
- Security and alarm systems
- Computers, terminals, and medical equipment
- Vehicles and fleet access

Integration with smart-home platforms such as Google Home and Amazon Alexa is supported through the mobile credential path, allowing ID Pulse to fit into broader building-automation workflows. Matter™ support [13] could also be added to the transmitter for further smart home integration.

Platform Integration

The ID Pulse credential layer is platform-agnostic by design. One adaptation path uses LEGIC® hardware and services to provide a unified experience for all users. Administrators can also use the LEGIC Connect cloud platform [14] to provision and manage credentials. Figure 2 shows the target architecture.

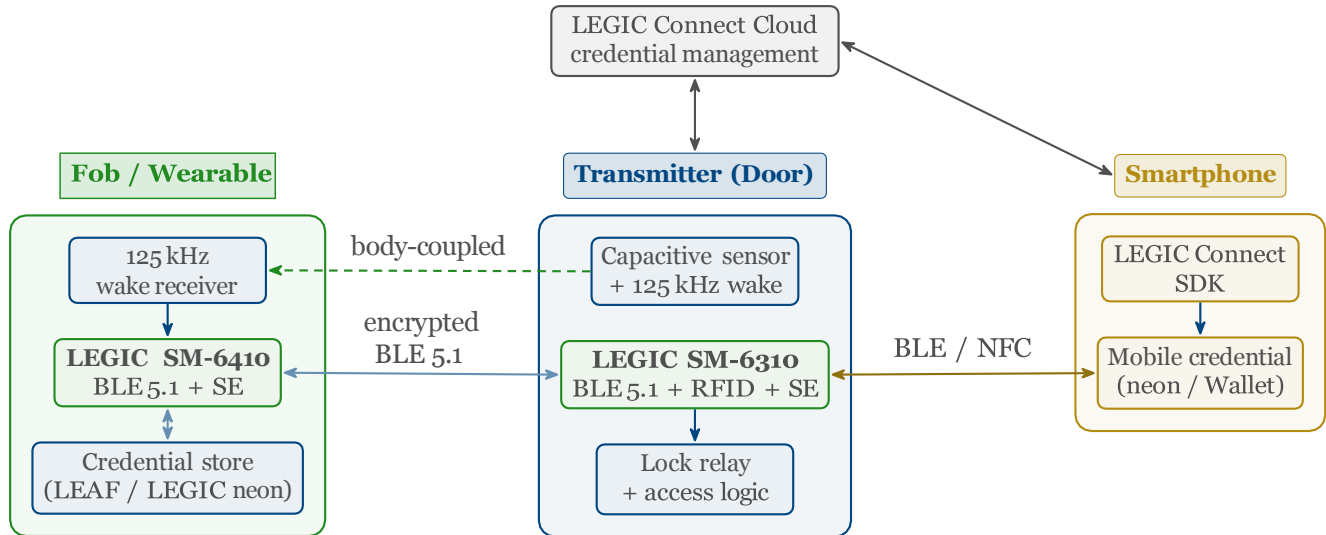


Figure 2: ID Pulse architecture with LEGIC SM-6310 (transmitter), SM-6410 (fob), and mobile credential path.

LEGIC SM-6310 (Transmitter) - Provides BLE 5.1 connectivity, multi-standard RFID reading, and an EAL5+ certified Secure Element [15] for credential validation [16]. The RFID capability also enables fallback authentication via contactless cards for able-bodied users.

LEGIC SM-6410 (Fob) - Secure Element and BLE 5.1 in a compact module [17]. Because the SM-6410 is part of the same LEGIC neon ecosystem as the mobile credential, administrators use the LEGIC Connect cloud platform to issue, manage, and revoke credentials over the air to both fobs and smartphones.

The use of LEAF Universal is another possible upgrade path. LEAF is an open, vendor-neutral credential standard [18] based on MIFARE® DESFire® EV2 [19]. ID Pulse can carry LEAF credentials within the existing Bluetooth exchange, enabling a single fob or card to work across any LEAF-compatible access system.

The ID Pulse architecture can also integrate with the HID® ecosystem. The body-coupled wake layer is unchanged; only the credential platform differs. Figure 3 shows the HID integration path.

