Mobile Access Credential Security White Paper

June 2020
Version 3

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

The information contained in this document is privileged and 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**

2. INTRODUCTION **4**

3. SECURITY OVERVIEW **4**

4. FOUNDATION OF SCHLAGE MOBILE ACCESS SECURITY **4**

4.1 Security and privacy by design 5
4.2 Built on proven security practices 5
4.3 Security updates and vulnerability management 5
4.4 Tested by internal and external experts 5

5. SCHLAGE MOBILE ACCESS CONSISTS OF MULTIPLE SECURITY LAYERS **6**

5.1 Software Development Kit (SDK) 6
5.2 On mobile devices 6
5.3 On readers 6
5.4 Mobile device to cloud 6
5.5 NFC credential messaging protocol 6
5.5.1 Mobile device to reader *6*
5.5.2 Key diversification and encryption *7*
5.5.3 Mitigation against man-in-the-middle attacks *7*
5.5.4 Credential data integrity *7*
5.6 BLE credential messaging protocol 7
5.6.1 Mobile device to reader *7*
5.6.2 Mitigation against man-in-the-middle attacks *7*
5.6.3 Mitigation against relay attacks *8*
5.6.4 Credential data integrity *8*
5.7 Back end 8
5.7.1 Account and access management *9*
5.7.2 Security monitoring *9*
5.7.3 Data protection *9*
5.7.4 Redundancy *10*
5.8 Third party assessment 10

1. Abstract

The Schlage Mobile Access Software Development Kit (SDK) provides our partners with the capability to create and manage both Near Field Communication (NFC) and Bluetooth Low Energy (BLE) mobile credentials. Allegion intentionally incorporated many layers of security into the design of the SDK, including data encryption at rest and in motion, key diversification, certificate pinning, and many patent-pending security features. The SDK was designed to protect against various types of attacks including Man-in-the-Middle, Replay, Relay, and Spoofing attacks. Importantly, a third-party independent security expert validated the design of our SDK during the design phase and conduct penetration testing at the end of the project to validate the implementation was resilient against known attacks.

2. Introduction

Schlage® empowers our partners to create and manage credentials that can be presented via an end user's mobile device (e.g., a smart phone). Schlage accomplishes this by providing them with the Schlage Mobile Access Software Development Kit (SDK) that implements the security protocol for the mobile credential for both NFC and BLE communication. This white paper will discuss the various security features employed.

3. Security overview

When designing the Schlage Mobile Access SDK for the creation of mobile credentials utilizing NFC communication, Schlage was guided by the security model described in the NXP Semiconductors Application Note AN10969, titled "System level security measures for MIFARE installations" and the NXP Semiconductor Application Note AN10922, titled "Symmetric key diversifications". Schlage's Mobile Access NFC Credential is Schlage's adaptation of the MIFARE DESFire EV1 card protocol in a virtual credential scenario.

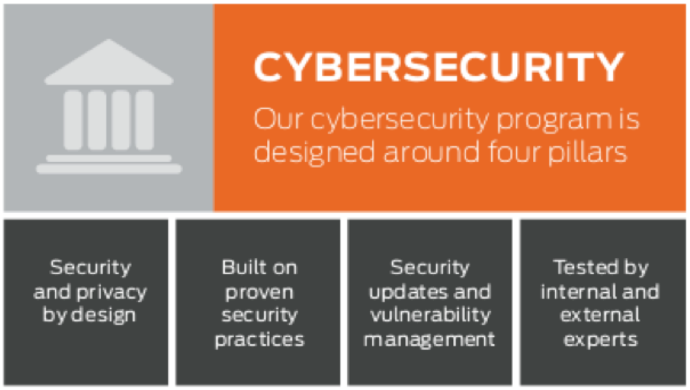
The relevant Application Notes may be found at:

- https://www.nxp.com/docs/en/application-note/AN10922.pdf
- https://www.nxp.com/docs/en/application-note/AN10969.pdf

In contrast, when designing the portion of the Schlage Mobile Access SDK that creates mobile credentials utilizing BLE communication, Schlage's patent-pending technology utilizes an Elliptic-curve Diffie-Hellman (ECDH) protocol to establish a secure session to securely deliver the encrypted and signed credential payload.

