

Infineon solutions unlocks seamless mobile credential interoperability with Aliro for access control

By Björn Scharfen: Ecosystem and Partner Management Digital Security and Identity
Marcel Konstantinov: Product Marketing and Management Trusted Sensing and Localization

As the demand for greater cybersecurity increases, so does the need for access control solutions. Companies and other organizations deploy access controls solutions to meet modern cybersecurity needs and legal compliance requirements related to data privacy. The purpose of access control solutions is to prevent unauthorized users and systems from accessing protected resources in a way that exceeds their permissions.

Access control solutions exist worldwide in places such as residential or commercial buildings, vehicles, shopping malls and parking lots. The transition from mechanical to digital keys for access control solutions involves an ecosystem of products to properly open, manage, distribute and secure the door, while preserving the solutions flexibility and interoperability.

Designing access control solutions is complicated due to system incompatibility and interoperability fragmentation across different companies' products that go into the solutions. The Connectivity Standards Alliance (CSA) launched the Aliro 1.0 specification, a unified standard for secured and seamless access control to fix interoperability fragmentation, on February 26, 2026. Established in 2002, CSA and its 800 members worldwide focus on creating universal open standards for IoT products.

https://community.infineon.com/t5/Blogs/Infineon-unlocks-seamless-mobile-credential-interoperability-for-access-control/ba-p/1228273

Aliro overview

Aliro is a digital access framework that enables interoperability for smart access. It is designed to support major applications across the entire access control ecosystem, including corporate offices, universities, hospitality venues, single and multi-family homes. It includes a comprehensive certification program managed through Authorized Test Labs and through liaisons with other industry consortia to harmonize the specification of the underlying technologies.

Aliro has been developed by greater than 200 cross-industry players, including Apple, ASSA ABLOY, Google LLC, **Infineon Technologies AG**, Last Lock, Inc., Samsung Electronics, and STMicroelectronics. It specifies the interaction between smartphones, wearables or other secured devices and the reader, utilizing its core principles of interoperability, flexibility, security and simplicity for the entire ecosystem.

Aliro is agnostic to the choice of back-end protocols. It uses well established connectivity and positioning technologies such as Near Field Communication (NFC), Bluetooth® LE, and Ultra-Wideband (UWB). Aliro utilizes asymmetric cryptography to facilitate trusted interactions between user devices and readers, while respecting user privacy.

Aliro alleviates the fragmented world of access control and lays the groundwork for significantly reducing implementation, integration and maintenance costs. It also offers higher flexibility within and across verticals and industry consortia (e.g., FiRa Consortium, Car Connectivity Consortium, NFC Forum, Bluetooth SIG).

How Aliro works using different wireless technologies

As stated above, Aliro is designed to be agnostic. It can be used with many types of connectivity technology, so the same digital key can work across different radios and device types. At close range, NFC enables fast, deterministic tap-to-unlock with very low energy usage and predictable user intent. This is great for turnstiles, elevators, and battery-constrained readers.

Bluetooth® LE extends the interaction distance to a few meters for discovery and remote control of the Aliro smart lock. Lastly, Aliro supports hands-free access by combining Bluetooth® LE and Ultra Wideband (UWB) technology. Bluetooth® LE is used for device discovery and wake-up, while UWB adds precise, secured ranging and directionality, allowing the user trajectory to be understood by the reader and granting access when user intent is determined. It also provides strong resistance to relay attacks via time-of-flight measurements.

While NFC (13.56Mhz) is mandatory for each deployment and supports legacy products, such as Smart Cards, Bluetooth® LE (2.4GHz) or Bluetooth® LE plus UWB (typically using channel 9 from 7.75GHz to 8.25GHz) are optional. Only the combination of Bluetooth® LE and UWB supports secured hands-free access through relay resistant distance measurements as well as in-out detection enabled by UWB and enhanced data transfer utilizing Bluetooth® LE.



