Research Report

Group 1 Tilburg

12-06-2025

Mohammed Salah – Lucas Lammers – Maher el Maziani – Obada Aljarrah – Mahmoud Ikhlaf – Rick Kanters

Contents

Version management

Version number	Date	Author	Changes
0.1	17-03-2025	Rick Kanters	Document created.
0.2	15-04-2025	Maher el. Maziani	Sub questions 1, 2, 5.
0.3	21-5-2025	Group 1 Tilburg	Feedback from group processed and document improved. House style applied.
0.4	23-5-2025	Group 1 Tilburg	Improved sub questions.
0.5	28-5-2025	Group 1 Tilburg	Sub questions 3 and 5 added

Introduction

This report presents an investigation into the digital security of the Flient Smart Lock, an advanced electronic locking system incorporating Bluetooth, Wi-Fi, NFC, mobile application interfaces, and biometric access control. The proliferation of smart home devices has heightened the necessity for comprehensive analyses of their security frameworks. Accordingly, this study systematically examines the potential vulnerabilities

This report is organized around a central research question, underpinned by five specifically formulated sub-questions that collectively establish the research framework. Each sub-question is treated separately in a chapter, in which the applied research methods are described, ranging from literature review and technical analysis to practice-oriented penetration tests and community-based threat assessments. For each sub-question, the findings corresponding to each sub-question are systematically analyzed and synthesized to derive substantiated conclusions concerning the system's security.

This report is directed towards educators, peers, and stakeholders possessing a technical background or interest in Internet of Things (IoT) and smart home security. By combining different methods and sources, the aim was to achieve as reliable, reproducible, and objective a research result as possible. Through this integrated approach, the report offers a comprehensive and verifiable assessment of the digital resilience of the Flient Smart Lock within the contemporary threat landscape.

Research Objective

This study aims to provide a comprehensive analysis of the digital security of the Flient Smart Lock. It focuses on identifying potential vulnerabilities within the technologies employed by the lock, including Bluetooth, Wi-Fi, and NFC. By analyzing and testing the system both theoretically and practically, we aim to determine to what extent the lock is resistant to unauthorized access, both digital and physical.

To get a complete picture of the security, the robustness of the used protocols and techniques is examined on paper, but especially the practical resilience in realistic scenarios. The research combines insights from existing literature on industry standards and known vulnerabilities with technical analyses of both the lock itself and the associated mobile application. In addition, structured penetration tests and simulated attack scenarios were conducted on the smart lock.

Through this combined approach, the aim of the research is to outline a reliable and applicable picture of the current security status of the Flient Smart Lock. Based on the findings, recommendations are also formulated that contribute to improving the digital security of the product.

Research Questions

This chapter delineates the primary research question that underpins the investigation. It is followed by the formulation of the central question, which constitutes the core focus of the study on the digital security of the Flient Smart Lock.

To answer this main question in a structured way, it has been elaborated into five sub-questions. Each sub-question addresses a specific aspect of the technologies used or the threat landscape and contributes to obtaining a complete and substantiated answer to the main question. Throughout the research, these sub-questions are analyzed, investigated, and answered individually.

Main Question

- How can we gain unauthorized access to the Flient Smart Lock?

Sub-questions

- Which technologies are used in the Flient Smart Lock and how do they work?
- How do the encryption methods and authentication protocols in the Flient Smart Lock compare to industry standards?
- How does the mobile app communicate with the Flient Smart Lock, which security protocols are used, and is it possible to manipulate and/or intercept the app?
- Are there previously discovered vulnerabilities that are still present in the Flient Smart Lock?
- How susceptible is the Flient Smart Lock to physical attacks, for example PIN code, lock, and fingerprint?

DOT-framework

This study was conducted utilizing the strategies and methodologies outlined in the Development Oriented Triangulation (DOT) framework. Each sub-question within this research is linked to specific research methods that help in obtaining valuable insights and ensuring the functionality and security of the smart lock. This approach makes it possible to test the smart lock in different phases and to extensively document the vulnerabilities found.

The methods are chosen based on the available resources for pentesting the smart lock. The aim is to ensure that sufficiently diverse methods are used to test and evaluate the security of the smart lock.

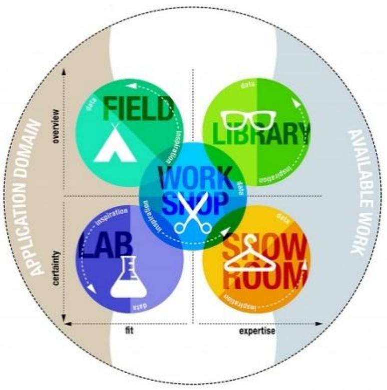

Figure 1 DOT-Framework

Which technologies are used in the Flient Smart Lock and how do they work?

The Flient Smart Lock Advanced is an advanced smart door lock that combines multiple technologies to provide secure and flexible access control. The subsequent section provides a detailed examination of the technologies employed in this study, elucidating their functionalities and integration within the research framework.

Wi-Fi and Bluetooth Communication:
The Flient Smart Lock uses Wi-Fi and Bluetooth for wireless communication. This allows users to operate the lock via a smartphone app. The communication protocols ensure a reliable connection between the lock and the user's devices, enabling remote access and management (Jeffrey, 2025).

A mobile-controlled door lock system that enables data exchange between devices is called Bluetooth. It connects to headphones and other accessories, usually in smartphones and other mobile devices. It is recently used in locks to enable keyless entry and connect locks with mobile devices. But how does a Bluetooth lock work and what exactly is it?

