

Baton: Certificate Agility for Android's Decentralized Signing Infrastructure

David Barrera, Daniel McCarney, Jeremy Clark, Paul van Oorschot
Carleton University, Ottawa



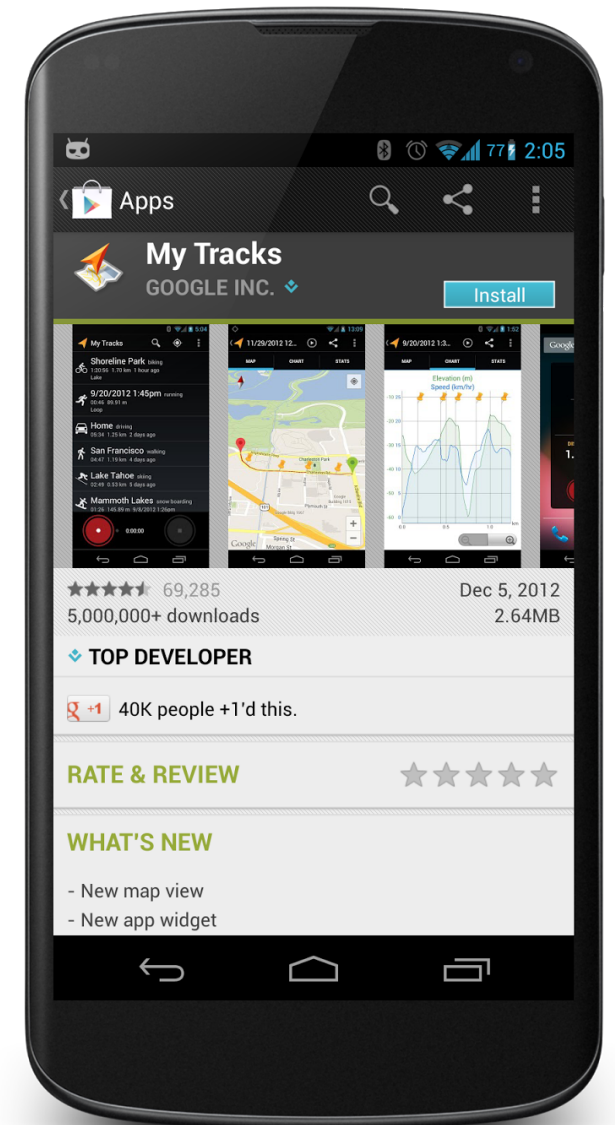
ETH*zürich*

General Problem

- Selective updates - Prevent files from being overwritten by unauthorized parties.
- Allow transparent authorized updates
- Doing this without a centrally trusted party (decentralized)

Android

- Apps must be digitally signed
- No central authorities
- Android uses a TOFU model for apps
- Application updates must be signed with the same private key as original



Limitations of Android Signing

- No method to update signing keys or certificates
- Google requires use of the same key pair for 35+ years!
 - Selling apps requires private key transfer
 - Changing key algorithm/size is not possible
 - No recovery from key compromise

Google attempts to change their signing key

Upgrading to Google Authenticator v2.15

We've released a new version of Google Authenticator which features a cleaner UI and better system integration. If you already use the app, you should be prompted to upgrade the next time you open it.



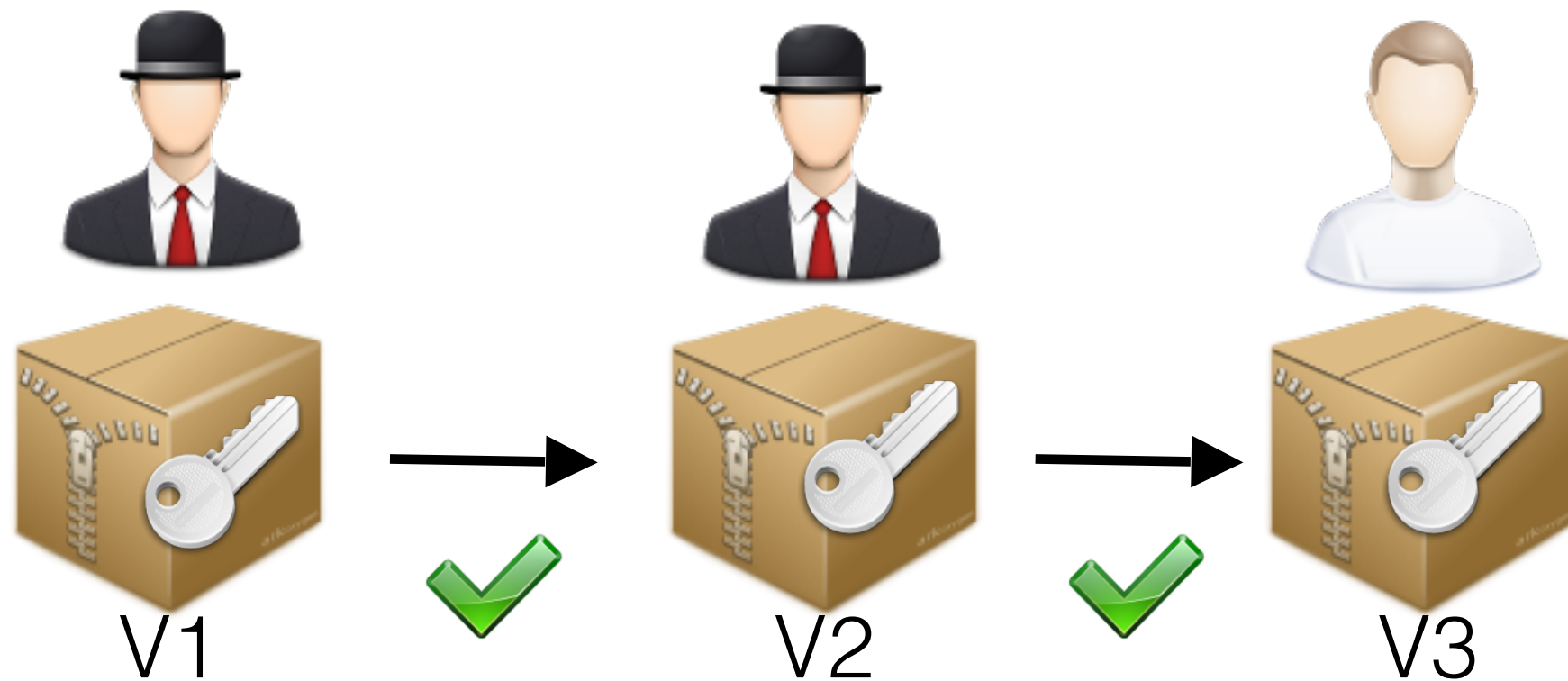
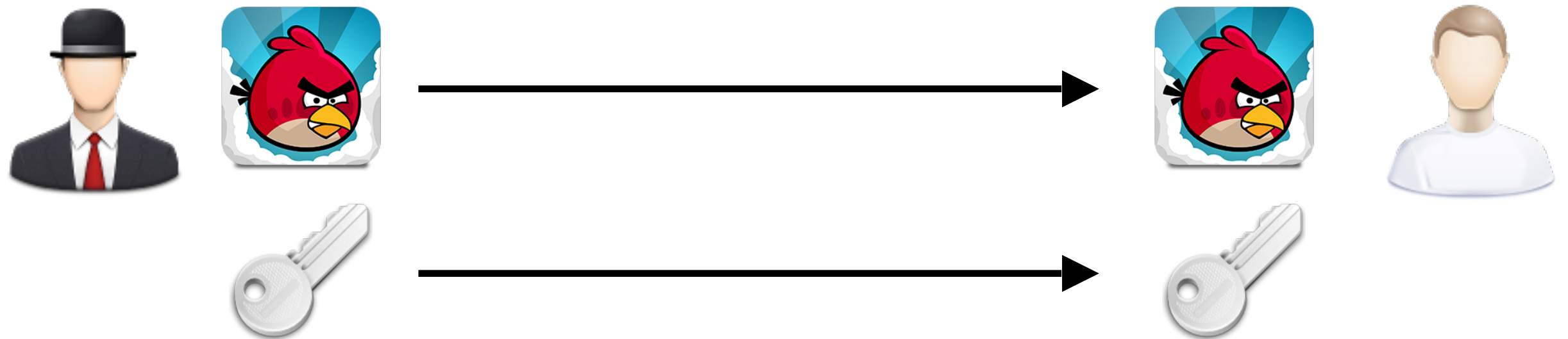
Upgrade steps for Authenticator 0.86 and earlier