4. Foundation of Schlage Mobile Access Security

At Allegion™ (parent company of Schlage), we strive to provide seamless access and a safer world. Security and privacy are at the core of what we do and what we think about every day. We take a broad and deep approach to ensuring safety and security to protect the devices, products and systems that, in turn, protect people and assets wherever they reside, work and thrive. Allegion has a Product Cybersecurity Program that's designed around four key pillars:



CYBERSECURITY

Our cybersecurity program is designed around four pillars

Security and privacy by design

Built on proven security practices

Security updates and vulnerability management

Tested by internal and external experts

4.1 Security and privacy by design

The concept of building security and privacy into technology solutions both by default and by design is a core expectation for Allegion's product development initiatives. Some of Allegion's core security principles in security and privacy by design are:

- Utilize a "Defense in Depth" approach to security through multi-layered security controls;
- Data is protected at rest and in motion;
- It is assumed external systems are insecure;
- Users and processes are authenticated and then their authorization is verified;
- Security is periodically reassessed; and
- Users' right to privacy is respected, and we strive to protect it.

4.2 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. A few of Allegion's security best practices include:

- Full-time global cybersecurity team committed to driving 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; and
- Static analysis tools utilized during implementation phase.
    - Source code analysis
    - Open source analysis

4.3 Security updates and vulnerability management

Allegion takes security concerns seriously and works to quickly evaluate and address them. Once a security concern is reported, Allegion commits the appropriate resources to analyze, validate, and provide corrective actions to address the issue.

- Firmware updates are encrypted and signed using a cryptographically secure method;
- Security issues are tracked to closure and root-cause analysis is performed;
- Lessons learned are incorporated into the development process to help prevent repeat issues.

4.4 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 guided by the OWASP Application Security Verification Standard (ASVS), 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); and
- Device testing (hardware analysis).

5. Schlage Mobile Access consists of multiple security layers

5.1 Software Development Kit (SDK)

The Schlage Mobile Access SDK is a product Allegion offers to our software partners. The Schlage Mobile Access SDK leverages patent-pending technology, allowing a partner to build into their software offering the ability for its customers to securely unlock doors they have access to using a mobile device (e.g., a smart phone). Only authorized partners have access to the SDK via the Allegion Developer Portal. The Allegion Developer Portal requires a login and authentication prior to gaining access.

5.2 On mobile devices

Mobile Apps utilizing the Schlage Mobile Credential SDK secure data at rest using platform-specific best practices such as iOS Keychain and Android KeyStore.

5.3 On readers

The reader needs to hold the master key(s) from which the diversified keys are computed. The reader protects the master key(s) by utilizing a Secure Access Module (SAM) on the reader. The SAM holds keys and performs cryptographic operations using those master key(s) without divulging the master key(s) themselves, nor the diversified keys. The SAM is designed to securely store the keys and resist attacks by hackers to extract the keys from the SAM for use in other equipment.

5.4 Mobile device to cloud

Schlage Mobile Credential message security utilizes cryptographic certifications and bi-directional signing. Data sent between endpoints is encrypted, authenticated, and protected against tampering during transport using TLS 1.2. Certificate pinning is also deployed.

5.5 NFC credential messaging protocol

5.5.1 Mobile device to reader

The NFC messaging protocol is a multi-step mutual authentication protocol intended to prove that the mobile device has access to the diversified key assigned to a particular Key Diversification Input (KDI). In general, the mobile device and the reader each generate a random 16-byte value (RNDA, RNDB) and encrypt these values along with random cryptographic nonces under the diversified key to prove the ability to encrypt and decrypt with that key.

5.5.2 Key diversification and encryption

The principle of key diversification is that no two credentials will hold the same key or keyset. This unique identifier can be used to determine the key / keyset to be used. Except for the smallest systems, it is unpractical for the reader to hold a list of all the keys / keysets of all credentials. Hence, the key / keysets must be calculated from a unique identifier. The unique identifier and other information are concatenated and encrypted and the result is the diversified key. The Schlage Mobile credential data utilizes the AES-128 key diversification method described in the NXP Semiconductor Application Note AN10922 titled “Symmetric key diversifications,” using the unique identifier as the Key Diversification input.