According to (Mmldigi, 2022), Bluetooth smart door locks are usually used in combination with a smartphone and are designed to protect you remotely. Once the lock is purchased, it must be paired with the primary device. The lock can only be unlocked by pressing a button on your smartphone. Instructions and temporary keys can also be given to other family members and/or colleagues. These mobile-controlled door locks are easy to install and a fantastic replacement for traditional door locks.

They must be connected to your Bluetooth to accept commands from your smartphone. After downloading and installing the app, you must enter a special access code on the device you are using. For most smart Bluetooth locks, people can create temporary virtual keys that only work at specific times. So, if you want to let someone in, you can create a temporary key that gives that person access at specific times.

Fingerprint Scanner:
A fingerprint scanner is used for biometric authentication. The user places their finger on the scanner, which scans the unique fingerprint patterns and compares them with stored data to grant access. This provides a secure and convenient way to unlock the door without the need for a physical key or code (Jeffrey, 2025).

The Flient Smart Lock uses an integrated fingerprint scanner that can store up to 300 unique fingerprints. The scanner recognizes a fingerprint within 0.1 seconds and immediately provides feedback in the case of a failed attempt (Flient® Smart Lock Advanced - Slimme Deurslot - Deurklink met Vingerafdruk - Met APP & WiFi - BlueTooth - Kantoor Slot - Zwart - Anti inbraak - TT lockApp, sd).

Biometric authentication is used by fingerprint-scanning door locks to scan and identify the unique fingerprint of each person. The smart lock links your fingerprint to the stored information when you place your finger on the sensor. The door is unlocked if it matches an authorized print, giving you secure access to your home without the need for cards or keys.
Compared to conventional door locks, fingerprint-scanning door locks are more convenient and secure due to their enhanced capabilities. By ensuring that only authorized individuals have access, these fingerprint scanner locks offer increased security (Strauss, 2025).

NFC Technology:
Nowadays, many smart locks in addition to Bluetooth also have NFC chips – a standardized set of rules applied to RFID chips. Radio-frequency identification, or RFID, is a technology that essentially

uses radio waves to transmit identification data between devices (How to Use NFC Door Locks (and Unlock Them With a Phone), sd).

Near Field Communication (NFC) technology makes it possible to open the lock with an NFC tag or card. The user holds the NFC tag or card close to the NFC reader of the lock, after which the lock reads the tag via wireless communication and verifies the access rights. With valid authorization, the door is automatically unlocked (Jeffrey, 2025).

Mobile App Integration:
The Flient Smart Lock is managed via a specially developed mobile application available for both iOS and Android platforms. This app forms the central control point for users and allows them to operate the lock via a wireless connection over Wi-Fi or Bluetooth Low Energy (BLE). The choice between Wi-Fi and Bluetooth depends on the context: Bluetooth is mainly used for direct proximity unlocking, while Wi-Fi enables remote access via a secure cloud connection.

The app offers a wide range of features that contribute to both convenience and security. For example, users can lock or unlock the door remotely, such as to grant access to a visitor when they are not at home themselves. Additionally, users can generate and manage digital keys, which means temporary or permanent access can be granted to other individuals, such as family members, domestic workers, or tenants. These keys can be configured with specific permissions and time limits, enabling fine-grained access control.

Another important feature is the configuration of access schedules, whereby access is only possible within certain time frames. This function is particularly useful for situations such as vacation rentals or office management. Furthermore, users can receive push notifications via the app for every door activity, including notifications of failed access attempts or sabotage attempts, which contributes to overall security and monitoring.

Keypad Entry:
The lock has a keypad for entering a code to unlock the door. Users can enter a predefined code to gain access, which is useful for situations in which other access methods are not available or preferred.

Traditional Key:
Despite being a smart lock, it also supports traditional key access. This provides a backup option in case of technical problems or for users who prefer the familiarity of a physical key.

Gateway:
The Gateway component enhances the functionality of the lock by enabling remote access and control via the internet, allowing users to manage the lock from anywhere in the world.

Security Features
The Flient Smart Lock is equipped with multiple built-in security measures designed to detect and prevent both digital and physical attacks. One of the core components of this security is the encrypted communication between the mobile application and the smart lock. Encryption protocols such as AES-128 or higher are used for this, ensuring that all data during transmission is encrypted and cannot be intercepted or read as plain text.

Additionally, the system has an automatic locking feature (“auto-lock”), in which the lock automatically locks itself after a pre-set period if no activity is detected. This prevents the door from being accidentally left open. Another convenient function is the passage mode, in which the lock remains temporarily open for events or during office hours, without requiring repeated unlocking.

In terms of access management, the Flient Smart Lock offers detailed configuration options. Users can create digital keys with specific rights, time restrictions, and logical conditions, such as access on certain days or times. This allows owners to assign different permissions per user, which is especially useful in shared living spaces or rental situations.

An important security measure against physical manipulation is the active alarm system. When a user enters an incorrect access code five times on the keypad of the lock, a security protocol is automatically activated.

This protocol triggers an internal alarm sound and temporarily blocks further input attempts to discourage brute-force attacks. At the same time, the owner receives a notification via the mobile app, making them immediately aware of a possible break-in attempt. This feature significantly contributes to the physical security of the system.

(Jeffrey, 2025)

Conclusion

The document analyses have contributed to an in-depth understanding of the operation and security structure of the Flient Smart Lock. Although not all technical specifications are publicly available, practical observations and user documentation provide sufficient starting points to conclude that the system has a versatile and well-thought-out security architecture.

In the following sub-questions, this theoretical foundation will be further deepened through concrete test cases. The applied technologies of the lock will be tested in controlled scenarios, with the aim of evaluating reliability and security in practice. In addition, any vulnerabilities will be identified and analyzed.

