KONTAK

WHITE PAPER

Company: Orema Software Inc.
Author: Kürşadcan Akay

What is Kontak?

Kontak is a **decentralized** application platform that provides Authentication and Authorization infrastructure by default. It serves as a **Super App** (Super Application) with **PaaS** (Platform as a Service) structure. In its design, Person, Digital Platforms and Physical Locations are defined as actors. It gives Digital Identities to these actors and uses **zk-SNARK** (Zero Knowledge Succinct Non-Interactive Argument of Knowledge) technology in interactions between them. Thus, it brings a definition of interaction that fully respects the Data Privacy of the parties. With its Super dApp concept, it makes it possible for end users (Person actor) to access Decentralized Applications under a single roof. It provides the Decentralized Applications under its own application , the opportunity to benefit from the capabilities of mobile environments (the ability that dApps do not have in the current state of the technique).

Mission

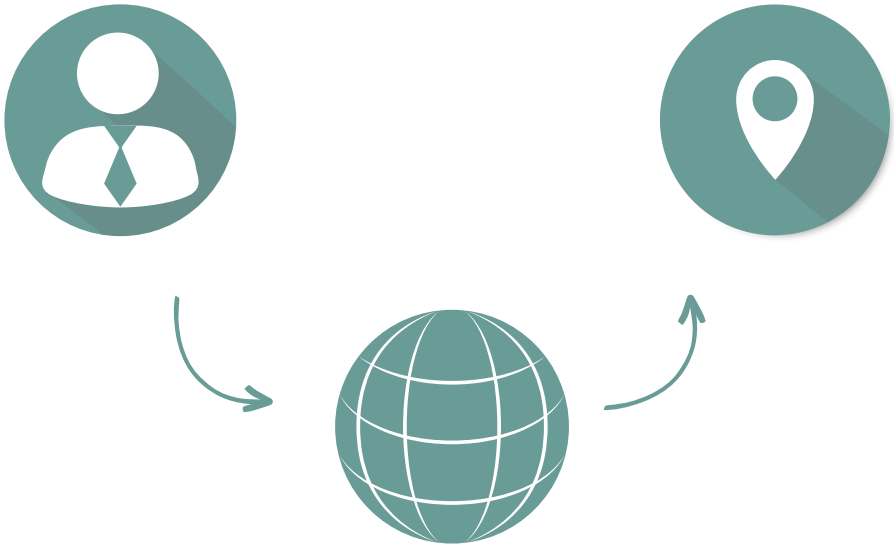
To bring a solution that fully respects data privacy in interaction scenarios by providing digital identities to people, digital platforms and physical locations. While providing new capabilities to decentralized applications, ensuring that they are easily accessible for end users from a single point.

Vision

To provide a solution with full respect for Data Privacy of interactions in varying contexts, including daily interactions, and make it accessible on a global scale.

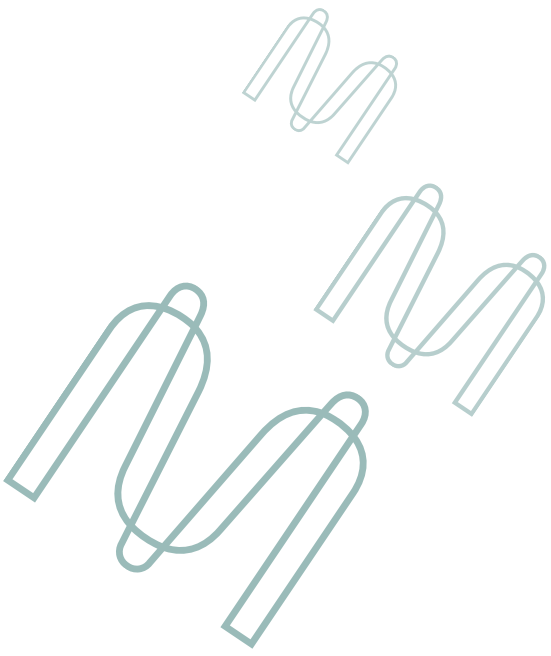
Kontak’s Problem Domain

- There is no solution which provides **Digital Identity** for **Person**, **Digital Platform** and **Physical Location** at the same time while providing completely data privacy.
- High need for **bureaucracy** at Authentication and Authorization steps in daily life.
- People cannot prove expected information from them **without revealing** information itself.
- There exists an **infrastructure investment** for the process of Authentication & Authorization for companies. To satisfy **security** standards, they have to purchase biometric authentication technologies such as Face Scanner units, Iris scanner units etc.
- **Physical Locations** dont have a **privacy-oriented** interaction channel even after visitors left the place.
- There is no automated and privacy-based way to reach services which provided that exact physical location.
- In versatile digital platforms, users have to fill seperate forms and **share their personal data** with authorities. And this digital platforms does not provide Data Privacy. Instead of this, they share users personal data with 3rd party authorities.
- In varying digital platforms, people have to **fill same form fields** as login, register etc. Actually these form requirements are almost same for each digital platform.



Kontak’s Solution Proposal

Person, **Digital Platform** and **Physical Location** are defined as actors of solution proposal. Interaction between these actors being determined with **Smart Contracts** on the **Mina blokchain** with the usage of **zk-SNARK.** Mina blokchain selected because of its features such as **layer-1** and **lightweight** blockchain network (22kB) infrastructure, zk-SNARK technology, privacy-oriented structure etc.In the interaction between the actors, there is a process-based role sharing in 2 basic roles, namely the **Verifying Party** and the **Verified Party**. The party that needs to present its identity is the Verified Party, while the party that verifies the identity presented is the Verifying Party. Data confidentiality of the parties is ensured by using **zk-SNARK** technology in the data exchange of the actors in the Authentication and Authorization processes. Afterwards, actors start to consume provided services at that context. Due to the context difference of the actors, the solution developed on a context basis. The actors and interaction procedures are described below.



