ALLEGION™

SCHLAGE®

ENGAGE Credential Sort and Encryption

Version 1.34

Contents

ENGAGE - Credential Sort and Encryption

REVISION CONTROL RECORD			
VER	**Date**	**DESCRIPTION OF CHANGE**	**AUTHOR**
0.01	01/28/2015	Initial draft	0.01
0.02	1/29/2015	Updates for production	R. Rayburn
1.00	7/21/2015	Correct some inconsistencies in the final example, add some explanation to the credential creation, and release to production	J. Baumgarte
1.10	9/2/2015	Correct a description of the length of the credential in the JSON	J. Baumgarte
1.20	9/8/2015	Correct secondary credential information for NDE and Jaguar. Various fixes from document review	J. Baumgarte
1.30	5/17/2016	Note that duplicate records are treated as unsorted	T. Anfield
1.31	11/7/2017	Updated document format to new .docx. No Content Changed	T. Holt
1.32	6/25/2018	Added comment about 0xFFFFFFFF credential not supported Formatting Updates for ENGAGE 6.1 Release	T. Holt
1.33	9/5/2018	Converted Document to markdown format	T. Holt
1.34	5/4/2020	Added multi-factor authentication section, corrected Door File byte assignments, corrected secondary credential information	C. MacCrindle

Introduction

Abbreviations Used In This Document	
BLE	Bluetooth Low Energy
Db	Database
ENGAGE™	Connectivity Platform Technology
JSON	Java Script Object Notation
NDE	Schlage ENGAGE™ Wireless Cylindrical Lock
UI	User Interface (ex. LED blink pattern)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
TBD	To Be Determined

How Do Alliance Partner's Need to Sort?

- Sort on the 16 bytes of Credential Data (PrimeCr)
- Sort on the unencrypted values of the PrimeCr
- Sort the PrimeCr from smallest to largest
- Encrypt the 16 bytes of the PrimeCr with the Site Key

Credentials with Secondary Credential Data

All credential data is stored in the 16 bytes of the PrimeCr. The first 8 bytes of the PrimeCr are reserved for the primary credential data and the second 8 bytes are reserved for the secondary credential.

As a result, the sort is based on the PrimeCr present in the user record. The lock will handle looking backwards and forwards if multiple user records exist with the same primary credential data and unique seconday credential data.

Keep in mind that secondary credentials usage is the equivalent to the second credential in a Credential + Credential sequence (example: card + pin). The secondary credential is only used once the primary credential has already been matched. In the case where there are no secondary credentials just pad the second 8 bytes of the primeCr with 0xFF.

NOTE: Access decisions cannot be guaranteed if you have a mixture of a primary credential without a secondary credential specified and then the same primary credential again with secondary credentials in the same door file. When the lock finds the first match for a primary credential it will act upon that entry and will not search for any other entry.

NOTE: Including two identical credentials in the same door file will result in the lock treating the database as unsorted. Please avoid duplicate entries in the door file to ensure optimized operation.

How Do I Turn PrimeCr Into 16 Bytes?

Pad the remaining bytes with 0xFF.

NOTE: ENGAGE edge devices do not support primary or secondary credentials unencrypted value of all 0xFF. 0xFF should be used for padding of the unencrypted credential data, not for the entirety of the unencrypted credential info.

Example:

- Starting with a 26-bit credential [0x23C5981].
- Left-shift the data until you get to the first byte boundary (32-bits, 40-bits, 48-bits, or 64-bits)
  - For a 26-bit credential, you need to left-shift (32-26=6); 6 times.
  - Left-shifting 6 times results in [0x8F16 6040].
- Finally, the remaining 12 bytes are padded with 0xFF which gives a 16 byte value of [0x8F16 6040 FFFF FFFF FFFF FFFF FFFF FFFF]. This value is now left justified and padded.

“Degraded” or “Optimized” Search Modes

The lock will record an audit stating the result of a user database presort verification upon downloading a new user database. The result will state if the presort verification succeeded (user database is confirmed to be sorted) or failed (user database was not sorted upon downloading from the OEM).

Difference Between “Degraded” and “Optimized” Search Modes

When the door file is sorted according to the Section below, "What Will a Sorted User Database Look Like?, the lock performs a binary search on the primary credential. This enables a very rapid search of the entire 5,000 user door file – usually within a hundred milliseconds. **NOTE:** Reader controllers have a 64,000 user door file. Even more care must be taken to ensure a sorted door file to ensure rapid door access decisions.