How do the encryption methods and authentication protocols in Flient Smart Lock compare to industry standards?

Bluetooth Low Energy (BLE) Communication
The TTLock smart lock system primarily uses Bluetooth Low Energy (BLE) for short-range communication between the lock and a mobile device. BLE is a popular choice in the smart lock industry due to its low energy consumption and secure data transmission.

BLE in TTLock:
AES-128 encryption**:** TTLock uses AES-128 to encrypt BLE communication. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that is widely applied in various sectors. AES-128 offers a good balance between performance and security.

Challenge-Response authentication**:** TTLock applies a dynamic authentication method in which a unique challenge is sent for each access attempt. The linked mobile device must respond with the correct cryptographic key, preventing the reuse of intercepted data (replay attacks).

Secure pairing: TTLock uses BLE pairing methods that ensure encryption keys are exchanged securely. Although "Just Works" pairing is often used, more secure methods such as Passkey Entry or Numeric Comparison are increasingly considered industry standard for additional protection.

Industry standard for BLE:
Within the industry, AES-128 is considered the most common encryption method for Bluetooth Low Energy (BLE), due to the balance between security and energy efficiency. Although used less frequently, AES-256 is considered a more ideal option, especially in applications where a higher security level is required.

Authentication within BLE generally takes place via a challenge-response mechanism. This ensures that devices can reliably verify each other without directly exchanging sensitive data.

For pairing devices, LE Secure Connection has been used since the introduction of BLE 4.2. This pairing method offers significantly better protection against eavesdropping and tampering, making it an important improvement compared to older BLE versions. The combination of these elements forms the core of secure BLE communication according to current industry standards.

Recommendations for Improving BLE Security:
To strengthen the security of Bluetooth Low Energy (BLE), it is advisable to switch from AES-128 to AES-256. This upgrade significantly increases the confidentiality of communication and offers better protection against future cryptographic attacks.
In addition, it is important to implement LE Secure Connections, a feature available since BLE 4.2. This provides stronger protection against man-in-the-middle attacks and prevents passive eavesdropping by using more advanced key exchange and encryption techniques.

Furthermore, periodically rotating BLE keys contributes to a more dynamic security model. By renewing keys regularly, the risk of prolonged exposure in the event of a compromised key is significantly reduced.
Together, these measures ensure a substantial improvement in overall BLE security. (Hlapisi, 2023) (Ren, 2025)

WiFi Communication
Through a special WiFi gateway, TTLock enables cloud integration for remote access, management, and monitoring. This provides additional functionality, such as unlocking doors remotely and receiving activity notifications.

WiFi in TTLock:

- TLS encryption: TTLock uses TLS (usually TLS 1.2 or higher) to secure the communication between the mobile app, the cloud, and the lock
    - TLS ensures authentication and encryption of all transmitted data.
    - TLS certificates verify the legitimacy of connected servers, which reduces the risk of man-in-the-middle attacks.
- JWT and OAuth 2.0: TTLock's cloud platform uses JSON Web Tokens for session management and access control. Tokens are time-bound and have limited access, which strengthens security in multi-user environments.

Industry standard for WiFi:
Within the industry, clear standards apply for WiFi security, with encryption and authentication at the center. TLS 1.2 is still widely supported, but TLS 1.3 is preferred due to its improved speed and security. It is therefore desirable to migrate to TLS 1.3 where possible to benefit from its more advanced cryptographic features.

In the area of wireless security protocols, the standard is shifting to WPA3. Although WPA2 is still most commonly used in practice, WPA3 offers significant advantages, such as better protection against password attacks and improved security on public networks. This development makes WPA3 the intended industry standard.

For authentication, OAuth 2.0 is generally used in combination with JSON Web Tokens (JWT). This method allows for secure and scalable access, with tokens assigning rights to users and devices in an efficient and controlled manner. This combination of techniques forms the backbone of a modern and robust WiFi security infrastructure.

Recommendations for Improving WiFi Security:

To improve WiFi security, it is advisable to switch to TLS 1.3. This version not only offers better performance through faster session handshakes but also increases security thanks to improved encryption protocols.
For additional protection of network communication, it is wise to implement Mutual TLS (mTLS). This ensures mutual authentication between client and server, so that only verified devices gain access.

Furthermore, it remains crucial to adopt WPA3 as the standard for wireless communication between router and gateway. WPA3 offers stronger protection against brute-force attacks and increases the security of public networks.
To further regulate access to network resources, short-lived access tokens can be used. These tokens reduce the risk in case of interception, especially when combined with secure refresh tokens and careful handling.

These measures together ensure a solid, future-proof security architecture. (WPA3 | TP-Link, sd) (contributors, sd)

NFC

TTLock locks support NFC technology (Near Field Communication), allowing users to unlock doors with contactless IC cards or NFC-compatible devices. This offers an alternative to using traditional keys or unlocking via Bluetooth on a mobile device.

NFC implementation in TTLock:

- Supported Devices
  TTLock uses MIFARE-compatible IC cards that operate on 13.56 MHz.
- Access Management
  Administrators can assign NFC cards via the TTLock app with the following access types:
  - Permanent – Cards remain valid indefinitely.
  - Timed – Cards are only valid within a specified time period.
  - Recurring – Cards are active at specific times on certain days of the week.
- Card registration
  NFC cards can be added directly at the lock via the administrator’s mobile device using Bluetooth. Remote registration is also possible via a TTLock card encoder when the lock is connected via a WiFi gateway.
- Access revocation
  Administrators can revoke card access via Bluetooth (near the lock) or remotely via the gateway.

