Product White Paper

LOOP

The flexible badge on your phone

1.Executive summary

Identification and authorization of an individual's access to assets has historically been via multiple methods (keys, cards, dongles...), depending on the use case and the desired trust model.

The most widely carried device is now the smartphone which gives an opportunity to virtualize access credentials whilst maintaining or improving trust.

There are significant barriers to moving to an online-only world so trusted, offline access methods must be available.

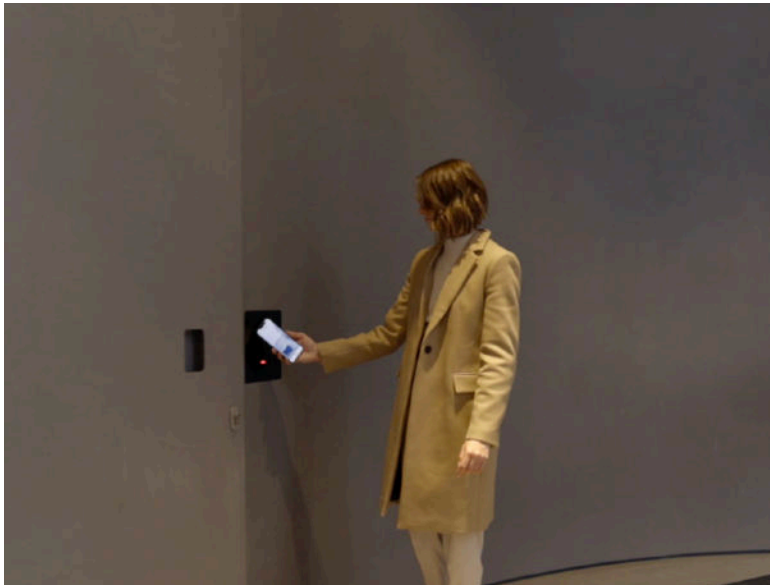
Mass deployment of digital credentials must be a painless user experience, for both major types of smartphones, otherwise implementation of mobile access credentials will fail.

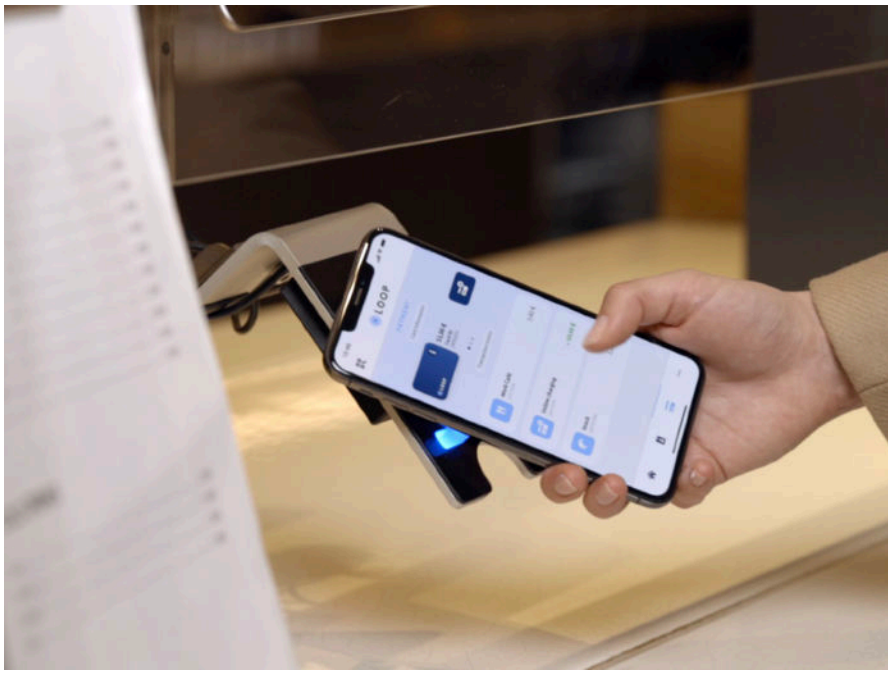
This white paper explains how to implement mobile credentials in a simple and secure way and gives instructions for testing the LEGIC Connect credential service with bluetooth readers.

