Auth made easy

Advanced user experience whilst improving security

IT | Trieste | 2022.06.05

AUTH YOU!

Executive summary

AUTH YOU! has been designed **to simplify access** whilst **enhancing security**.
It can play a **single factor** or **MFA** role on both **web** environment and **physical** devices, with a **centralized permission management.**

Password-less solution, it enables **web SSO**; based on **standard protocol** like SAML whilst offering **customer** the **opportunity to build own extension**.

It offers also a **2nd factor** with **enhanced security,** if compared with usual **Google and Microsoft authenticators.**

OnPrem or onCloud approach available, can have a modular adoption with authentication only, or including authorization and 2nd factor.

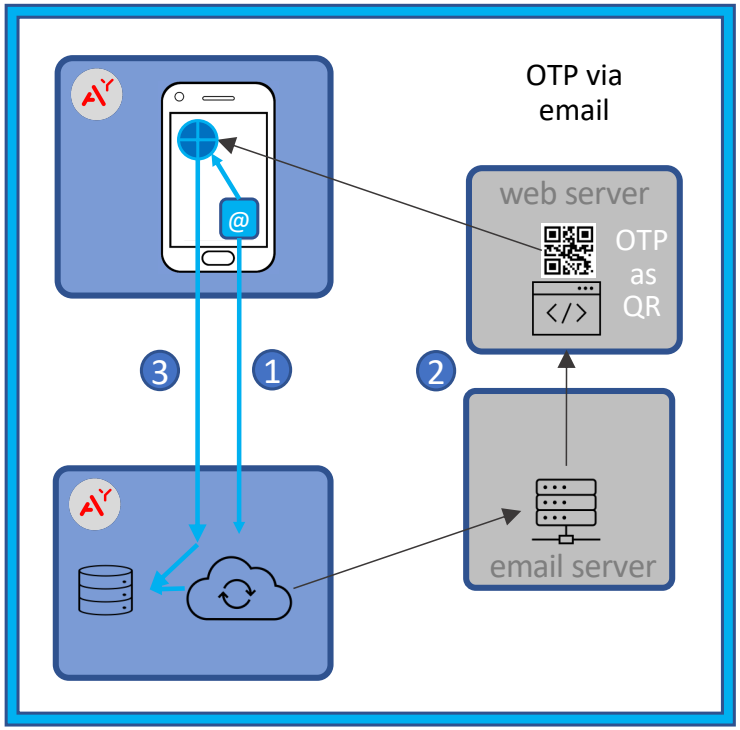
Auth made easy

The full picture of provisioning

Download the app from public Google or Apple stores, and install it on the smartphone

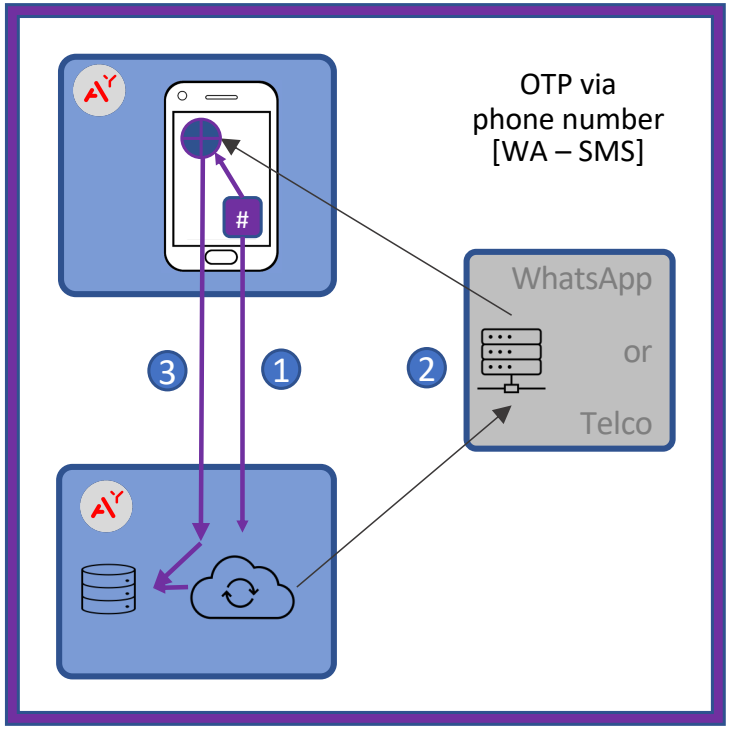
1. Require an OTP, linked to email address or phone number
2. Transport OTP via external server
3. Combine OTP and email address or phone number and make server to check correctness to validate association