Security considerations

TTLock uses NFC cards described as “MIFARE-compatible” but does not provide specific information about the exact type of card used. In practice, MIFARE Classic is often used — a technology known for its widespread use, but unfortunately also for its outdated and vulnerable security mechanisms. For applications requiring a higher level of security, MIFARE DESFire is preferable. These cards offer more advanced encryption standards, such as AES, and are therefore significantly more resistant to attacks.

In terms of authentication, TTLock also leaves room for improvement. There is no clarity about the use of secure protocols such as a mutual challenge-response mechanism when communicating with NFC cards. The absence of such methods increases the likelihood of cloning or replay attacks, especially when cards with lower security levels are used. This uncertainty emphasizes the need for transparency and strengthening of authentication techniques within the system.

Industry standards for NFC Security

Within the industry, technologies such as MIFARE DESFire EV1 and EV2 are considered the standard for NFC security. These support AES encryption and mutual authentication, which are essential for achieving secure communication between card and reader. Because of these properties, they are particularly suitable for applications where a high level of security is required, such as access control in sensitive environments.

A crucial aspect of NFC security is the handling of cryptographic keys. It is vital that these keys are securely stored and managed, and that they are renewed regularly. This prevents malicious actors from using a compromised key for extended periods or from easily copying cards.

In addition, audit logging plays an important role in ensuring the integrity of an NFC system. By keeping detailed access logs, abnormal behavior can be detected in time and security incidents can be responded to quickly. This combination of technology, key management, and monitoring forms the core of a robust NFC security policy.

Recommendations for TTLock NFC Security

For better NFC security within the TTLock system, it is important that clarity is provided on which card types are actually supported. The distinction between MIFARE Classic and MIFARE DESFire is essential in this regard, as these cards differ significantly in their security capabilities. Transparent communication on this enables users to make well-informed choices based on their security needs.

In environments where security is a high priority, it is recommended to actively promote the use of MIFARE DESFire EV1 or EV2. These cards support strong encryption and mutual authentication, making them significantly more robust against cloning and tampering than older card types.

Additionally, it is important that TTLock provides insight into the authentication mechanisms used when reading NFC cards. When it is unclear whether challenge-response or other security layers are in place, uncertainty arises about the system’s resilience to attacks such as replay or card cloning.

Finally, it would be valuable if TTLock optionally supports a rolling code mechanism or a dynamic key system. By renewing or varying keys with each interaction, the risk of successful card duplication is significantly reduced, and the overall security of the system increases.

Comparison of Smart Locks

This comparison highlights the most important security and functionality features of three popular smart locks in relation to current industry standards. This provides insight into which models meet basic and advanced requirements for security and ease of use.

Feature/ Industry standard	TTLock	Blugate 66	August Smart Lock	Industrienormen
BLE Communication	Yes	Yes	Yes	Yes
BLE Encryption	AES-128	AES-128	AES-128	AES-128/ AES-256
BLE safe pairing	Yes (LE)	N.A.	Yes	LE Secure Connections
Challenge-Response Authentication (BLE)	Yes	Yes	Yes	Yes
WiFi Support via Gateway	Yes	Partly	Yes (built in)	Yes (Via gateway or direct)
TLS Encryption (WiFi)	TLS 1.2	N.A.	TLS 1.2/ 1.3	TLS 1.2/ 1.3
OAuth 2.0 + JWT Authentication	Yes	N.A.	Yes	Yes
WPA3 WiFi Security	Optional	N.A.	N.A.	WPA3
Cloud-Based Management	Yes	N.A.	Yes	Yes
Mobiele App Integration	Yes	Yes	Yes	Yes
AES-256 Support	No (default)	No	Optional	Optional
NFC Support	Yes (IC cards)	N.A.	No	Yes (DESFire EV1/EV2)

(How to use NFC door locks (and unlock them with a phone), n.d.) (Blugate 66 | Full Lock system, n.d.) (How August Smart Locks work | August Home, n.d.)

All three smart locks comply with the basic security according to the industry standards, but there are clear differences in the level of advanced security and functionality.
August Smart Lock scores the best because it fully supports the latest encryption standards (AES-256), modern WiFi security (TLS 1.3, WPA3), and robust authentication mechanisms. TTLock follows with a solid basis but lacks the latest security protocols in some areas. Blugate 66 lags behind due to limited support for secure pairing and incomplete WiFi security.

Conclusion

The encryption methods and authentication protocols that Flient Smart Lock applies via the TTLock platform show strong similarities with the applicable industry standards, but also show some points of attention where improvement is possible.

In the area of Bluetooth Low Energy (BLE) communication, Flient uses AES-128 encryption and a challenge-response mechanism for authentication. This corresponds with what is generally accepted within the sector. However, there remains room for improvement, such as the application of LE Secure Connections, which since BLE 4.2 is considered the standard for secure pairings.

Although AES-128 provides sufficient protection, upgrading to AES-256 would be a more logical choice in environments with higher security requirements. Additionally, information is missing about the periodic rotation of keys, which is an important aspect for reducing long-term vulnerability in wireless communication.

The WiFi component of the system largely meets expectations. The application of TLS 1.2 for data transmission between lock, app, and cloud offers a good basic security, and the use of OAuth 2.0 and JWT strengthens the control over user sessions. In the context of contemporary security standards, however, TLS 1.3 would be preferable due to improved performance and stronger encryption. The implementation of mutual TLS would also be a valuable addition to realize mutual authentication between client and server.