2.Takeaways

Smartphones offer the ability to improve trust models at the same time as the user experience

any2any have developed both a universal secure wallet and the user onboarding support platform to enable the implementation of mobile access credentials





Introduction

Think of the badge you must remember to take with you to the office every day that you hold up to a door reader when you want to get into the office lobby or other door? Or that you need to wave over the printer, or even use to pay for your lunch in the staff restaurant? A mobile credential on a smartphone does the same thing via a mobile app that allows you to access a physical space, a printer, your lunch...

Mobile credentials allow for all this without having to carry around traditional plastic cards and key fobs. When combined with biometrics, or other challenge/response methods mobile credentials can be more secure than plastic cards.

But...Implementing mobile credentials means a change of process for HR and security teams when onboarding users, for reception staff when granting temporary access to guests

1. Why use mobile credentials?

More Secure Credentials and Better Protection

Mobile credentials are more secure than traditional access cards. Think how easy it is to say to someone “lend me your passcard”. It’s much less likely to work if you say “lend me your smartphone”.

Device biometrics (fingerprint and Face Unlock) and enterprise security establish trust by verifying true identity.

Instant and Easy to Install

Mobile credentials are very easy to use for users, many people will already use their smartphone for purchases and ticketing, simple for property managers to authorize and simple to install for security integrators.

A great experience for Tenants, Employees, Residents, Students, Visitors....

Mobile credentials provide a truly mobile-first experience for tenants, employees, residents.anyone visiting or using your spaces... Making it easier for them to move about a facility or apartment, and allowing them to open doors and use keyless entry across multiple locations with their smartphone.

Cost-effective

Plastic cards and key-fobs are cheap to purchase but costly to configure and distribute. It’s much easier and cheaper to install an app and scan a QR code or click a link.

2. Implementation challenges

Too many apps

Smartphone users have become weary of installing an app every time they need an additional function. However, users need to be encouraged to install somewhere to hold their mobile credentials. Preferably, one wallet to hold all their credentials and use those credentials for multiple functions.

Network connectivity

Users cannot always rely on there being network connectivity in all places they may need to use their credentials. The app must work everywhere whether online or offline.

Security

Apps must be secured against cloning and unauthorised use. Device IDs are not enough to establish and verify identity. Many legacy radio frequency technologies from over 25 years ago are still in use today, which can be breached easily using a $15 card cloner bought online.

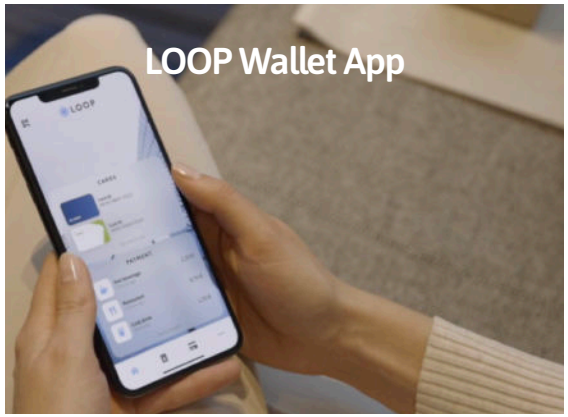
Privacy

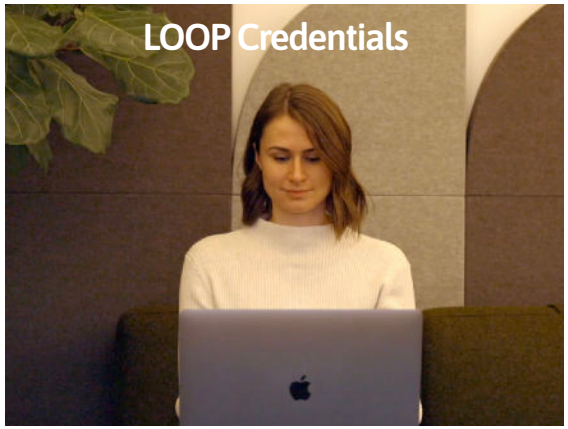
Apps must collect the minimum of personal information and its use must be transparent to the user to gain confidence that privacy is being protected. The GDPR guidance for data minimisation and anonymisation must be followed by application platforms.

3. LOOP overview

To meet the requirement for an offline, secure, multifunctional/multicard mobile credential any2any have developed LOOP. LOOP is a set of applications built on the any2any experience platform (see ‘ About any2any’ section for more details).