When the door file is not sorted, the lock will remain functional, but must check every credential starting from the first entry to the final entry in the file. As a result, a search of the “last” user in the file may take a few seconds to complete, during which the user has no indication that anything is going on at the lock. So the user will present his/ her card to the lock and the lock will beep, indicating that the card was read, but will give no other UI until a few seconds later when the credential is matched and the door unlocks.

Keep in mind that “degraded” mode is completely detectable and avoidable. The lock will tell the server when the door file is not sorted as an audit.

What Will a Sorted User Database Look Like?

Let's look at an example of 5 users. We will only list the PrimeCr values since this is the only field that needs to be sorted.

Ref ID for Visual Purposes	PrimeCrs (*UN*sorted, not encrypted)
1	[0x8F16 6045 FFFF FFFF FFFF FFFF FFFF FFFF]
2	[0x8F16 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
3	[0x7F16 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
4	[0x7F18 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
5	[0x7F12 6540 FFFF FFFF FFFF FFFF FFFF FFFF]

Ref ID for Visual Purposes	PrimeCrs (sorted, not encrypted)
5	[0x7F12 6540 FFFF FFFF FFFF FFFF FFFF FFFF]
3	[0x7F16 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
4	[0x7F18 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
2	[0x8F16 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
1	[0x8F16 6045 FFFF FFFF FFFF FFFF FFFF FFFF]

What Type of Encryption is Used?

Encryption Type

Each set of 16 byte Credential Data (primary credential = 8 bytes, secondary credential = 8 bytes) will be encrypted using AES-256 Cipher-Block Chaining (CBC) with an Initialization Vector (IV) of zero, where the key is your secure Site Key. Depending upon the tool used to encrypt the credential data, it may be easier to use "Electronic Codebook" (ECB) for each credential since the IV is zero for each credential and they are not chained together.

Encryption Example

For the table below, the site key was: [0x1234 5678 90AB CDEF 1234 5678 90AB CDEF 1234 5678 90AB CDEF 1234 5678 90AB CDEF]. The online tool at **aes.online-domain-tools.com** was used to generate the encrypted values – this tool can do both CBC and ECB. Other tools can only use ECB and will work just fine. An example of another tool can be found here: **http://www.hanewin.net/encrypt/aes/aes-test.htm**

Ref ID for Visual Purposes	PrimeCrs (sorted & encrypted)
5	[0x3411 0EA5 49AA 549A A73F F06D C93B 63B4]
3	[0xCD38 8DD0 ACA9 7174 9203 D015 9264 C379]
4	[0x3BB9 9478 5B06 A240 1814 0A60 13CE 7477]
2	[0x77EB 0B84 7C38 08F5 A8F8 2844 622B F531]
1	[0x33DE CE61 76AF 0095 F8A0 EEE4 04D6 1F24]

What Should be Sent to the Lock in the Door File?

Taking the example in section 8, user 5's primary credential should be 16 bytes. See the example below:

"primeCr":"34110EA549AA549AA73FF06DC93B63B4",

"prCrTyp":"card",

"scndCrTyp":"null"

Adding Secondary Credential Data for Multi-Factor Authentication

The reader controller device implements four types of schedule authentication enforcement: single factor (1f), two factor (2f), single factor by two people (1fx2) and two factor by two people (2fx2). In single factor authentication, a single valid credential presentation grants access. In two factor authentication, a single user presents a primary credential followed by a secondary credential. Both must be valid and in the correct order for the device to grant access. In single factor by two people authentication, the device requires a valid credential from two distinct users to grant access, order does not matter. Finally, in two factor by two user authentication, the device requires two distinct users to each present two valid credentials to grant access.

What differences are there when adding a user with a Secondary Credential?

For the primary credential data, the process remains the same as discussed in the “How Do I Turn PrimeCr into 16 bytes?” except, the primary credential data is only padded to 8 bytes rather than 16 bytes.

The second 8 bytes of the 16 total bytes becomes the secondary credential data. The same left-shifting of the data is performed and then the secondary credential data is padded to 8 bytes. The padded and shifted primary and secondary credential data is then concatenated to achieve a 16 byte value.

