BUILDING A SMART CITY

The Problem

The demand for secured authentication has become apparent and the need for Smart City users to navigate themselves around a technology advanced city becomes more prevalent. Users would require identity access to all areas ranging from entering parking lots and buildings to making use of the city's municipality mobile and web app to request and track basic services and other cloud and web apps.

The Solution

Authlogics proposes their **Passwordless authentication solution** with the use of Tap, Push, Biometric and PINgrid technologies. Our Passwordless authentication solution replaces passwords with a knowledge factor or patterns as a "something that you know" factor for ease of use and a uniform logon experience across desktops, web, mobile and cloud apps.

Tap: For convenience, instead of typing in a username/account ID as part of a logon they can simply tap their trusted device on a reader to identify themselves.

Push: Our Push technology uses a network connection to send an authentication request on a user's mobile through the installed app for the user to accept the request or reject it. Once the user taps the request, they are then authenticated using the built-in biometric technology fingerprint/face ID/Iris scan.

Biometric: Biometrics are fairly secure, quick to use and are highly convenient for users. To avoid the expense and complexity usually associated with biometrics Authlogics leverages the biometric information and readers already setup on users' mobile devices. This can be used quickly and easily in combination with an out of band Push login or door access after a Tap.

PINgrid: Our patented and award-winning PINgrid technology shows a grid filled with random numbers which changes every 60 seconds and each user has a pattern specific to them. Once the grid is shown, the user would look at the numbers behind the pattern and type in the relevant area to log in - pattern in all cases remains in the user's mind.

As our solution allows multiple integration points with RADIUS, SAML, ADFS and OpenID connect as well as SDK integration with Android and iOS applications, we could cover all the above-mentioned requirements.

Entrance

To enter the main entrance of an apartment or office building, or even a parking lot that uses an android/iOS based entry system, the Smart City owner could do this with ease. The user would simply tap their phone on a reader after a biometric unlock to gain entry.

Payment

Similarly, if they link their credit/debit card with the Smart City public transport account and the user decides to purchase a ticket, the user only needs to enter their credentials and authenticate themselves for the system to deduct the money from their payment card and provide them with a ticket. This can be done online or directly inside a Smart City app.

Service Request

If the user wants to request a service from the municipality, they can use the same way to the authenticate themselves on their website or Smart City app and safely request the service.

Internal & Backoffice Users

The staff member at the smart city could also make use of the secured authentication. They could use the system to login securely to their desktop computers, request services through the staff website, login to their webmail and cloud SSO platforms. The IT staff members could use the solution to login to Linux servers, network and RADIUS enabled devices.

Helpdesk

The IT helpdesk will receive an Authlogics Operator Portal to help the services users.

Self Service Portal

The user of the service can also enroll themselves and make changes to their service account by logging on to the self-service which will reduce the load and cost of helpdesk.