5.5.3 Mitigation against man-in-the-middle attacks

As part of this verification, each side (i.e., the reader and the mobile device) is careful to check the cryptographic nonces to ensure they are not simply a replayed version of previous encrypted packets. This check is critical as it protects against an attacker that simply tampers with encrypted blocks. Once both parties have received RNDA and RNDB, the mobile device and reader derive a session key based on these inputs. They use this session key to encrypt some encrypted credential material, which is sent from the mobile device to the reader.

5.5.4 Credential data integrity

The NFC credential data is encrypted and hashed before it is transported using the 128 Bit Advanced Encryption Standard (AES 128) in Cipher Block Chaining (CBC) mode and 16 Bit Cipher Based Message-authentication Code (CMAC 16).

5.6 BLE credential messaging protocol

5.6.1 Mobile device to reader

The system does not rely upon the standard BLE security protocol. The patent-pending BLE messaging protocol is a multi-step Elliptic-curve Diffie-Hellman (ECDH) protocol to establish a secure session to securely deliver credential payload. In general, the mobile device and the reader each generate ephemeral ECC keys and then perform a key exchange that results in a temporary 256 Bit Advanced Encryption Standard (AES 256) session key to encrypt and decrypt session communication.

5.6.2 Mitigation against man-in-the-middle attacks

As part of this verification, each side (i.e., the reader and the mobile device) is careful to validate the cryptographic nonce to ensure they are not simply a replayed version of previous encrypted packets. In addition, the credential that is transmitted to the reader is encrypted and then signed using 256 Bit Advanced Encryption Standard (AES 256) in Cipher Block Chaining (CBC) mode and 256 Bit Elliptic-cure Digital Signature Algorithm (ECDSA 256), as it protects against an attacker that simply tampers with encrypted blocks.

5.6.3 Mitigation against relay attacks

The Schlage Mobile Access system protects against a relay attack by utilizing a unique Public/Private key pair of the reader. The security model for preventing this attack is similar to certificate pinning except in this case we are using an ECC Public/Private key pair.

So, on first credential presentation to the reader, the mobile device will remember ("PIN") the public key unique of that reader. The PIN is the public key of the reader which is encrypted by the session key and signed by the associated private key. Every subsequent credential presentation of the reader's PIN is validated against the user's mobile device pin-sets prior to sending the credential.

