TECHNICAL OVERVIEW

WaveLynx
technologies corporation

Author: Taylor Schmidt
Version: 1.0
Revised: November 17, 2020

Mobile Credential Platform

INTEGRATION ARCHITECTURES & DATA SPECIFICATIONS

ABSTRACT

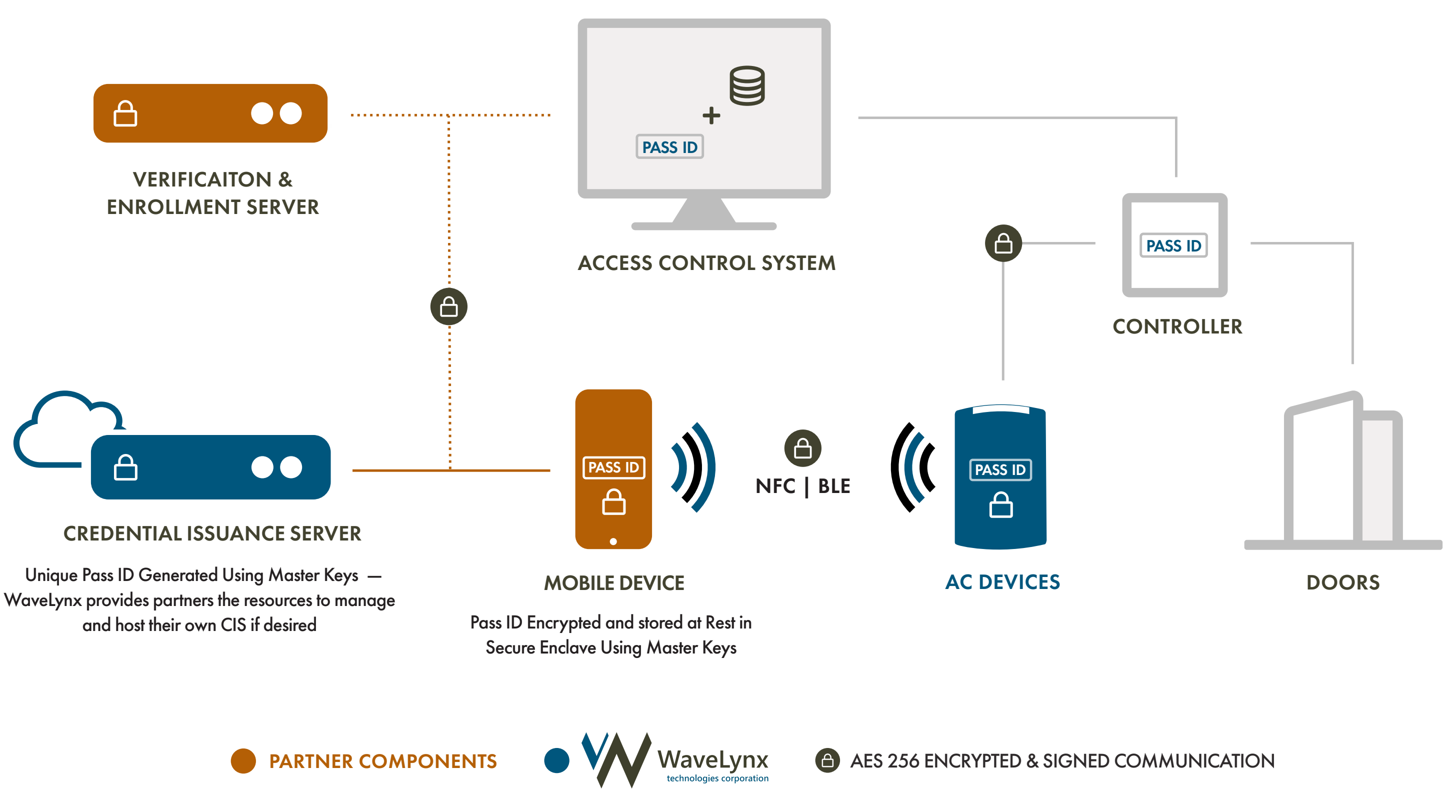
WaveLynx offers a flexible path for integrations which allows partners to build mobile credential applications rapidly.

The Mobile Credential Platform provides the following advantages:

- **Pre-built** — all base components needed to build a Mobile Credential Platform.
- **Reference Mobile Applications** — for iOS® and Android®, which handle credential issuance and reader communication.
- **Partner Freedom** — to repackage and add features, functionality, and branding.