With regard to NFC access, important questions remain unanswered. Flient does not indicate which type of MIFARE cards are used. If it concerns MIFARE Classic, there are significant security risks, as these cards are vulnerable to cloning and replay attacks. Modern applications generally use MIFARE DESFire EV1 or EV2, which do meet the requirements of secure encryption and mutual authentication. The lack of transparency about the type of card and the authentication protocols used makes it difficult to fully assess the effectiveness of this security layer.

How does the mobile app communicate with the Flient Smart Lock, which security protocols are used, and is it possible to manipulate and/or intercept the app?

Mobile applications that control smart devices, such as smart locks, form an essential part of the Internet of Things (IoT) ecosystem. In this study, the communication between the Flient Smart Lock app and the associated backend server was analyzed based on practical penetration tests. Two test cases were conducted for this purpose: Test Case 2 – Weak Encryption and Test Case 4 – APK Reversing. These test cases served as an empirical basis for identifying the protocols used, security measures, and vulnerabilities.

Test Case 2 – Weak Encryption

Test Case 2 – Weak Encryption shows that communication between the mobile application and the server takes place via HTTPS, using Transport Layer Security (TLS) version 1.2. TLS is a widely accepted standard for secure data transmission and protects against eavesdropping, tampering, and spoofing (Patil, 2025). Analysis with Wireshark and Burp Suite showed that the TLS handshake is executed correctly and that the data stream is effectively encrypted.

The password traffic between the app and server is also hashed. However, the outdated MD5 hash function is used, which is known to be vulnerable to collision attacks and brute-force attacks (The md5 hashing algorithm is insecure, sd). Although MD5 prevents passwords from being transmitted in plaintext, the algorithm is not suitable for modern security requirements.

Test Case 4 – APK Reversing

In Test Case 4 – APK Reversing, the APK of the Flient app was decompiled using tools such as APKTool and JADX. The analysis of the source code revealed several serious security issues:

- **Hardcoded secrets:** The code contains hardcoded values such as API keys, client secrets, UUIDs, and passwords. This poses a direct risk of unauthorized access to the backend or to smart lock functionalities.
- **Lack of code obfuscation:** The application is not obfuscated, which significantly increases the readability of the source code and sensitive logic (Brook, 2024).
- **Insecure cryptography:** In addition to using MD5 for hashing, a hardcoded AES key is present, which is combined with the device's MAC address to generate encryption keys. This makes the encryption reproducible and therefore vulnerable.
- **Privacy-sensitive permissions:** The app requests access to, among other things, location, microphone, contacts, and storage. Although these permissions may be technically necessary, they increase the attack surface and the risk of misuse (Hick, 2021).

The combination of a properly implemented TLS connection with a poorly secured internal architecture creates a false sense of security. The presence of hardcoded secrets and the lack of code protection make it relatively easy for attackers to access sensitive functionalities or mimic parts of the protocol. As a result, attacks such as spoofing, replay attacks, and manipulation of firmware updates are not unthinkable.

G2 Gateway
One of the ways the mobile app communicates with the Smart Lock is through the G2 Gateway. This Gateway allows the lock to be unlocked remotely, even when you're not at home. Communication takes place via Wi-Fi and Bluetooth Low Energy (BLE): the mobile app sends data via Wi-Fi to TTlock's cloud server, which then forwards the data to the Gateway, and the Gateway unlocks the lock via BLE.

The cloud server knows which lock the data should be sent to because the MAC address of the Smart Lock is linked to the public IP address of the network where the lock is located. During communication, the data traffic is encrypted using a hardcoded AES key and a generated AES key. The hardcoded AES key can be retrieved through reverse engineering of the app. The generated AES key is created using a fixed method: a randomly generated 16-byte code is encrypted using the hardcoded AES key. In addition, the communication between the Gateway and the server is secured with TLS 1.2 encryption.

In theory, it is possible to emulate the Gateway (Aronsky, 2024), allowing the lock to be unlocked via a spoofed Gateway. However, our tests have shown that this has not been successful so far.

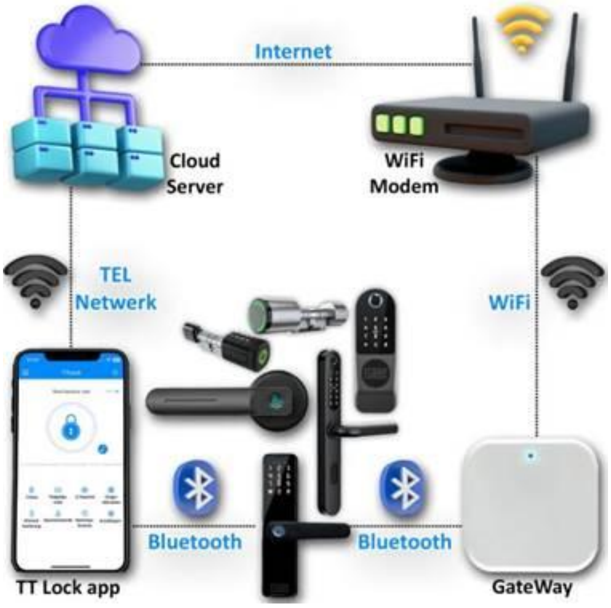

Figure 2 Lock - Gateway communication

BLE (Bluetooth Low Energy)

Regardless of whether the lock is opened via the app or the gateway, BLE communication always takes place. In Test Case 3 – BLE Sniffing, we intercepted and inspected the BLE traffic between the app and the lock. This revealed that BLE version 4.x is used. For BLE versions higher than 4.0, AES-CCM is used (DigiKey Employee, 2021).

