ECOLE DES MINES DE SAINT-E´ TIENNE

**Covid-19 pandemic and** **proximitytracing**

*Submitted by:* Aninda MAULIK, CPS2

*Supervisor:*

Prof. P. JAILLON

January 13, 2021



**Contents**

1. [**Synthesize and draw all exchanges describe in protocol specification for the**](#_bookmark0) [**two proposal**](#_bookmark0) **2**
   1. [proximity contact recording](#_bookmark1) 2
   2. [exposure verification](#_bookmark2) 2
   3. [infection declaration](#_bookmark3) 2
2. [**Explain why people say DP-3T is decentralised protocol and not Robert:**](#_bookmark6) **2**

[**3 3**](#_bookmark7) **4**

* 1. [What are main privacy goals expressed for each protocol?](#_bookmark8) 4
  2. [How these two protocols fulfills these goals?](#_bookmark13) 4
  3. [Point out the pros and the cons for each protocol?](#_bookmark4) 6

1. [**Imagine you have to implement a contract tracing system using one of the**](#_bookmark12) [**two protocol**](#_bookmark12) **6**
   1. [Describe the global infrastructure (with required equipment placed) of your solution (take into account all different users populations: general](#_bookmark11)

[population, administration, medical teams)](#_bookmark11) 7

* 1. [What are the main security points you should take into account in your solution and explain how you solve it.](#_bookmark9) 9

1. [**In the two protocols, a server is required at exposure verification and infec- tion declaration. Imagine you are the owner (administrator) of the server and be able to observe all communications with your server at any time. Imagine you are a telecom operator and be able to to observe all communications, you**](#_bookmark10)

[**are also able to localize cell phone**](#_bookmark10) **10**

* 1. [in these two situations, explain how the flows could be exploited, what](#_bookmark5)

[the attacker could learn and what protocols’ properties cannot be respected](#_bookmark5) 10

[**References**](#_bookmark5) **10**

Thank you for using [www.freepdfconvert.com](http://www.freepdfconvert.com/) service!

Only two pages are converted. Please Sign Up to convert all pages. <https://www.freepdfconvert.com/membership>