ACCESS CONTROL SYSTEM ARCHITECTURE

With Partner & WaveLynx Mobile Platform Components



Unique Pass ID Generated Using Master Keys — WaveLynx provides partners the resources to manage and host their own CIS if desired

Pass ID Encrypted and stored at Rest in Secure Enclave Using Master Keys

REVISION HISTORY

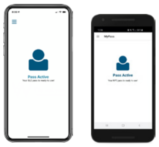
Version	Date	Author	Changes
1.0	November 17, 2020	Taylor Schmidt	Initial Version

CONTENTS

Access Control System Architecture 1
Revision History 2
1.0 WaveLynx Platform Components 3
2.0 Platform Partner Components 3
3.0 Mobile Credential User Flow 4
4.0 Example Integration & Customization Opportunties 5
5.0 SAMPLE USE CASES 6
Path 1: Identity Verification & Pass ID Enrollment 6
Path 2: Biometric Verification at the Door 6
Path 3: Invitation Enrollment 6
Path 4: Visitor Management 6
APPENDIX A: Credential Payload & Access Control Data 7
WaveLynx Issued Credential Payload 7
Partner Enrollment Payload Example 7
Access Control Data Format 7

1.0 WAVELYNX PLATFORM COMPONENTS

Reference Mobile Application



Starter Android and iOS applications that embed the WaveLynx SDK and handle all communication with Access Control Devices via Bluetooth®, NFC and the WaveLynx Credential.

Credential Issuance Server (CIS)

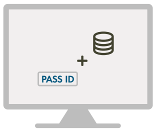
- The CIS handles the creation of secure, unique, credential payloads to be used by the mobile applications. Accessed over TCP/IP via REST API.
- Creates and provisions keys and IDs to mobile devices.

Access Control Device

- RFID readers which authenticate mobile credentials and interface with existing Access Control Systems via industry standard protocols.

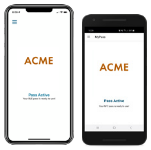
2.0 PLATFORM PARTNER COMPONENTS

Access Control System (ACS)



The partner must provide or connect to an Access Control System. This allows the user's credential to be validated at the door.

Reference Mobile Application Branding



Reference mobile applications must be redesigned with partner logos, color schemes, etc.

Mobile Auto-Enrollment Functionality

(Optional)

- This enables the association of the Pass ID with the user's identity inside the partner's management system.
- This functionality should also perform verification/validation of the user's identity through the use of partner specific login, phone number verification, etc.
- The partner should also perform the necessary "syncing" or "push" operations necessary to add the user's mobile Pass ID to their system.

Verification & Enrollment Service (VES)

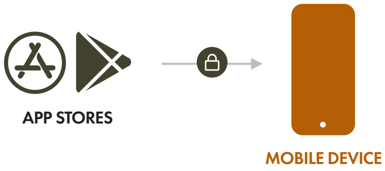
(Optional)

- Partner supplied interim server for integration and ingestion of Pass IDs into ACS
- The VES infrastructure allows the partner's mobile application to "sync" credential/identity data with the overall system.
- This component can take the form of a cloud service, on-prem access control server, etc.

3.0 MOBILE CREDENTIAL USER FLOW

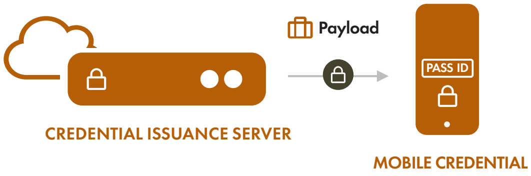
Step 1: Application Download

- The user downloads the mobile application from the publicly available app stores.



Step 2: Credential Issuance

- Upon first open, the app automatically pings the WaveLynx Credential Issuance Server and receives a guaranteed unique credential payload.
  - *The app will automatically parse the credential payload contents and store the data in the device's secure element or similar.*
- Once this operation is complete, the user's mobile application has all the info it needs to authenticate with Access Control Devices, but they have not yet been enrolled into an Access Control System to gain entrance.