Access enabled services on smartphone directly



@ Insert email address

Combine OTP and email address

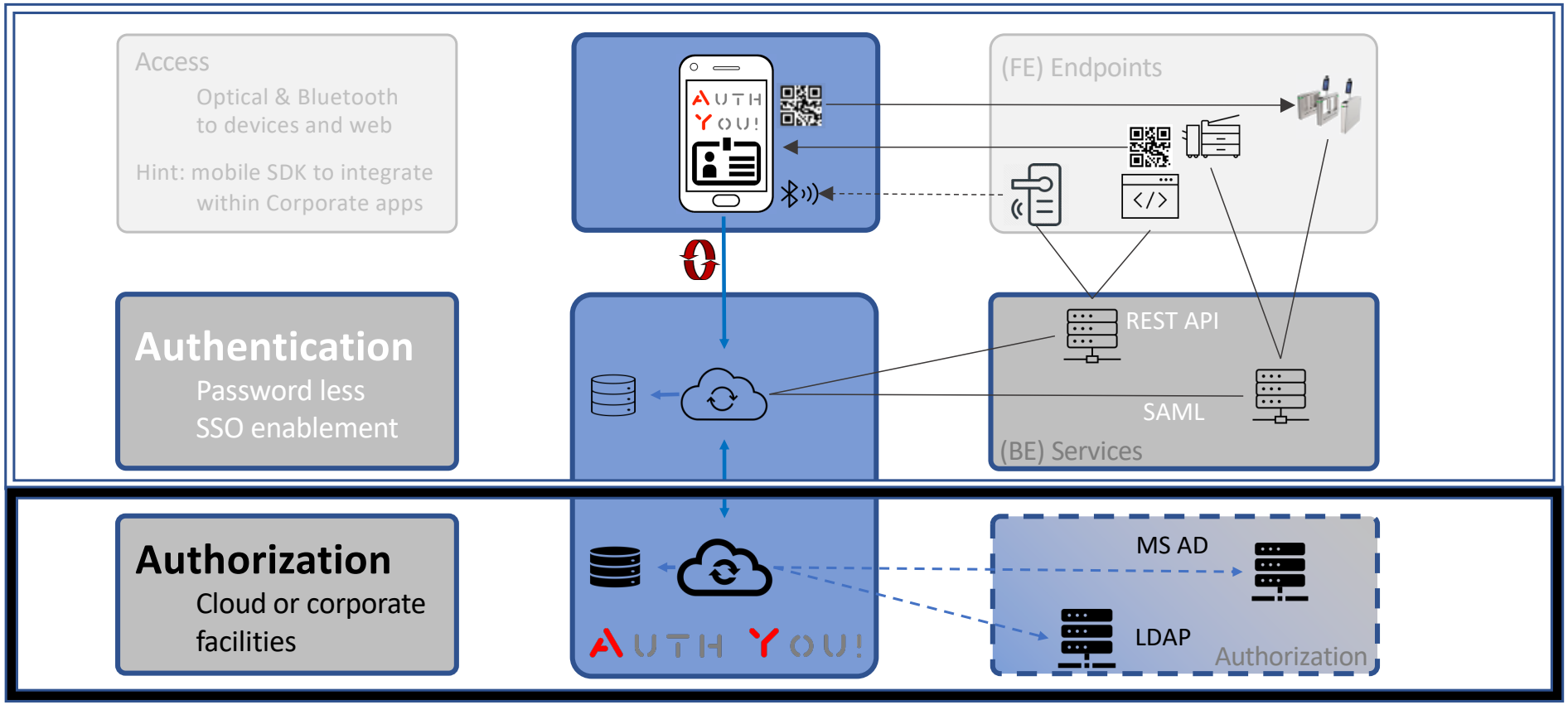


Insert phone number

Combine OTP and phone number

Auth made easy

The full picture of access on another device

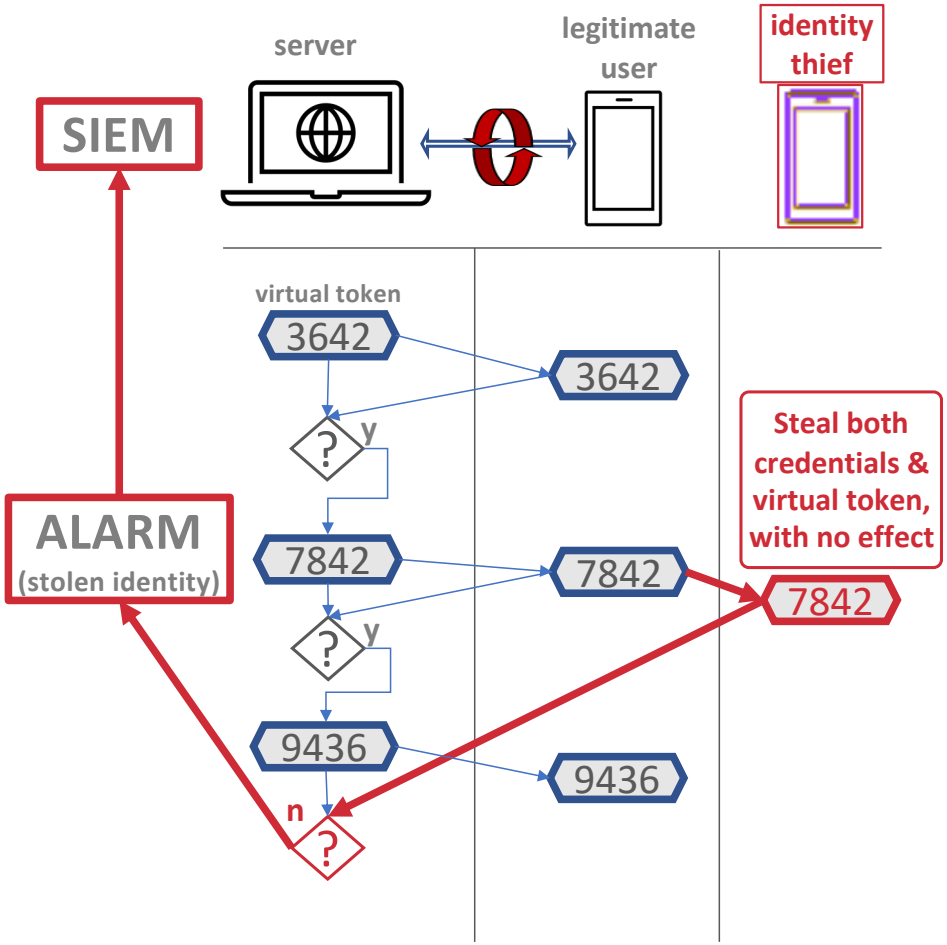


ADDITIONAL FEATURES	• 2nd factor push through WhatsApp CDN & SMS • Secure replica of Google & Microsoft Authenticator

oneTime nesting

How it works

PATENT PENDING



Nest OTP within main OTP process itself → ***Identity thief has to steal both credentials AND virtual token, which is changed at every interaction***

oneTime nesting

The OTP concept can be nested in each different segment of the main OTP process. An additional, hidden «**virtual token**» is exchanged between phone and server; it's an extra OTP, indeed.