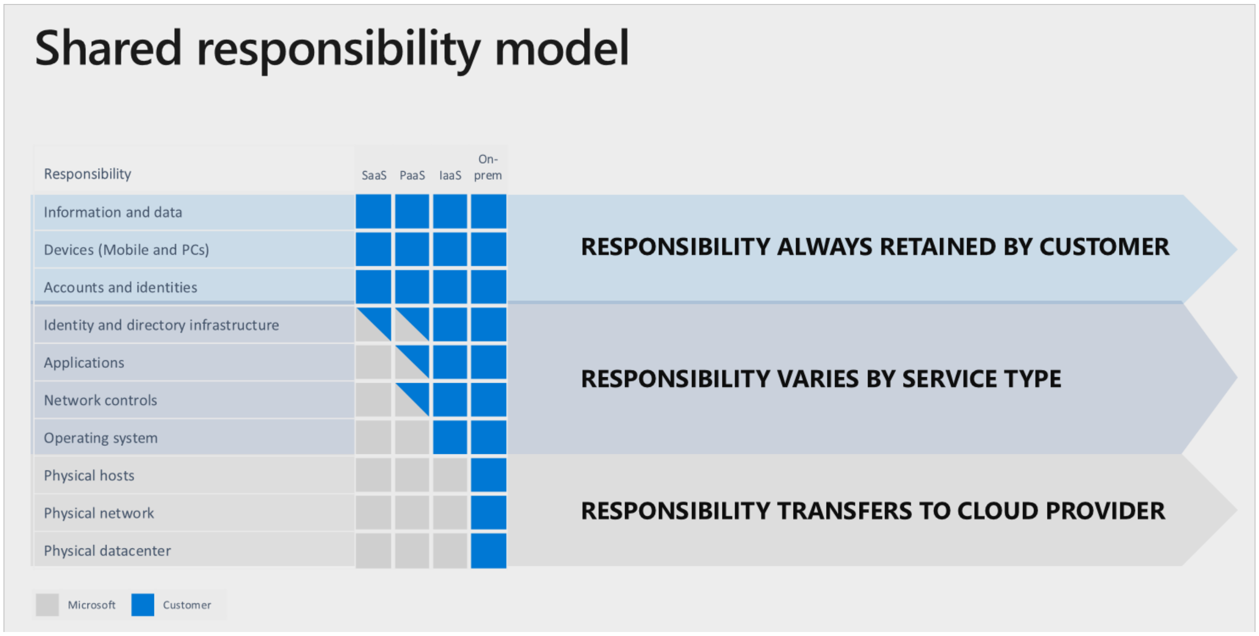
5.6.4 Credential data integrity

The Schlage Mobile credential data is encrypted and signed before it is transported using the 256 Bit Advanced Encryption Standard (AES 256) in Cipher Block Chaining (CBC) mode and 256 Bit Elliptic-cure Digital Signature Algorithm (ECDSA 256) using a shared key derived via the Elliptic-curve Diffie-Hellman (ECDH) algorithm. For each interaction, a new keypair is generated.

5.7 Back end

The Schlage Mobile Access cloud is hosted in the Microsoft Azure Cloud. "Microsoft Azure runs in datacenters managed and operated by Microsoft. These geographically dispersed datacenters comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The datacenters are managed, monitored, and administered by Microsoft operations staff. The operations staff has years of experience in delivering the world's largest online services with 24 x 7 continuity." More details may be found at: https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

The Microsoft Azure Cloud employs a shared responsibility model. Under the shared responsibility model, some security tasks are handled by the cloud provider (Azure in this case) and some tasks are handled by Allegion. Microsoft illustrates this shared responsibility model, with the following diagram.



Shared responsibility model

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◪	◪	🟦	🟦
Applications	⬜	◪	🟦	🟦
Network controls	⬜	◪	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

⬜ Microsoft 🟦 Customer

Shared responsibility in the cloud [Webpage image] retrieved from docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Allegion utilizes a PaaS (Platform as a Service) type of deployment in the Azure cloud. With the PaaS deployment that Allegion utilizes, Allegion has the responsibility of securing the data, endpoints, and account and access management.

5.7.1 Account and access management

Allegion utilizes Role Based Access Control (RBAC) with minimal permissions to restrict system access to authorized users.

5.7.2 Security monitoring

The Schlage Mobile Access cloud system monitors traffic for anomalies and intrusions utilizing Microsoft Azure Monitor tools such as Application Insights and Log Analytics.