This is a fairly secure protocol that is difficult to decrypt. Due to this encryption, we were unable to view the intercepted traffic. We also attempted to replay the traffic to possibly unlock the lock, but it turned out that a rolling code algorithm is used. This prevents BLE traffic from being reused.

As far as we have tested, the BLE communication between the app and the lock is secure. Further testing is required to fully assess the security of BLE.

Conclusion

The answer to the sub-question is that the mobile app communicates with the Flient Smart Lock through a combination of TLS-encrypted traffic with the server, BLE for local communication with the lock, and a G2 Gateway for remote access. Despite the use of recognized security protocols such as TLS 1.2 and AES-CCM, practical research shows that the security within the application architecture is seriously lacking. The presence of hardcoded keys, outdated hash functions, and the absence of code obfuscation make the app vulnerable to reverse engineering and manipulation.

As a result, it is possible to intercept or mimic parts of the communication process. The security may seem solid at first glance, but further analysis shows that it does not provide sufficient protection against well-prepared attacks. Real security requires more than just encrypting data traffic.

Are there previously discovered vulnerabilities that are still present in the Flient Smart Lock?

Community Research
For this study, community-based information gathering was used, analyzing existing data from reputable cybersecurity sources. The primary information sources included the National Vulnerability Database (NVD), Exploit Database (Exploit-DB), CVE Details, peer-reviewed academic literature, reports from cybersecurity companies, and relevant contributions on blogs and forums within the security community.

A structured search methodology was applied to identify vulnerabilities (CVEs) directly related to the Flient Smart Lock, to map recurring vulnerabilities in similar smart locks, and to evaluate whether these weaknesses could also apply to the Flient system.

Findings
Based on the research, two CVEs were found that are explicitly linked to the Flient Smart Lock: CVE-2023-50129 and CVE-2023-50124. Nevertheless, publicly available information about the security of this product is limited. The manufacturer follows a closed policy regarding vulnerability management, resulting in a lack of transparency and public assessments. However, the absence of publicly reported vulnerabilities does not automatically mean that the product is secure. Underreporting is a known issue with many IoT devices, which may allow risks to go unnoticed.

Analysis of similar smart lock products revealed several relevant vulnerabilities. For example, in the Shenzhen Dragon Brother FB50 (CVE-2019-13143), a vulnerability in the cloud API was discovered that enabled re-binding attacks. In another case, known as SweynTooth (CVE-2019-17517), a buffer overflow in a Bluetooth Low Energy (BLE) chipset allowed attackers to remotely crash the lock. Additionally, research by F-Secure showed that the KeyWe Smart Lock in 2019 used a weak BLE pairing method, allowing interception of the cryptographic key exchange and unauthorized unlocking of the lock.

Relevance to the Flient Smart Lock
Although only two specific CVEs are known for the Flient Smart Lock, the vulnerabilities found in other smart locks point to broader security risks. These include account takeover through insecure APIs, vulnerabilities in the BLE protocol such as those seen with SweynTooth, and insecure implementations of cryptography during Bluetooth pairing.

Recommendations for Testing Strategies
To determine whether these vulnerabilities are also present in the Flient system, it is recommended to test BLE communication for susceptibility to crashes, analyze cloud service endpoints for weak access control, and verify whether firmware properly implements security patches. This approach aligns with the lab portion of the Library & Lab method.

Conclusion
This community research shows that there are indeed publicly known CVEs for the Flient Smart Lock; two of them were reported by Secura. These vulnerabilities, along with known issues in similar smart lock products, provide valuable insights. They point to recurring security patterns within the smart lock domain and should be investigated within the Flient system to properly assess its resilience. This research supports the preparation phase of security testing activities within the Library & Lab method of the DOT framework.

Security tests

Titel: NFC Copying via Flipper Zero

Verify whether the previously discovered NFC cloning vulnerability is still present in the current version of the Flient Smart Lock.

Associated CVE number:

CVE-2023-50129

Test Method:

A Flipper Zero device was used to read the NFC signal of an authorized tag and then attempt to gain access using the cloned signal.

Procedure:

- An authorized NFC tag was scanned using the Flipper Zero.
- The captured data was replayed to the lock.
- It was observed whether the lock accepted the cloned NFC tag.

Result:

The vulnerability is still present: the lock accepted the cloned NFC tag. A demo video of the security test is available via the following link: https://streamable.com/ncnp7u.

Recommendation:

Use newer versions of NFC chips such as the MIFARE DESFire EV2 and a corresponding NFC reader that applies stronger encryption.

CVE-2023-50124 (Secura, 2023)

During the investigation, it was found that CVE-2023-50124, a vulnerability identified by Secura in the Flient Smart Lock, could not be reproduced within the scope of our test setup. Reproducing this vulnerability requires physical disassembly of the device and direct access to internal hardware components. Since the device was provided on loan, we chose not to open it due to the risk of damage.

However, based on the available information, we expect that this vulnerability is likely still present, as the same hardware appears to be in use since the time of Secura's report. The CVE is therefore most likely still exploitable, although we were not able to independently confirm this.

How susceptible is the Flient Smart Lock to physical attacks, for example PIN code, lock, and fingerprint?

Security Test

Objective:

To investigate how the Flient Smart Lock behaves under physical attacks targeting the PIN code, mechanical lock, and biometric authentication.

Mechanical Lock (Physical Key)

In the examination of the mechanical lock, attention was given to the design of the key and the behavior of the lock during lockpicking attempts. The key uses a dimple profile with double-sided grooves and multiple notches. Lockpicking attempts with standard tools showed that the pins consistently reset to their original position despite applied torsion. This indicates a certain level of lockpicking protection.

