



Allegion ENGAGE™
Wi-Fi® Middleware
Security Fundamentals
White Paper

MARCH 2025
Version: pre2

Allegion Product Cybersecurity Team

Allegion plc
Hague Road Technical Center
8750 Hague Road
Indianapolis, IN 46256
cybersecurity@allegion.com

KRYPTONITE ■ LCN ■  ■ STEELCRAFT ■ VON DUPRIN

© 2025 Allegion plc. All rights reserved. ALLEGION, KRYPTONITE, LCN, PIONEERING SAFETY, SCHLAGE, STEELCRAFT, ISONAS and VON DUPRIN are the property of Allegion plc. All other brand names, product names or trademarks are the property of their respective owners.

The information contained in this document is proprietary. If the reader is not a representative of the intended recipient, any review, dissemination or copying of this document or the information it contains is prohibited. If you have received this document in error, please notify the sender and delete the document.

Table of Contents

1	ABSTRACT	3
1.1	DEVICES AND TECHNOLOGIES.....	3
2	FOUNDATION OF ALLEGION SECURITY	3
2.1	SECURITY AND PRIVACY BY DESIGN.....	4
2.2	BUILT ON PROVEN SECURITY PRACTICES	4
2.3	SECURITY UPDATES AND VULNERABILITY MANAGEMENT.....	4
2.4	TESTED BY INTERNAL AND EXTERNAL EXPERTS	4
3	ENGAGE WI-FI SECURITY	5
3.1	OUTER LAYER – TLS ENCRYPTED IP COMMUNICATION LAYER.....	5
3.2	INNER LAYER – PRODUCTION KEY	5
3.3	LOCAL LAYER – SITE KEY.....	5
4	ENGAGE™ BLUETOOTH LOW ENERGY SECURITY	6
4.1	LAYERED SECURITY	6
4.2	INNER LAYER – PRODUCTION KEY	6
4.3	LOCAL LAYER – SITE KEY.....	6
4.4	BLE COMMUNICATION LAYER – TEMPORARY KEY.....	6
4.5	ENGAGE™ BLE AUTHENTICATION.....	7
5	ALLEGION ENGAGE WI-FI MIDDLEWARE SERVER SECURITY	7
5.1	ALLEGION ENGAGE WI-FI MIDDLEWARE WEB MANAGEMENT SERVER.....	7
5.2	ALLEGION ENGAGE WI-FI MIDDLEWARE VIRTUAL CONTROLLERS	8
5.3	ALLEGION ENGAGE WI-FI MIDDLEWARE DATA STORAGE	8
6	CONCLUSION	8

1 Abstract

As a proud member of Allegion's family of pioneering brands, Schlage products are dedicated to delivering seamless access and a safer world.

Allegion ENGAGE™ Wi-Fi Middleware serves as a bridge for seamless interoperability between devices utilizing Schlage ENGAGE™ locks in non-real-time Wi-Fi mode and access control systems that expect real-time connectivity. By enabling communication between these systems, the middleware ensures efficient integration and functionality, catering to environments where real-time connected locks are expected.

1.1 Devices and Technologies

The following devices are supported with the Allegion ENGAGE™ Wi-Fi Server:

- Schlage NDEB Mobile Enabled Wireless Cylindrical Locks
- Schlage LEB Mobile Enabled Wireless Mortise Locks

2 Foundation of Allegion Security

Security and privacy are at the core of what we do and what we think about every day. We take a comprehensive approach to ensuring safety and security to protect the devices, products, and systems that safeguard people and assets wherever they reside, work, and thrive.

Allegion has a Product Cybersecurity Program that's designed around four key pillars:



2.1 Security and privacy by design

Incorporating security and privacy into technology solutions by default and by design is a fundamental expectation for Allegion's product development initiatives. Key principles guiding Allegion's approach to security and privacy by design include:

- Defense in Depth: implementing multi-layered security controls.
- Data Protection: ensuring data is secure both at rest and in motion.
- Assumption of Insecurity: Operating under the assumption that external systems may be insecure.
- Authentication/Authorization: Authenticating users and processes, followed by verification of their authorization.
- Periodic Security Reassessment: Regularly reviewing and updating security measures.
- Respect for Privacy: users' right to privacy is respected.