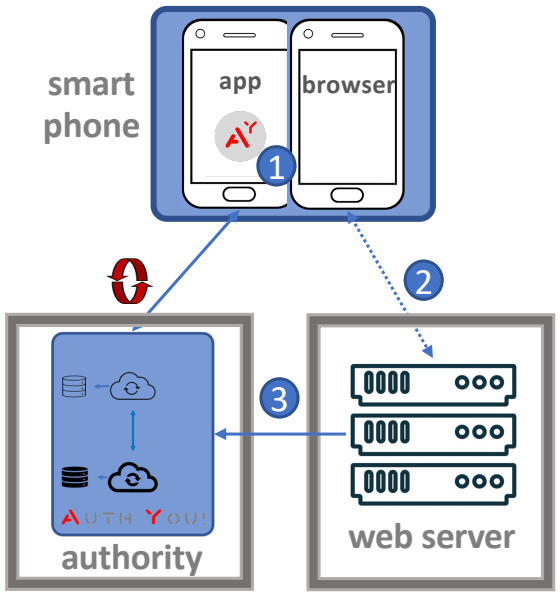
This «virtual token» value is **updated** by the server **at every interaction**; so it's valide once only.

The «*oneTime nesting*» is **a security measure on top** of the main OTP process; and the usage **can be extended** to reach a **sort of mutual authentication**.

Auth made easy

Use case 1: access to browser on smartphone directly

‘IdP initiated’ approach made easy



1. AuthYou! app requires OTP, performs a full auth process and passes the auth codes to the browser (FE, indeed).
2. FE (Front End) asks BE (Back End) for contents, passing auth codes too.
3. BE checks auth codes against authority, and on success enables service usage and sends back service list.

Login, and get list of services

[UX] services menù

[SEC] avoid fraudolent links (phishing)

