KU LEUVEN

A keyboard that manages your passwords in Android

PRISMS 2014
Aalborg, 11-14 May 2014

Faysal Boukayoua
Vincent Naessens
Bart De Decker

KU Leuven

Overview

- Motivation
- Approach
- Implementation
- Other considerations
- Evaluation
- Conclusion

KU LEUVEN

Motivation: passwords

Poor usability

Insecure

Motivation: passwords on mobile devices

Typing inconvenience

“There’s an app for everything”

KU LEUVEN

Motivation: widely used mobile solutions

	Platform-based account mgmt	Browser pwd mgmt	Password vaults
Secure provisioning?	Yes	Yes	No
Disruptive to workflow?	No	No	Yes
Support for all passwords?	No	No	Yes
Changes to app?	Yes	No	No
Portable to other platforms?	Yes, but different APIs	Yes	Yes

Approach: key concepts

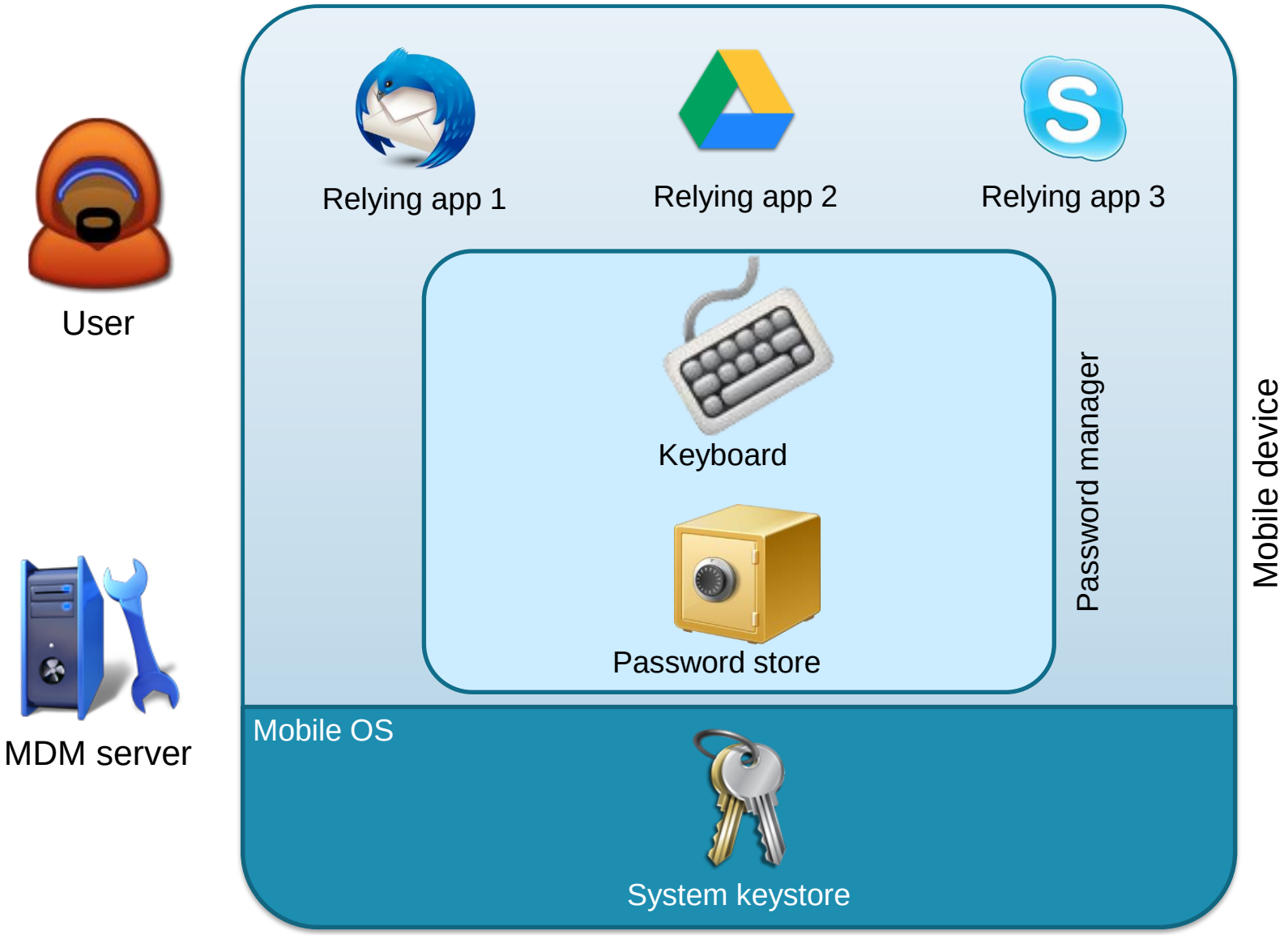
Passwords through the keyboard

Secure password storage

App authentication

User authentication

Approach: architecture



Approach: protocol




User | **Keyboard** | **Password store** | **Relying app**

1. Log in
2. Prompt for user name and password
3. Request user name and password
4. Get account(s) for relying app
5. Return account(s)

If [multiple accounts]