LOOP has three components:



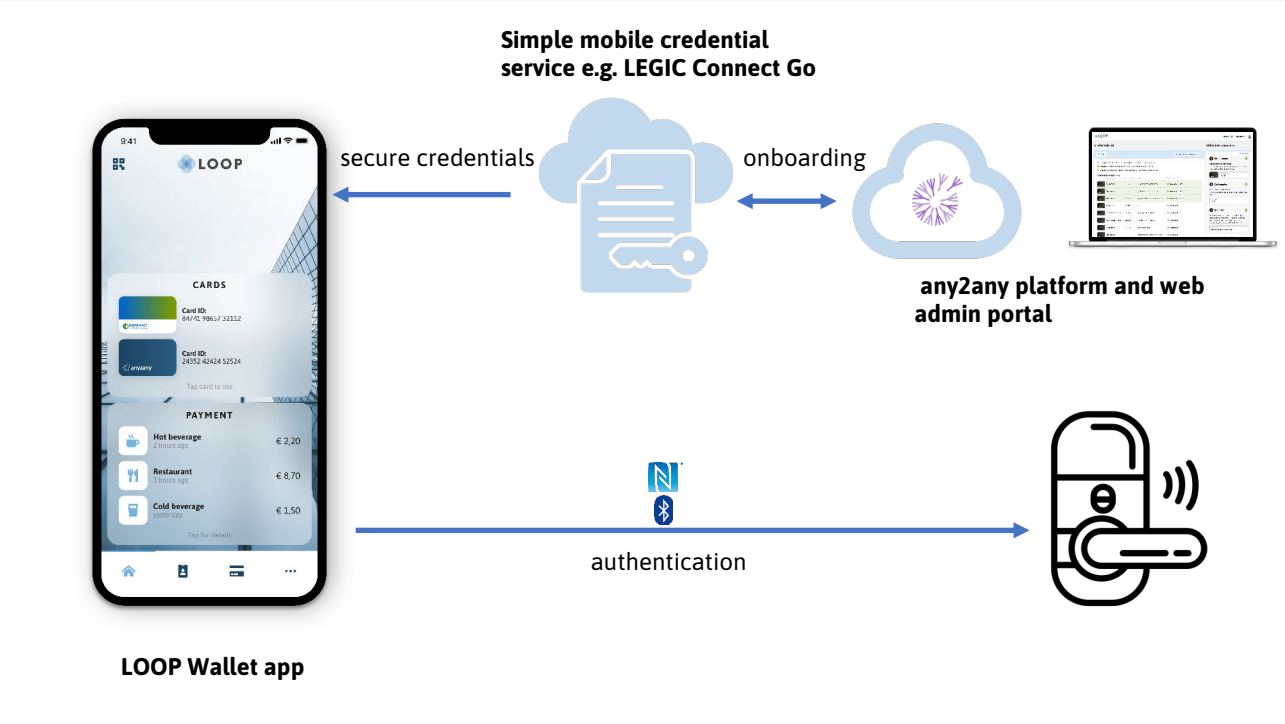


4. Architecture

LOOP was designed to be flexible to address multiple architectures using mobile credentials

