swidch

OTAC auth Design Guide

swIDch Ltd.

swIDch
Address: 1st floor, 3 More London Pl, London SE1 2RE
Tel: +44 (0) 2032834081
Mail : developer@swidch.com

Contents

Introduction

This document is intended for administrators who will be using the OTAC auth app available on the PLCNext Store and the mobile app on Google Play store and Apple Apple store. This mobile app works together with the backend OTAC service that typically protects web applications such as a PLC application. The mobile app generates a One Time Authentication Code (OTAC) which is the world's first one-way dynamic authentication technology that enables users to authenticate to PLC devices via their phone.

- **App Details**: Experience rapid and secure user/device authentication through OTAC's 8-character code.
- **Quick and Easy, No Registration**: Streamlined authentication without the hassle of sign-up or login processes. Your privacy is paramount; no personal information required.
- **Secure Authentication with OTAC Code**: Ensure robust security with time-sensitive OTAC codes. Safely access your accounts using a code that expires after a specific duration.
- **Manage Multiple Accounts Easily**: Effortlessly authenticate multiple accounts using a single OTAC auth app. Register and manage up to 20 accounts securely.

Download the App

PLCNext Store
You can download the OTAC auth app from the PLCNext Store:

OTAC auth - MFA Server

OTAC auth - MFA Client

Mobile App
You can download the OTAC auth app from the respective Google and Apple app stores:

GET IT ON Google Play

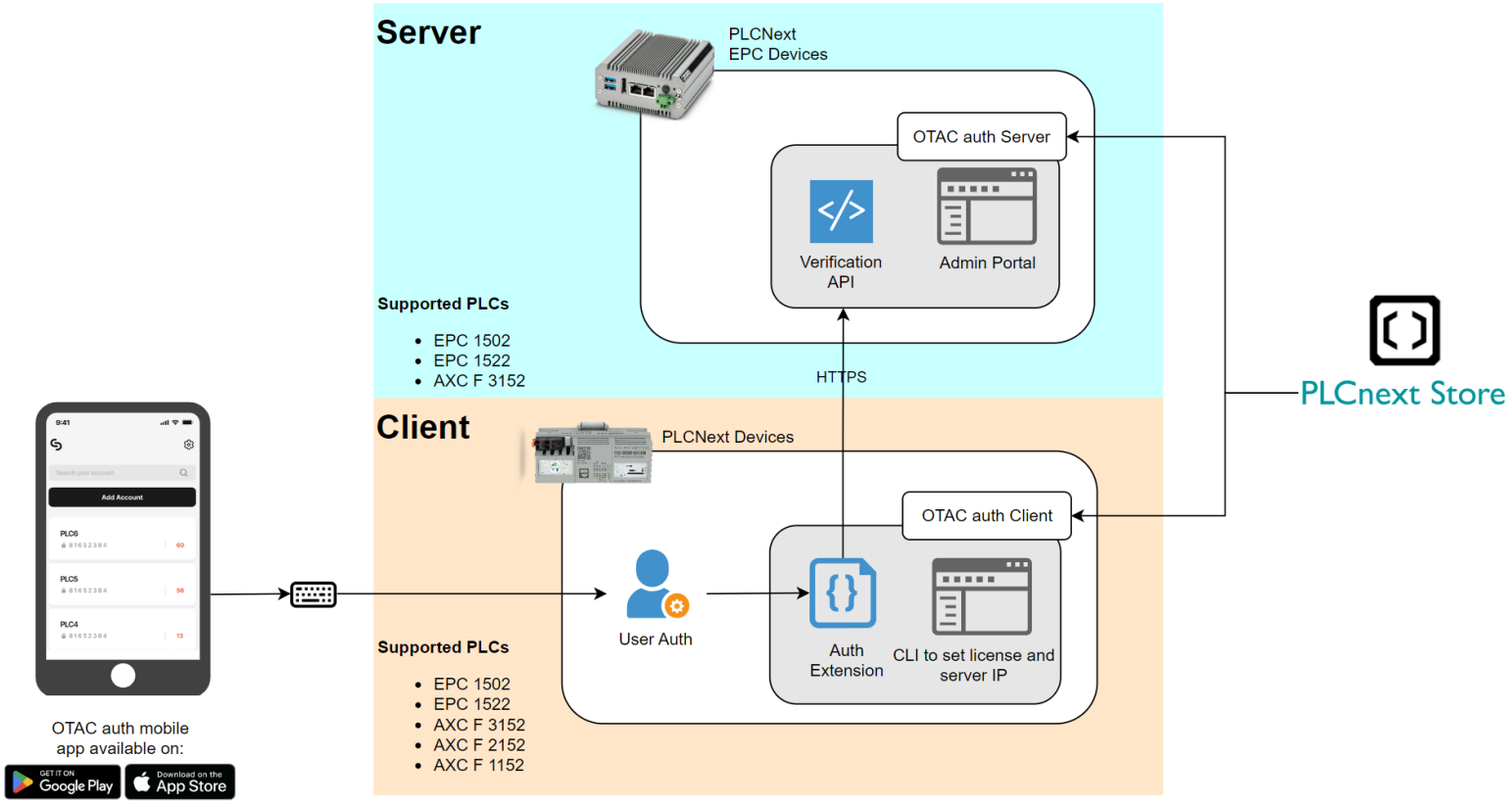
Download on the App Store

Design

The purpose of the app is to secure the PLC web login with single step Multi Factor Authentication. Once a PLC is protected with our solution, users can authenticate to PLC utilizing our dynamic 'one-time authentication code' (OTAC) technology. The code is generated on our mobile app (available on Google Play and Apple App store), is valid for a short period of time and even works offline. OTAC combined with device biometrics and/or PIN provides a highly optimized and secure authentication solution specifically for ICS/OT security challenges.