Earlier versions of Authenticator are unfortunately unable to export user data, so you will need to follow these instructions to make sure you do not lose access to your Google account during the Authenticator upgrade process.

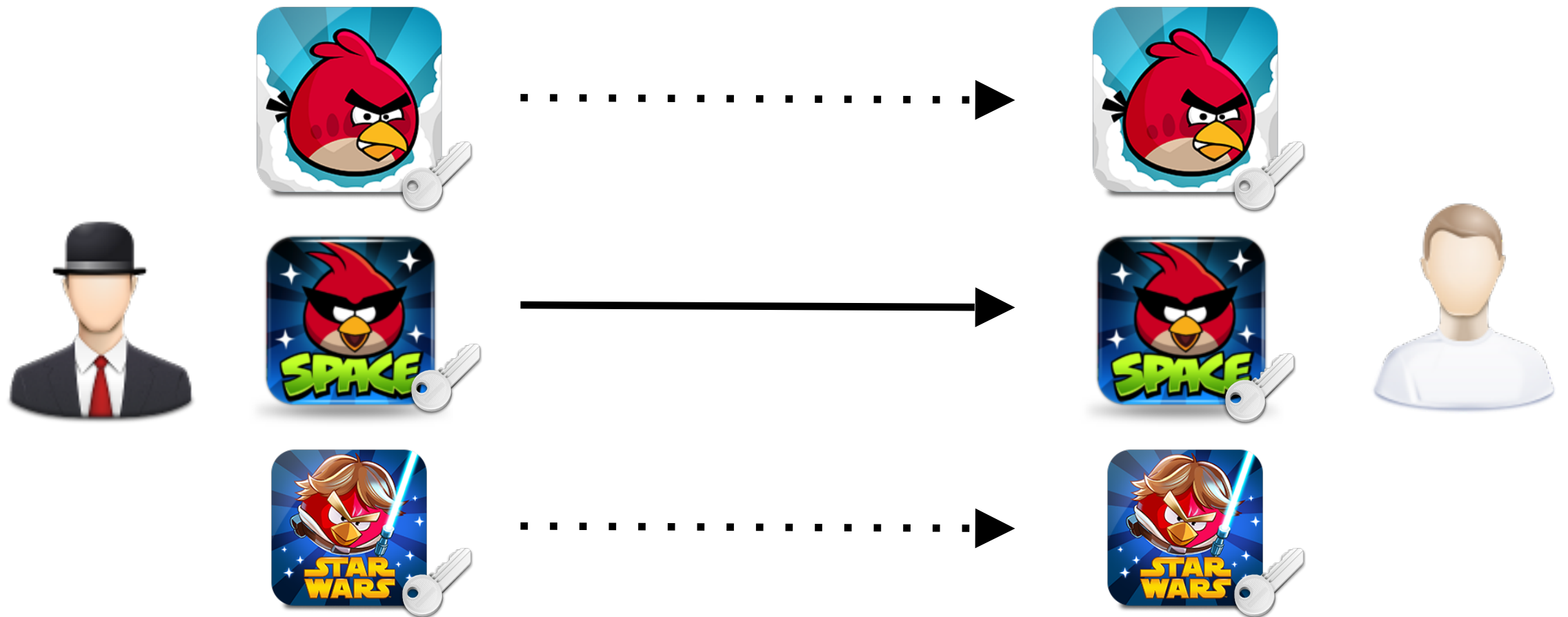
Note: as of Authenticator 0.62, only devices running Android version 2.1 and later are supported.