1. Person

The **person** actor is defined to greet actual person. Today, key actor of people's interactions between digital platforms, physical locations and people is smartphones. Because of that, a mobile application named **Kontak**, designed to provide a suitable solution.

Kontak mobile application provides a **Digital Identity** service. People can add/verify their claims on their account and this service acts as a **Self-sovereign Identity** . All of the information that people have added here is stored only on their mobile device. Claims are being completely stored on users local device while ensuring about claims are not shared by any 3rd party. The data is stored only at the mobile storage of the person's device, the data is not stored or processed on any remote server.

At the interactions of the person actor with others. The Authentication and Authorization procedure is carried out with the smart contract at **Mina blokchain**. When an interaction occurs with person and others, **zk-SNARK** technology being used to provide data privacy. Thanks to zk-SNARK, any data of person not revealing with other parties without loosing any abililty of the interaction.

Kontak mobile application designed in the **SuperApp** concept to enable access to various services. In this way, the person who has verified and/or unverified information in the application can reach the service providers that they want to interact with through the application. With this concept, which allows hosting and integration of more than one application, people get rid of the cost of installing each app even if they need just to related app just for a very short time.

2. Physical Locations

Physical Location actor defined as a physical places that provide services in a physically defined context. School, hospital, shopping mall, bank etc. Physical locations are being capable of interact with mina smart contracts thanks to physically located identification units called **Kontak Point**.

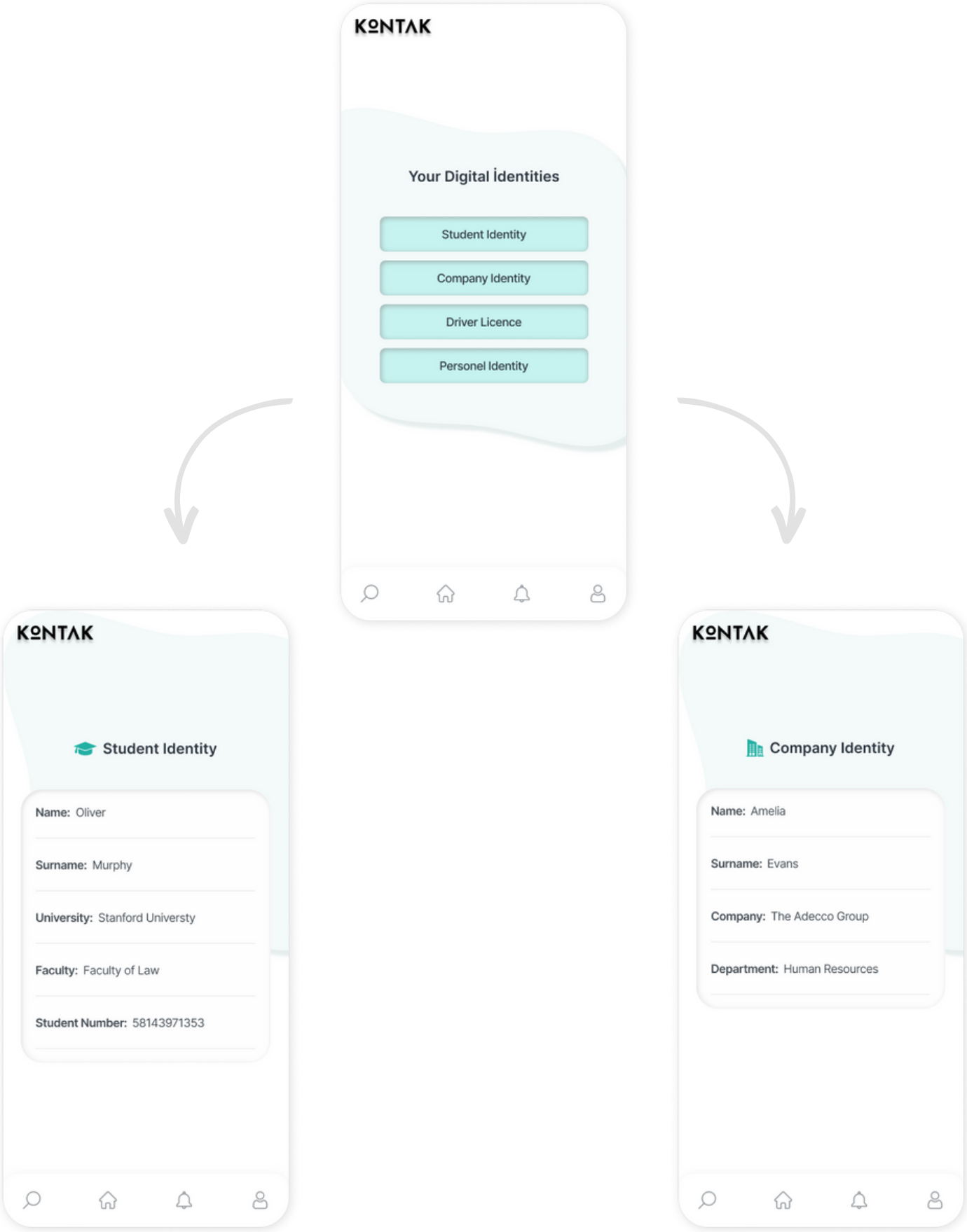
Kontak Point is a low-cost computer. A tablet, raspberry Pi, Arduino etc. It located physically at related places enterance, broadcasts pysical locations identifier in varying protocols such as **BLE** (Bluetooth Low Energy), **IEEE 802.11** (Wifi and subprotocols), **QR Code** etc. Related places physical interaction requirements being configured by provided web interface.

3. Digital Platforms

Digital Platform actor defined as parties that provide services on digital contexts. Social media platforms, websites, mobile apps, dApps etc. They provide an Authentication and Authorization gateway with Kontak to the users. Depending on the context of the Digital Platform, Kontak implementation gateway varies.