Key Findings:

- Likely presence of anti-pick mechanisms such as spool pins or false set protection.
- Standard lockpicking techniques were therefore ineffective.

PIN Code

For the PIN code entry, we specifically looked at potential information leakage through the physical use of the keypad. Fingerprints and grease traces can reveal which buttons are used frequently, increasing the likelihood of discovering the code.

Key Findings:

- Smudge attacks exploit grease smudges to identify used buttons.
- The number of possible code combinations can be significantly reduced as a result.
- The vulnerability depends on:
- The length of the PIN code.
- The presence of lockout mechanisms after multiple incorrect attempts.
- Possible randomization of buttons or other additional measures

In the case of the Flient Smart Lock, it was found that after five incorrect attempts, the lock is automatically locked. Unlocking is then only possible via the corresponding admin panel. This mechanism significantly hinders brute-force attacks. Although smudge attacks can theoretically expose a weak point, in practice it is difficult to accurately determine the correct PIN code from smudges alone—especially if the lock is used in a dynamic environment or cleaned regularly. Nevertheless, it remains a point of concern when additional protections are absent.

Fingerprint Scanner
The fingerprint scanner is the third verification method. The main focus here was to assess whether the scanner could be fooled using physical fake fingers. In theory, leftover fingerprints could be used to create molds.

Key Findings:

- Spoofing using silicone prints or 3D printing is a known attack scenario.
- The effectiveness of such an attack strongly depends on the type of sensor used:
- High-quality sensors with liveness detection offer resistance to this.
- Cheaper sensors without anti-spoofing measures are more vulnerable.
- Without concrete information about the scanner used, this remains a risk factor.

In our test, we attempted to trick the scanner using a simple fake finger based on a forged print. However, this attack attempt was unsuccessful. Whether this was due to built-in anti-spoofing measures or other technical characteristics of the scanner could not be determined due to a lack of insight into the exact sensor model. The vulnerability therefore remains theoretically possible but was not reproducible in practice.

Conclusion

In our research, the Flient Smart Lock demonstrated a reasonable level of physical security against common attack techniques targeting three key authentication mechanisms: the mechanical lock, the PIN code input, and the fingerprint scanner.

The mechanical lock, based on a dimple key profile, showed clear resistance to standard lockpicking techniques. The presence of possible anti-pick mechanisms such as spool pins or false set structures prevented us from successfully opening the lock using conventional tools. This indicates an above-average level of security within this product segment.

The PIN code input is theoretically vulnerable to smudge attacks, in which grease traces on the keypad may reveal the digits that were pressed. In practice, however, it proved difficult to reliably reconstruct a full code from this. Moreover, the system includes an effective lockout mechanism: after five incorrect attempts, the lock is blocked and can only be accessed again via the admin panel. This significantly hinders brute-force attacks, although it is still recommended to implement additional protections, such as key randomization.

The fingerprint scanner was tested for vulnerability to spoofing using a fake finger. Our attack attempt failed, but it remains unclear whether this was due to liveness detection, sensor resolution, or other built-in protections. Due to the lack of documentation on the specific sensor model used, the vulnerability remains theoretically present, although we could not confirm it in practice.

In summary, the Flient Smart Lock demonstrates solid physical security against standard attack methods. The combination of lockpicking-resistant mechanics, PIN code lockout, and (potential) biometric anti-spoofing contributes to a strong overall level of protection. However, it is recommended to provide transparency about the technologies used and to consider additional measures against information leakage through physical use.

Community Research

Objective:

To gauge what experiences, concerns, and vulnerabilities have been shared by users and experts in the community regarding similar smart locks.

Found in literature and communities:

According to Secura, physical security aspects are often underemphasized in smart locks. Manufacturers generally focus primarily on the software side.

Common concerns in the community:

- Poor physical build quality makes the lock vulnerable to brute force (forcing the lock).
- Users report cases where cheap sensors in the fingerprint scanner are easy to fool.
- PIN code leaks due to smudge attacks are widely recognized as a real risk.
- Some users report that mechanical backup keys are often poorly secured (low-complexity keys).

Recommendations from the community:

- Use long PIN codes.
- Regularly clean the keypad to remove fingerprints.
- Use keypad covers or randomizer layouts.
- Always combine physical security with software-based monitoring.

Additional vulnerability identified by Secura

Secura identified a specific critical vulnerability during its analysis (CVE-2023-50124), which has direct implications for the security of the biometric system in the Flient Smart Lock.

The fingerprint scanner uses an AES1711 module, which is physically located in the door handle. Two screws on the exterior make it relatively easy to remove the sensor. By connecting the sensor via UART to a debug board, an attacker can use the default password to add new fingerprints. The lock then only checks whether the presented fingerprint matches a registered template, without performing any additional authentication.

Summary:

- Physical access to the sensor can be gained within minutes by removing the external screws.
- Via UART access with default credentials, a new fingerprint can be programmed.
- After reinstalling the sensor, only the new fingerprint is accepted; the original user is locked out.
- This attack is relatively easy to perform and requires only limited technical means.
- The fundamental problem is that the system relies on the integrity of the stored fingerprints without external verification or encryption.

Conclusion – Community Research

The community confirms that physical attacks on smart locks are a known issue, especially with cheaper models that lack advanced physical protection. The PIN code, key, and fingerprint scanner all pose potential attack vectors.

Conclusion

The principal research question addressed in this study is: To what extent is unauthorized access to the Flient Smart Lock feasible? The findings indicate that, despite the integration of contemporary security technologies, the lock is susceptible to unauthorized access.