1. First [switch to text or voice verification codes](#). (You will switch back to using Authenticator verification codes in the following step.) Be sure to follow this process for all accounts you have configured in Authenticator.
2. Follow [these instructions](#) to download the new version of Google Authenticator from Google play and configure your Google Account in it.
3. Once you have confirmed as part of the previous step that you are able to successfully generate valid verification codes using the new Authenticator, it is safe to uninstall the old version of the app. **Because both versions have the same icon, make sure to check the version number before uninstalling: you want to keep version 2.15.**

App transfer



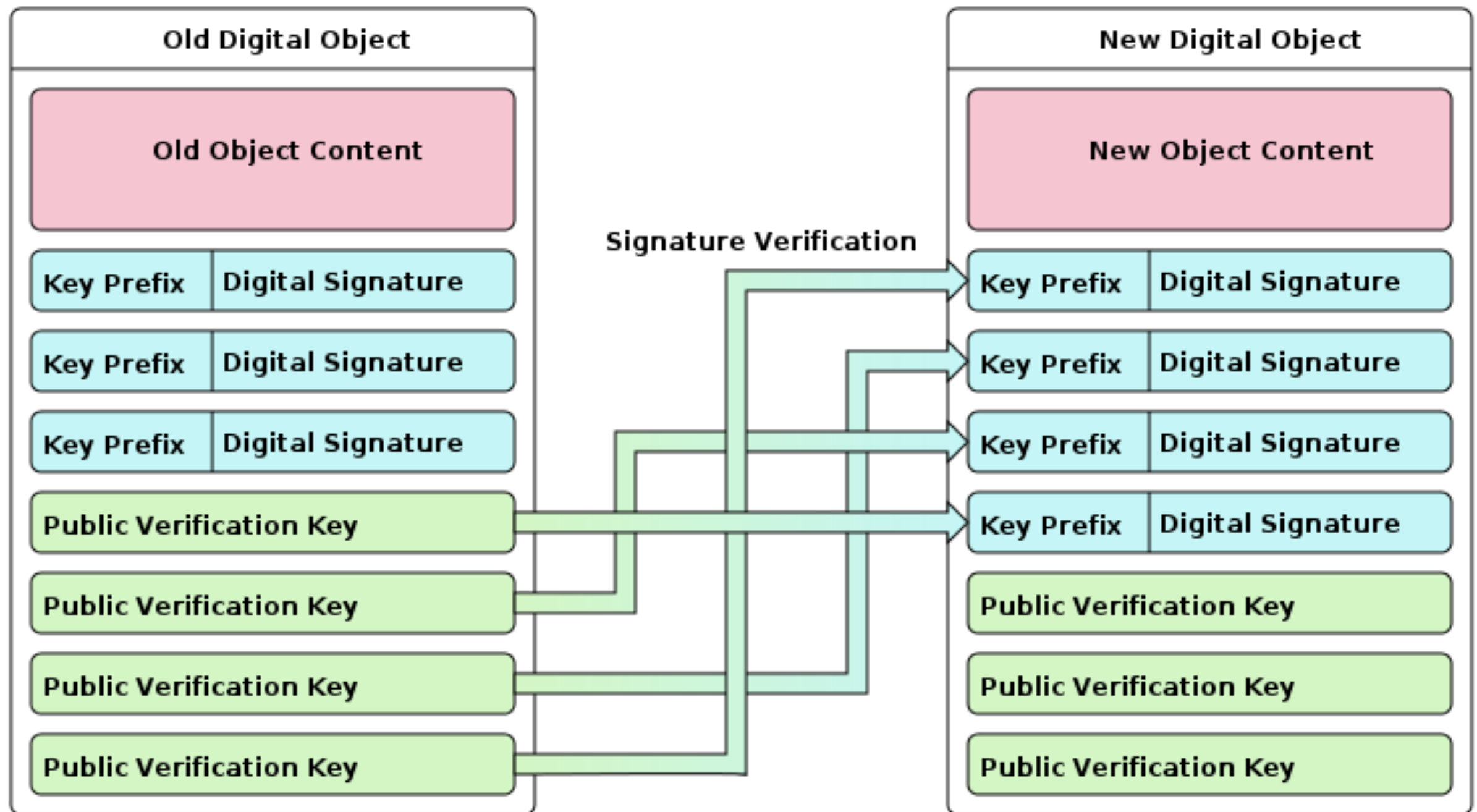
App transfer



Related Work