Websites provide an Authenticate option with the displayed QR code. Users can scan the displayed QR Code with the Kontak Mobile App to to authenticate. On mobile application, **Continue with Kontak** button exists. Which is configured as a **deeplink** and interacts with Kontak Mobile App. Each of these ways are interacting with Kontak Mobile App to complete Authentication and Authorizaton process

Digital Identities on Kontak



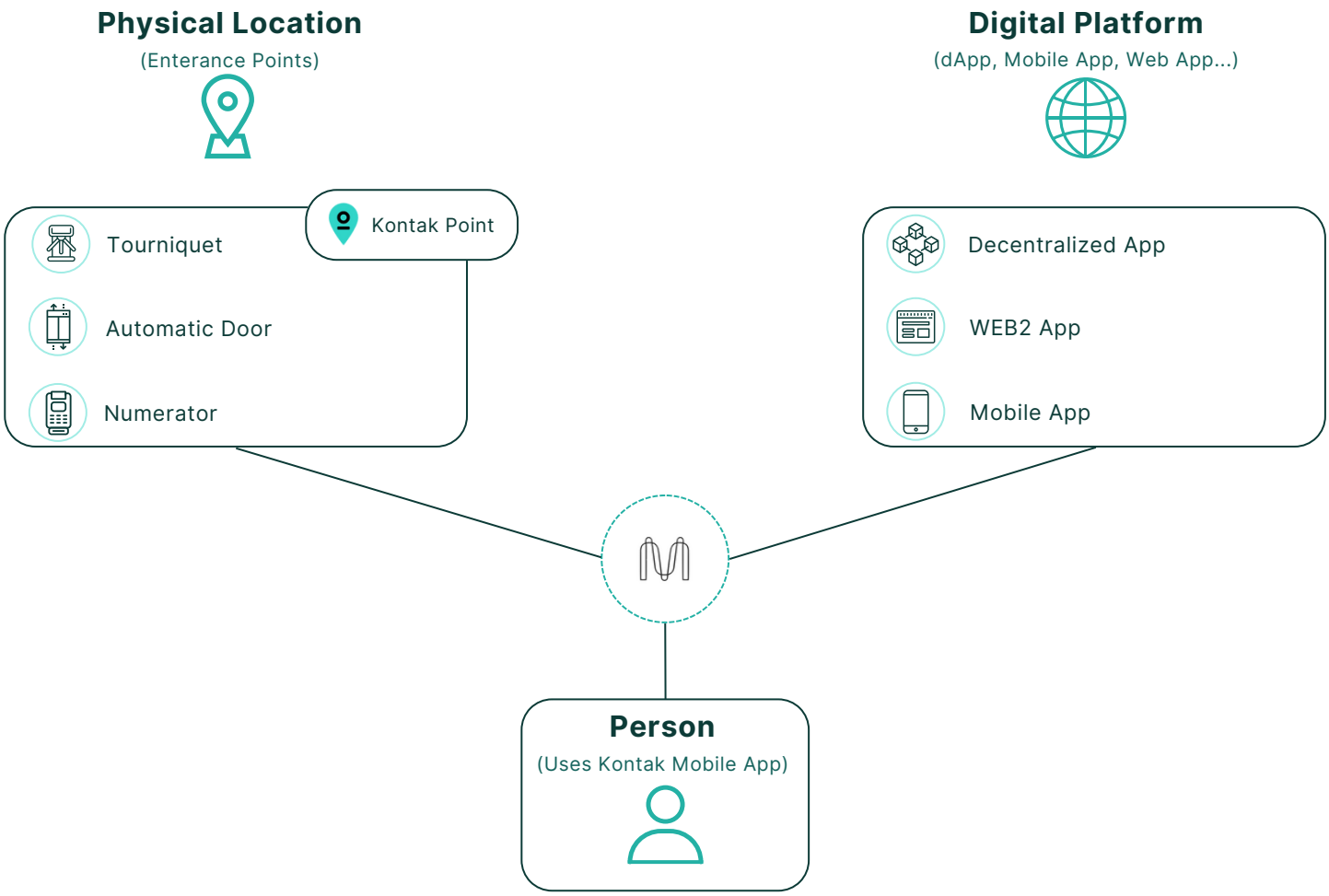
Goals

The goals planned to be achieved with the Kontak project are as following:

- Providing an autonomus and contactless Authentication and Authorization solution for Digital Platforms and Phyiscal Locations.
- Providing an enhancement model for security/privacy concerns with the usage of both MFA and zk-SNARK.
- Eleminating digital steps such as Register, Log In, Verify Mobile Phone , Verify Payment Method etc.
- Developing a decentralized solution that eliminates the obligation of data sharing with 3rd party verification authorities.

- Introducing a new concept to anonymous profiles by offering the possibility of creating a profiles that can contain verified information without revealing data. Thus, preventing disinformation, pollution, troll accounts, pirate users, fake accounts etc. while respecting data privacy.
- Presenting related services at that exact phyical location to visitors while eliminating service costs.
- Eliminating identity tracking
- Bringing the mobile capabilities to the to decentralized applications
- Making Decentralized Applications accessable for the users of mobile environment.

