Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementatio

Implementatio Details

Encrypted

Trivia

KeyChain Extension and Integration

Kjell Braden, Marvin Dickhaus, Cassius Puodzius

Fachbereich Informatik TU Darmstadt

February 15, 2013

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementatio

Implementation

Details

Encrypted SMS

- 1 Motivation
- 2 Requirements
- 3 Implementation Issues
- 4 Implementation Details
- 5 Encrypted SMS
- 6 Trivia

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementation

Implementation

Encrypted

Trivia

1 Motivation

- 2 Requirements
 - 3 Implementation Issues
- 4 Implementation Details
- 5 Encrypted SMS
- 6 Trivia

Herp Der2

KeyChain Extension and Integration

> Braden, Dickhaus, Puodzius

Motivation

Requirements

Issues

Implementation

Encrypted

- blubb
- bla
- bluh

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementatio

Implementation

Encrypted

- 1 Motivation
- 2 Requirements
- 3 Implementation Issues
- 4 Implementation Details
- 5 Encrypted SMS
- 6 Trivia

Herp Der3

KeyChain Extension and Integration

Braden, Dickhaus, Puodzius

Motivation

Requirements

Issues

Implementation Details

Encrypted

- blubb
- bla
- bluh

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementation Issues

Implementation
Details

Encrypted

SMS

- 1 Motivation
- 2 Requirements
- 3 Implementation Issues
- 4 Implementation Details
- 5 Encrypted SMS
- 6 Trivia

Existing Android API

KeyChain Extension and Integration

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementation

Implementation

Encrypted

Trivis

Issues

Java Cryptography Architecture (JCA)

- offers interfaces for SecretKey/PublicKey/PrivateKey
- offers factories for ciphers, signature schemes etc. to work on the corresponding implementation of keys

native (C++) keystore daemon

- stores key material encrypted using phone lock passphrase, pin or pattern
- offers an OpenSSL engine for loading JCA Key objects from the store without exposing the key material itself, but...
 - there is no real access control
 - only RSA keys are supported
 - attempting to use the keys for anything causes a SIGSEGV in dalvik :-(

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementatio

Implementation Details

Encrypted SMS

Frivia

- 1 Motivation
- 2 Requirements
- 3 Implementation Issues
- 4 Implementation Details
- 5 Encrypted SMS
- 6 Trivia

Overview

KeyChain Extension and Integration

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementatio

Implementation Details

Encrypted SMS

- a system app for key management, such as
 - key generation
 - import/export/deletion of key pairs
 - granting key access
- a public API which allows
 - encryption / decryption
 - signing / verification / MAC
 - generation / import of symmetric keys
 - key agreement protocols

Key Identification

KeyChain Extension and Integration

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementation Issues

Implementation Details

Encrypted

- each key is referenced by a unique string alias
- keys can be assigned to contacts using the Key Management app
- each assignment has a *key usage type identifier*
 - arbitrary string token (application defined)
 - apps can request a key with a given type for a given contact
 - this way the user can easily choose which key to use for which app, and replace keys once they are obsoleted

API usage

KeyChain Extension and Integration

Braden, Dickhaus, Puodzius

Motivatio

Requirements

Implementatio

Implementation Details

Encrypted

- API calls are forwarded using binder IPC to the keychain system app
- system app checks if the calling app is allowed to use the key
- system app may present the user with a dialog to authorize the access
- if authorized, the system app processes the request and sends the result back to the caller

Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementati

Implementation

Encrypted SMS

- 1 Motivation
- 2 Requirements
- 3 Implementation Issues
- 4 Implementation Details
- 5 Encrypted SMS
- 6 Trivia

Herp Der5

KeyChain Extension and Integration

> Braden, Dickhaus, Puodzius

Motivation

Requirements

Implementation

Implementation

Encrypted

SMS Trivia

- blubb
- bla
- bluh

Braden, Dickhaus, Puodzius

Motivation

Requirements

Issues

Implementation Details

Encrypted

- 1 Motivation
- 2 Requirements
- 3 Implementation Issues
- 4 Implementation Details
- 5 Encrypted SMS
 - 6 Trivia

Trivia

KeyChain Extension and Integration

Braden, Dickhaus, Puodzius

Motivatio

Requirements

Implementat

Implementation

Details

Encrypted SMS

- time spent building full images: approx. 80 hours
- RSA 1024-bit key generation
 - regular MIPS emulator image: 10 minutes
 - x86 emulator image using VT-x/AMD-V: less than 5 seconds