Server-Client Architecture

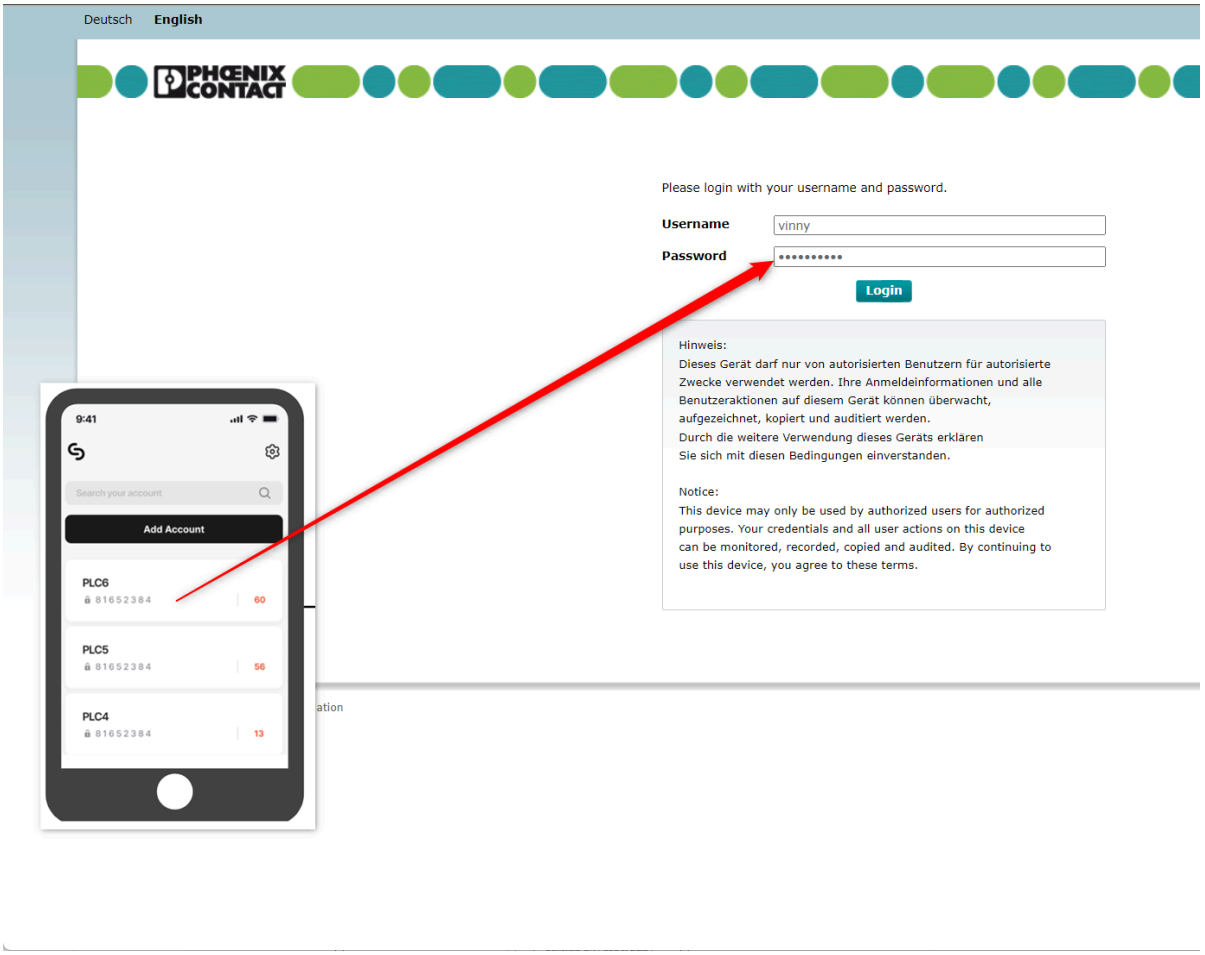
The OTAC auth app is split into the two apps: server app and the client app. This solution is intended to run the server app on a central more powerful edge PLC such as EPC 1522/1502, while the client app has a much smaller footprint and can run on any PLC. This allows the same solution to be deployed on multiple PLCs. The client app only contains the “Auth Extension” responsible for redirecting the user authentication to the server app. The client app also comes with CLI tools to easily set the licenses and the IP address for the server.



The app contains the following key components:

- **Mobile App**: This is responsible for generating the OTAC running on android or iOS.
- **Server**
  - **Admin Portal**: This is a web server that runs the management portal and is also used for the registration.
  - **Verification API**: This is the back end service responsible for verification and securely storing the user secrets.
- **Client**
  - **Auth Extension**: This is a library that redirects the user's username and password from PLC's WBM the verification service.
  - **CLI**: CLI tools to easily set the licenses and the IP address for the server