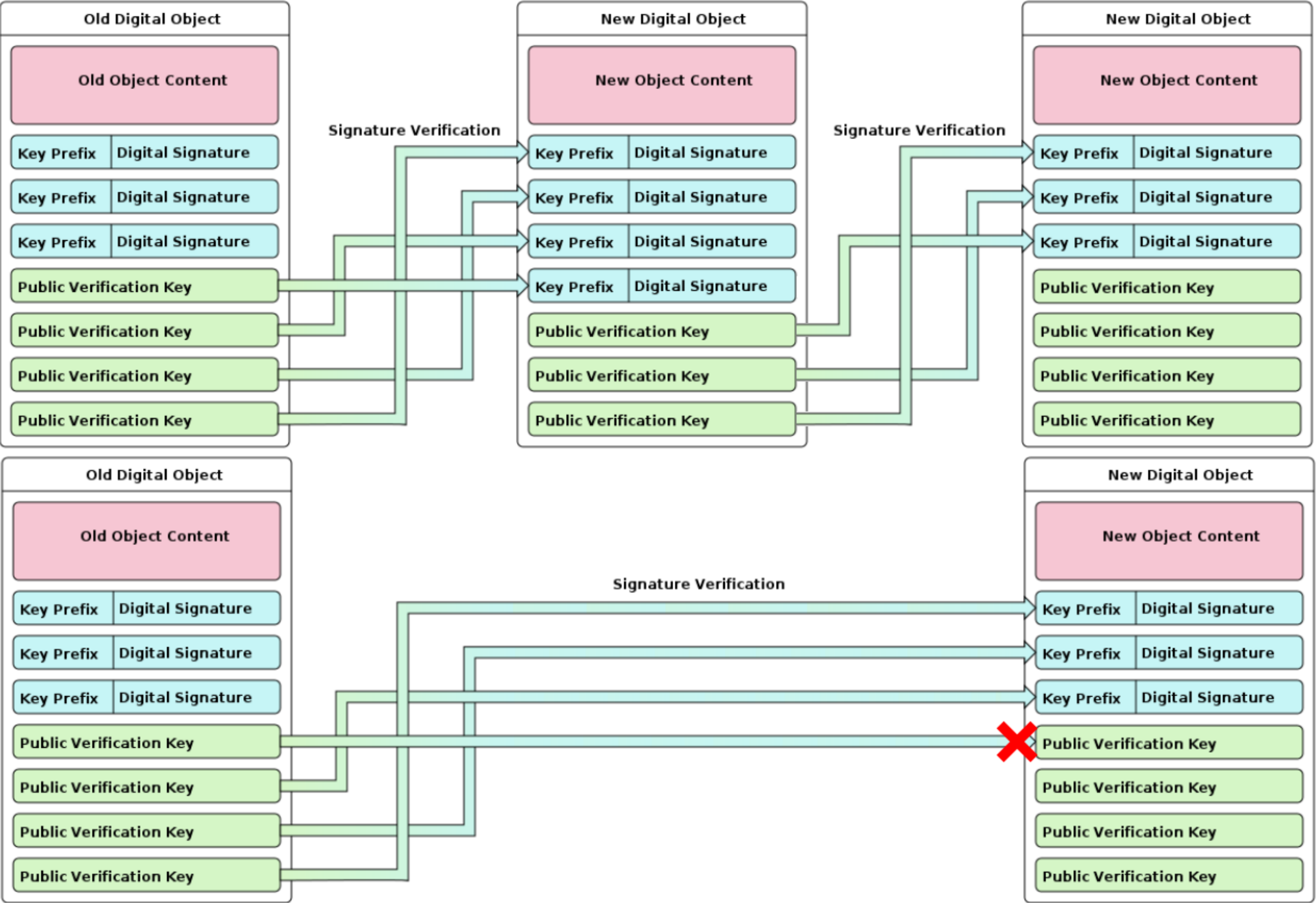
- Key-locking (Wurster and Van Oorschot, 2007)
- Digitally sign files we wish to protect
- OS policy: “Only allow updates if new version includes signatures that can be verified by keys in the current version”

Key-locking



Key-locking Limitations

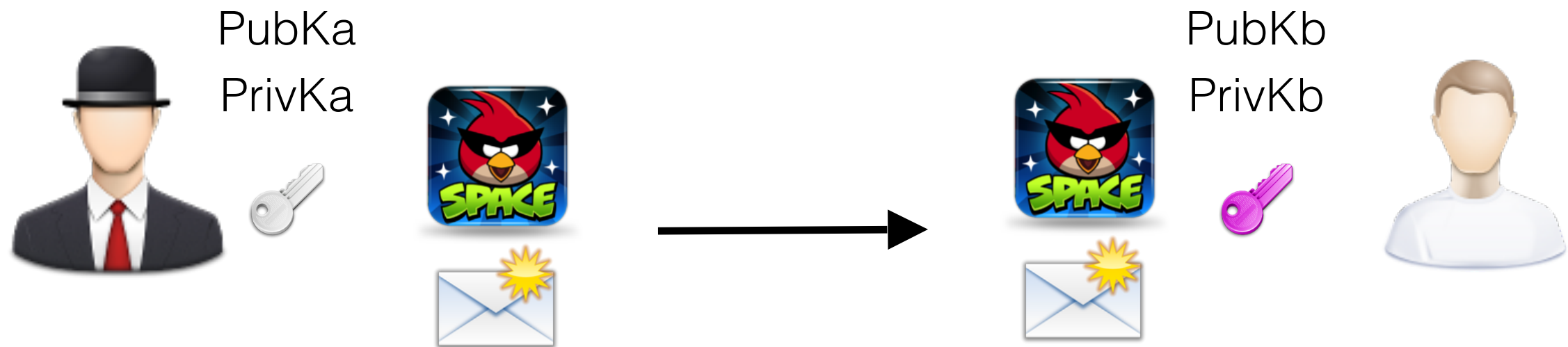
- History of key transitions is ephemeral
- Intermediate updates cannot be skipped
- Would break compatibility with the signatures used on Android applications




Baton

- Protocol to assert delegation of signing authority
- Builds on the ideas of Key-locking
- Improvements:
 - Keeps a history of key delegations
 - Allows skipping intermediate updates
 - Per-app

Baton



 = **SigPrivKa** { *"I authorize the holder of PrivKb* to release updates to Angry Birds Space"* }