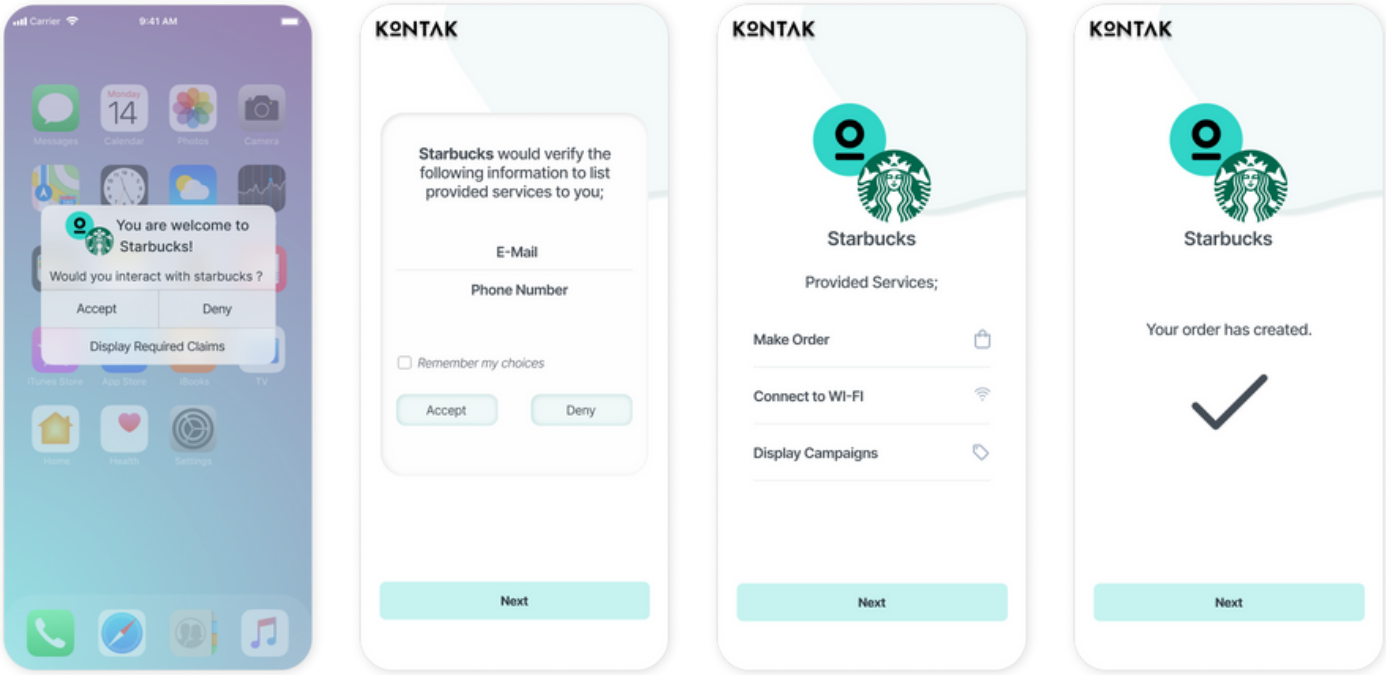
Actor Diagram



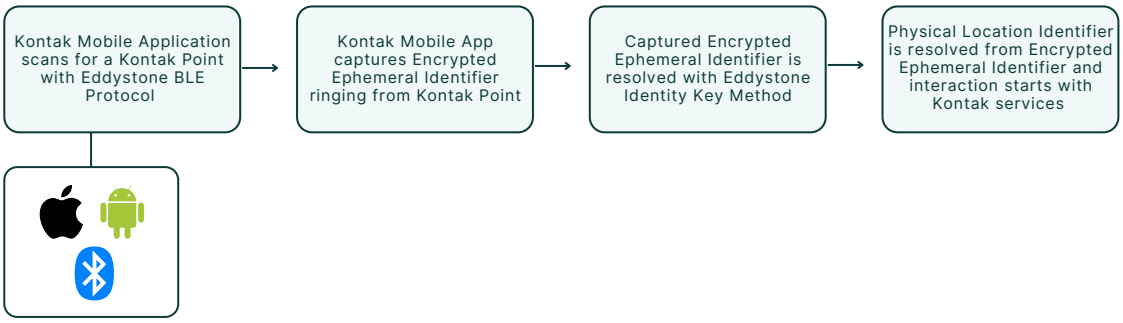
The diagram given above displays the actors and several real life samples.