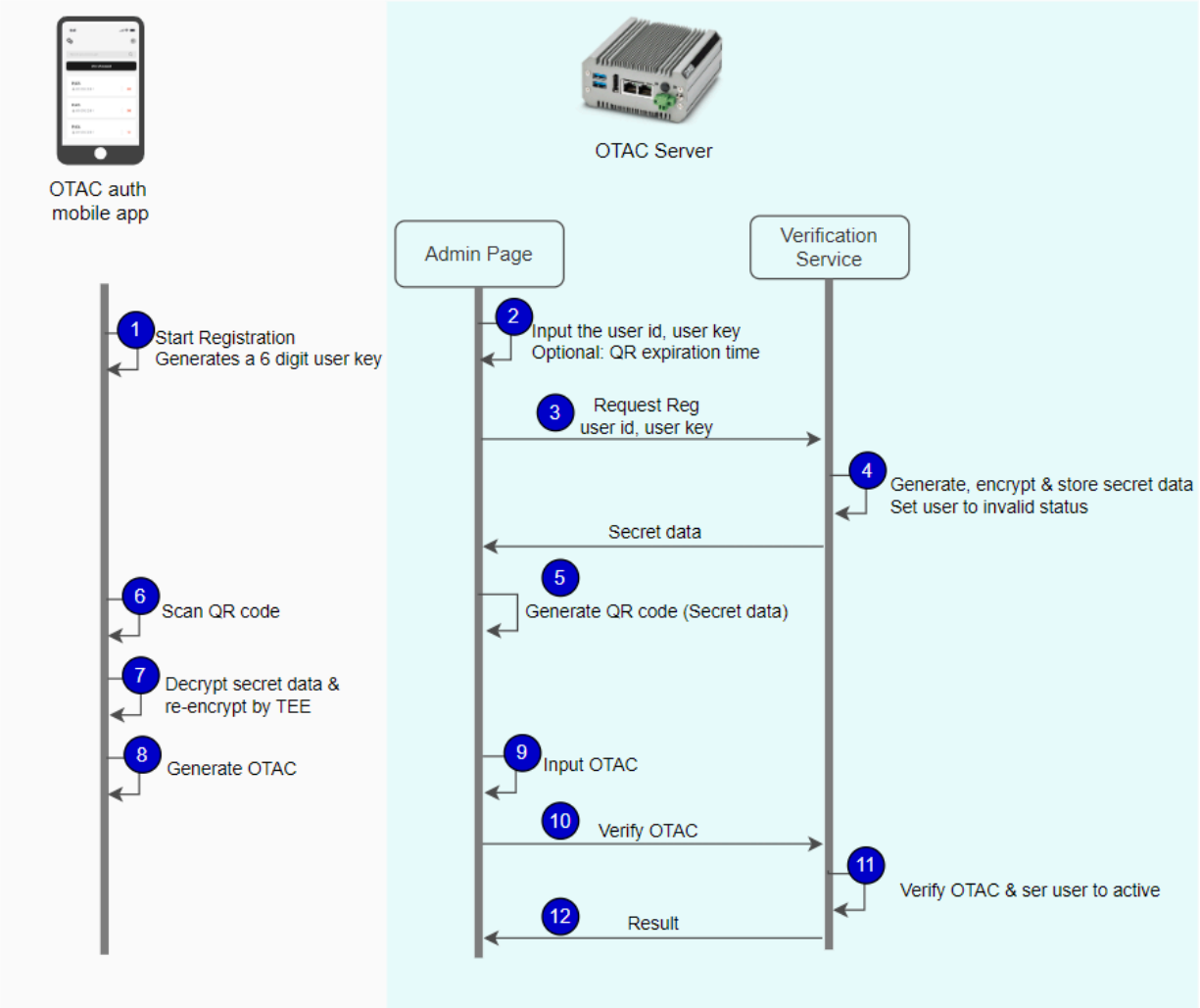
User Login Experience



Once the PLC is protected by OTAC auth, the user will not have to remember any passwords. They simply use the mobile app that generates one time-use OTAC valid for a few seconds as their password.

User Registration

The standard registration process happens in combination with the end user and admin user, the detailed steps are described below the diagram.