6. Display accounts
7. Select account

8. Get account
9. Return user name and password

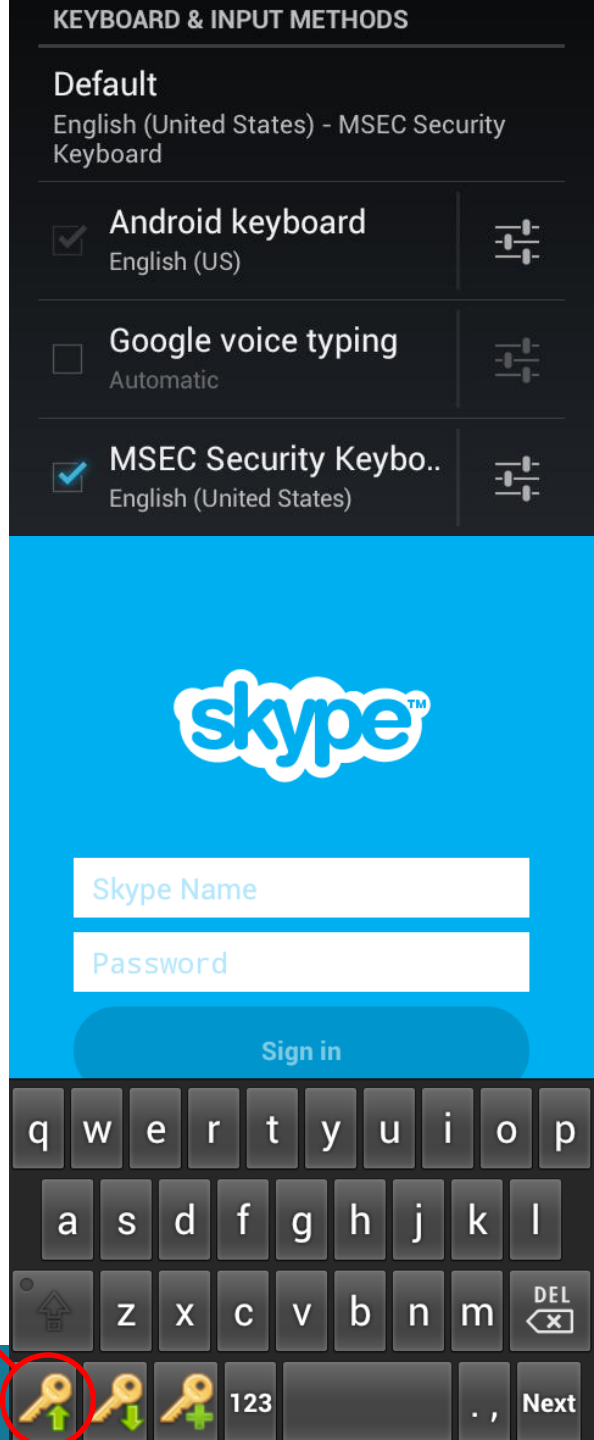
Repeat for user name, password

10. Prompt to indicate corresponding field
11. Indicate corresponding field
12. Populate field

Implementation: prototype

- Google Nexus 4
- Android 4.3
- All components in 1 app package
- Configure in *Language and Input*