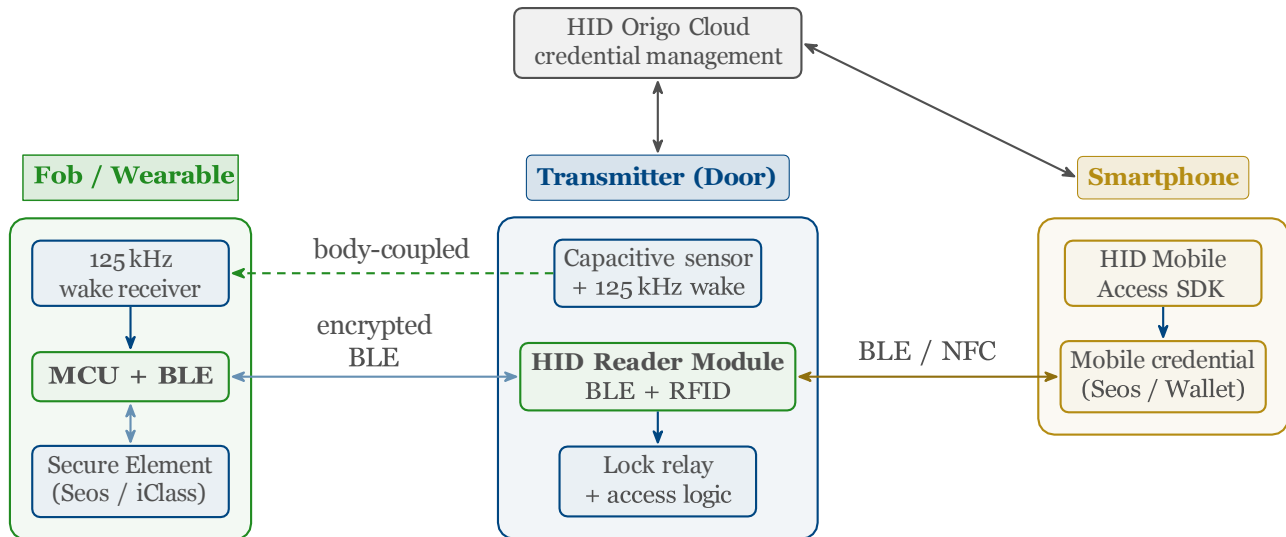


Figure 3: ID Pulse architecture with HID reader module (transmitter), Seos credential (fob), and HID Origo mobile credential path.

HID Reader Module (Transmitter) - An HID multi-technology reader such as the Signo or iCLASS SE range [20], supporting native BLE, NFC, and 125 kHz credential technologies with OSDP secure channel communication. These readers accept Seos®, iCLASS SE, and MIFARE® credentials, support Apple and Google Wallet, and maintain backward compatibility with legacy HID card populations.

HID Origo™ (Cloud) - HID's cloud credential management platform [21]. Origo provisions Seos credentials over the air to Apple Wallet, Google Wallet, and the HID Mobile Access app, with no physical card handling required.

This dual-path approach means that an ID Pulse deployment can adopt whichever credential ecosystem the building already uses, or support both simultaneously.

Future Direction

The two-layer architecture of ID Pulse is designed so that the credential transport can evolve independently of the wake mechanism. A possible next step is the adoption of Ultra-Wideband (UWB) in place of BLE for the credential exchange layer.

UWB offers precise ranging (centimetre-level accuracy) [22], inherent resistance to relay attacks [23] through time-of-flight verification, and very low latency. As UWB support becomes available in security modules and mobile devices, ID Pulse can transition the credential layer from BLE to UWB while retaining the same 125 kHz body-coupled wake, the same user experience, and the same credential management platform.

Alternatively, Bluetooth 6.0 offers even more features than Bluetooth 5.1 through its Channel Sounding feature [24]. This addition brings centimetre-level ranging to Bluetooth itself, providing many of the security benefits of UWB, including relay attack prevention through precise distance measurement. For ID Pulse, this means enhanced security by integrating new Bluetooth 6.0 MCUs such as the Nordic nRF54L. The system could verify that a credential is physically present at the door rather than being relayed from a distance, confirming that the touch and wake-up are valid. As Bluetooth 6.0 adoption grows across smartphones and embedded modules, this represents a natural evolution path that preserves the current architecture while strengthening security.

Conclusion

ID Pulse solves a problem that the access control industry has largely ignored: how to provide secure, independent access to people who cannot operate a card, a fob, or a phone. By using the human body as a signal path, the system removes the barrier entirely: the user simply touches the door.

For able-bodied users, the same technology delivers a faster, more private hands-free experience without the privacy burden of facial recognition.

This combination of accessibility, privacy, security, and openness is not yet addressed by existing access control platforms, presenting an opportunity for integration rather than replacement.

Bluetooth® is a registered trademark of Bluetooth SIG, Inc. TouchGo™ is a trademark of dormakaba. VingCard™ is a trademark of ASSA ABLOY. HID®, Seos®, Signo®, iCLASS SE®, and Origo™ are trademarks of HID Global / ASSA ABLOY. SALTO® is a registered trademark of SALTO Systems S.L. Matter™ is a trademark of the Connectivity Standards Alliance. LEGIC® is a registered trademark of LEGIC Identsystems AG. MIFARE® and DESFire® are registered trademarks of NXP Semiconductors. All other trademarks are the property of their respective owners.