Simple Mobile Credential Services

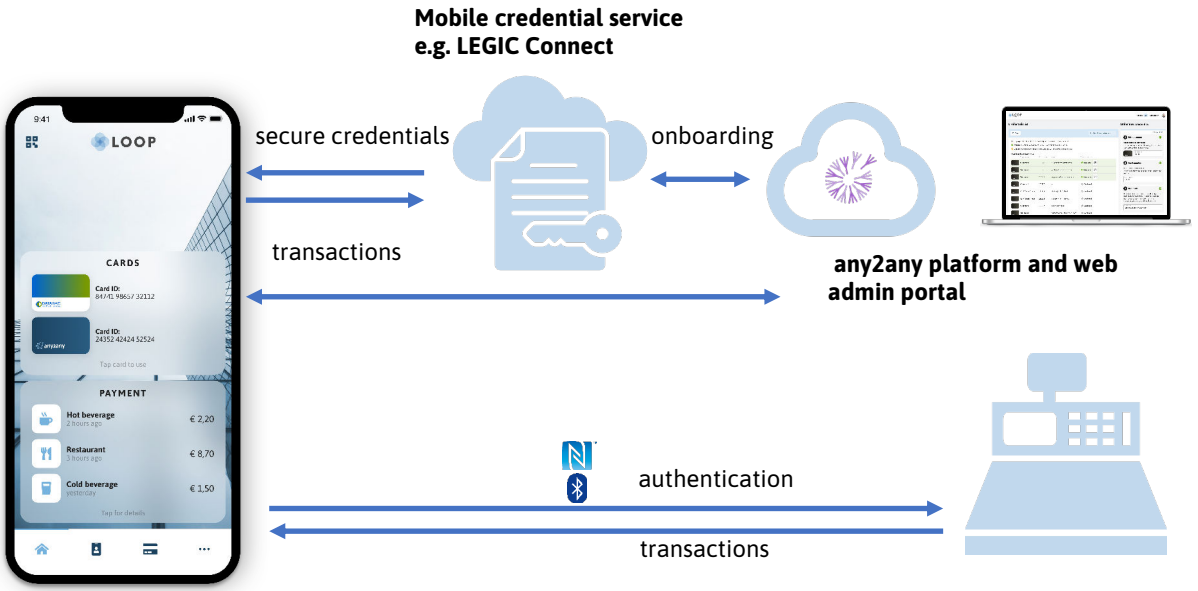
Cloud services such as LEGIC Connect Go are designed for secure issuance of mobile credentials to be used with a mobile application developed with their SDK. LOOP Wallet enables the secure storage and use of those credentials.



4. 1 Architecture

Mobile Credential Service Platform

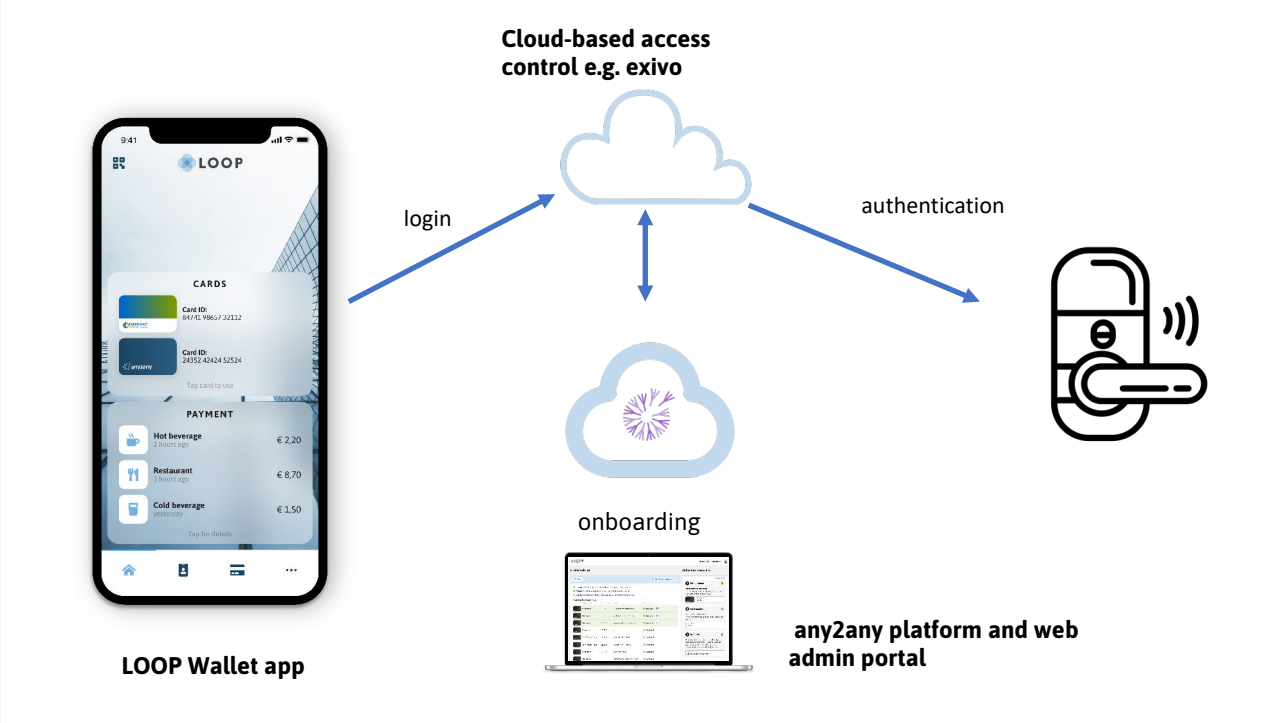
Comprehensive cloud platforms such as LEGIC Connect provide a stack of trusted services.For example, the ability to capture and store transaction information for payment systems.