5.7.3 Data protection

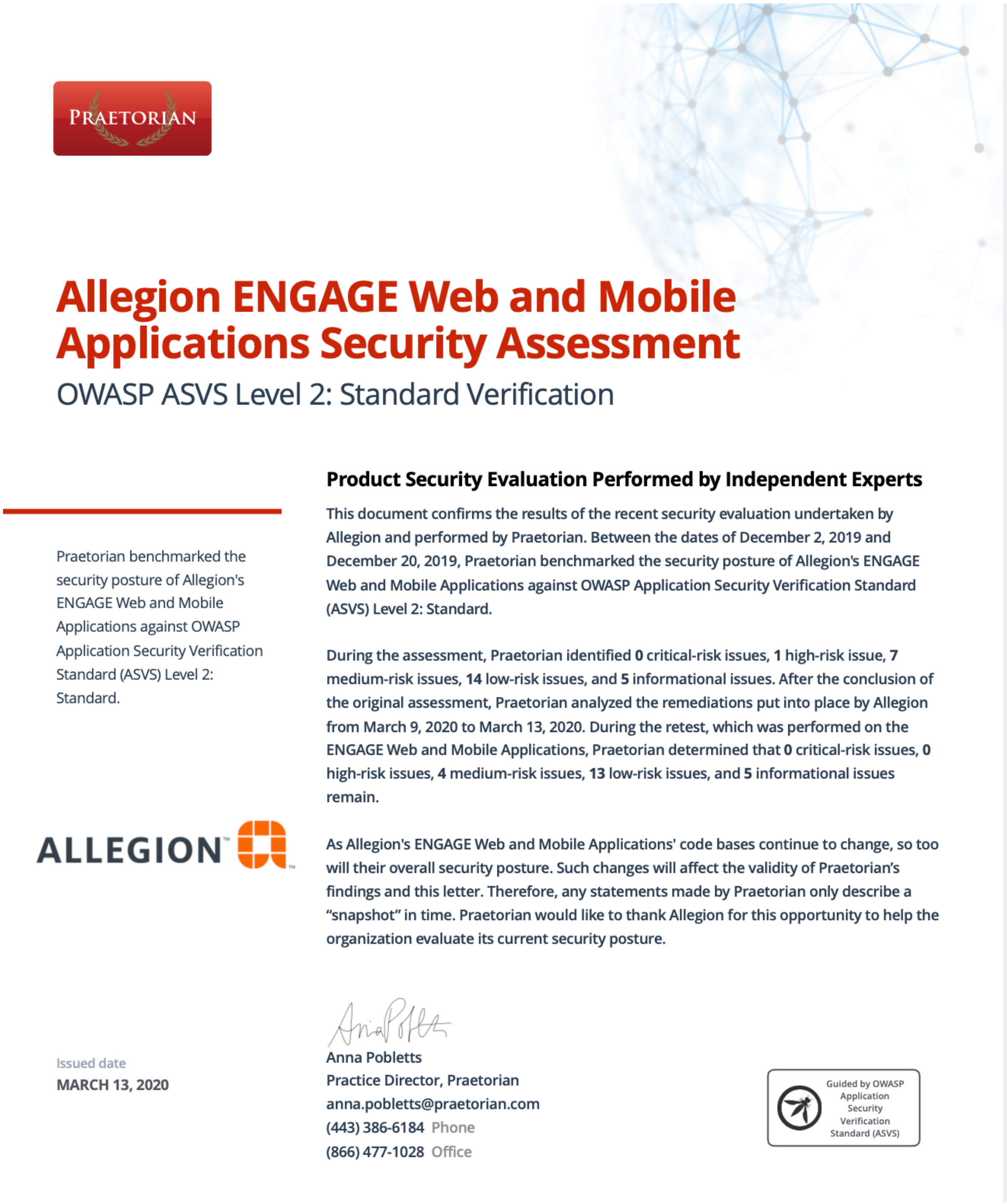
The Schlage Mobile Access cloud encrypts data in storage and in transit to align with best practices for protecting confidentiality and data integrity. For data in transit, Azure uses industry-standard transport protocols between Microsoft datacenters and within datacenters themselves. Also, data is geo-replicated between the primary and secondary datacenters. Sensitive data (e.g. keys) are secured in the cloud using Microsoft Key Vaults.

5.7.4 Redundancy

The Schlage Mobile Access cloud is hosted in two of the Microsoft Datacenters in the United States of America. This includes the primary datacenter on the East Coast and a fully redundant hot disaster recovery site on the West Coast.

5.8 Third party assessment

Allegion engaged an Independent Security Expert to evaluate the product security. Please see the below overview for more information.



PRAETORIAN

Allegion ENGAGE Web and Mobile Applications Security Assessment

OWASP ASVS Level 2: Standard Verification

Praetorian benchmarked the security posture of Allegion's ENGAGE Web and Mobile Applications against OWASP Application Security Verification Standard (ASVS) Level 2: Standard.

Product Security Evaluation Performed by Independent Experts

This document confirms the results of the recent security evaluation undertaken by Allegion and performed by Praetorian. Between the dates of December 2, 2019 and December 20, 2019, Praetorian benchmarked the security posture of Allegion's ENGAGE Web and Mobile Applications against OWASP Application Security Verification Standard (ASVS) Level 2: Standard.

During the assessment, Praetorian identified **0** critical-risk issues, **1** high-risk issue, **7** medium-risk issues, **14** low-risk issues, and **5** informational issues. After the conclusion of the original assessment, Praetorian analyzed the remediations put into place by Allegion from March 9, 2020 to March 13, 2020. During the retest, which was performed on the ENGAGE Web and Mobile Applications, Praetorian determined that **0** critical-risk issues, **0** high-risk issues, **4** medium-risk issues, **13** low-risk issues, and **5** informational issues remain.