Person-Physical Location Interaction

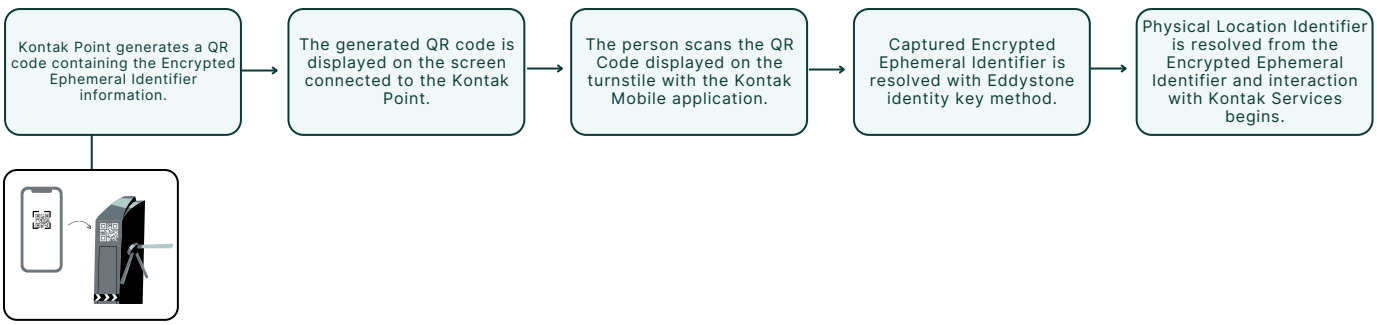
UI Flow



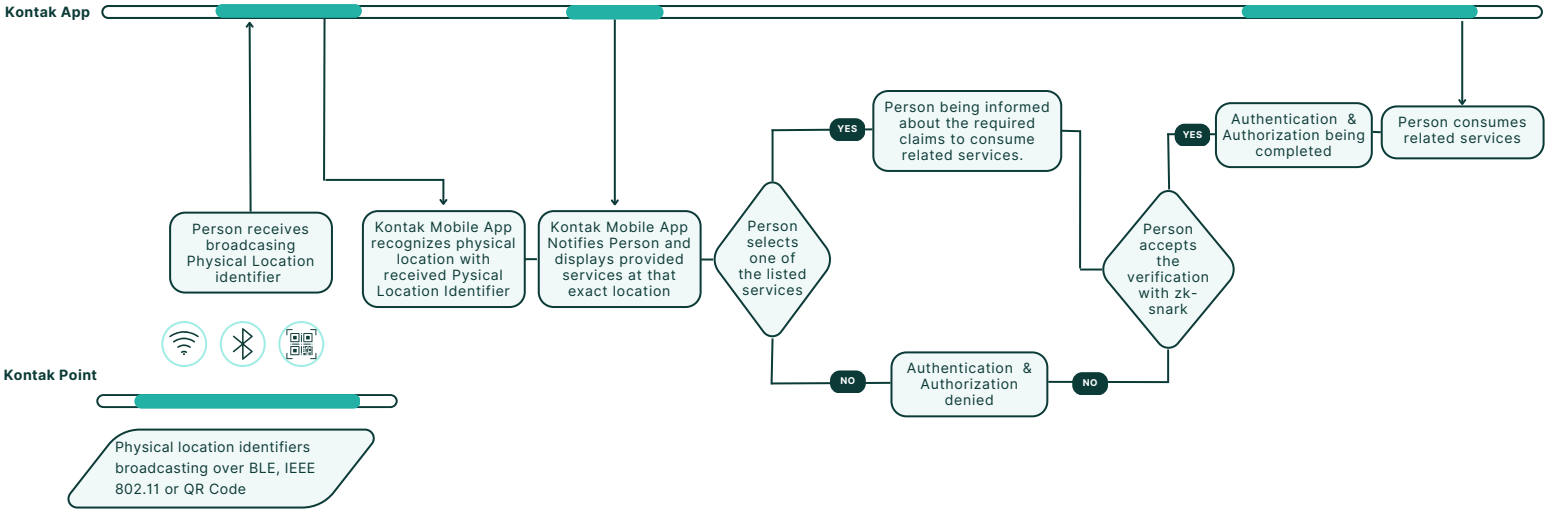
BLE Flow



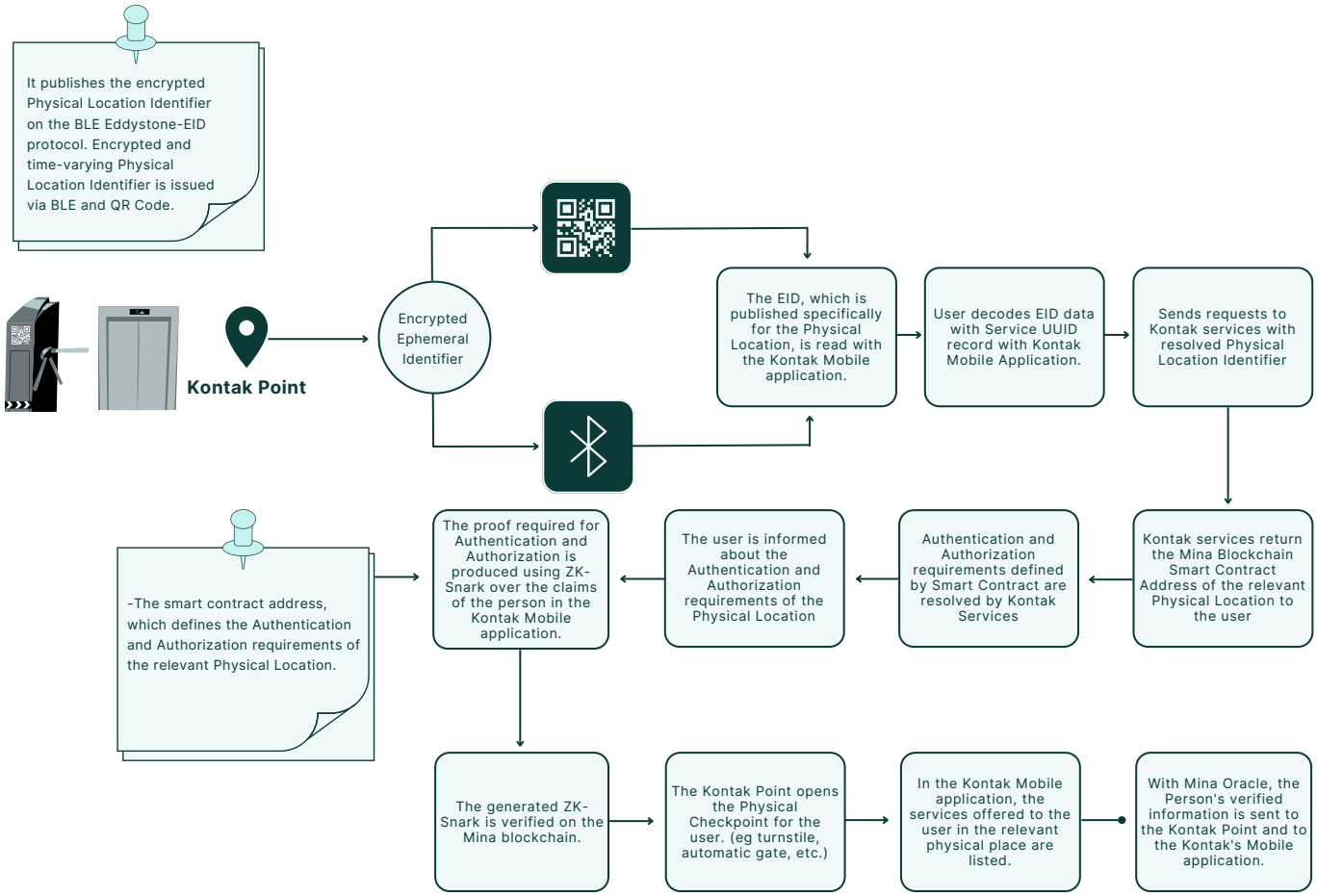
QR Flow