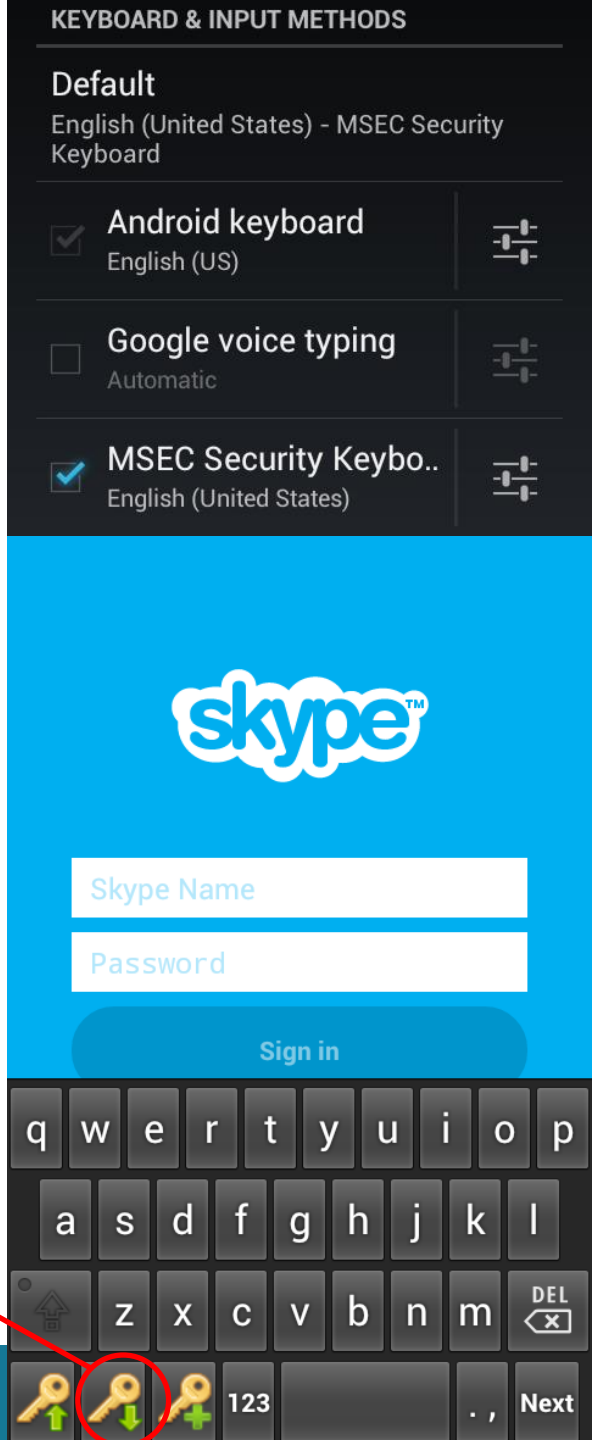
Retrieve user name and password



Implementation: prototype

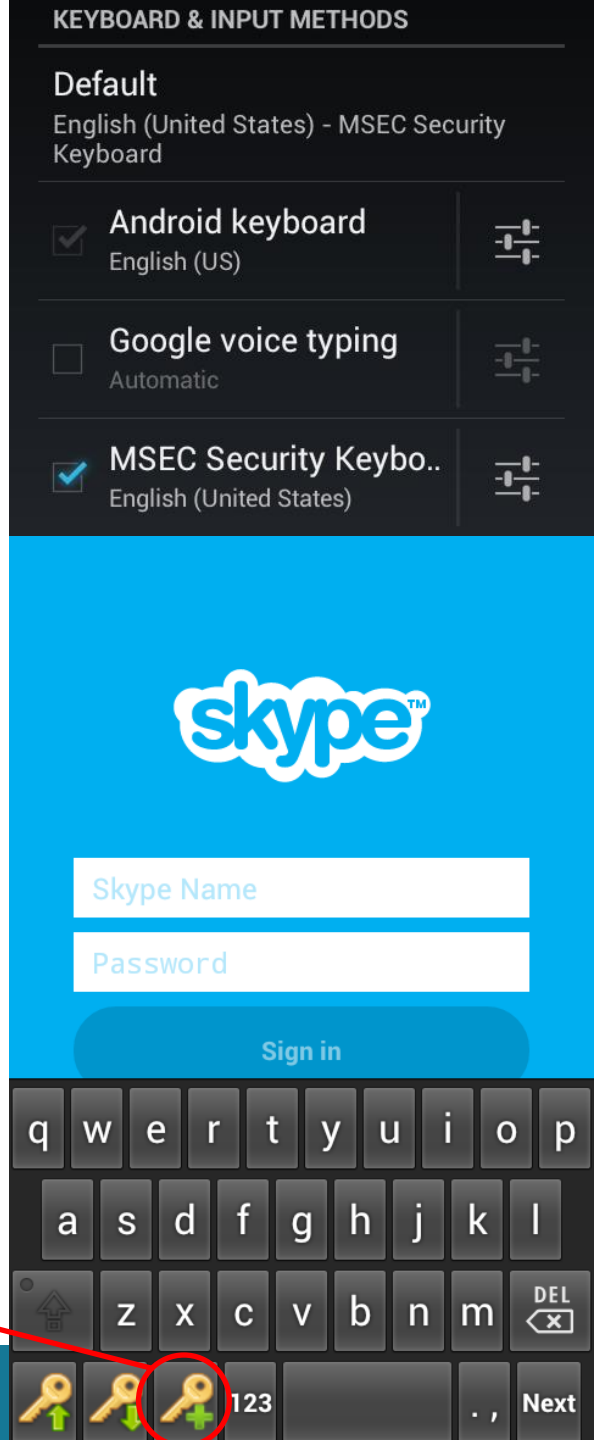
- Google Nexus 4
- Android 4.3
- All components in 1 app package
- Configure in *Language and Input*

Store user name and password



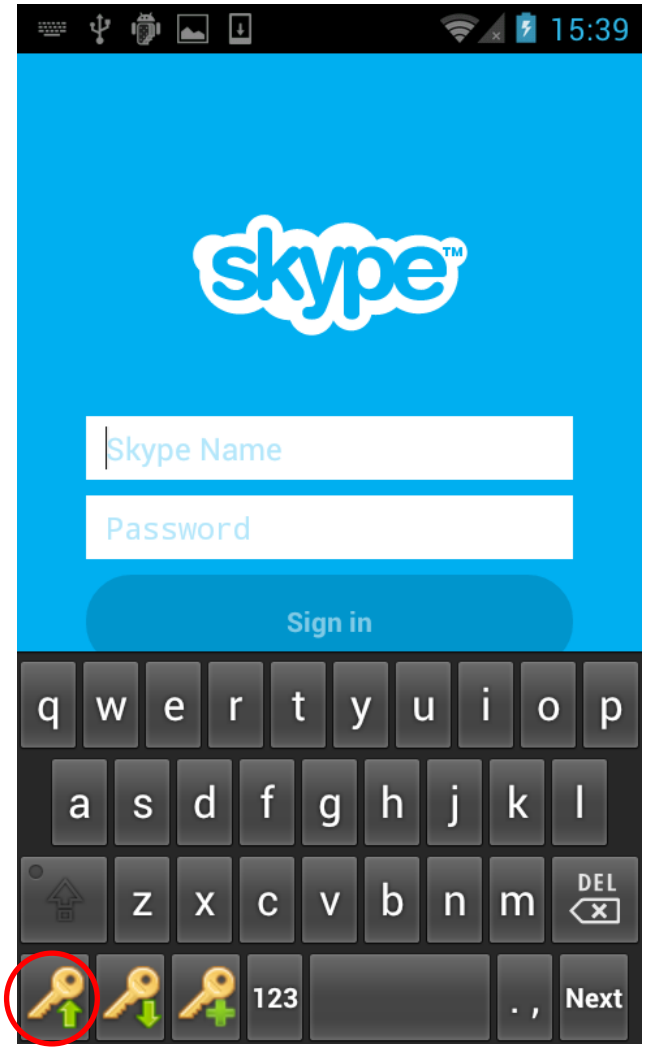
Implementation: prototype

- Google Nexus 4
- Android 4.3
- All components in 1 app package
- Configure in *Language and Input*