*PrivKb can also be a set of keys and corresponding policy for consensus

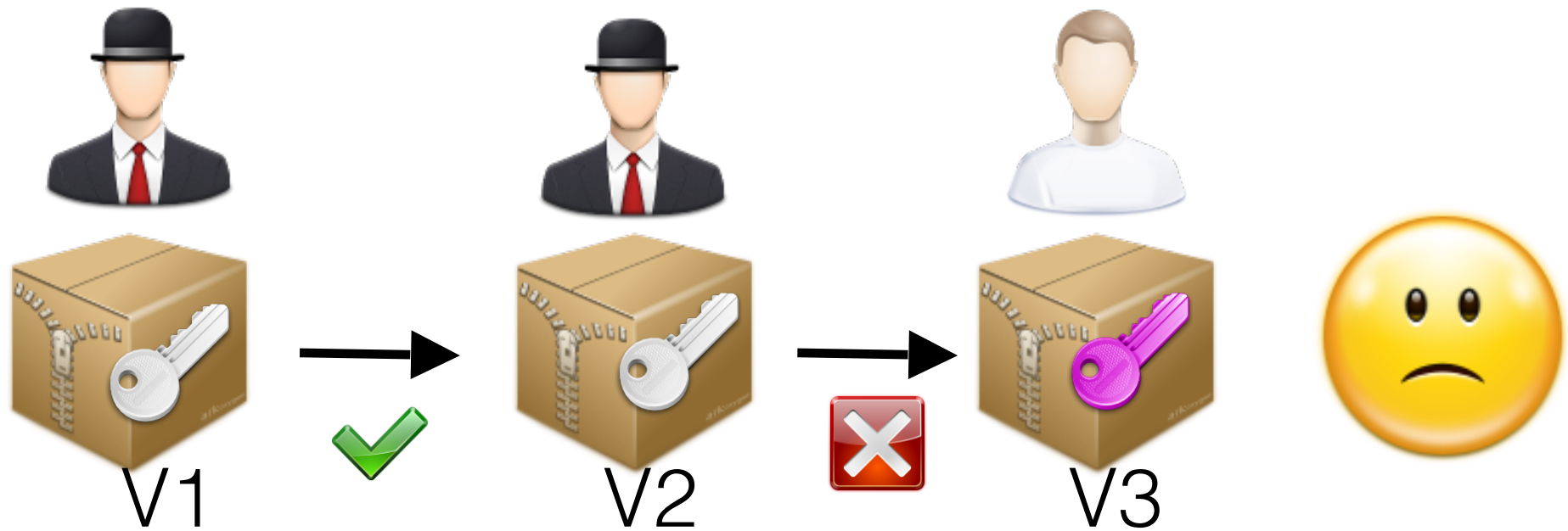
Baton Delegation Tokens

- Package name, version
- Set of currently used certificates
- Set of new certificates
- Hash of previous token (if available)

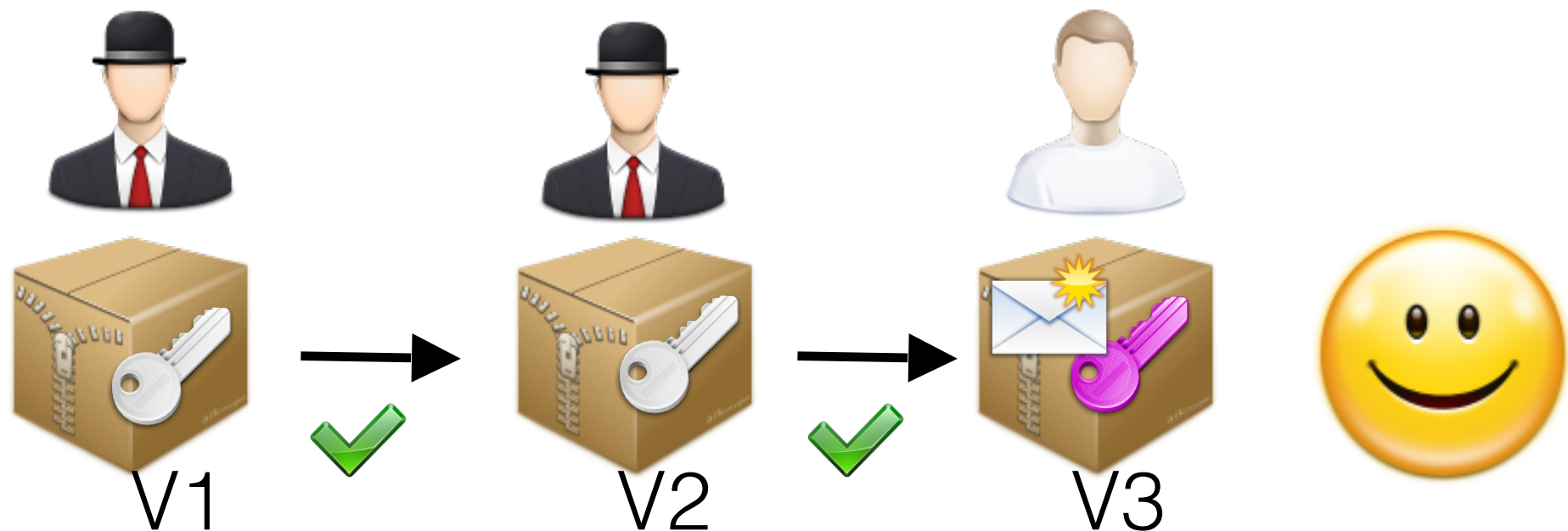


Baton

Without
Baton



With
Baton



Baton

- Usability benefits:
 - No user action required
 - Transparent: updates as usual
- Opt-in: developers only go through this process if switching keys
- Lightweight: no additional servers, low storage overhead
- Encourages key management best practices

Implementation

- Modifications to Android's installer framework
- No changes to “outer” signatures
- Ensure that we preserve compatibility
- Eclipse plugin to generate Baton delegation tokens