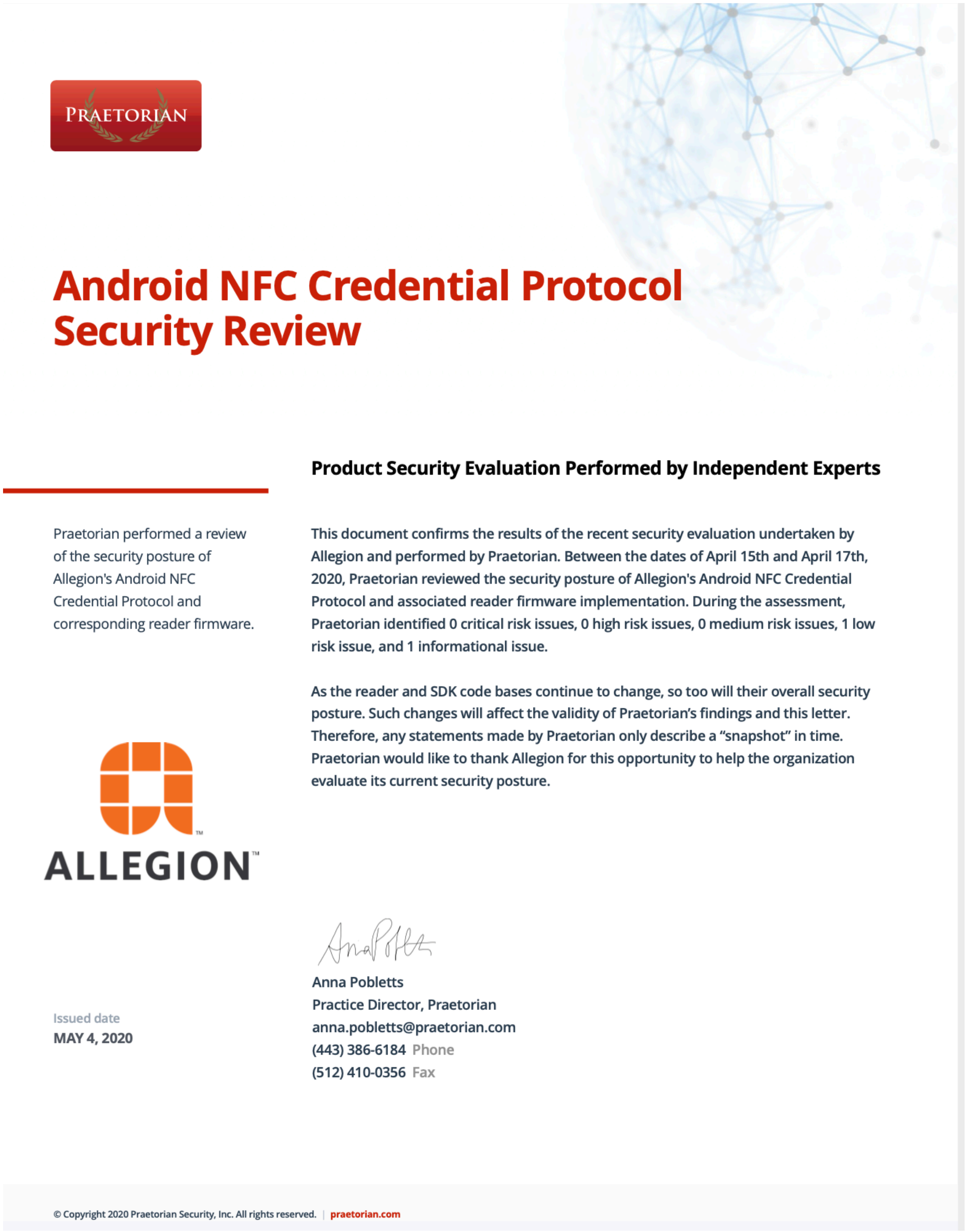
ALLEGION

As Allegion's ENGAGE Web and Mobile Applications' code bases continue to change, so too will their overall security posture. Such changes will affect the validity of Praetorian's findings and this letter. Therefore, any statements made by Praetorian only describe a "snapshot" in time. Praetorian would like to thank Allegion for this opportunity to help the organization evaluate its current security posture.

