Table of Contents

Chapter 1

Chapter Heading

1.1 Section Heading

1.1.1 SubSection Heading

SubSubSection Heading

Paragraph Heading   with some text after

- Itemize

- One

- Two

1. Enumerate

2. One

3. Two

Description Description

One First

Two Second

Table	Headers	here
Lots of	rows	go here
Right Aligned	Left aligned	Centered

Table	Paragraph
Small header	lots of writing that can turn into a paragraph and will take up all of the remaining space in the page.
This	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

[?]
[?]
[?]
[?]
[?]

This is a sentence in green
This is in red
This should be blue.

'\\' above means `newline`. Repeated white space is always treated as a single whitespace—space, tab, newline.

Paragraphs are separated by a blank line.

- `Typewritter font`

- *Emphasised is better than bold/italics with* emph *inside*

- **Bold font with *emph inside***

```
public void javaMethod() {
   doSomething();
   if (happy) {
      clap(hands);
   }
   return new String("Really want to show it.");
}
```

Listing 1.1: This is the caption

Chapter 2

Introduction

2.1 Motivation

As the popularity of mobile communications devices increases, there is a growing tendency to use these as a convenient means of reviewing and revising documents on-the-move. Where these documents are of a confidential nature, particular attention must be paid to the fact that mobile devices are more vulnerable to compromise that traditional desktops, which are usually more extensively protected by the security measures implemented as part of an organization's internal network.

There are multiple mechanisms for keeping files secure on company servers whilst allowing employees the necessary permissions to work collaboratively with sensitive data as required. As the mobile device culture becomes more prevalent in the workplace, the addition of Mobile Device Management (MDM) applications empowers users to also access corporate data via their mobile devices whilst still allowing IT departments to retain a degree of control over data security.

Thus, it is acknowledged that maintaining the security of confidential documents can be challenging, even with the weight of a corporate IT infrastructure behind it. In this project, we seek to address the issue of allowing groups of users from different organizations (i.e. with no shared IT infrastructure) to collaborate securely on confidential documents and furthermore, to access these documents via a smartphone or tablet computer whilst minimizing the risk of exposing sensitive information to a potential attacker.

2.2 Project Aims

The primary aim of this project was to implement a scheme for the secure sharing of confidential documents between small (typically ¡ 15) groups of collaborators, subject to the following constraints:-

- Groups are self-organizing and represent multiple organizations, hence they cannot draw on the support of any central IT services.

- The documents involved are confidential in nature and hence should be encrypted both in transit and at rest.

- Group members wish to be able to access documents on a mobile device which is running the Android operating system.

- The solution devised should use only well-tested cryptographic techniques and standard libraries and should minimize the amount of trust to be placed in a third-party.

In pursuit of these aims we developed a solution called Securely Share, consisting of a detailed design of the security components of the system and a prototype android application (SecurelyShare) to provide a platform on which to implement and evaluate the various security features. It was acknowledged that, in a live setting, documents would usually originate on a PC rather than on a tablet device and thus the system would also need to a PC-based component. However, within the time constraints of the project it was considered infeasible to develop a fully featured system; our solution is submitted rather as a 'proof of concept'.

2.3 Overview of Report

The subsequent chapters of this report will deal with the design, implementation and evaluation of the project. Chapter 2 introduces some of the background material on key technologies used and presents an overview of the android applications reviewed as part of our preliminary research. In the light of this research, Chapter 3 presents a detailed analysis of the problem and expands the aims outlined in TODO into a more complete project specification, including details of the threat model against which we are attempting to defend. Chapters 3 and 4 deal with the solution design and implementation Need detail of rest of chapters here

Chapter 3

Background

Chapter 4

Analysis and Specification

Chapter 5

Solution Design

Chapter 6

Implementation

Chapter 7

Evaluation