FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA

Software Systems Architecture

Submission deadline: 27 April 2020 • Estimated lenght: 4-8 pages • Estimated duration: 180-240min

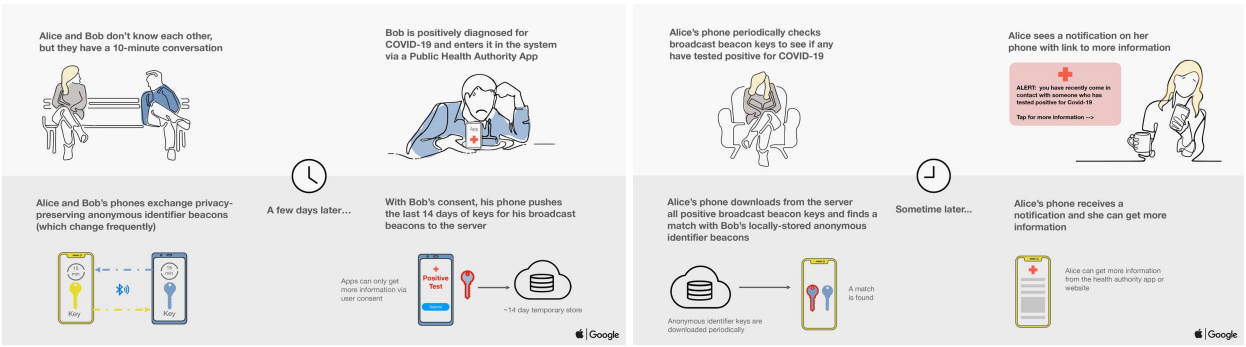
Before starting your individual assignment, please carefully read the description of the software system below and answer the questions **always justifying them succinctly and clearly**, eventually mentioning the bibliography or references that support them. In many cases, there are several ways of addressing an issue, but often there is only one unquestionably way considered the best, and therefore it is key to provide a perfect justification. When useful, you may explicit all the assumptions you made to answer the questions.

Yet Another Privacy Preserving Contact Tracing System (shortly yaPPCT) is a system being designed at FEUP that aims to help citizens and governments fight the spread of Covid-19 by preventing people from being exposed to SARS-CoV-2. It is based on tracking and reporting of known possible transmissions and uses contact tracing mobile apps, while preserving the privacy of the individuals, allegedly.

The yaPPCT system aims to provide different kinds of services for citizens and public health organizations through web and mobile apps, and also strongly encrypted backend services using APIs.

The yaPPCT system can be seen as logically structured in the following kinds of subsystems: contact tracing services at operating system level, end-user apps, information repositories, and data analysis services.

It must support the notion of citizens, devices, signals between devices and environment (e.g. beacons), citizens' events (e.g. cross-pathing, movement), risky proximity interactions between citizens in different situations (seating, walking, running, cycling, etc.) using different contact tracing technologies (Bluetooth, GPS, ultrasonic), locations, suspect and confirmed cases of infection, social circles (family, work, leisure, etc.).



It is easy to perceive the enormous privacy risks of such a system, being preservation of privacy a huge non-functional requirement for the design of the whole system. Due to the "surveillance smell" of yaPPCT, another possible name for it was coined a long time ago by a George Orwell's dystopian novel, in 1949.

Resources:

- https://www.apple.com/pt/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
- https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/
- https://www.novid.org/

Ademar Aguiar, Tiago Boldt Sousa

Architectural Styles [20%]

1. Consider the perspective of the global yaPPCT system and especially the very critical requirement privacy preservation and surveillance risks. Envision an architecture for the whole yaPPCT system. **In that architecture, which key architectural styles (2-3) do you see as helpful to design the overall system, and why? For the explanation please draw a UML physical architectural diagram of yaPPTC highlighting the components and connectors that you suggest should exist, implement and instantiate the styles mentioned.**

Architectural and Design Patterns [4 x 20%]

Considering the design patterns you studied (mainly POSA and GoF), suggest patterns for each one of the design issues below and justify their usefulness (pros and cons) to solve each issue.
For each issue, you should document:

a. candidate patterns: which and why;
b. selected patterns: why the choice for them;
c. issue resolved: a partial UML class diagram, a sequence diagram, when applicable, briefly describing the envisioned solution, both textually and diagrammatically, and how the pattern's roles, operations and associations were mapped in the concrete solution;
d. consequences: explain the benefits and liabilities of the resulting solution, eventually comparing with other possible alternatives, and pointing other well-known cases doing the same; which forces were balanced and how; which eventual new issues were created.

2. yaPPCT must support the notion of interactions between citizens, which may take place in different situations (seating in an infected area, breathing for some time in an infected room, etc.) and may require different technologies (Bluetooth, GPS, ultrasonic, etc.). The level of risk of each kind of interaction depends a lot on the perspective of the public health experts analyzing the data, requiring fine-tuning, to adjust distances, times and other factors to each situation.
How to cope with such diversity of types of interactions to end up with a design that is easy to extend and maintain with new situations and respective risk assessments?

3. Much of the data collection of yaPPTC is performed by citizens' mobile devices, which may go offline due to lack of Wi-Fi or mobile data connection. This situation must be handled anyway by the app and the system, to continue sending and receiving signals to and from other devices and the rest of the system, and then later synchronized when online again.
Which design patterns do you suggest implementing to add the online/offline capabilities so that the apps and system are fully functional in both modes?

4. When a citizen is confirmed as Covid-19 positive by the public health authority, the citizen is asked to share the recently registered interactions with the public health authorities and through them to other citizens as well, so that each can identify themselves and be immediately notified as suspects in order to become more alert in case of related symptoms. From the confirmation moment to notifications, there are processes that may vary considerably, depending on the authorities involved.
How do you suggest coping with the diversity of such confirmation and notification processes and hide them from the backend services and mobile apps?

5. The larger the user base, the larger amount of data and processing capacity needs to be available for the yaPPTC system, requiring a well-defined strategy for scalability.
Identify in your system architecture the likely bottlenecks and suggest strategies to mitigate them. Identify and elaborate on the practices or patterns adopted, describing how they can be instantiated with technology.

The End.