One device only & detached login

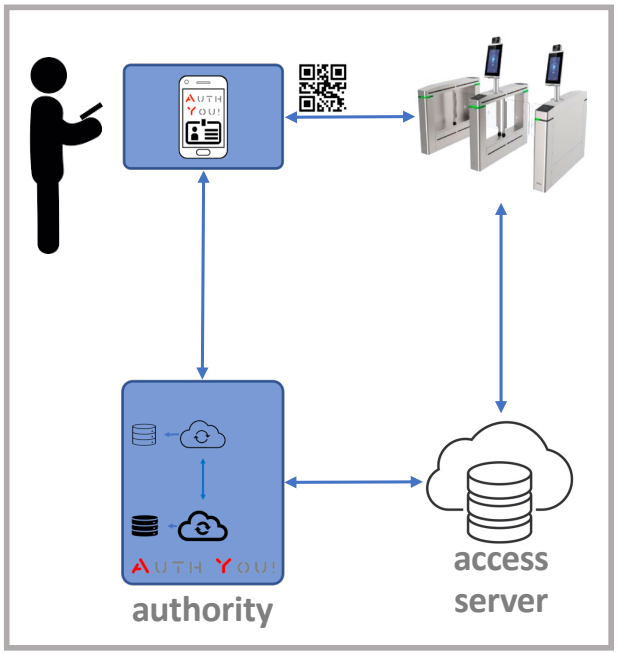
[UX] biometric access to the app

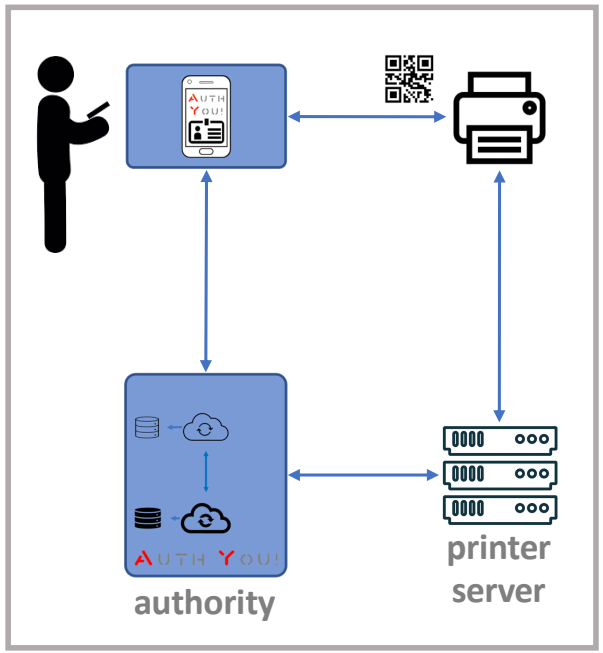
[SEC] OTP refresh under the hood

Effective, viable, frictionless, secure proposition

Auth made easy

Use case 2: access to devices





Login under control of both entities

[UX] no credentials to be typed

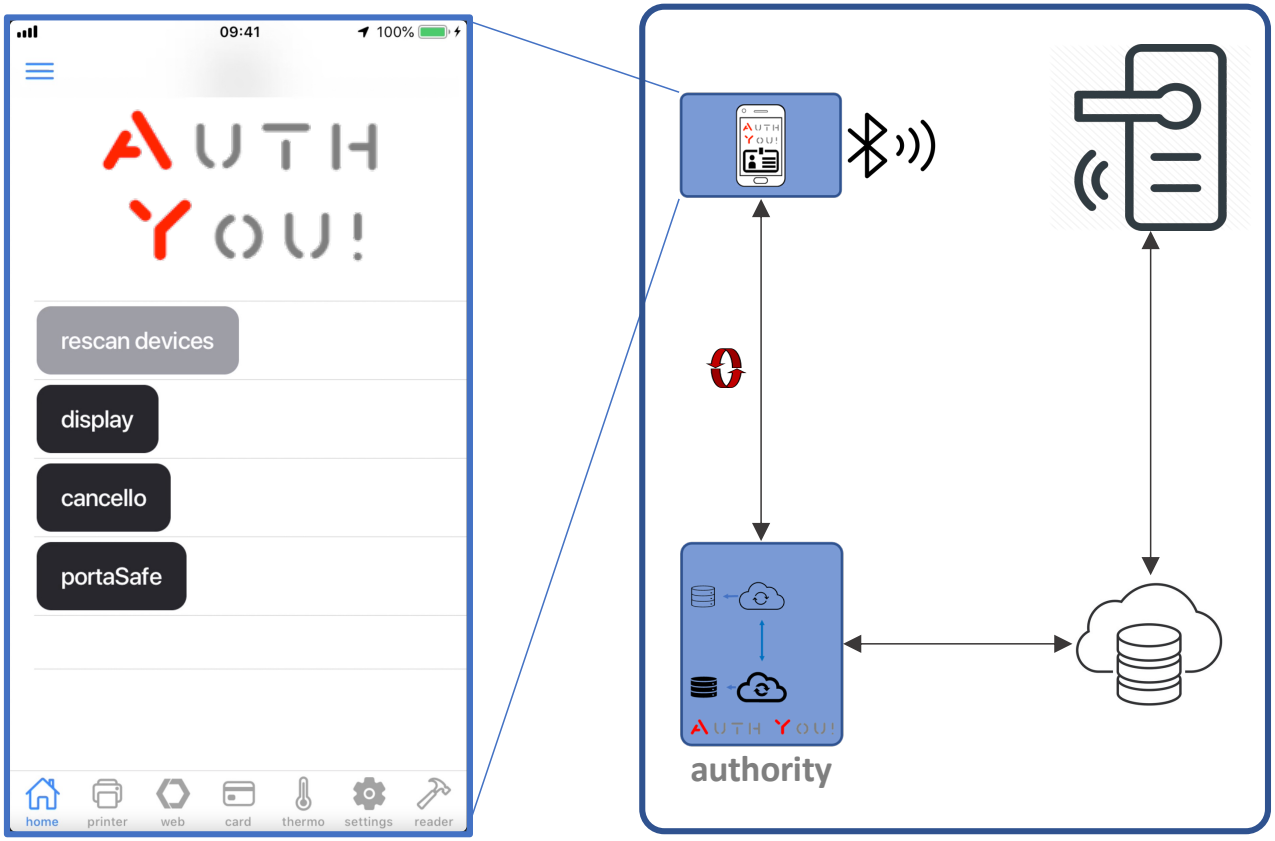
[SEC] application server is part of the login process