Basic Interaction Flow



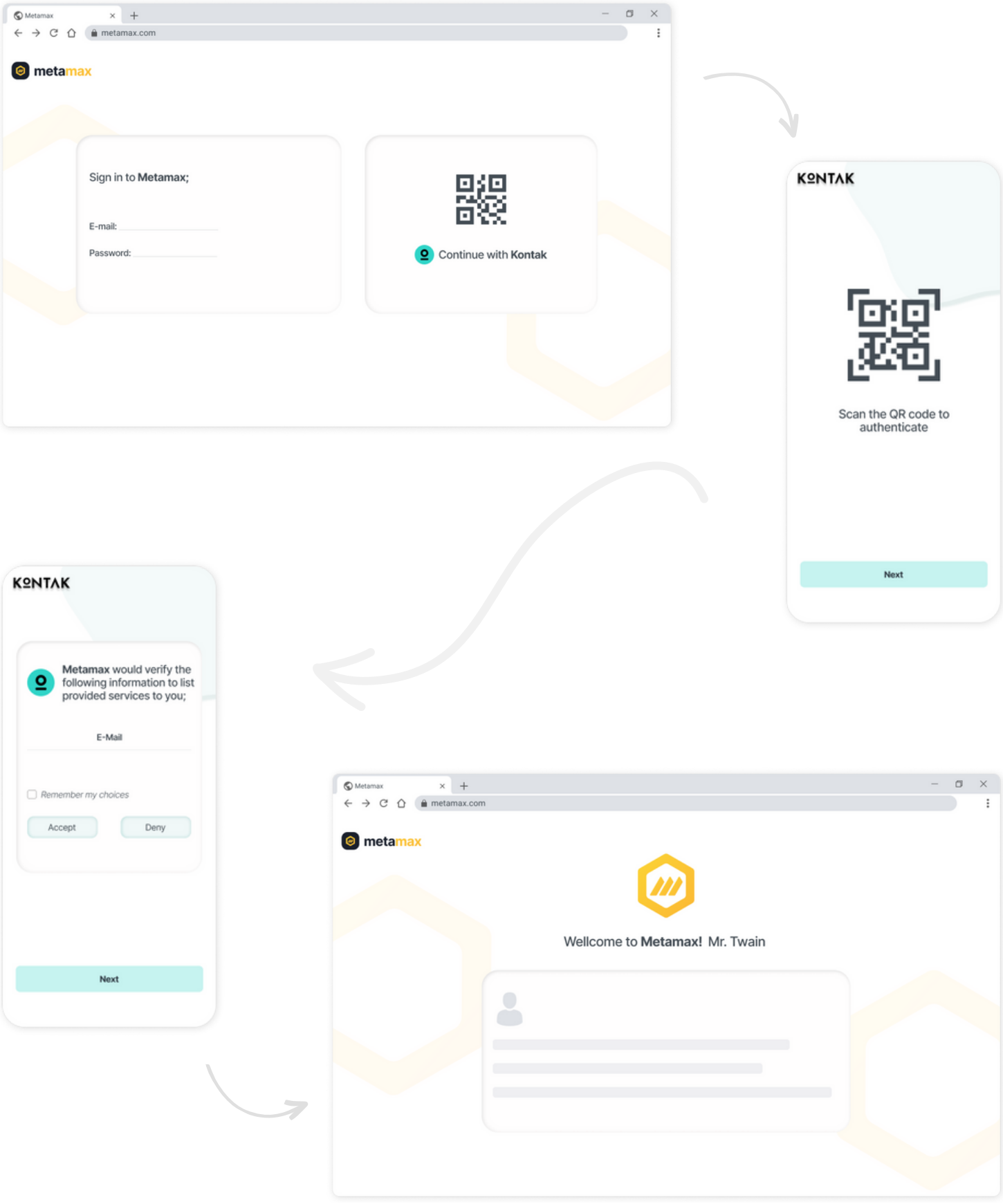
Detailed Interaction Flow



Person- Digital Platform Interaction

UI Flow

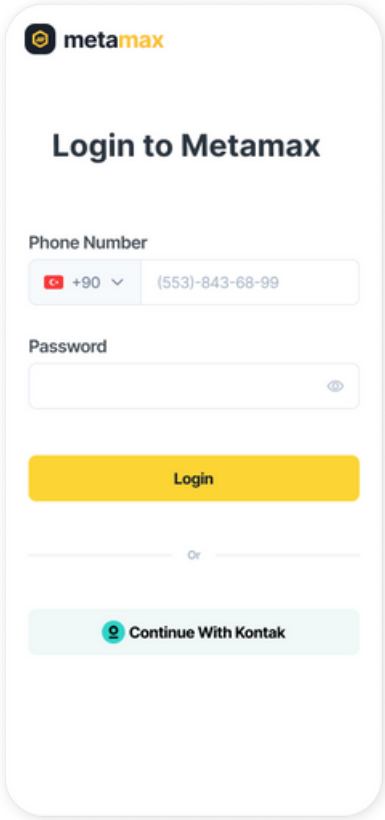
Desktop Web App - Kontak interaction