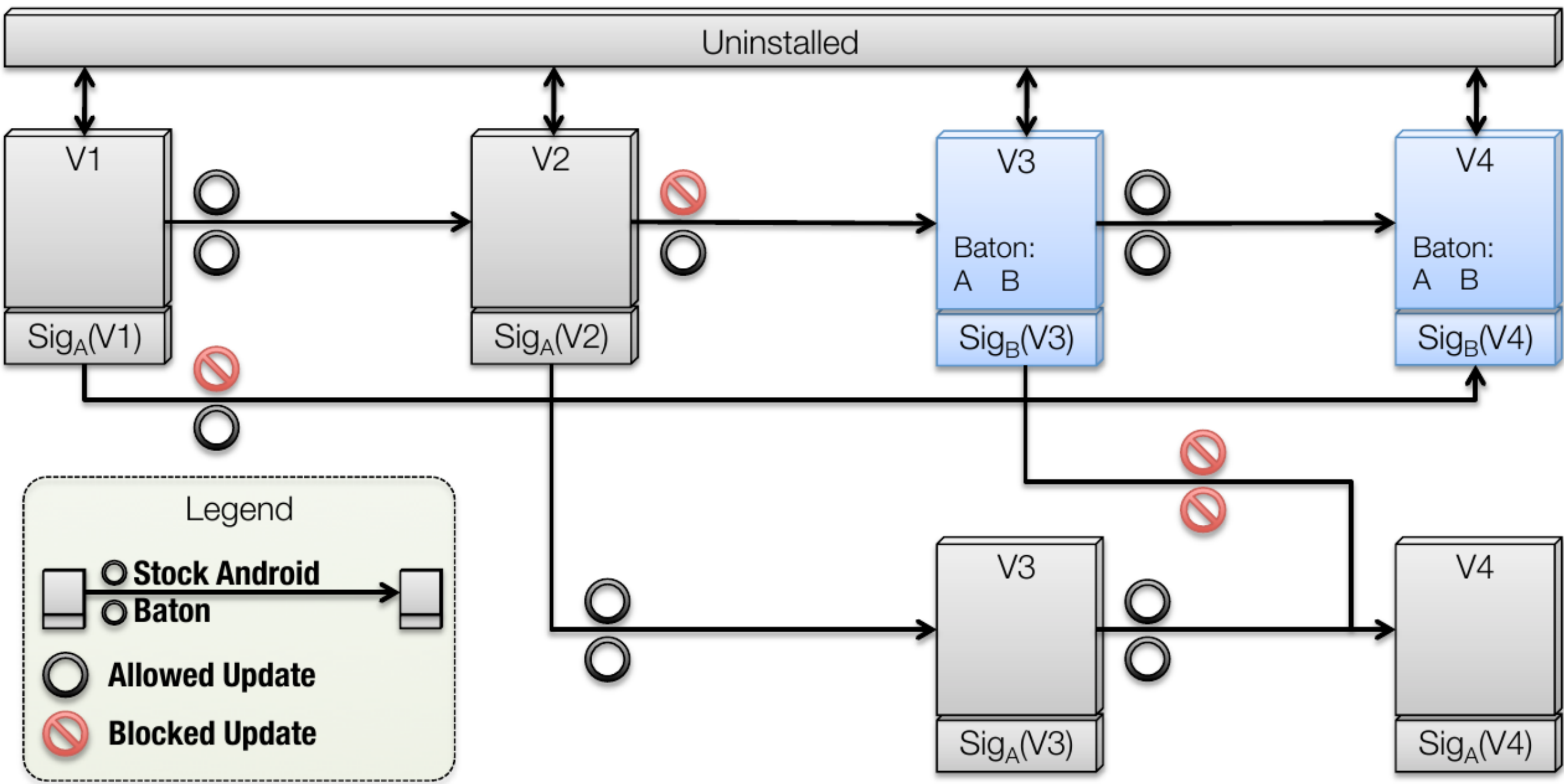
Limitations

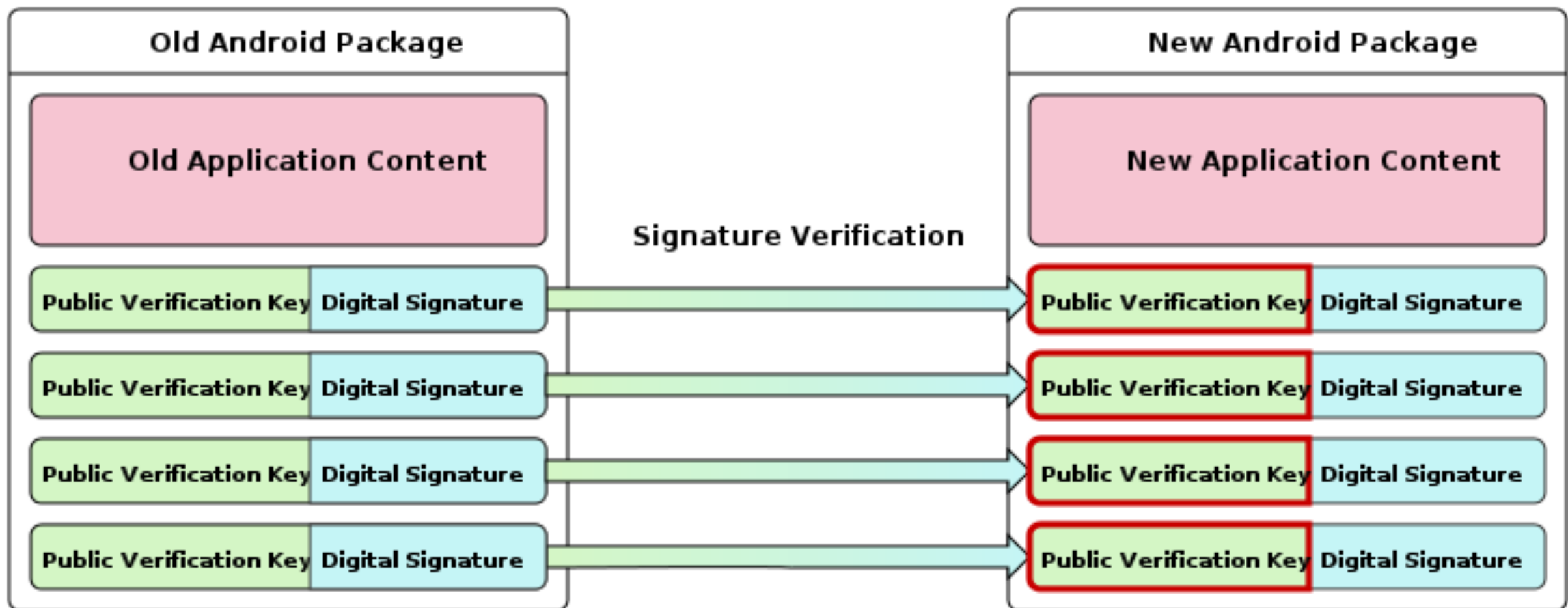
- Must keep tokens and public keys for as long as users are expected to update
- Does not allow recovery from key loss

