dSik Group Assignment 5 - DA1 - Group 01

Alex Kire Hansen[1], Christian Zhuang-Qing Nielsen[2], og Johan Lomborg Knudsen[3]

[1]201505082, 201505082@post.au.dk
[2]201504624, christian@czn.dk
[3]201508691, 201508691@post.au.dk

16. maj 2017

Exercise 6

Rewrite the text so that it can be called a security policy

- First we authenticate different people and institutions by requiring their digital signature, which is also to identify them. This way, we can limit people top only vote *once* per vote as well as only being able to vote in the ones they are allowed. The digital signature works like an authenticated key exchange in this case.

- When a vote is registered on the server, there will be a counter there which increments after each registered vote. This counter will be properly synchronised on every machine. This way, when people have voted, they can receive the current value of the counter which functions as a way to see the number of people who have voted so far. The counter uses a primitive value-type, so it will not contain any information beyond the number of voters.

- To ensure that no adversary can collect information about what people voted, we use a confidentially secure method to encrypt all the received information. Furthermore, when one votes we can look up in the central person register (CPR) to collect information about gender, age and postal number. Only a reference to this information is saved on the server, and this is not pulled until the voting has completed. It should also be mentioned that everything we store in our servers are securely encrypted using AES-256, so only our organisation can decrypt the private information.

- Finally, before the information is published, we make a check to see if each demographic group of people contains at least 25 people. If not, the demographic information (age, gender, postal address) is exempt from the

statistics and never pulled from CPR. Their vote, however, still counts in the final settlement.