The analysis revealed that the system employs multiple technologies, including Bluetooth, Wi-Fi, NFC, and biometric authentication. While this multi-faceted approach enhances versatility, it concurrently amplifies the potential attack surface, thereby increasing the risk of vulnerabilities.

Encryption protocols implemented within the system partially adhere to industry standards; however, they exhibit deficiencies that could be exploited. Notably, the absence of advanced encryption standards such as AES-256 and TLS 1.3 compromises the robustness of data protection mechanisms.

Security assessments of the associated mobile application uncovered several critical issues, including the presence of hardcoded cryptographic keys and the utilization of outdated cryptographic algorithms. These vulnerabilities facilitate potential manipulation and unauthorized access.

Furthermore, the study identified that known security vulnerabilities persist within the system. Specifically, the NFC functionality and physical access to the fingerprint scanner were found to be particularly susceptible to exploitation.

Physical penetration testing demonstrated that while the lock resists conventional bypass methods, it remains vulnerable to targeted attacks.

In conclusion, the research indicates that, although the Flient Smart Lock incorporates advanced security features, practical implementation flaws render it susceptible to unauthorized access. This underscores the necessity for enhanced security measures and adherence to contemporary cryptographic standards to fortify the system against potential threats.

Figures

Bibliography

Aronsky, L. S. (2024, Februari 20). *Say Friend and Enter: Digitally lockpicking an advanced smart lock (Part 1: functional analysis).* Retrieved from alephsecurity: https://alephsecurity.com/2024/02/20/kontrol-lux-lock-1/

Blugate 66 | Full Lock system. (n.d.). Retrieved from https://www.fulllocksystem.com.ar/blugate-66/

Brook, C. (2024, March 24). *What Is Code Obfuscation & How Does It Work?* Retrieved from digitalguardian: https://www.digitalguardian.com/blog/what-code-obfuscation-how-does-it-work

contributors, W. (n.d.). *Transport layer security*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Transport_Layer_Security

DigiKey Employee. (2021, Maart 4). *A basic introduction to BLE 4.X Security - Wireless and IoT / RF and Wireless - DigiKey TechForum - an electronic component and Engineering solution Forum.* Retrieved from DigiKey TechForum - an Electronic Component and Engineering Solution Forum.: https://forum.digikey.com/t/a-basic-introduction-to-ble-4-x-security/12501

Flient® Smart Lock Advanced - Slimme Deurslot - Deurklink met Vingerafdruk - Met APP & WiFi - BlueTooth - Kantoor Slot - Zwart - Anti inbraak - TT lockApp. (n.d.). Retrieved from bol.com: https://www.bol.com/nl/nl/p/flient-smart-doorlock-slimme-deurslot-deurklink-met-vingerafdruk-met-app-wifi-bluetooth-kantoor-slot-zwart-anti-inbraak-tt-lockapp/9300000128216261/

Hick, B. (2021, January 27). *Android's "Dangerous" Permissions*. Retrieved from thebinaryhick: https://thebinaryhick.blog/2021/01/26/androids-dangerous-permissions/

Hlapisi, N. (2023, September 22). *Bluetooth LE: security modes and procedures explained*. Retrieved from Technical Articles: https://www.allaboutcircuits.com/technical-articles/bluetooth-le-security-modes-and-procedures-explained/

How August Smart Locks work. (n.d.). Retrieved from August Home: https://august.com/pages/how-it-works

How August Smart Locks work | August Home. (n.d.). Retrieved from https://august.com/pages/how-it-works

How to use NFC door locks (and unlock them with a phone). (n.d.). Retrieved from https://www.getkisi.com/academy/lessons/how-to-use-nfc-door-locks

How to Use NFC Door Locks (and Unlock Them With a Phone). (n.d.). Retrieved from getkisi: https://www.getkisi.com/academy/lessons/how-to-use-nfc-door-locks

Jeffrey. (2025, January 2). *Deur Openen op Afstand met Telefoon: Wij testen het uit!* Retrieved from Domotiseren.nl: https://domotiseren.nl/reviews/flient-smart-lock-advanced/

Mmldigi. (2022, December 8). *What is Bluetooth door lock & how do they work?* Retrieved from betechiot: https://www.betechiot.com/what-is-bluetooth-door-lock/

Patil, K. (2025, March 25). *Why Is TLS 1.3 Better And Safer Than TLS 1.2?* Retrieved from appviewx: https://www.appviewx.com/blogs/why-is-tls-1-3-better-and-safer-than-tls-1-2/

Ren, K. (2025, May 1). *Bluetooth LEsecure connections - numeric comparison*. Retrieved from Bluetooth® Technology Website: https://www.bluetooth.com/blog/bluetooth-pairing-part-4/

Secura. (2023, 1 1). *Safety risks in common smart home devices*. Retrieved from www.secura.com: https://www.secura.com/services/iot/consumer-products/security-concerns-in-popular-smart-home-devices

Strauss, C. (2025, March 26). *Everything you need to know about fingerprint door lock system.* Retrieved from gvlock: https://www.gvlock.com/blog/fingerprint-smart-locks/

The md5 hashing algorithm is insecure. (n.d.). Retrieved from datadoghq: https://docs.datadoghq.com/security/code_security/static_analysis/static_analysis_rules/go-security/import-md5/

TTLock Locks | *Seam API Docs*. (n.d.). Retrieved from https://docs.seam.co/latest/device-and-system-integration-guides/ttlock-locks

WPA3 | *TP-Link*. (n.d.). Retrieved from TP-Link: https://www.tp-link.com/us/wpa3/