References

- [1] U.S. Department of Justice, *Americans with disabilities act of 1990*, <https://www.ada.gov/>, Public Law 101-336, 1990.
- [2] UK Government, *Equality act 2010*, <https://www.legislation.gov.uk/ukpga/2010/15/contents>, Chapter 15, 2010.
- [3] N. Aydin, Y. Murt, and S. Erdogan, “Touchless technologies in the post-covid era: A review of applications and trends,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 8, 2021. doi: 10.14569/IJACSA.2021.0120847
- [4] European Parliament and Council, *Regulation (eu) 2016/679 of the european parliament and of the council (general data protection regulation)*, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, Official Journal of the European Union, 2016.
- [5] M. Wegmueller, M. Oberle, N. Felber, N. Kuster, and W. Fichtner, “Signal transmission by galvanic coupling through the human body,” in *IEEE Transactions on Instrumentation and Measurement*, vol. 59, 2010, pp. 963–969. doi: 10.1109/TIM.2009.2031449
- [6] C. Gomez, J. Oller, and J. Paradells, “Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology,” *Sensors*, vol. 12, no. 9, pp. 11 734–11 753, 2012. doi: 10.3390/s120911734
- [7] Bluetooth SIG, “Bluetooth core specification version 5.1,” Bluetooth Special Interest Group, Tech. Rep., 2019.
- [8] dormakaba, *Touchgo: Body-coupled access control*, https://www.dormakaba.com/gb-en/offering/products/electronic-access-data/technology-and-function-principals/touchgo-ka_235545, Accessed: 2026-02-15, 2024.
- [9] dormakaba, *Touchgo care: Access solutions for healthcare*, <https://www.dormakaba.com/touchgo-care-en/the-solution>, Accessed: 2026-02-15, 2024.
- [10] Phoniro (ASSA ABLOY), *Phoniro: Digital key management for home care and senior living*, <https://www.phoniro.com/solutions/electronic-locks/>, Accessed: 2026-02-15, 2025.
- [11] HID Global, *Touchless access control solutions*, <https://www.hidglobal.com/solutions/touchless-access-control>, Accessed: 2026-02-15, 2026.
- [12] SALTO Systems, *Innovative solutions to aged care security*, <https://saltosystems.com/en/blog/revolutionizing-senior-care-role-modern-electronic-access-control/>, Accessed: 2026-02-16, 2025.
- [13] Connectivity Standards Alliance, *Matter: The foundation for connected things*, <https://buildwithmatter.com/>, Protocol specification, 2024.
- [14] LEGIC Identsystems AG, *Legic connect: Cloud-based credential management platform*, <https://www.legic.com/products/software/legic-connect>, Platform overview, 2024.
- [15] Common Criteria, *Common criteria for information technology security evaluation: Evaluation assurance level 5+*, <https://www.commoncriteriaportal.org/>, Part 3: Security assurance components, 2022.
- [16] LEGIC Identsystems AG, *Sm-6310 secure module: Ble 5.1, rfid and secure element*, <https://www.legic.com/products/modules/sm-6310>, Product datasheet, 2024.
- [17] LEGIC Identsystems AG, *Sm-6410 secure module: Ble 5.1 and secure element*, <https://www.legic.com/products/modules/sm-6410>, Product datasheet, 2024.

- [18] LEAF Coalition, *Leaf universal: Open credential standard*, <https://leaf-coalition.org/>, Technical specification, 2024.
- [19] NXP Semiconductors, *Mifare desfire ev2: Contactless multi-application ic*, <https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire>, Product datasheet, 2023.
- [20] HID Global, *Hid signo readers: Next generation multi-technology access control*, <https://www.hidglobal.com/product-mix/signo-readers>, Product datasheet, 2025.
- [21] HID Global, *Hid origo: Cloud-based credential management platform*, <https://doc.origo-hidglobal.com/>, Platform documentation, 2025.
- [22] A. Alarifi et al., "Ultra wideband indoor positioning technologies: Analysis and recent advances," *Sensors*, vol. 16, no. 5, p. 707, 2016. doi: 10.3390/s16050707
- [23] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," *Networks and Distributed Systems Security (NDSS) Symposium*, 2011.
- [24] Bluetooth SIG, "Bluetooth core specification version 6.0," Bluetooth Special Interest Group, Tech. Rep., 2024, Introducing Channel Sounding for precise distance measurement.