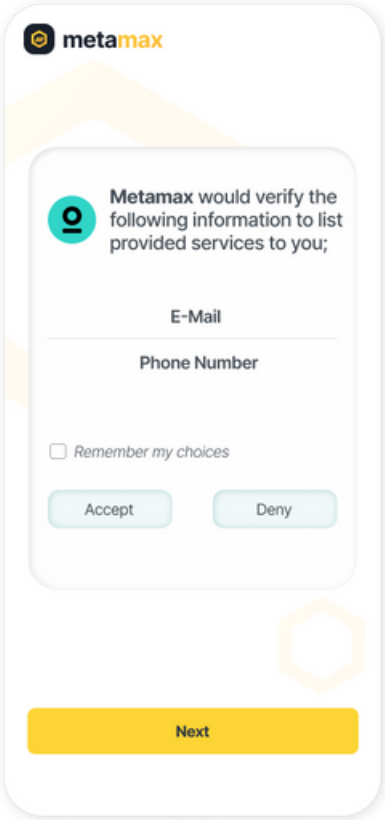


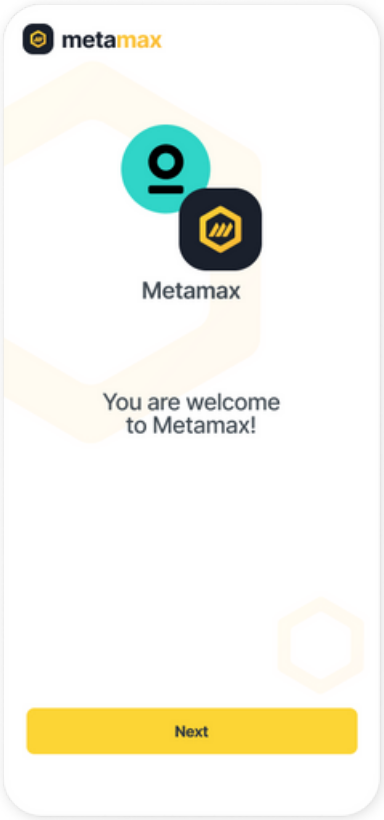
Person- Digital Platform Interaction

UI Flow

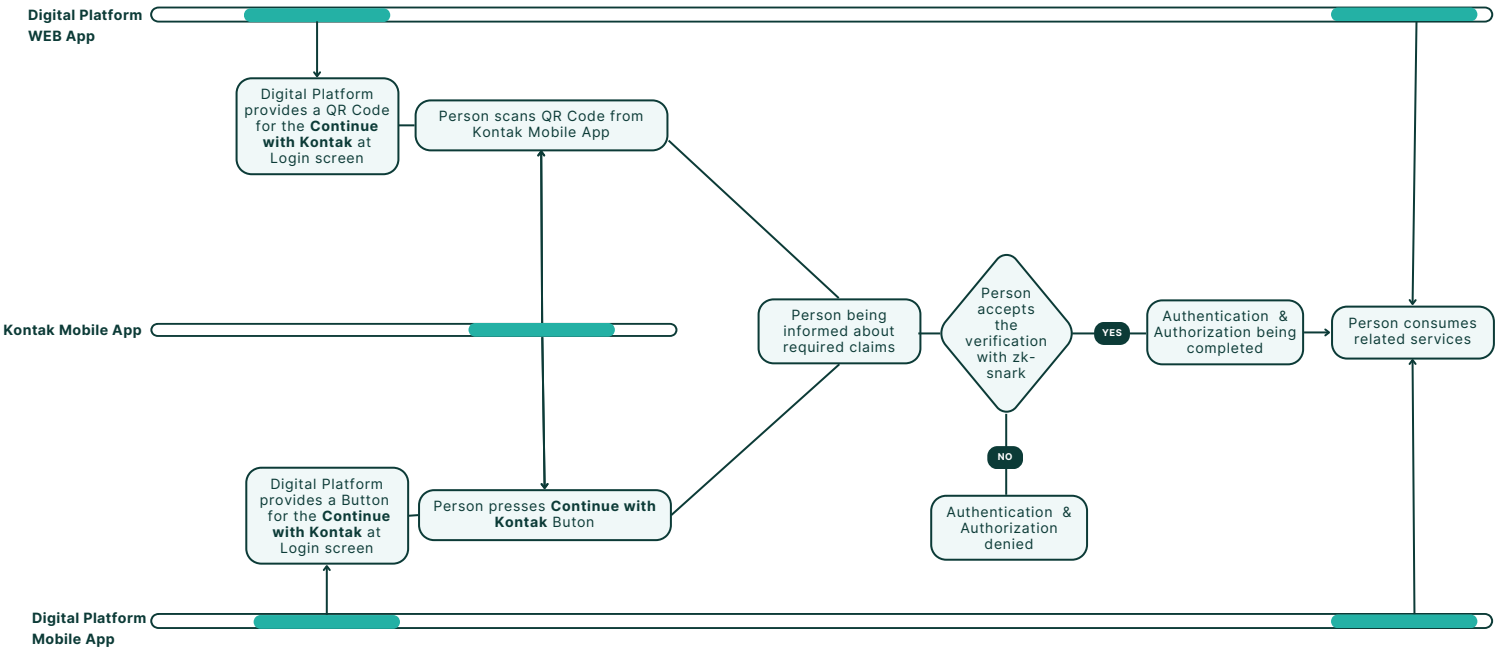
Mobile App - Kontak interaction