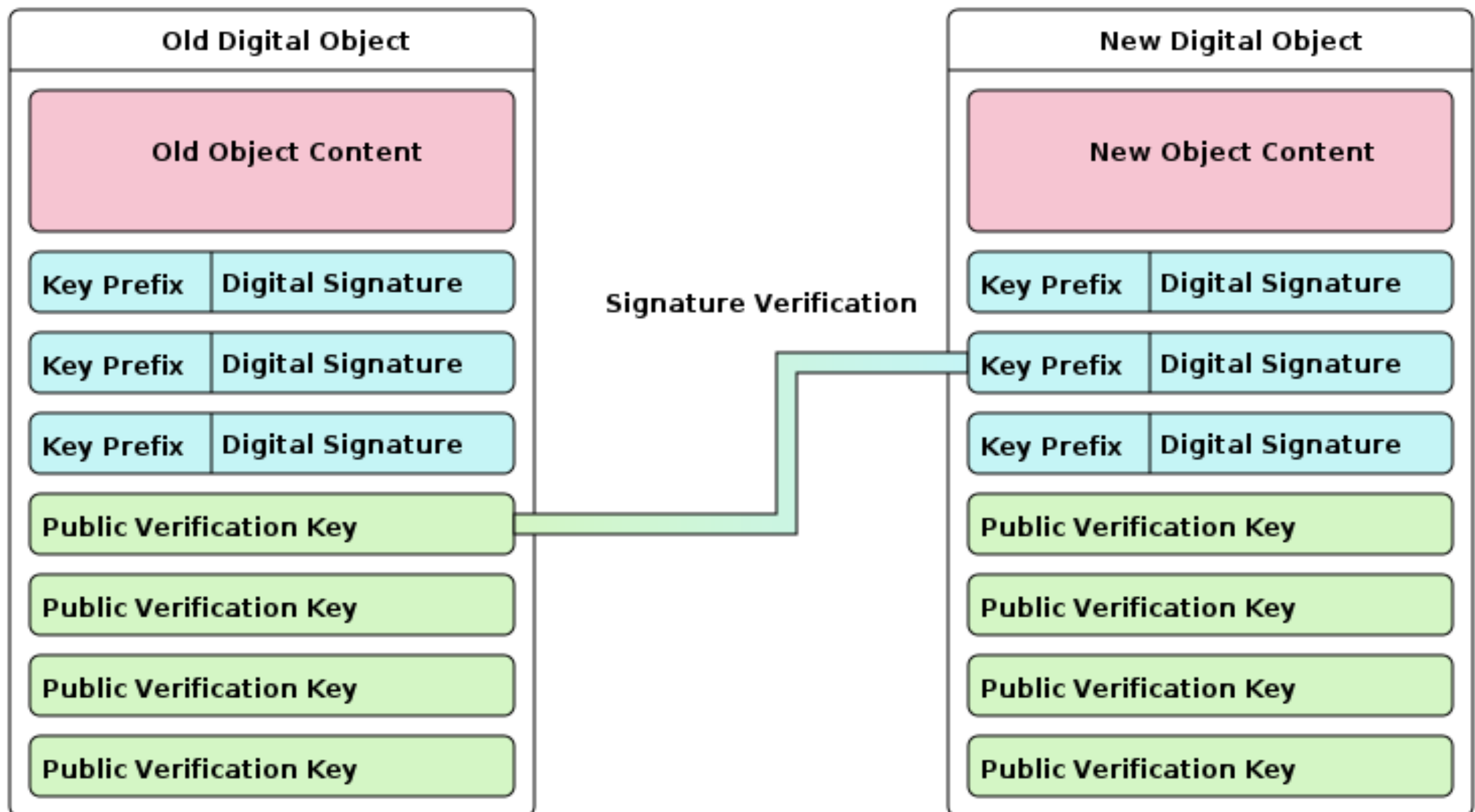
Shameless plug: www.androidobservatory.org