4. 2 Architecture

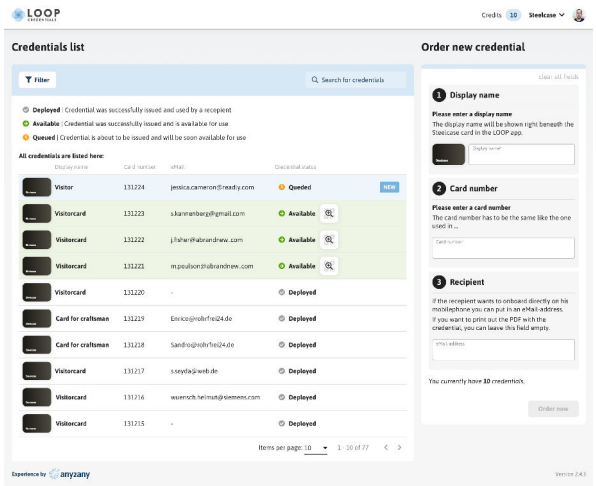
Online authentication

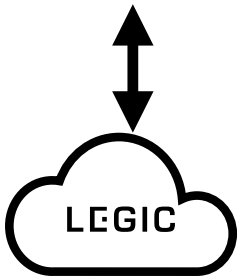
An alternative approach to storing a credential on a mobile device is to use an app to authenticate to a cloud service that then authenticates the user to the access control device.



LOOP Workflow

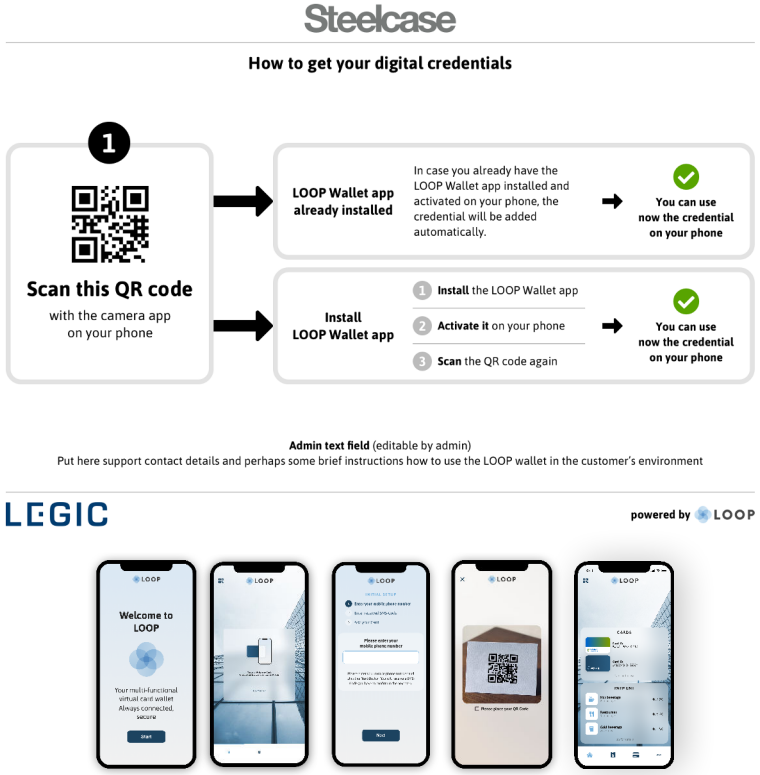
1 Order a credential





2 Provision a credential

3 Distribute credential to user



4 User onboards credential

4. 4 Onboarding

1. Order a credential

LOOP is sold through resellers. To set up the account the end customer orders a batch of credentials (like ordering a batch of cards) which are then available for distribution to users. On the web admin, the customers' administrator (could be HR, Security, or Front Desk) enters the end users' details.

2. Provision the credential from a trusted source

LOOP Admin automatically requests a credential from the LEGIC Connect cloud

3. Distribute credential to end user

this could be via email or, as in this example, by printing a QR code.

4. Onboard credential

the user scans the QR code or clicks the email link which will prompt them to install the LOOP Wallet app (if they don't already have it) and then download their mobile credential from LEGIC Connect.