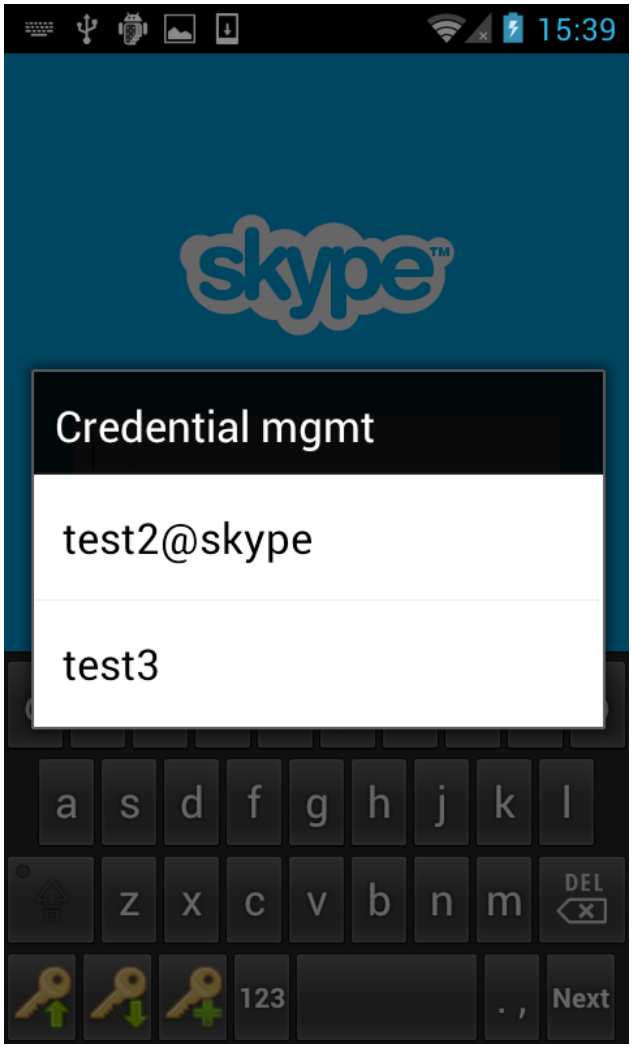
Generate strong password (auxiliary)