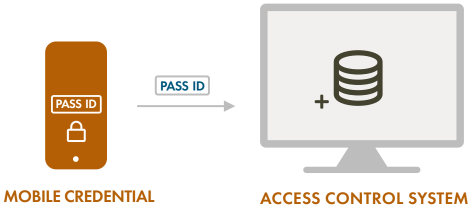


This credential payload contains data similar to the following. See **Appendix A** for more details.

```
{
    “authkey”: “30af4390c...”,
    “payload”: “49be2309a8e44...”,
    “badgedisplay”: “12345678”
}
```

Step 3: Pass ID Enrollment (Partner Responsibility)

- In order for a user to gain access when they present their device to a reader, they must have their Pass ID enrolled in the partner's Access Control System.
  - *It is up to the partner to add this functionality to the mobile applications provided in the integration package.*
- In order to enroll the user in the system, the mobile application must correlate the user's identity to the Pass ID assigned by the Credential Issuance Server.



Step 4: Credential Presentation

- Once enrolled, the user may simply present their device to any WaveLynx access reader in the same manner they would a physical credential. The application will detect the reader, perform an authentication, and transmit the credential to the Access Control System.

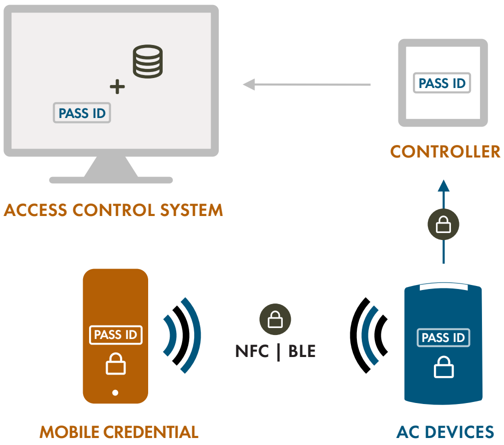
The mobile applications have slightly different user experiences depending on the mobile platform:

iOS®

- BLE Only.
- The application must be running on the device, but may be in the foreground or background.
- The phone may be unlocked or locked (the credential read may take slightly longer to register in the locked state).

Android®

- NFC only be default.
- BLE functionality for custom use cases.
- The application does not need to be running on the device to use the NFC credential.
- The phone may be locked or unlocked, but the screen must be illuminated for the NFC interface to activate (i.e. no black screen).

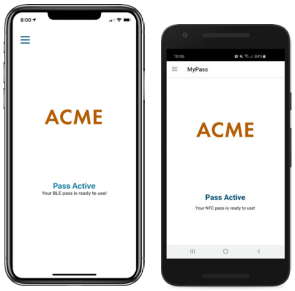


4.0 EXAMPLE INTEGRATION & CUSTOMIZATION OPPORTUNTIES

The following is an example implementation path a partner may take to perform an integration with the WaveLynx mobile credential platform. This is by no means the only path to take for an integration.

Step 1: White Label Branding (Required)

- Partner rebrands the reference applications with their logos, color schemes, etc. This is required for any private labelling integration.



Your BLE pass is ready to use!

Your NFC pass is ready to use!

Step 2: Credential Issuance Server (CIS)

- If the partner's use case requires it or the partner desires to host their own credential issuance server, WaveLynx can provide resources and reference designs to do so.
- Note that all partner hosted CIS systems are required to use a custom mobile credential and access reader keyset. WaveLynx can provide support/services for keyset management and provisioning.

CREDENTIAL ISSUANCE SERVER

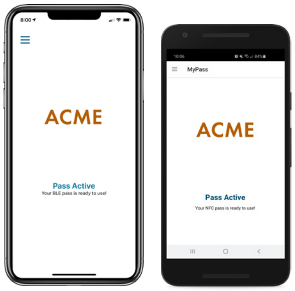
Step 3: Verification & Enrollment Service (VES)

- Partner creates a Verification & Pass ID Enrollment Service to collect and associate user identities with their assigned mobile Pass ID.
- This service is accessible to the partner mobile applications, as well as their identity management/access control software.
- Having a Verification & Pass ID Enrollment Service allows mobile credentials to be seamlessly (and remotely) enrolled.

VERIFICAITON & PASS ID
ENROLLMENT SERVER

Step 4: Pass ID Enrollment

- Partner adds user interface elements to collect a device holder's uniquely identifying information such as phone number, email, etc.
- Once collected, the partner adds functionality to push this information to their VES and subsequently enroll the mobile credential in their ACS.



Your BLE pass is ready to use!

Your NFC pass is ready to use!

