DIMA PROJECT OFFICIAL DOCUMENTATION

“Watchdog”

Claudio Rizzo
800471

Emanuele Uliana
799256

4/7/2014

Teacher: Prof. Luciano Baresi

Version 1.0

Indice

Chapter A: Project context and purpose

1 Context

2 Purpose

Chapter B: Project planning

3 Time schedule

Chapter C: Requirements analysis

4 Actors

5 Functional requirements

5.1 Mobile phones association

5.2 Mobile phone remote localization

5.3 Mobile phone remote mark

5.4 Mobile phone remote alarm triggering

6 Non-functional requirements

6.1 Privacy and security: problems and solutions

6.1.1 Sender authentication

6.1.2 Message integrity/authentication/non forgeability

6.1.3 Message confidentiality

6.1.4 Asymmetric keys management

6.1.5 Symmetric key management

6.1.6 Public keys mutual authentication

6.1.7 Final recap

6.2 Human friendly interface and transparency

6.3 Performance

7 Use cases

7.1 Initialization wizard

7.2 Mobile phones association

7.3 Remote control: localization

7.4 Remote control: mark stolen/lost/both/found

7.5 Remote control: alarm triggering/untriggering

Chapter D: Design

8 Application Architecture

9 Design Patterns

10 Crypto protocols and alogrithms

10.1 Elliptic Curves key pair generation

10.2 Socialist Millionaire Protocol

10.2.1 Public key request

10.2.2 Public key sending

10.2.3 Question sending

10.2.4 Hash sending

10.2.5 Ack and password salt sending

10.2.6 Second half

10.2.7 Error management

10.3 Elliptic Curves Diffie Hellman key exchange

10.4 Command Protocol

10.4.1 First message

10.4.2 Second message

10.4.3 Third message

10.4.4 Fourth message

10.4.5 Error management

10.4.6 Timeout management

10.5 Elliptic Curves Digital Signature Algorithm

10.6 AES256GCM

Chapter E: Testing

11 Crypto testing

12 Protocol testing

Chapter F: Installation and usage manual

13 Installation

14 Usage

14.1 Initialization wizard

14.2 Change application settings

14.3 Send a command message