NFC, Bluetooth® LE and UWB

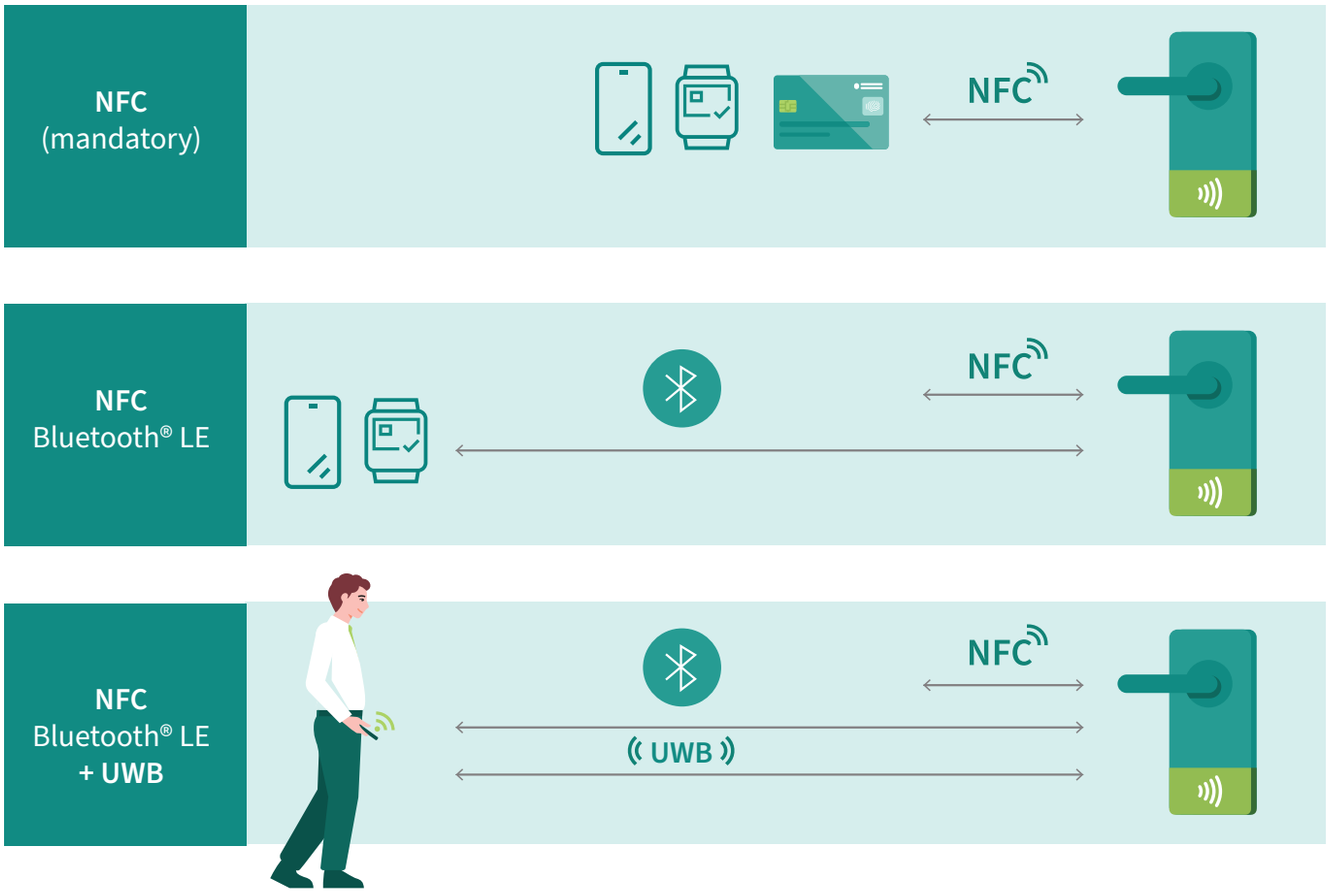


Figure 1 This diagram demonstrates how NFC and UWC work together using the Aliro standard

Security considerations

Aliro centers on modern, hardware backed cryptography and mutual authentication between a user device (e.g., Phone, watch or card) and a reader device. Aliro's security architecture is versatile and can support online and offline operation of smart access devices. It accommodates multiple credential types and lifecycles, including long lived device-bound mobile credentials, time limited or single use guest passes, role/group credentials, and site specific or area scoped keys, with issuance, renewal, suspension, and revocation managed by a backend system. All these elements give Aliro the flexibility to operate in private households, commercial access control and in the hospitality industry.