Loop also allows for bulk onboarding of multiple users by uploading a spreadsheet in the Web Admin.

4. 5 Use cases

Here are some examples made possible once an individual's identity can be verified via a mobile credential:

1. Guest access
2. Contractors
3. Fine grained access to high value assets in a data centre
4. Closed-loop payment for staff restaurants
5. Student access to educational resources, accommodation, and payment for services
6. Ticketing for events
7. Age-restricted purchases
8. Covid status

5 . Chain of trust

There are multiple elements to consider when establishing a chain of trust for mobile identification and verification:

1. Identifying the user of the credential
2. Linking the user's device to the user's identity
3. Ensuring that the issued credential is installed on the user's device
4. Security controls to prevent compromise of the credential-issuing infrastructure
5. Ensuring that the reader of the mobile credential correctly identifies valid credentials
6. An access control system to grant/deny access to the space or resource for verified users

A simple example of where a chain of trust might break down is the use of Bluetooth ID as a simple identification method. This is quite common in proximity unlocking of computers. In this case simple possession of the Bluetooth device is enough to gain access and Bluetooth IDs are trivial to spoof. In addition, Bluetooth implementations can be manipulated to downgrade security so Bluetooth ID alone is definitely not suitable for secure access.

The chain of trust for a suggested implementation of any2any LOOP using LEGIC credentials would look like this:

1. The user's identity and business requirement for a credential is verified by a responsible corporate team. This could be HR, Security, Facilities, IT...

2. The administrator of the mobile credentials requests a new credential for the user. This could be delivered via email or, if physical verification is required, by the user being given a QR code to scan which downloads the credential.

3. For the LOOP Wallet app there is also an additional registration check for the mobile phone number so that there is an audit trail of which credential is associated with which mobile device.

4. The LEGIC connect infrastructure is certified under ISO 27001 with regular compliance checks

5. The LEGIC embedded secure element will only recognise validated credentials

6. Now that an individual has been identified and verified, the access control system can grant/deny access as required.

6. Audit and control

The move to using a smartphone brings additional opportunities for enhanced verification, communication with the user, and logging and reporting.

One of the challenges with traditional RFID cards is the difficulty in tracing a card back to an individual user, especially in cases where temporary / guest cards are issued.

Mobile credentials enable more granular reporting on when credentials were issued, activated, and used.

7. Extending the use

Until now we have considered mobile credentials largely as a replacement for the 'dumb' plastic card.

Because of the ability to have a two-way communication, mobile credentials are also ideal for use as identification and reporting for closed loop payment systems.

Applications like LOOP are a good starting point.