2.2 Built on proven security practices

Security technology is important to security, but the practices of the people who develop that technology are more important. These practices are the foundation of security. It is crucially important that security practices be good ones. Allegion's key best practices include:

- Full-time global cybersecurity team committed to embedding security into software and firmware development process.
- Cybersecurity training for all developers and testers.
- Security and privacy requirements defined during requirements phase.
- Threat modeling conducted during design phase.
- Static analysis tools utilized during implementation phase.
- Open-source analysis to ensure the security of third-party components.

2.3 Security updates and vulnerability management

Allegion takes security concerns seriously and acts to quickly evaluate and address them. Upon receipt of a security concern, Allegion promptly allocates the appropriate resources to analyze, validate, and provide corrective actions to resolve the issue.

2.4 Tested by internal and external experts

To help product teams address emerging security challenges, Allegion utilizes both internal and external experts to conduct penetration testing. These tests are guided by the [OWASP Application Security Verification Standard](#), which provides the range in coverage and level of rigor applied to each product/solution. This testing includes:

- Penetration testing (run-time analysis)

- Reverse engineering (binary analysis)
- Code reviews (static analysis)
- Threat modeling (design analysis)
- Device testing (hardware analysis)

3 ENGAGE™ Wi-Fi Security

ENGAGE™ Wi-Fi communication relies on a defense in depth strategy that consists of multiple layers.

The configuration of the wireless access point that a lock system is connecting to will impact the security of the Wi-Fi connections. In a separate White Paper titled “ENGAGE Wi-Fi Network Requirements” Allegion provides recommendations on best practices for both security and compatibility with Allegion devices. When configured with recommendations, Wi-Fi access points will use WPA2 to provide both authentication and encryption to Wi-Fi connections.

3.1 Outer Layer – TLS Encrypted IP Communication Layer

ENGAGE™ NDEB and LDEB devices use Transport Layer Security (TLS) version 1.2 to protect all IP connections. The TLS protocol aims to provide confidentiality, integrity, and authenticity of communications using cryptography. It is part of both the transport and the application layer of the TCP/IP model. With TLS, asymmetric encryption based on digital certificate chains is used to establish temporary symmetric keys used for communication. All data flowing across IP connections is then encrypted with these symmetric keys.

3.2 Inner Layer – Production Key

Before deployment, devices must first be captured using the Bluetooth® Low Energy (BLE) based ENGAGE™ Mobile Application. This process ensures that production key is utilized to transfer the site key and initial configuration into the device. The primary purpose of the production key is to prevent unauthorized access by prohibiting attackers from attempting to factory reset or reprogram the lock.

3.3 Local Layer – Site Key

The next layer allows anyone with appropriate access to the ENGAGE account to manage access for any device on that account. This unique AES-256 bit key protects all credentials used throughout the system, allows for authentication of remote endpoints, and allows for encryption of data at rest.

4 ENGAGE™ Bluetooth Low Energy Security

All ENGAGE™ devices use BLE as the method of communication with a mobile device. The design team took many factors into consideration in choosing to adopt BLE as the communication protocol to these devices. From the outset, it was determined that no ENGAGE™ device would rely on the BLE security protocol for any communication because the likelihood of that protocol being attacked and hacked was very high. To ensure the security of the ENGAGE™ system, a custom security protocol, using off-the-shelf encryption standards and best practices, was developed to meet our high security standards. To prove out the security of the method that is used, our devices and protocols have been third-party tested, and the protocol has been verified to utilize some of the most secure methods available.

4.1 Layered Security

It is a widely accepted principle in security that the most effective methodologies are built on a layered approach. Designs that have layered security rely on the many layers to protect sensitive information. ENGAGE™ was built with this same methodology in mind. Further, every key used in ENGAGE™ is an AES-256 bit key, which has nearly as many permutations as there are atoms in the observable universe – therefore, it is not possible to determine the key by brute force attacks with conventional technology. Finally, no ENGAGE™ device will react to any command or request until all of these layered security needs are met.

4.2 Inner Layer – Production Key

The highest security layer in ENGAGE™ is a unique AES-256 bit key programmed into every device. This key is programmed in an Allegion factory and is known only to Allegion. The purpose of this key is to allow the device to be uniquely captured on the final customer's door and to allow subsequent keys to be securely transmitted to that specific device. The fundamental purpose of this key is to prohibit an attacker from attempting to factory reset and reprogram the lock.