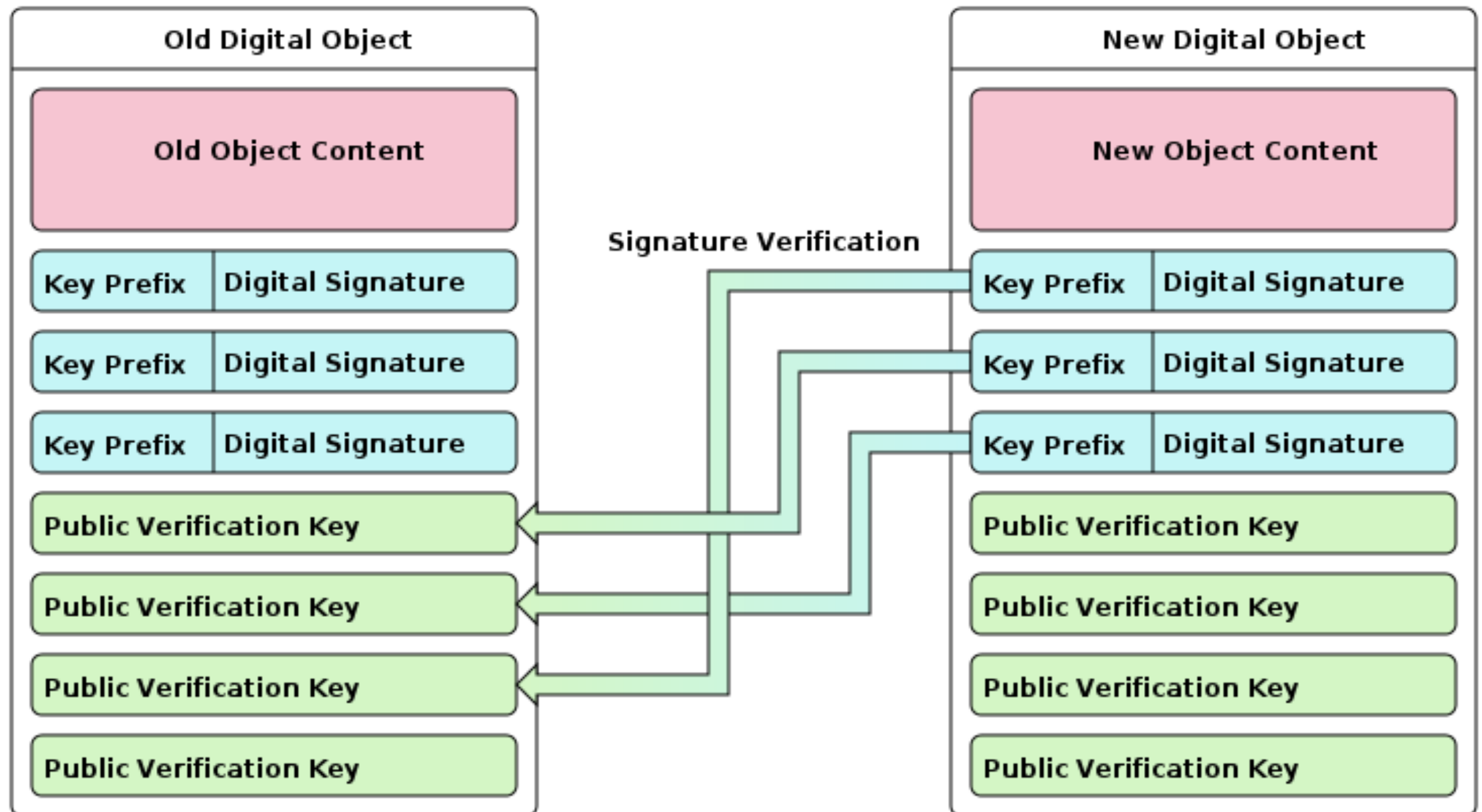
Thank you Questions

Contact:
@davidbb
david.barrera@inf.ethz.ch

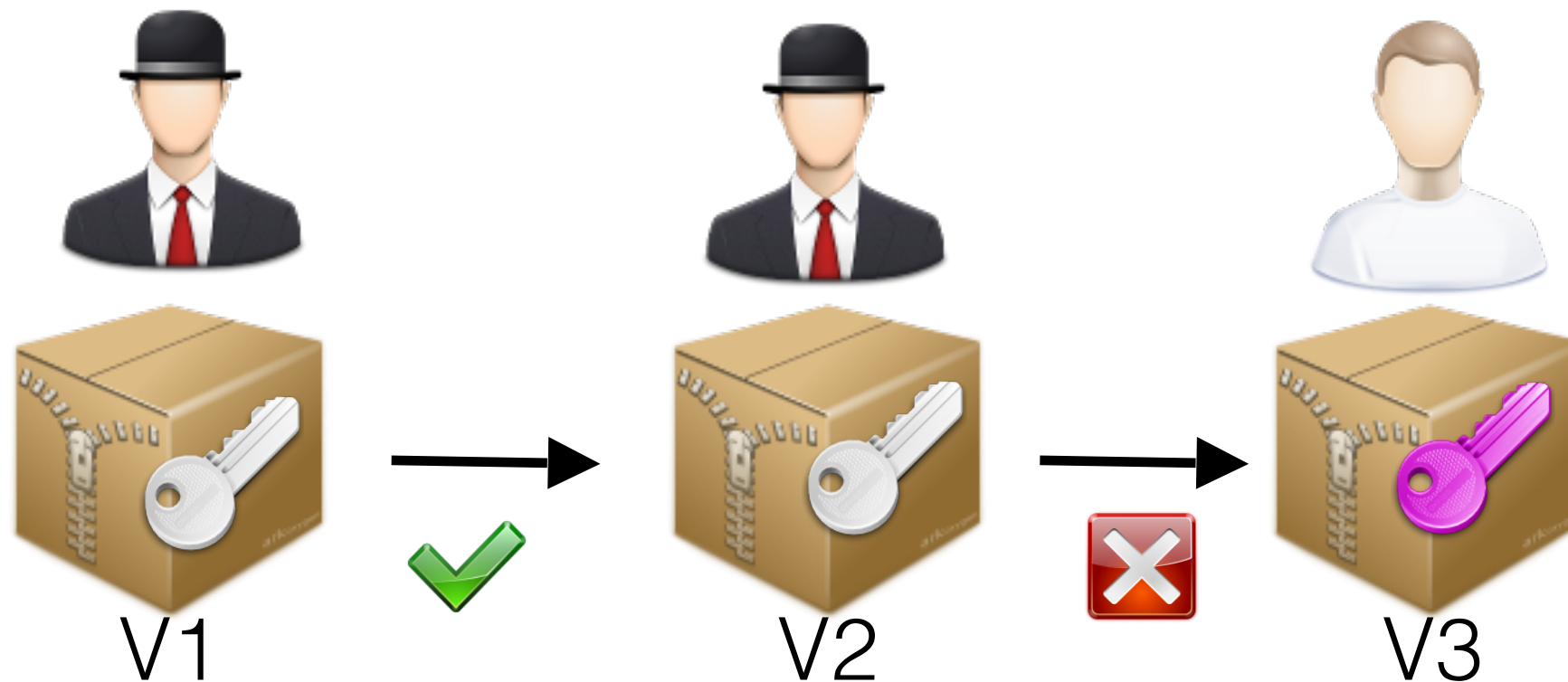








App transfer



Change Signing Key