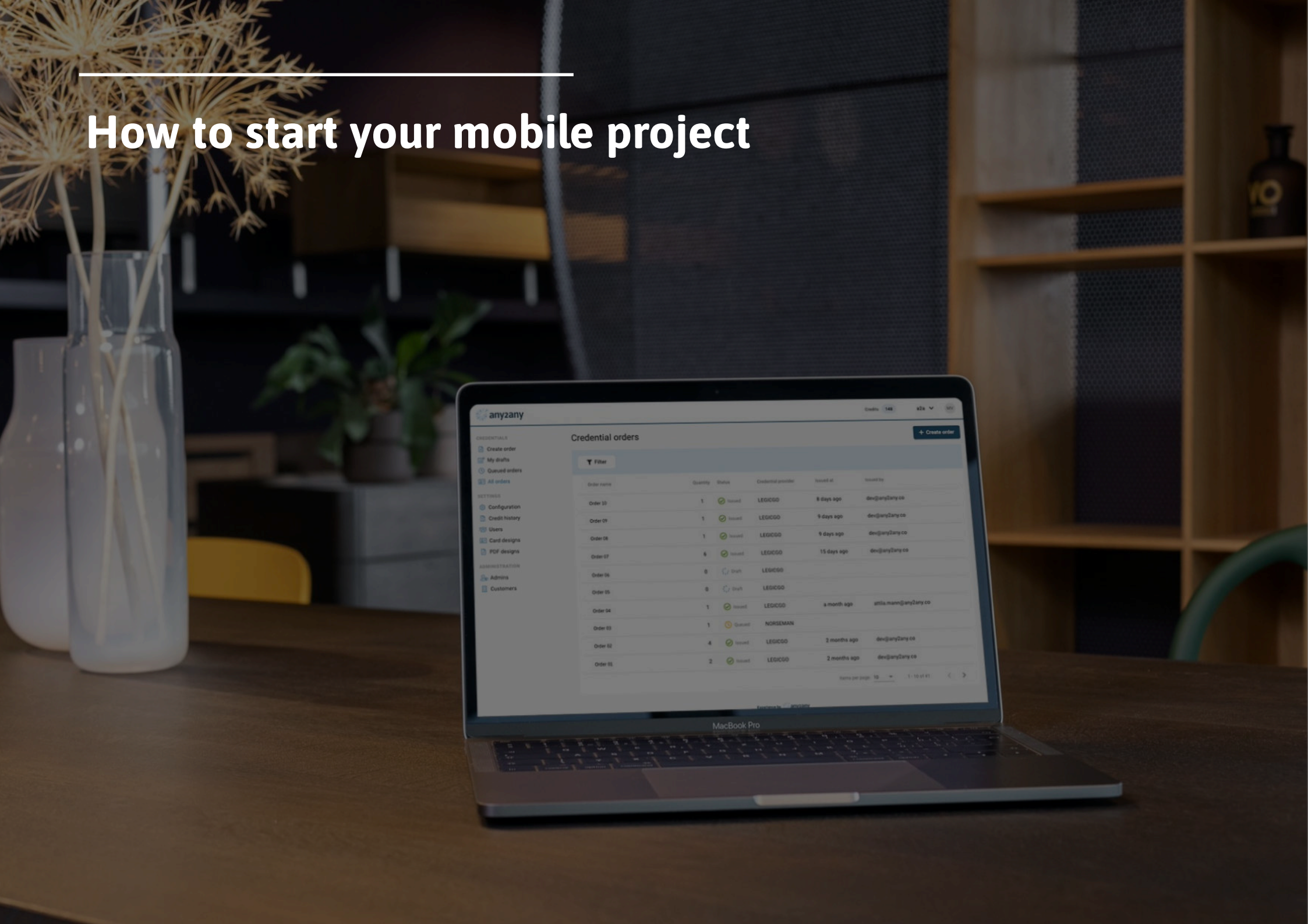
Building applications on top of an experience platform like any2any allows organisations to customise the user experience to their particular requirements.

About any2any

any2any GmbH is a cloud-based platform provider renowned for creating branded experiences for employees and visitors. Founded in 2015, it provides secure connected solutions through the any2any platform, with integrated access control , branded visitor management, mobile closed-payment, corporate and residential parking, identification, and authentication.

In addition, any2any offers unique software services for the secure creation and instant deployment of virtual encrypted credentials to smartphones. LOOP, the multi-functional secure wallet solution complements physical RFID cards, for use with hybrid identification, access, visitor management, payment and printing applications. Visit www.any2any.co for more information.

How to start your mobile project



1. Reader technology

We work with readers based on a number of technologies to which we are adding all the time:

LEGIC 63xx	BlueID
LEGIC 43xx + Bluetooth Module	WiFi PIN
BioID	

Readers where we have proven working solution include:

3rd Millenium	Häfele
Brivo	PHG
FATH	Dormakaba
ISEO	Zuccetti
Brivo	Dormakaba exivo
Uhlmann & Zacher	

1.1 Reader configuration

MobileAppId:	*0x0461B87C / 73513084*
ProjectId:	*0x0461C05E / 73515102*
FileId:	*all 12bytes 00 (default file)*
Format:	*Wiegand by default, can be something else if needed*
RO Key:	*B0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF*
RW Key:	*A0A1A2A3A4A5A6A7A8A9AAABACADAEAF*
WO Key:	
Enc Key:	*C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF*

The information given below is specifically for readers using the LEGIC 63xx chip or 43xx with Bluetooth module. If you are working with a different reader technology, please contact us.

To make the reader recognise the mobile credential, the readers need to be configured correctly. Please use the following details to setup your reader then contact us for test credentials to import into LOOP Wallet.

2 . Getting a credential for testing:

Contact sales@any2any.co for a test credential. We will also talk you through the process for signing up as a technology partner.

Don’t want to talk to us yet?

Scan the QR code from your mobile device. To register for a LEGIC credential and get instructions for installing the LOOP Wallet app.

If you are a potential end customer

Contact sales@any2any.co We will ask some qualifying questions and then engage with one (or more) of our technology **partners** to design a solution for your needs.