Smals
vzw-asbl

www.smals.be

Secured and integrated mobile App for government communications

1. Abstract

A system for communication between government and citizens has been conceived based on a mobile app, using a high quality identification system, strong authentication, encryption, advanced pseudonymization, and integration with government applications and services such as secured mail box or digital wallets.

2. Introduction, Goals, Context

During the Covid19 pandemic, Belgian government IT services responded quickly with solutions to administrate tracking, tracing, and eventually vaccination of citizens. An important pillar of these projects was, and remains to this day, the option to send someone a short message with an instruction or other important info, such as a PCR code. The obvious answer to implement this capability, was the use of the cell phone network's Short Message Service (SMS).

Using SMS, we were able to reach millions of people expediently. The expense, however, was proportionate. At some point during the crisis costs rose to a very high level, and they are expected to remain high for some time. This problem was seen as one of several linked to the chosen approach. SMS, all things considered, is a technology over 30 years in age, and has other disadvantages. For example, the texts are sent in clear text, readable by intermediaries, such as the carrier. Also, in and of themselves, they only allow for purely textual content, not multimedia. Guarantees with regard to the identity of the person receiving the messages could be enhanced. The use of the mobile phone number had a good fit with the tracking and tracing use case, but did not enable a more general adoption for government communications.

A solution based on mobile applications (Apps) has therefore been conceived. There are many examples of Apps being able to receive messages, containing any kind of content, over the internet, and informing the user with a timely notification. The conceived solution can reduce dependence on SMS and replace many other communication channels. In future embodiments, it will evolve towards a reusable service, operating as an App, capable of centralizing a citizen's communication with government services entirely. To expedite adoption by as many people as fast as possible, the first embodiment will leverage the existing **CovidSafeBe App**, already installed on 8.5 million smartphones, using it to encourage the public to install the new communications App.

3. Solution description

The concept includes integration of the following technologies in order to provide an integrated and secure communications system:

- Fully service oriented design, disclosed by APIs, where the central SMIS (see section 4) governs which channels are used to contact a citizen, and several other services control only a specific channel (such as the Mobile App channel, but also, non-exhaustively, SMS and e-Mail).
- Integration with secure mailbox systems such as e-Box, so messages can contain a link to a document in the e-Box that, when clicked on, can open that document in a mobile App.

- Integration in a digital wallet.
- Identification of the citizen based on a high quality identity scheme and base registry such as used for the NISS number.
- Strong authentication mechanisms such as ITSME.
- End-to-end Encryption between an eGovernment system that sends a message to a citizen, and that citizen's device, which means the SMIS will only know the sender and the channel preferences, and any service specific to a channel will only know where it is sending a message.
- A pseudonymization system, meaning that the SMIS does not know the addressee and the initial sender does not get additional information about the addressee (such as phone number when only the NISS is known, or vice versa).
- Asynchronous feedback, e.g. via an event subscription mechanism, making it possible to alert a sending application when a message delivery was attempted, when it was successful, and perhaps even when it was read.
- A broadcast mechanism, allowing messages to be sent to groups of people or even the entire country.
- Automated code of conduct imposed on applications using the messaging service, so that citizens do not feel they receive too many messages of little significance.

4. Initial embodiment

A thorough description of the solution requires us to make a distinction between a short-term strategy, a first embodiment focused on mitigating the SMS expenses currently involved in dealing with the pandemic, and a longer-term strategy, with further embodiments focused on streamlining the eGovernment's communication with its citizens.

For the short-term strategy, the high-level architecture for the entire implementation is depicted in Figure 1. Key to our approach is the development of a number of centralized, reusable services, and the development of a mobile Application to receive messages for a citizen. For the first embodiment, an initial version of the "Short Messaging Integration Service" (SMIS) meant to unify the use of all communication channels towards the end user, will be built. Furthermore this first embodiment includes the mobile Application itself, plus a second service, specifically meant to drive the transmission of messages, coming from SMIS, towards this App.