4.3 Local Layer – Site Key

The next layer allows anyone with appropriate access to the ENGAGE™ account to manage access for any device on that account. This unique AES-256 bit key protects all communications and data associated with that site.

4.4 BLE Communication Layer – Temporary Key

This AES-256 key is used to encrypt the data between the mobile application and the device. This key is unique to each mobile device, and to further protect the customer, it expires daily. Therefore, each mobile device is daily issued a unique key to allow it to

communicate with ENGAGE™ devices. This key is no longer accepted after that day and the mobile device will need a new one. This is among the reasons why the ENGAGE™ mobile application requires access to the internet in order to operate.

Further mechanisms are in-place to prevent replay attacks against any device preventing attempts to reuse this key at any time, or to even prevent reuse of an entire communication sequence.

4.5 ENGAGE™ BLE Authentication

ENGAGE™ devices employ a patented, layered security algorithm with multiple security keys in order to authenticate devices before communicating with them using BLE. Only after authentication does the device allow any information to be sent or gathered.

Initially, the peripheral (ENGAGE™ device) does not have information about the central device until the communication has been established. This means that any central can attempt to connect to an ENGAGE™ device. However, only those devices (ex. the ENGAGE™ Gateway) and applications (ex. the ENGAGE™ mobile app) that possess the correct authentication token and adhere to the security protocol can maintain the connection to perform operations.

To enhance security, if authentication is not successfully established within a few seconds of connection to an ENGAGE™ device, the ENGAGE™ device will break the connection. This prevents unauthorized access and ensures that only legitimate interactions are allowed.

5 Allegion ENGAGE™ Wi-Fi Server Security

Similar to other IP connections in ENGAGE, Wi-Fi Middleware components use Transport Layer Security (TLS) version 1.2 to protect all IP connections. The TLS protocol aims to provide confidentiality, integrity, and authenticity of communications using cryptography.

5.1 Allegion ENGAGE™ Wi-Fi Middleware Web Management Server

The Web Management Server supports customer provided certificate from a trusted certificate authority for use with TLS encrypted connections via HTTPS. The web management server optionally supports integration with Microsoft's Entra ID product suite for unified authentication with other enterprise identity and access management products.

5.2 Allegion ENGAGE™ Wi-Fi Middleware Virtual Controllers

Virtual Controller connections between the high level access control system and the individual virtual controllers use a proprietary binary protocol protected with TLS 1.2.

5.3 Allegion ENGAGE™ Wi-Fi Middleware Data Storage

Allegion ENGAGE Wi-Fi Middleware utilizes Microsoft SQL Server for data storage. Customers have the option of locating the database on the same machine as the Web Management Server and Virtual Controllers, where the database can be completely isolated from remote connections. Customers can also choose to locate the database remotely for compatibility with corporate guidelines. Remote databases can authenticate using Microsoft Entra ID.

6 Conclusion

The communication capabilities of ENGAGE devices inherently create potential opportunities for attacks. However, Allegion has implemented robust security protocols specifically designed to mitigate these risks. These protocols provide protection against wireless attacks, such as sniffing and replay, and are continuously monitored, tested, and updated to address emerging threats. Additionally, our security measures undergo rigorous validation by multiple third-party experts to ensure the algorithms employed remain resistant to known and evolving attack vectors.

By combining advanced encryption techniques, ongoing assessments, and industry-leading best practices, Allegion reinforces its commitment to delivering secure and reliable solutions for protecting people, assets, and systems.

About Allegion

KRYPTONITE ■ **LCN** ■  ■ **STEELCRAFT** ■ **VON DUPRIN**

The information contained in this document is proprietary. If the reader is not a representative of the intended recipient, any review, dissemination or copying of this document or the information it contains is prohibited. If you have received this document in error, please notify the sender and delete the document.

At Allegion (NYSE: ALLE), we design and manufacture innovative security and access solutions that help keep people safe where they live, learn, work and connect. We're pioneering safety with our strong legacy of brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss®, and Von Duprin®. Our comprehensive portfolio of hardware, software and electronic solutions is sold around the world and spans residential and commercial locks, door closer and exit devices, steel doors and frames, access control and workforce productivity systems. For more, visit www.allegion.com.