Authority can logically lock all services for a user.

Application server can add additional checks (e.g. face temperature on thermo scanner).

Auth made easy

Use case 3: access to devices via radio



How it works

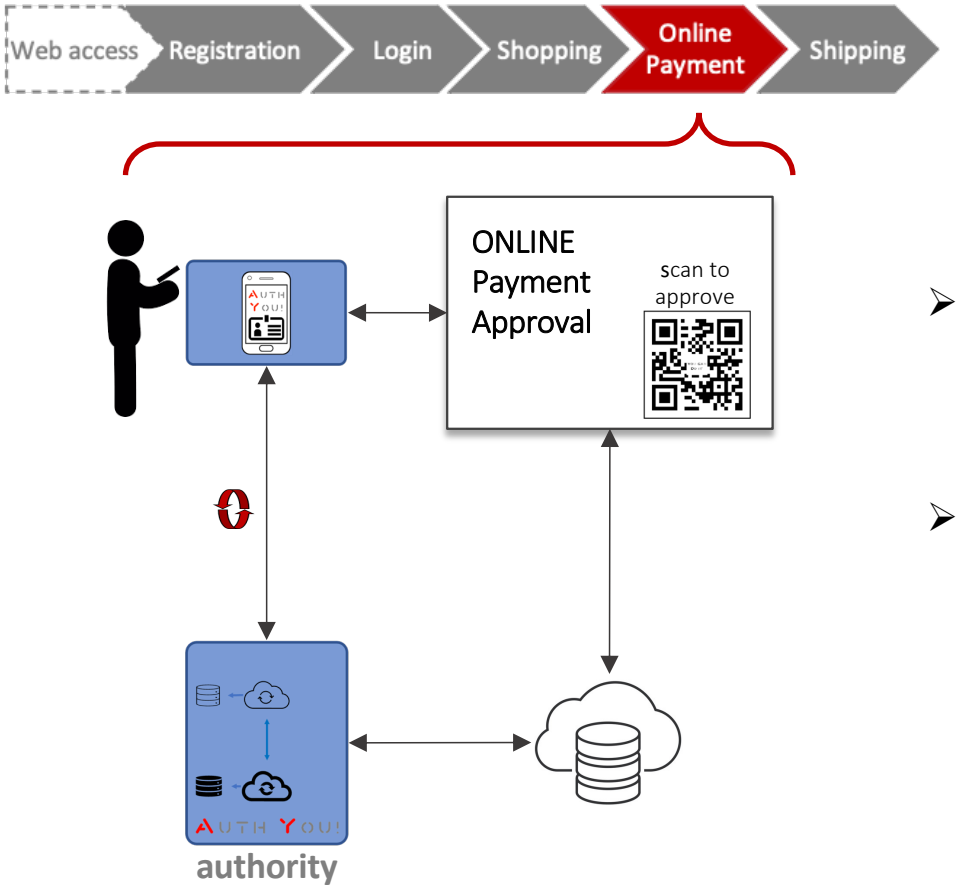
1. The app scans for Bluetooth enabled devices (door, gate, virtual turnstile), or the list of available controlled objects is downloaded from central server.
2. The user can open/close each of them with a single click on available buttons on the smartphone screen.