Implementation: retrieving an account



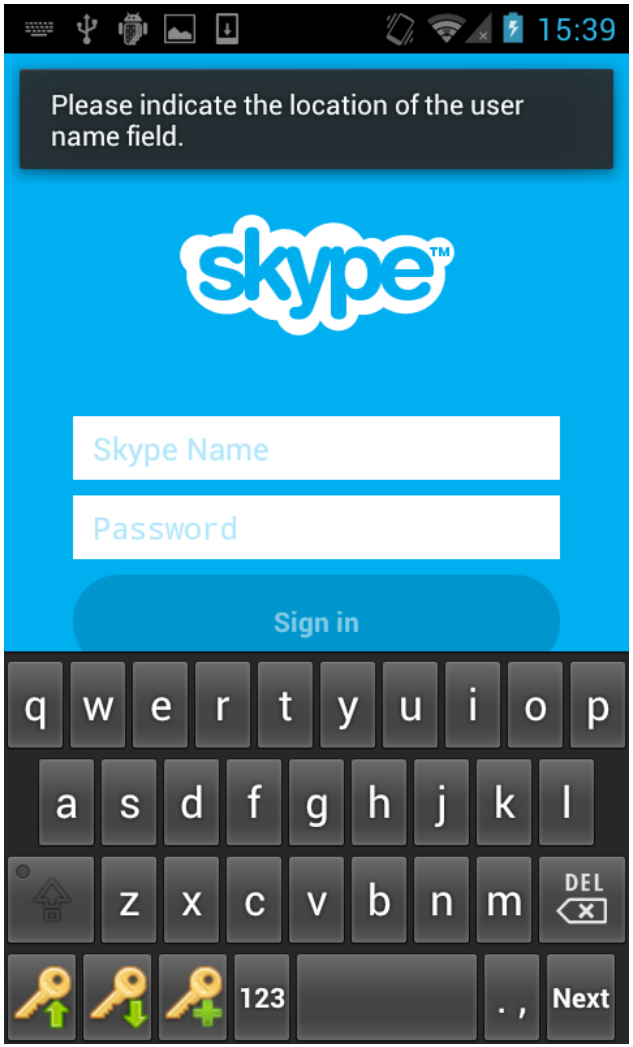
KU LEUVEN

Implementation: retrieving an account



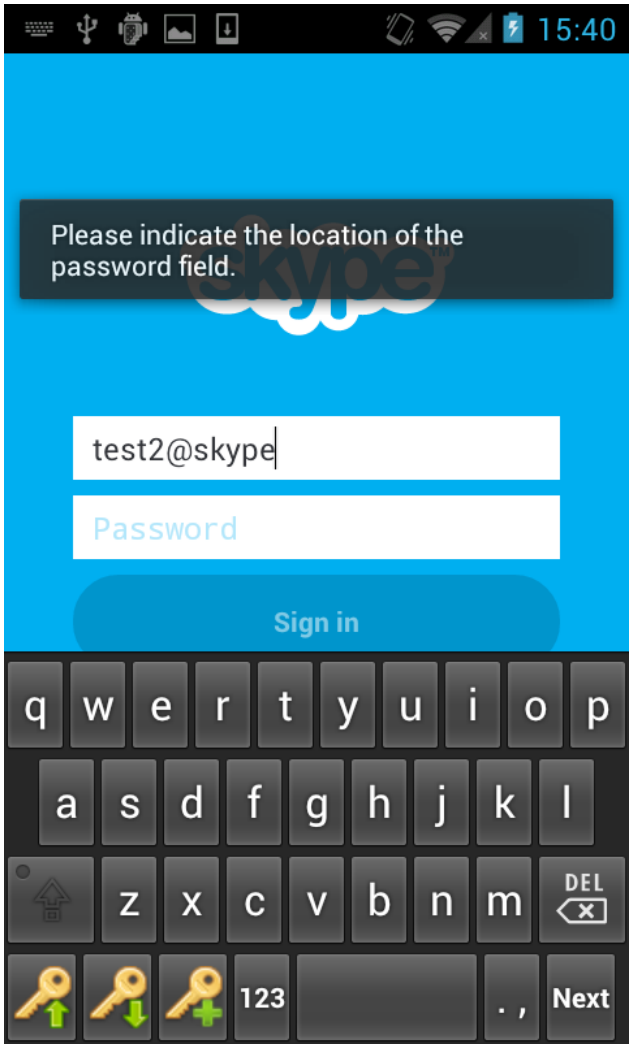
KU LEUVEN

Implementation: retrieving an account



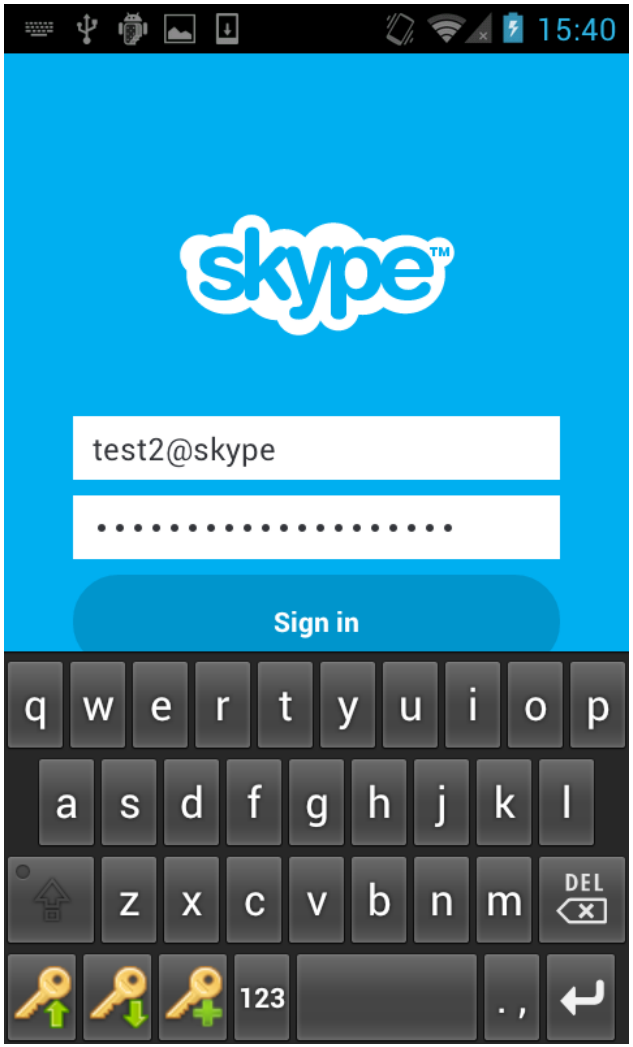
KU LEUVEN

Implementation: retrieving an account



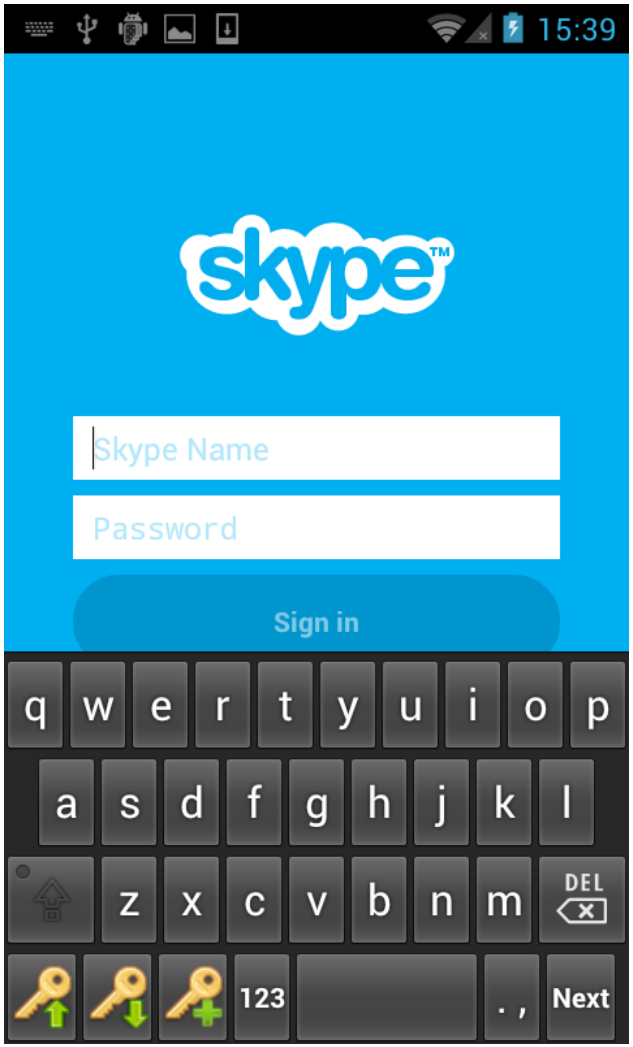
KU LEUVEN

Implementation: retrieving an account



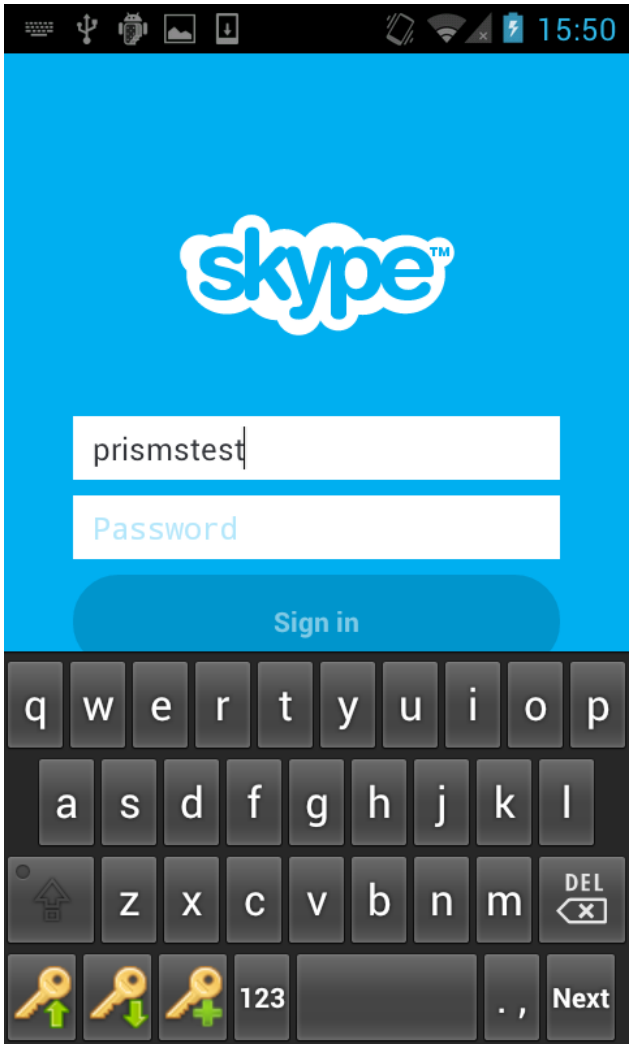
KU LEUVEN

Implementation: storing an account



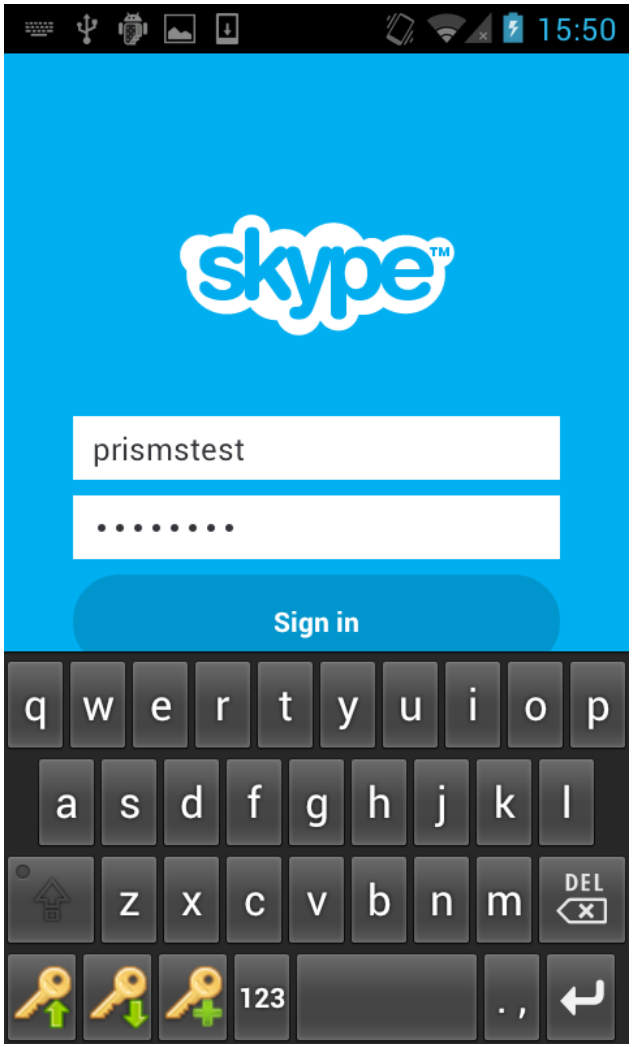
KU LEUVEN

Implementation: storing an account



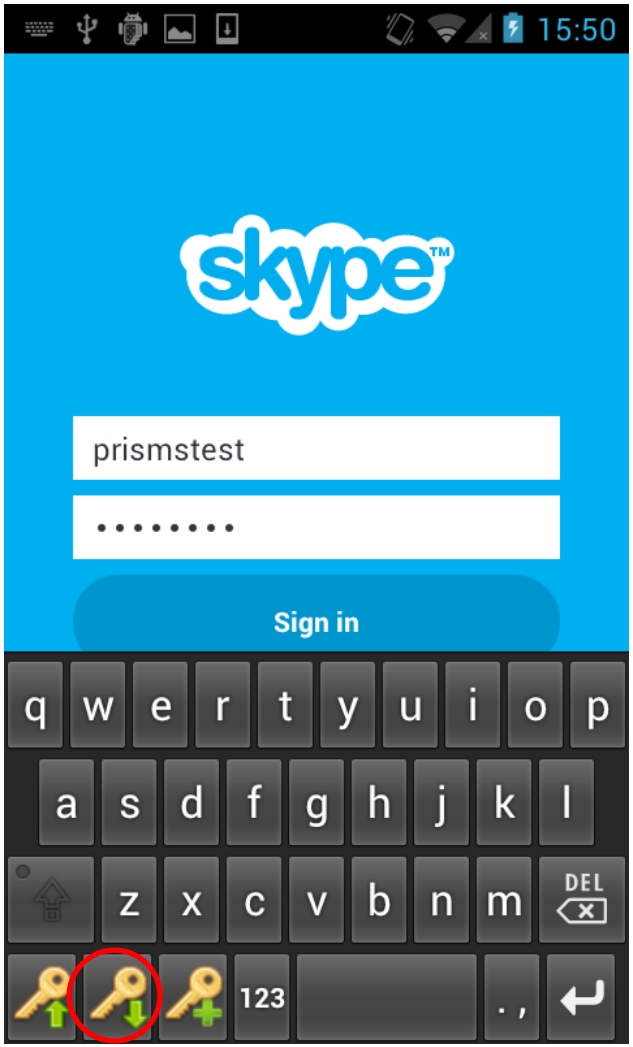
KU LEUVEN

Implementation: storing an account



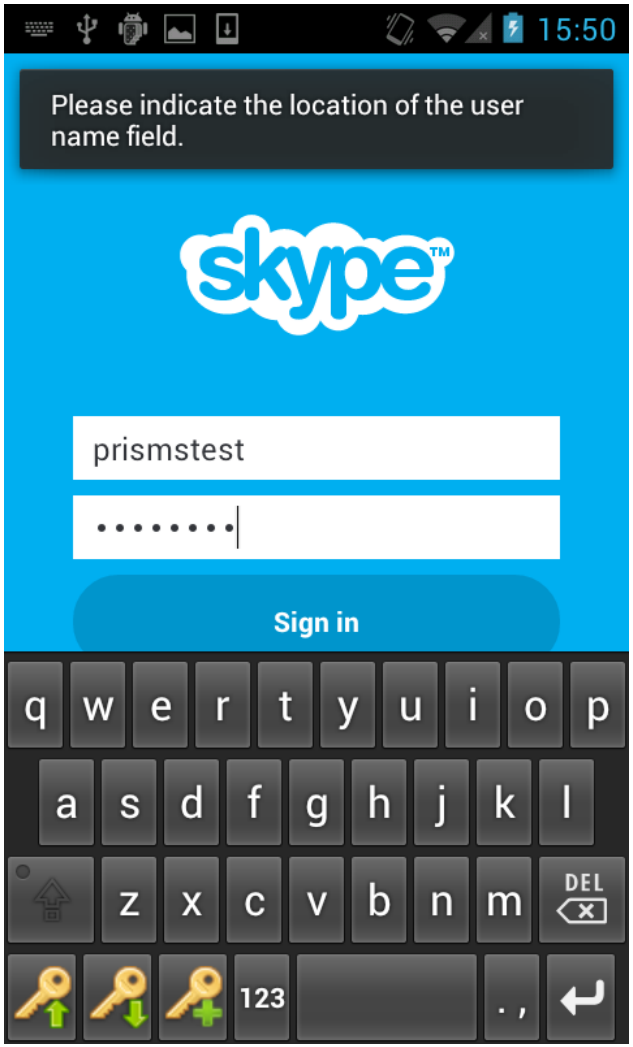
KU LEUVEN

Implementation: storing an account



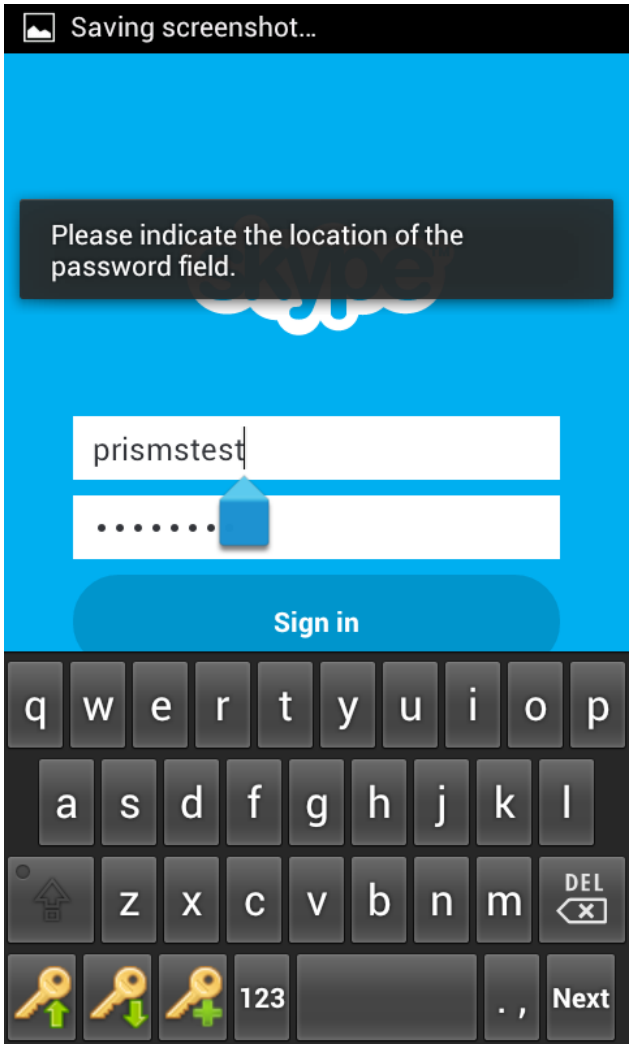