A typical Aliro interaction

An Aliro interaction already starts before the door opens and involves several steps:

1. Enrollment/provisioning: In this step, the issuer verifies a user and securely delivers a credential to the user's device, binding it to the hardware and setting the scope, validity, and revocation rules.
2. Discovery and PHY layer negotiation: At the door, the reader advertises capabilities. The device selects the best technology for access, and a secured session is established based on a challenge-response mechanism to prove possession and prevent replay.
3. If available and required by the implementation, UWB distance bounding confirms that the device is truly nearby before the credential is presented.
4. Afterwards, the reader evaluates the underlying policy that includes who, where, when, how close, and required factors.
5. Finally, it actuates the mechanism (unlock/deny) and records an event log entry for audit.



Beyond the basic access transaction, Aliro also supports different OEMs device management requirements (e.g., On device updates to extend/narrow permissions, background refresh of revocation lists and rapid revocation for lost device and key sharing.) Systems using Aliro also can implement failover behaviors, such as requiring a tap via NFC if hands free fails or enforcing stricter time windows when offline, to maintain safety, security, and a predictable user experience across a wide range of environments.

How Infineon supports Aliro 1.0 now and in the future

Infineon has been contributing to the development of the Aliro standard since 2021. We work closely with CSA's global Access Control ecosystem partners, ensuring the future adoption of Aliro across companies and other organizations worldwide including Infineon's broad product portfolio, such as microcontrollers, connectivity solutions, and security products.

Use Case: Infineon's products support smart door lock implementations

As an example, let's see how this process works using Infineon solutions for a smart lock implementation. PSOC™ microcontrollers (MCUs) act as the secured host in readers, orchestrating NFC, Bluetooth® LE and UWB while handling policy, logging, and actuator control. With secured boot, true random number generation, hardware crypto, and deep-sleep modes, PSOC™ MCUs let locks respond quickly while keeping keys and firmware protected, while ModusToolbox™ Software speeds up the integration and development.

AIROC™ Bluetooth® LE combos provide the proximity layer Aliro relies on for discovery and communication backbone for hands-free access. The solution's Bluetooth® LE 5.2 features, like extended/periodic advertising and privacy-preserving address rotation, enable quick, energy-efficient discovery, secured session bootstrapping, and a smooth handoff to UWB when ranging is required.

Infineon's UWB solutions add precise, secured two-way ranging for distance-bounding and strong relay-attack resistance. Implementations aligned with IEEE 802.15.4z deliver timestamped time-of-flight measurements with centimeter level accuracy to reliable detect user intent for access. Paired with a PSOC™ MCU's host, readers can fuse BLE presence with UWB distance to enable reliable hands-free access.

On the security side, Infineon is a long-term leading provider of Common Criteria certified Secure Elements used in Smart Cards, wearables or other smart devices. They support NFC interaction, hardware-backed key storage as well as today's ECC-based schemes, which are important for Aliro implementations as of today.

As security requirements change over time, continuous adaptations to potential threats are required. CSA takes security very seriously and has established a dedicated Product Security Working Group.

One good example of security over time is post-quantum cryptography (PQC). As cybersecurity threats increase, there is a concern on how to handle the rise of quantum computers which may endanger the security of IoT implementations and are expected to be available in the foreseeable future.

This is where CSA is expected to develop standardized solutions based on PQC for Aliro and other work groups, protecting data and communication from future threats posed by quantum computing.

Infineon is a pioneer in hardware based PQC and invests in solutions across its product portfolio. It has received the world's first Common Criteria Certification for a post-quantum cryptography algorithm (PQC) on a security controller in early 2025 and in late 2025, the industrial microcontroller family became compliant with the PQC requirements

To learn more about Infineon's smart door locks solutions, click on the link.

What's next for Aliro?

CSA, Infineon and the other ecosystem partners are working on Aliro enhancements based on ecosystem requirements and existing implementation learnings. These enhancements may include new application-level features, technology standards implementations, security enhancements or updating regulatory requirements, while maintaining backwards compatibility to safeguard current investments.

Sources

Aliro FAQ
Aliro launch page
Aliro press release