Unconnected PAN network, like door of hotel rooms, are prone to attack.

Connected devices remediate this threat by checking validity against a trusted authority.

Auth made easy

Use case 4: embed within other processes



- **Can be used within existing processes, as 2° factor**
  [UX] authorization requests can be **queued** on central server and retrieved by user when it' s **more convenient**
  [SEC] not always-on push channel to smartphone
- **Suited for asyncronous events / offline batch**
  [UX] **no need to switch app** (e.g. PayPal), no account needed
  [SEC] e.g. payment by batch job after verification

2nd factor

Google & Microsoft Authenticator review, with added extra security

1 – how does it work

'Authenticator' apps are based on a 2005 RFC document, the assumption of which is that the storage is secure. So, a static password plus current timestamp are used to derive a 6-digits TOTP.

When enrolling, a content similar to the above one is shown.

otpauth://totp/Google%3Aicebox4all%40gmail.com?

secret=lsnheffbfk7p5f6a3rnh6p3bjxyum7lz

&issuer=Google

2 – the app stores secrets in a sqlite file

/data/data/com.google.android.apps.authenticator2/databases

AUTH YOU!

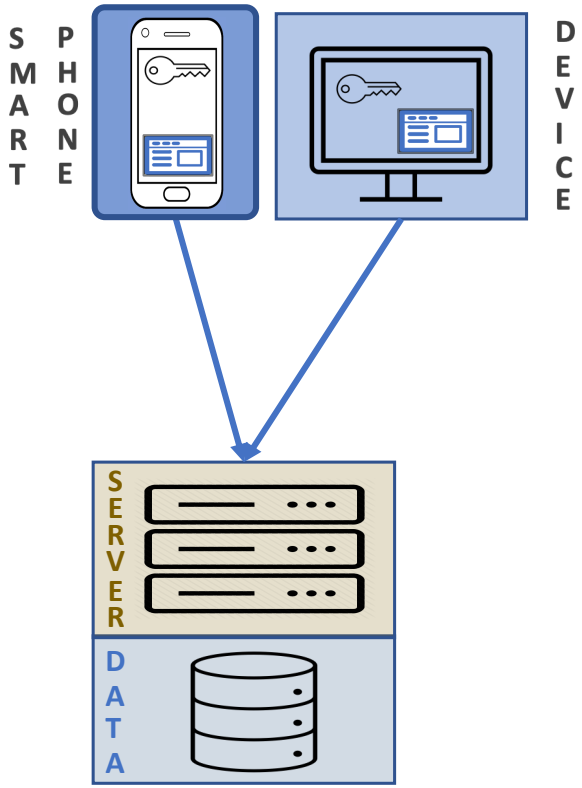
For each account, secrets are stored on server, not on smartphone.

6-digits TOTP are generated server-side, and returned as a result of a service request; this service is available only to authenticated users.

So, the added security of AuthYou! transforms an easy clonable secret in a robust service, whose access is limited with an OTP access.

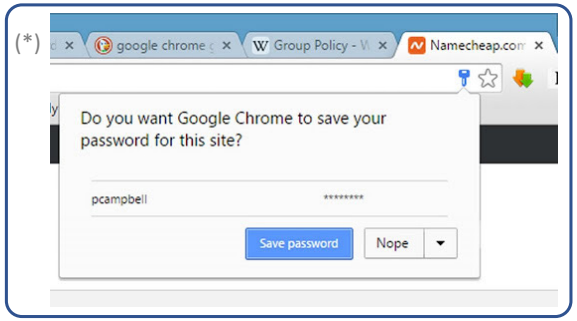
Remediated!