Issued date
MARCH 13, 2020

Anna Pobletts
Practice Director, Praetorian
anna.pobletts@praetorian.com
(443) 386-6184 Phone
(866) 477-1028 Office

Guided by OWASP Application Security Verification Standard (ASVS)



PRAETORIAN

Android NFC Credential Protocol Security Review

Product Security Evaluation Performed by Independent Experts

Praetorian performed a review of the security posture of Allegion's Android NFC Credential Protocol and corresponding reader firmware.

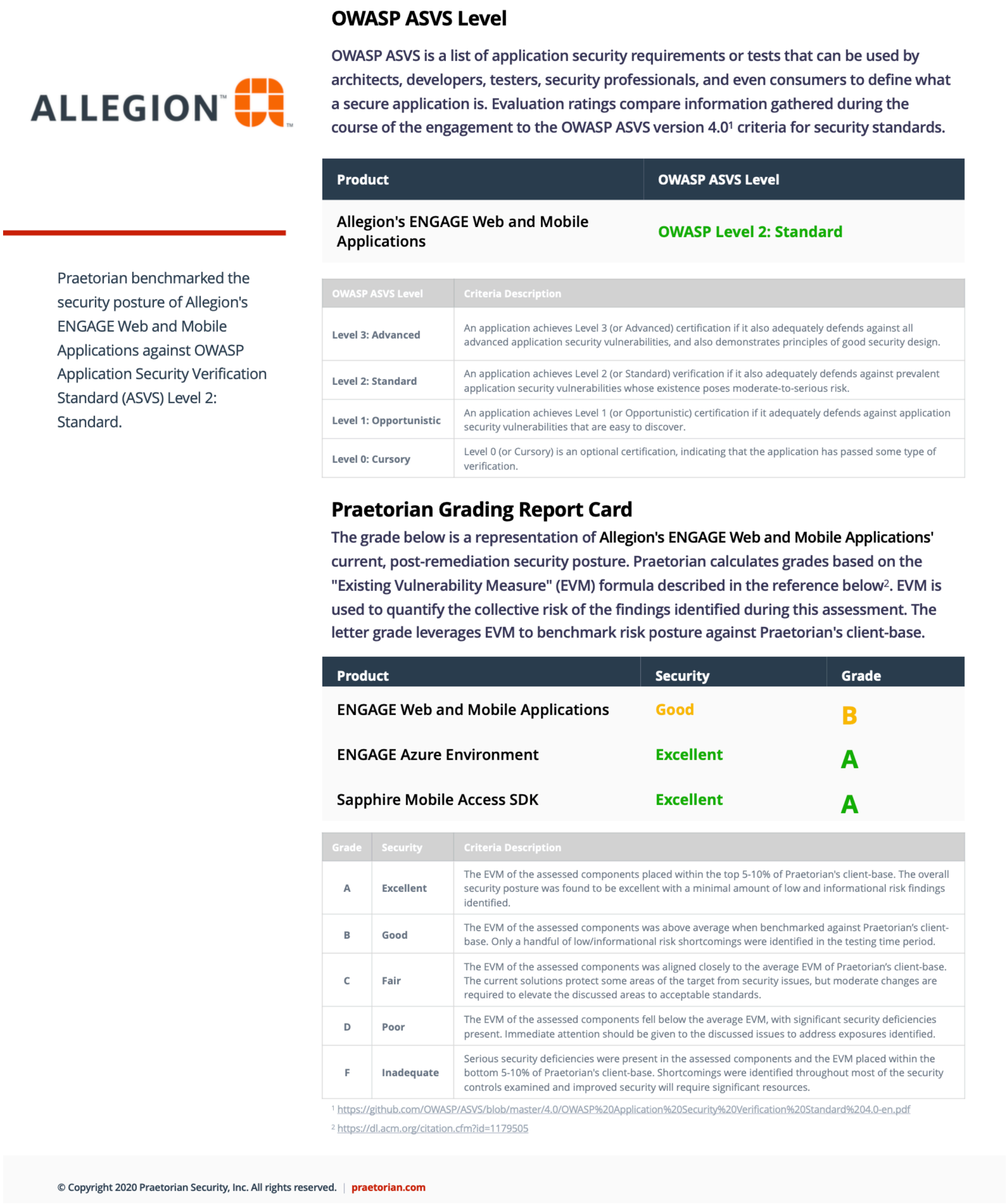
This document confirms the results of the recent security evaluation undertaken by Allegion and performed by Praetorian. Between the dates of April 15th and April 17th, 2020, Praetorian reviewed the security posture of Allegion's Android NFC Credential Protocol and associated reader firmware implementation. During the assessment, Praetorian identified 0 critical risk issues, 0 high risk issues, 0 medium risk issues, 1 low risk issue, and 1 informational issue.