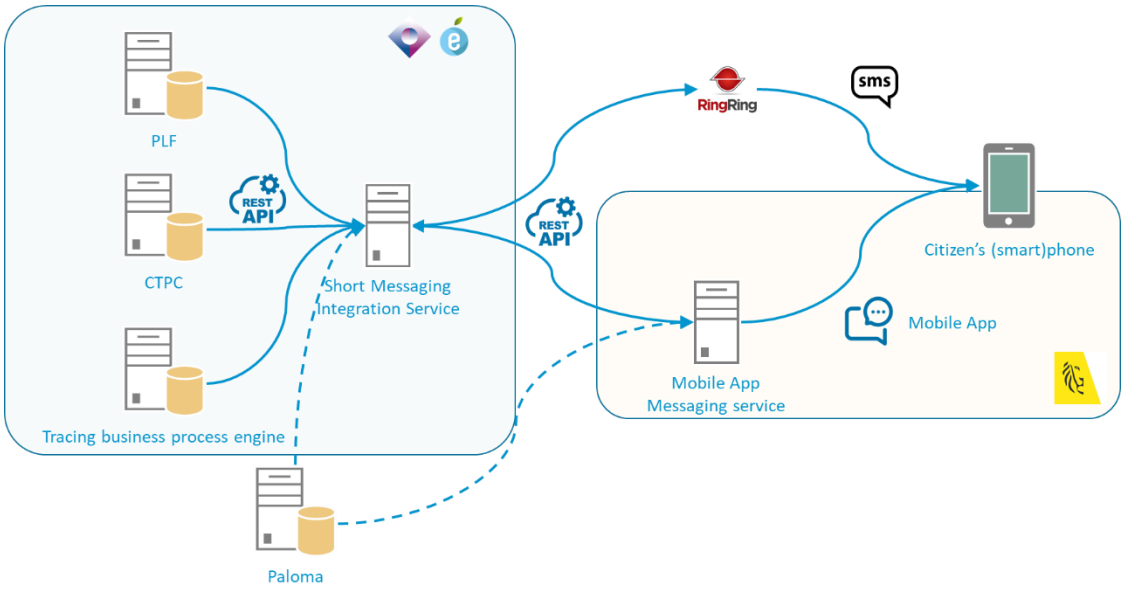

Figure 1 High-Level Architecture

4.1. Short Messaging Integration Service

The Short Messaging Integration Service (SMIS), one of the central components in this solution, will receive messaging requests, via a REST API, from three already existing services (PLF, CTPC and the Tracing BP engine).

The SMIS will be able to use the Mobile App Messaging service or the existing service by RingRing, to send its messages. The primary scheme will be to first try to send a message via the App, and to fall back to SMS, should the former fail for some reason.

On the picture, you can also see the Paloma service. It is yet to be decided whether that service will use the SMIS in the first embodiment or in (one of the) later embodiments.

4.2. Mobile App Messaging Service + App

The basic functionality of the App in the first embodiment is relatively simple: it will serve to receive and display short messages coming from a government institution, containing text and certain media, such as two-dimensional images, allowing, for example, the depiction of QR codes. It will also employ the smartphone's functionality called "notifications", giving the end user an immediate audiovisual queue when new messages are received.

To steer the transmission of messages, a central component is required: the Mobile App Messaging service. This will be a reusable service, offering the capability to other services to transmit a message to an individual citizen. The first implementation of this service should also provide the following immediate feedback to the calling service: whether the App is installed for this citizen, and whether they have the notifications turned on or off at that moment.

4.3. Authentication and Security

To be able to receive a personal message, a citizen will need to provide some form of identification. There are two possibilities here: phone number, or NISS.

Since for the initial embodiment, SMS is used, the short term strategy will focus on the former, using a simple mechanism often used to confirm an end user's phone number. The user will register their phone number in the App. A confirmation SMS will then be sent with a unique code. The user then has to fill in this code in the App to prove they are the owner of the phone number.

5. Expected benefits of the complete solution

- Cost benefits due to reduced number of SMS messages.
- High quality identity based on government base registries.
- Strong authentication based upon high quality identification.
- Privacy protection with encryption and pseudonymization.
- Integration with multiple business systems and multiple administrations.
- Integration with multiple services, e.g. eBox or digital wallet.
- Communication from multiple administrations to mobile systems form multiple recipients without knowledge of the phone number of the device.