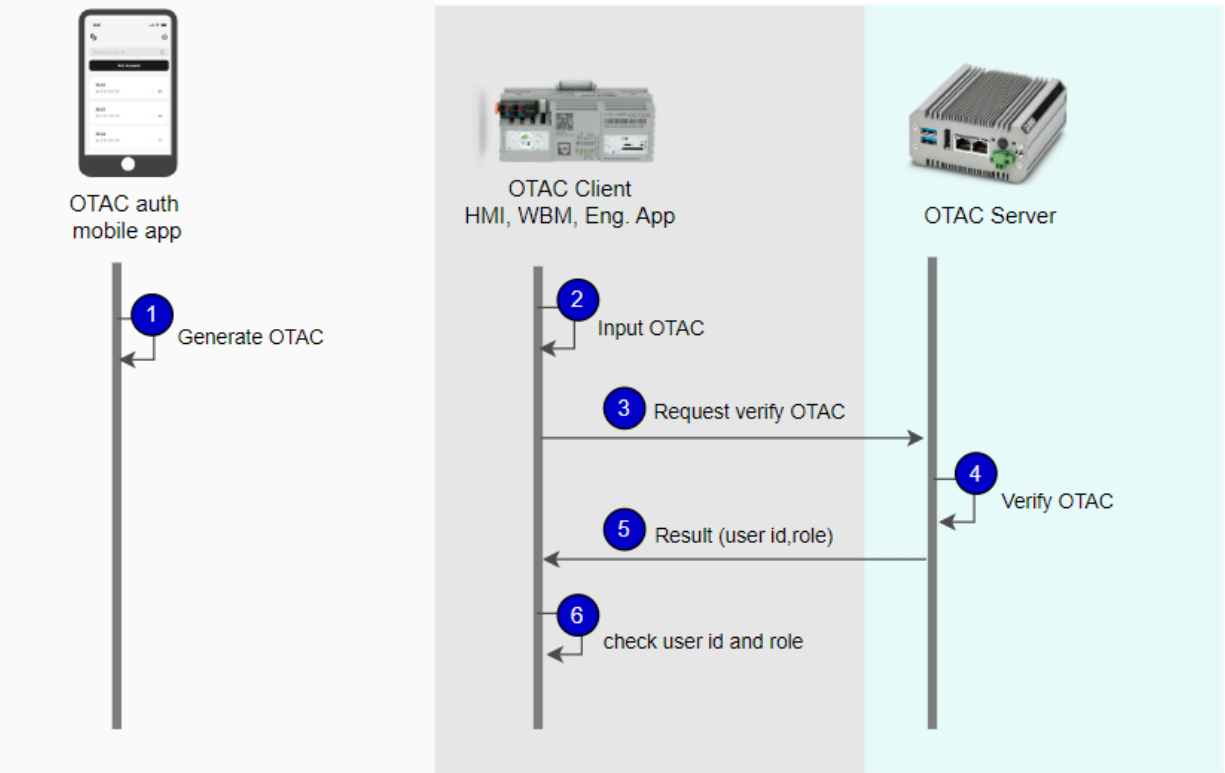


1. The first time the user opens the mobile app, they are guided through a registration process. The app first generates a random 6 digit user_key. This key is used later to encrypt and decrypt (in step 4 & 7) the secret data during transit.
2. On the Admin Portal and administrator starts the onboarding process by creating a user object and providing the following details:
    - user_id (username)
    - system_id (this is ID of the PLC device they are allowed to login in to, this parameter is optional)
    - the user_key generated on the users mobile device
3. The user_id, system_is and user_key are sent to the OTAC Server
4. The OTAC server generates a secret key for the user and encrypts it with the user_key. At this point the user status is set to invalid
5. The encrypted secret data is shown as a QR code on the admin portal.

6. The user on their mobile app can now either scan the QR code via the camera or input the secret data manually via the keyboard.
7. The secret data is decrypted using the user_key and the user secret is extracted. The user secret is then re-encrypted with a new private key and the private key is stored securely on the devices TEE (Trusted Execution Environment)
8. This finishes the pairing process, but to finish the registration process the user is asked to generate an OTAC code.
9. The administrator on the admin portal inputs the first time generated OTAC code from the user mobile.
10. The OTAC is passed to the OTAC server
11. The server verifies the OTAC and sets the user status to valid and
12. returns a successful message back.

User Authentication

While logging into the PLC, the user is prompted for a username and password. In the password field the user has to input the OTAC generated on their mobile phone. The detailed steps are described below the diagram.



1. The user opens the OTAC auth mobile app on the phone.
2. The user inputs their username and the OTAC from the mobile phone as the password.
3. The PLC passed the username, OTAC, PLC id and the device id to the OTAC Server.
4. The OTAC Server verifies the OTAC, PLC id and the device id and…
5. …returns the result along with the user id and users roles back to PLC
6. The PLC checks the result along with the user id and the roles to allow user access.