KU LEUVEN

Implementation: storing an account



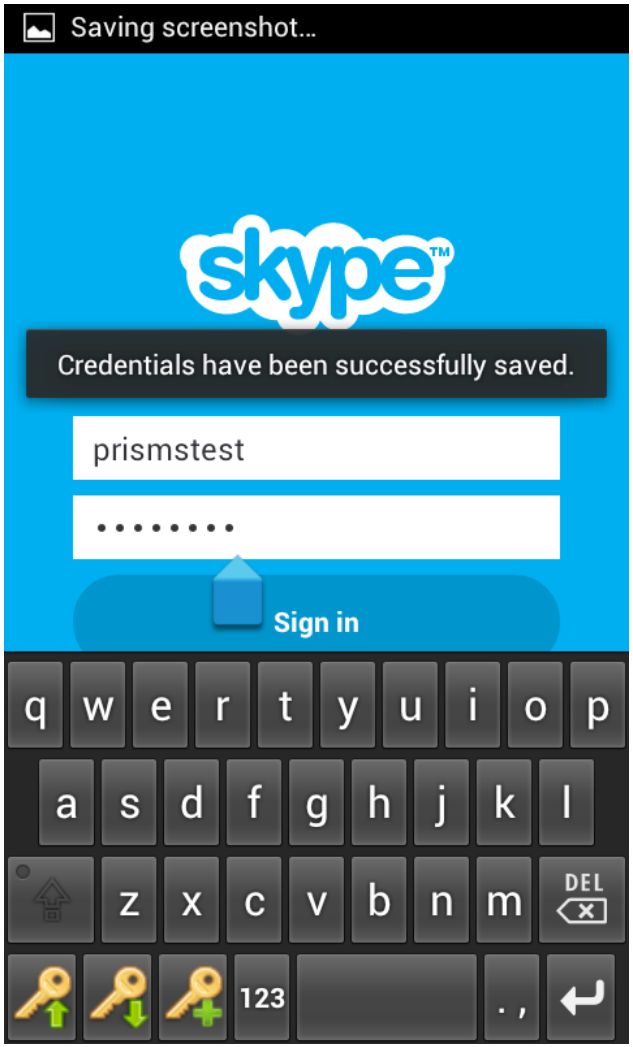
KU LEUVEN

Implementation: storing an account



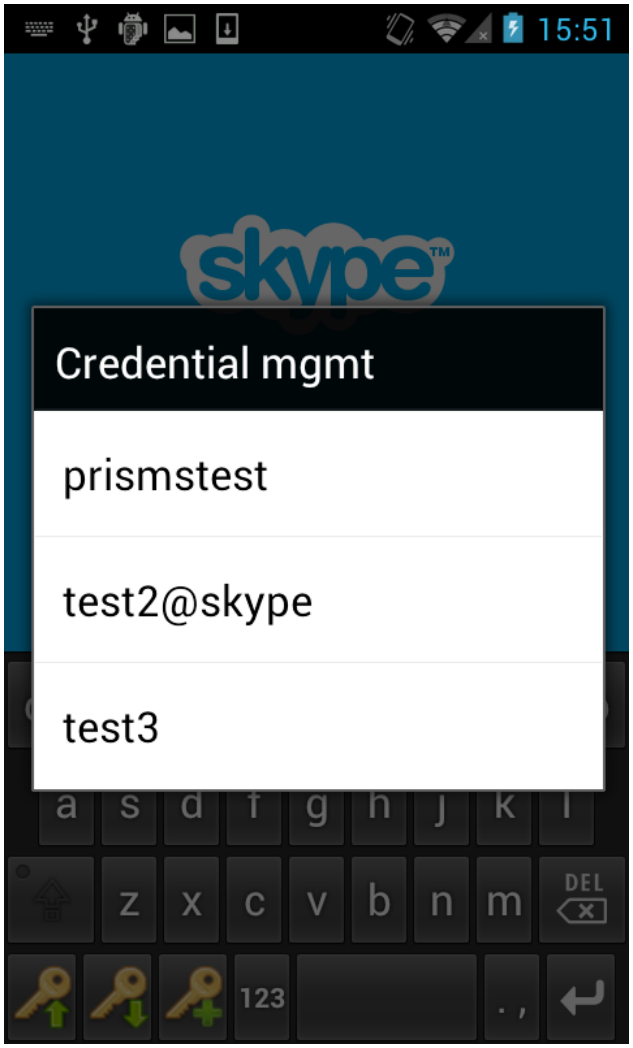
KU LEUVEN

Implementation: storing an account



KU LEUVEN

Implementation: storing an account



KU LEUVEN

Implementation: keyboard

Input Method Editor

Input Method Clients

Android Input Method Framework (IMF)

- Strict separation between
  - client apps
  - client apps and editor (IME)
- Only one client *active* at once
- IME change only by user, not app
- Not just keyboards: voice, handwriting,…

KU LEUVEN

Implementation: password store

- Symmetric encryption
- Protect crypto key using KeyChain
  - Android 4.3+: hardware-backed RSA key storage
  - App-level credential access