Example:

- Primary Credential Data
  - Starting with a 26-bit credential [0x23C5981].
  - Left-shift the data until you get to the first byte boundary (32-bits, 40-bits, 48-bits, or 64-bits)
  - For a 26-bit credential, you need to left-shift (32-26=6); 6 times.
  - Left-shifting 6 times results in [0x8F16 6040].
  - Finally, the remaining 4 bytes are padded with 0xFF which gives an 8 byte value of [0x8F16 6040 FFFF FFFF]. This value is now left justified and padded.
- Secondary Credential Data
  - Starting with a 6 digit PIN [823456].
  - The PIN has data in the first byte boundary, so it does not need to be left-shifted
  - The remaining 5 bytes are padded with 0xFF which gives an 8 byte value of [0x8234 56FF FFFF FFFF]. This value is left justified and padded.
- Combining the Credential Data
  - The primary and secondary left justified and padded credential data is now concatenated [0x8F16 6040 FFFF FFFF 8234 56FF FFFF FFFF].

Sorting The User Database

Let’s look at an example of 5 users with a mix of primary crednential data only and primary and secondary credential data.

Ref ID for Visual Purposes	PrimeCrs (*UN*sorted, not encrypted)
1	[0x8F16 6045 FFFF FFFF FFFF FFFF FFFF FFFF]
2	[0x7F18 6040 FFFF FFFF 4EBB CA00 FFFF FFFF]
3	[0x8F16 6040 FFFF FFFF 8234 56FF FFFF FFFF]
4	[0x7F16 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
5	[0x7F12 6540 FFFF FFFF FFFF FFFF FFFF FFFF]

Ref ID for Visual Purposes	PrimeCrs (sorted, not encrypted)
5	[0x7F12 6540 FFFF FFFF FFFF FFFF FFFF FFFF]
4	[0x7F16 6040 FFFF FFFF FFFF FFFF FFFF FFFF]
2	[0x7F18 6040 FFFF FFFF 4EBB CA00 FFFF FFFF]
3	[0x8F16 6040 FFFF FFFF 8234 56FF FFFF FFFF]
1	[0x8F16 6045 FFFF FFFF FFFF FFFF FFFF FFFF]

Encrypting The Credentials

There is no change to the encryption method in the “What Type of Encryption is Used?” section.

Example:

Ref ID for Visual Purposes	PrimeCrs (sorted & encrypted)
5	[0x3411 0EA5 49AA 549A A73F F06D C93B 63B4]
4	[0xCD38 8DD0 ACA9 7174 9203 D015 9264 C379]
2	[0x144B F72D B826 70AF 2829 D8EB 4ADF A47A]
3	[0x2E6D 12D7 C45E F8A9 9B9F 39F6 60E5 BAAC]
1	[0x33DE CE61 76AF 0095 F8A0 EEE4 04D6 1F24]

What Should be Sent to the Lock in the Door File?

For the example above there are two sets of two factor credential data. The first being a card+pin (Ref ID 3) and the second being a card+card (Ref ID 2). In each of these cases, the credential data is only sent to the device in the “primeCr” tag, but both credential type tags, “prCrTyp” and “scndCrTyp”, must be populated according to the credential types.

Ref ID 1: Single Factor

“primeCr”:”33DECE6176AF0095F8A0EEE404D61F24”,

“prCrTyp”:“card”,

“scndCrTyp”:”null”

Ref ID 2: Two Factor, Card+Card

“primeCr”:”144BF72DB82670AF2829D8EB4ADFA47A”,

“prCrTyp”:”card”,

“scndCrTyp”:”card”

Ref ID 3: Two Factor, Card+PIN

“primeCr”:”2E6D12D7C45EF8A99B9F39F660E5BAAC”,

“prCrTyp”:”card”,

“scndCrTyp”:”pin”

Ref ID 4: Single Factor

“primeCr”:”CD388DD0ACA971749203D0159264C379”,

“prCrTyp”:”card”,

“scndCrTyp”:”null”

Ref ID 5: Single Factor

“primeCr”:”34110EA549AA549AA73FF06DC93B63B4”,

“prCrTyp”:”card”,

“scndCrTyp”:”null”

Other Items to Note About Multi-Factor Authentication

- A two factor user may use their primary credential during a valid single factor or single factor by two user schedules.
- Overlapping schedules are enforced based on the order they are entered. For example, schedule 1 is a single factor schedule Monday through Friday and schedule 2 is a two factor schedule Friday through Sunday. Both schedule 1 and schedule 2 have identical start and stop times. If the user is assigned to both schedule 1 and 2, then schedule 1 will be enforced Monday through Friday and schedule 2 will only be enforced on Saturday and Sunday.
- If multiple user records share the same primary credential the device cannot guarantee access decisions. The device will make its access decisions based on the first matched primary credential. It is highly recommended to not create a user database the contains multiple user records with the same primary credential data.

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**

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ENGAGE - Credential Sort and Encryption, Rev. 06/20
www.allegion.com/us

ALLEGION™