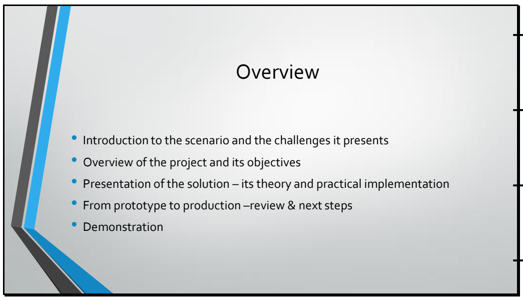
Slide 1

Securely Share

An android-based application for the secure sharing of confidential documents

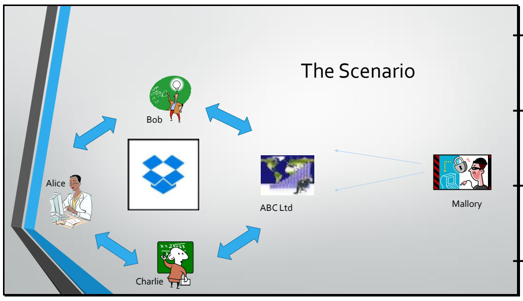
Slide 2



Overview

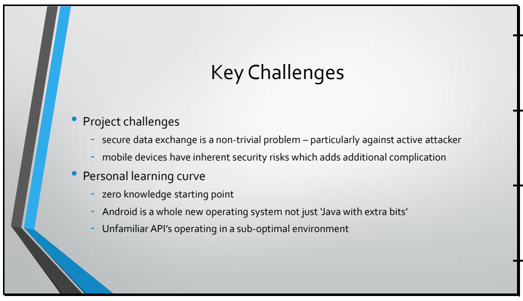
- Introduction to the scenario and the challenges it presents
- Overview of the project and its objectives
- Presentation of the solution – its theory and practical implementation
- From prototype to production –review & next steps
- Demonstration

Slide 3



The Scenario

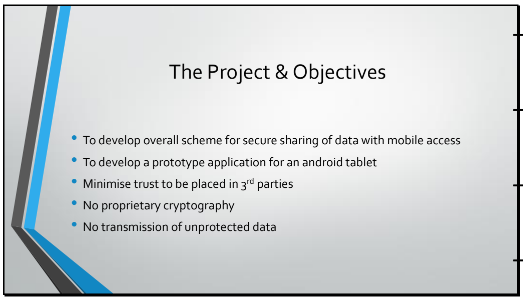
Slide 4



Key Challenges

- Project challenges
  - secure data exchange is a non-trivial problem – particularly against active attacker
  - mobile devices have inherent security risks which adds additional complication
- Personal learning curve
  - zero knowledge starting point
  - Android is a whole new operating system not just 'Java with extra bits'
  - Unfamiliar API's operating in a sub-optimal environment

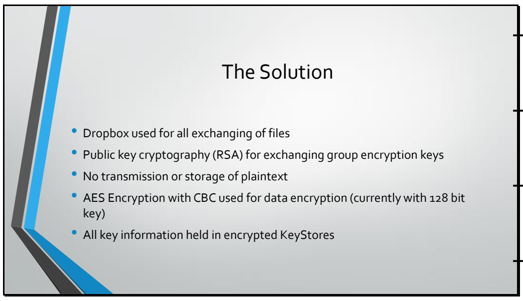
Slide 5



The Project & Objectives

- To develop overall scheme for secure sharing of data with mobile access
- To develop a prototype application for an android tablet
- Minimise trust to be placed in 3rd parties
- No proprietary cryptography
- No transmission of unprotected data

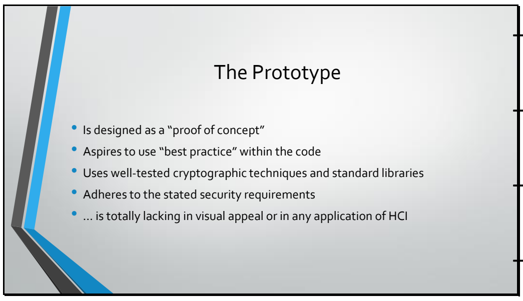
Slide 6



The Solution

- Dropbox used for all exchanging of files
- Public key cryptography (RSA) for exchanging group encryption keys
- No transmission or storage of plaintext
- AES Encryption with CBC used for data encryption (currently with 128 bit key)
- All key information held in encrypted KeyStores

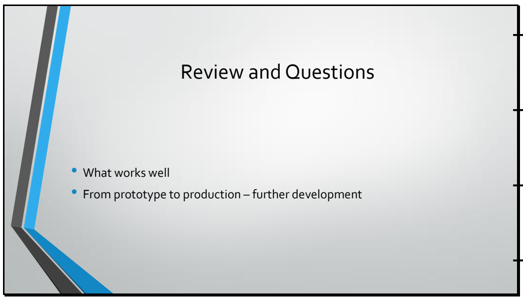
Slide 7



The Prototype

- Is designed as a "proof of concept"
- Aspires to use "best practice" within the code
- Uses well-tested cryptographic techniques and standard libraries
- Adheres to the stated security requirements
- … is totally lacking in visual appeal or in any application of HCI

Slide 8



Review and Questions

- What works well
- From prototype to production – further development