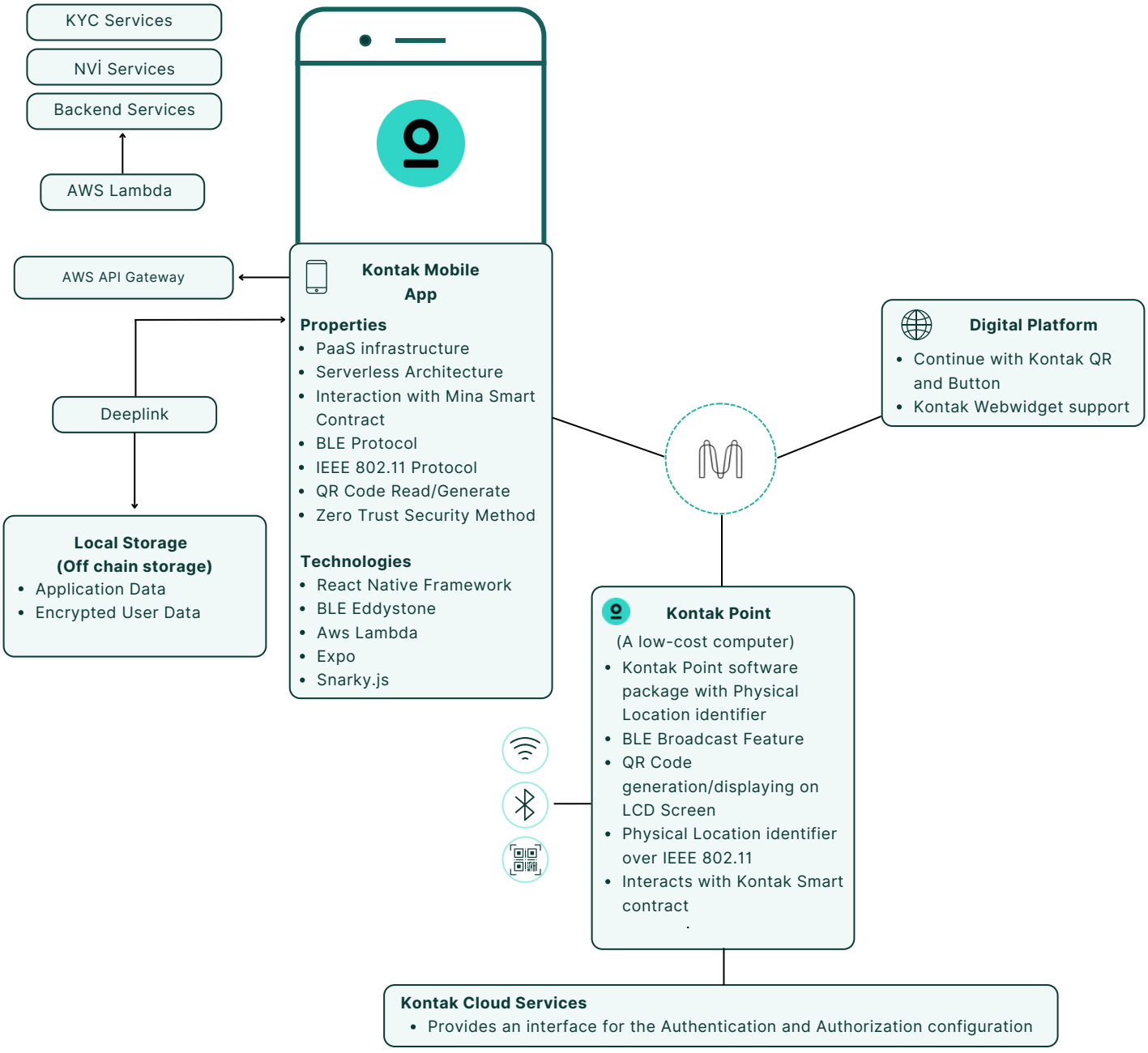




Interaction Flow



General Feature Diagram

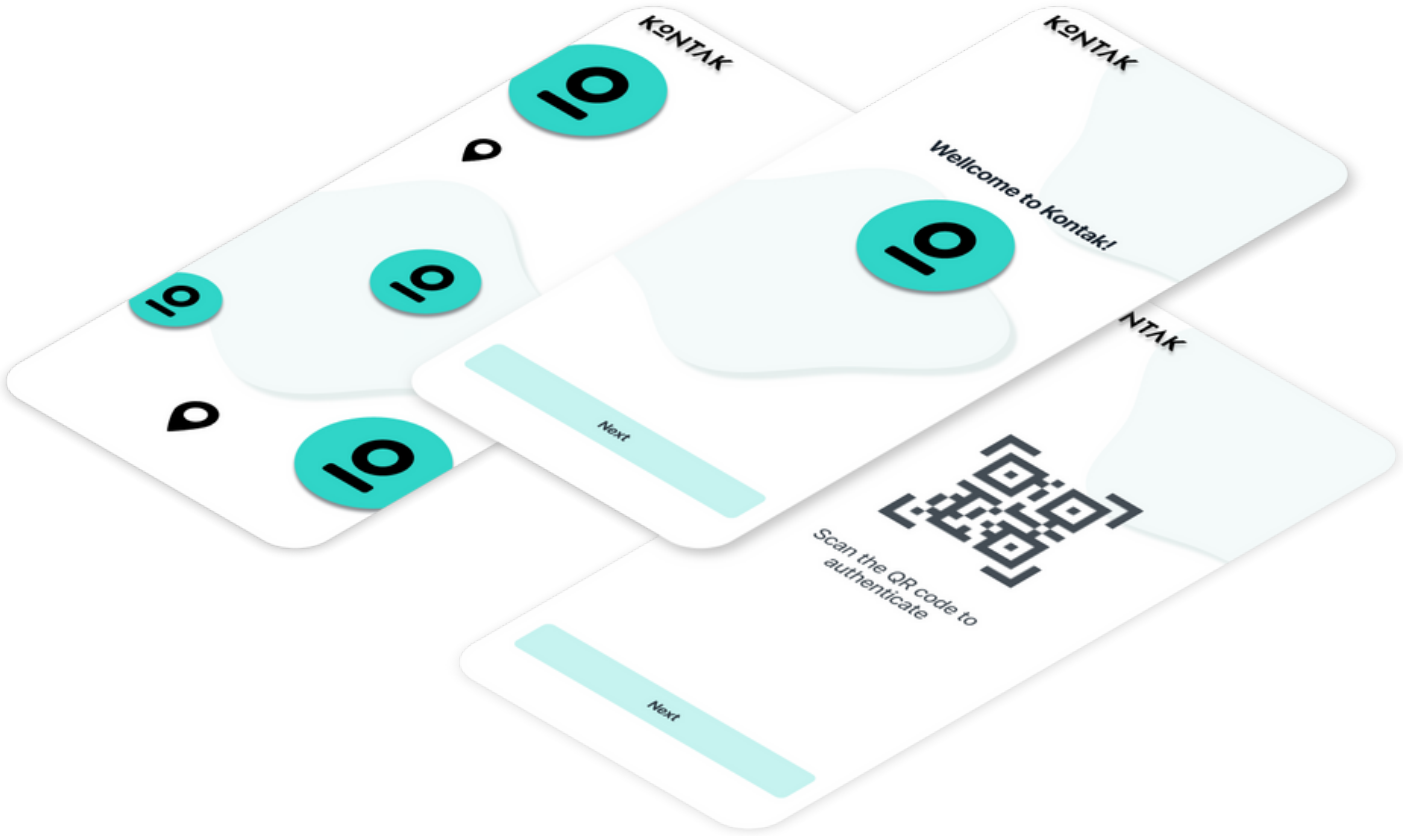


Kontak is backed by

desiRd

metamax

OREMA



Contact: contact@kontak.org