- Alternative: symmetric key in secure element

KU LEUVEN

Implementation: user authentication

- System passcode
- Android Device Administration API
  - Force enabled passcode
  - Strength requirements
  - Max inactivity for lock screen
  - Others:
    - Max failed attempts
    - Expiry
    - Password history restrictions
    - …

KU LEUVEN

Implementation: app authentication

- Access control to app passwords
- Compound app ID
  - Package name (e.g. *com.skype.raider*)
  - Developer signature
- Extension: password pooling
  - Why?
    - Same authentication infrastructure
    - Browsers
  - How?
    - Same signature
    - User-composed lists
    - …

KU LEUVEN

Other considerations

- Subdivision for website passwords

```
Android app
  └ Website domain
```

- Mobile Device Management
  - Password policies
  - Password pooling between apps
  - Require hardware-backed KeyChain
  - Application white- / blacklists

- Backups: recovery from loss
- Synchronisation: multi-device access

KU LEUVEN

Evaluation

	Platform-based account mgmt	Browser pwd mgmt	Password vaults	Our approach
Secure provisioning?	Yes	Yes	No	Yes
Disruptive to workflow?	No	No	Yes	No
Support for all passwords?	No	No	Yes	Yes
Changes to app?	Yes	No	No	No
Portable to other platforms?	Yes, but different APIs	Yes	Yes	Currently only Android

Conclusion

- Passwords are:
  - here to stay… for now
  - more cumbersome on mobile devices
- Contributions
  - Interoperability
    - No platform or app changes
    - Support for all passwords
  - Usability: integration in user's workflow
  - Secure provisioning and storage

KU LEUVEN

Q&A

KU LEUVEN