As the reader and SDK code bases continue to change, so too will their overall security posture. Such changes will affect the validity of Praetorian's findings and this letter. Therefore, any statements made by Praetorian only describe a "snapshot" in time. Praetorian would like to thank Allegion for this opportunity to help the organization evaluate its current security posture.

ALLEGION™

Anna Pobletts
Practice Director, Praetorian
anna.pobletts@praetorian.com
(443) 386-6184 Phone
(512) 410-0356 Fax

Issued date
MAY 4, 2020



ALLEGION

Praetorian benchmarked the security posture of Allegion's ENGAGE Web and Mobile Applications against OWASP Application Security Verification Standard (ASVS) Level 2: Standard.

OWASP ASVS Level

OWASP ASVS is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, and even consumers to define what a secure application is. Evaluation ratings compare information gathered during the course of the engagement to the OWASP ASVS version 4.0[1] criteria for security standards.

Product	OWASP ASVS Level
Allegion's ENGAGE Web and Mobile Applications	OWASP Level 2: Standard

OWASP ASVS Level	Criteria Description
Level 3: Advanced	An application achieves Level 3 (or Advanced) certification if it also adequately defends against all advanced application security vulnerabilities, and also demonstrates principles of good security design.
Level 2: Standard	An application achieves Level 2 (or Standard) verification if it also adequately defends against prevalent application security vulnerabilities whose existence poses moderate-to-serious risk.
Level 1: Opportunistic	An application achieves Level 1 (or Opportunistic) certification if it adequately defends against application security vulnerabilities that are easy to discover.
Level 0: Cursory	Level 0 (or Cursory) is an optional certification, indicating that the application has passed some type of verification.

Praetorian Grading Report Card

The grade below is a representation of Allegion's ENGAGE Web and Mobile Applications' current, post-remediation security posture. Praetorian calculates grades based on the "Existing Vulnerability Measure" (EVM) formula described in the reference below[2]. EVM is used to quantify the collective risk of the findings identified during this assessment. The letter grade leverages EVM to benchmark risk posture against Praetorian's client-base.

Product	Security	Grade
ENGAGE Web and Mobile Applications	Good	B
ENGAGE Azure Environment	Excellent	A
Sapphire Mobile Access SDK	Excellent	A

Grade	Security	Criteria Description
A	Excellent	The EVM of the assessed components placed within the top 5-10% of Praetorian's client-base. The overall security posture was found to be excellent with a minimal amount of low and informational risk findings identified.
B	Good	The EVM of the assessed components was above average when benchmarked against Praetorian's client-base. Only a handful of low/informational risk shortcomings were identified in the testing time period.
C	Fair	The EVM of the assessed components was aligned closely to the average EVM of Praetorian's client-base. The current solutions protect some areas of the target from security issues, but moderate changes are required to elevate the discussed areas to acceptable standards.
D	Poor	The EVM of the assessed components fell below the average EVM, with significant security deficiencies present. Immediate attention should be given to the discussed issues to address exposures identified.
F	Inadequate	Serious security deficiencies were present in the assessed components and the EVM placed within the bottom 5-10% of Praetorian's client-base. Shortcomings were identified throughout most of the security controls examined and improved security will require significant resources.

[1] https://github.com/OWASP/ASVS/blob/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0-en.pdf

[2] https://dl.acm.org/citation.cfm?id=1179505

The information contained in this document is privileged and 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.

About Allegion™

Allegion (NYSE: ALLE) is a global pioneer in seamless access, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion secures people and assets with a range of solutions for homes, businesses, schools and institutions. Allegion had $2.9 billion in revenue in 2019 and sells products in almost 130 countries. For more, visit www.allegion.com.. .