5.0 SAMPLE USE CASES

Path 1: Identity Verification & Pass ID Enrollment

1. User downloads/installs the application.
2. Upon first open, the user enters their mobile phone number. They then receive a text message containing a code, which verifies the authenticity of their device/identity.
3. After phone number verification, the mobile application receives a mobile credential from the WaveLynx Credential Issuance Server and stores this locally on the device.
4. The mobile application then sends the credential Pass ID and phone number to the partner's VES. Once received by the management service, the mobile credential is associated to the device holder and given door access rights.
5. The user is now free to present their mobile device to any WaveLynx reader to gain access.

Path 2: Biometric Verification at the Door

1. Download, enrollment, etc. can be identical to Path 1 in terms of how the mobile application is downloaded and the mobile credential is enrolled in the partner's system.
2. Upon first open, the user enters their mobile phone number. They then receive a text message containing a code, which verifies the authenticity of their device/identity.
3. After phone number verification, the mobile application receives a mobile credential from the WaveLynx Credential Issuance Server and stores this locally on the device.
4. The mobile application then sends the credential Pass ID and phone number to the partner's VES. Once received by the management service, the mobile credential is associated to the device holder and given door access rights.
5. The user enrolls their biometric data into the application, which "locks"/encrypts the mobile credential at rest. This can be done via a third party SDK/module handling 2 factor authentication.
6. Partner adds functionality to mobile applications which require the use of biometric data (fingerprint, facial recognition, etc.) to "unlock"/decrypt the mobile credential stored locally on the device.
7. Before using their device for access, a user must authenticate their biometric data, allowing the mobile credential to be sent to the WaveLynx reader.

Path 3: Invitation Enrollment

1. Administrator enrolls user identity into the partner system.
2. Upon Pass ID Enrollment, the partner system sends the user an email/text invitation to download the mobile application and receive credential.
3. The user opens email and downloads application.
4. Upon first open, the mobile application receives credential from WaveLynx Credential Issuance Server and stores it locally on the device.
5. The user then enters an authentication code contained in the invitation email. This code is used to associate their identity with thePass ID stored locally in the mobile application.
6. The mobile application then sends both the Pass ID and invitation authentication code to the VES system. The VES system then enrolls the Pass ID and gives the user access rights.
7. The user is now free to present their mobile device to any WaveLynx Ethos Reader with Wiegand or OSDP to gain access.

Path 4: Visitor Management

1. Administrator adds a new user to their visitor management system for access on a particular day/time.
2. An email is sent to the visitor with instructions on downloading the mobile application + a temporary badge authentication code. The visitor then downloads the mobile application.
3. Upon first open, the mobile application receives credential from WaveLynx Credential Issuance Server and stores it locally on the device.
4. The user then enters an authentication code contained in the invitation email. This code is used to associate their identity with the Pass ID stored locally in the mobile application.
5. The mobile application then sends both the Pass ID + invitation authentication code to the partners VES system. The VES system then enrolls the Pass ID and gives the user access rights for the specified day/time.
6. The user is now free to present their mobile device to any WaveLynx reader to gain access during their visit.
7. After the specified visit has expired, the partner's visitor management system automatically revokes access right for the user's assigned credential.

APPENDIX A: CREDENTIAL PAYLOAD & ACCESS CONTROL DATA

WaveLynx Issued Credential Payload

Example payload structure issued from WaveLynx Credential Issuance Server and stored locally on device. This access control data embedded within this payload will be randomly assigned and guaranteed unique by the WaveLynx Credential Issuance Server.

See Access Control Data Format for details on bitstream format and construction.

```
{
    “authkey”: “30af4390c...”,
    “payload”: “49be2309a8e44...”,
    “badgedisplay”: “12345678”

}
```

Field	Description
authkey	Reader authentication key
payload	Signed and encrypted credential sent to access reader
badgedisplay	Embedded badge number to be used in enrollment with ACS

Partner Enrollment Payload Example

Example payload used to enroll device in the partner ACS. This will vary based on the partner requirements, but should provide identifying information to associate the cardholder’s identity in the ACS with Pass ID issued by the WaveLynx server. The partner should take the badgedisplay field issued along with the credential as the enrollment field for the credential number. This will often be a phone number, email, or auth code.

```
{
    “phone”: “123456789”,
    “auth”: “44444”,
    “badgedisplay”: “12345678”
}
```

Access Control Data Format

“MyPass” credentials are embedded with a 32 bit UID, which acts as the access control data for the ACS. The partner system should handle this format accordingly:

```
W32-5
Number of bits: 32
B B B B B B B B B B B B B B B B B B B B B B B B B B B B B B B B
No Facility Code
Pass ID Range:  0 – 4,294,967,295
No Parity Bits
```