Common authentication risks & 2nd factor



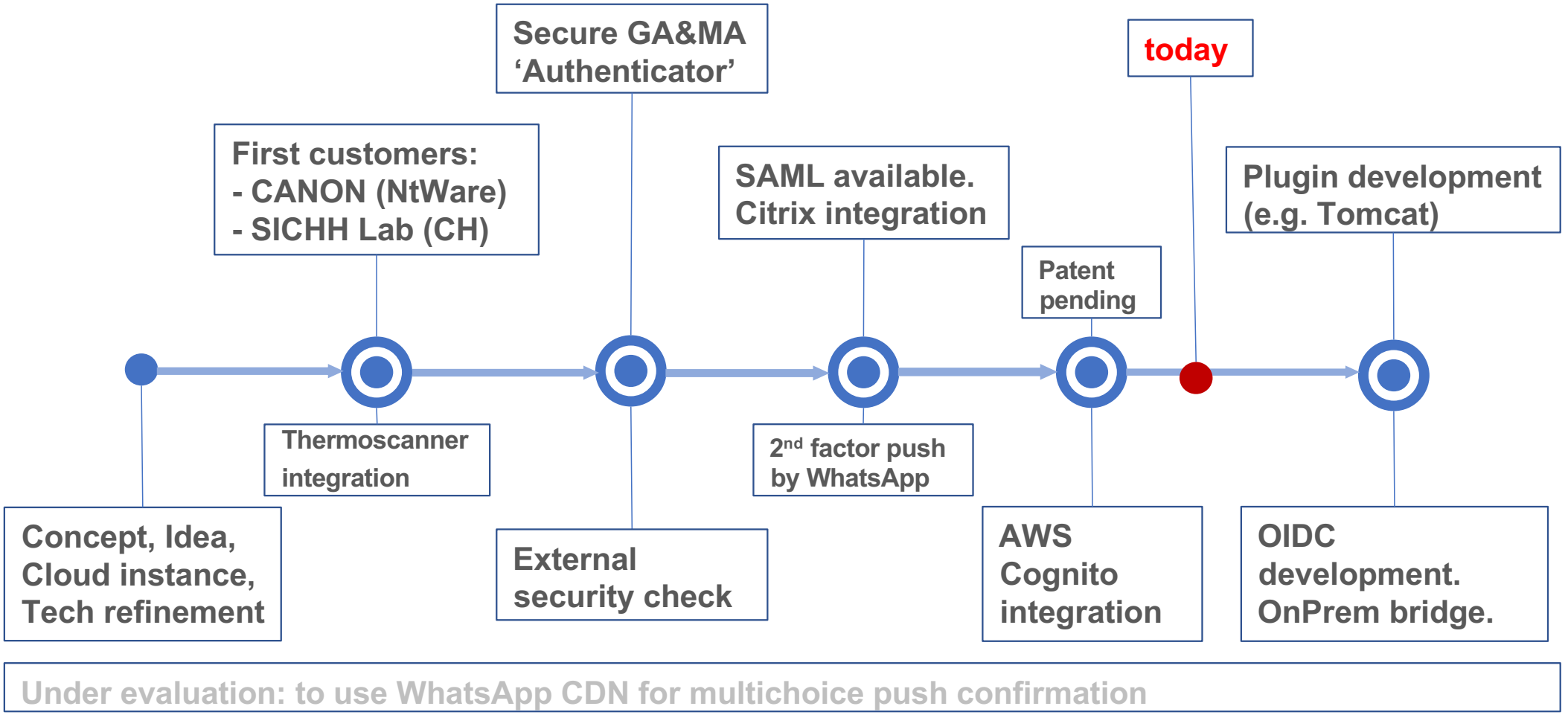
Weaknesses of commonly used auth methods

Weaknesses	Risks
Credentials to be inserted every time	Forgotten/stolen password
Cookies as identity proxy, browser storing password(*)	ID theft, permanent access
2nd factor secrets stored on phone	Lost device, migration



AuthYou!

the roadmap



Under evaluation: to use WhatsApp CDN for multichoice push confirmation

Auth made easy

Thank you