

 **Links and References:**
<https://tinyurl.com/MacADUK-EB>



Escrow Buddy

A Tool for Escrowing Missing FileVault Recovery Keys

Elliot Jordan

MacAD.UK Conference • May 24, 2024

 **Links and References:**
<https://tinyurl.com/MacADUK-EB>

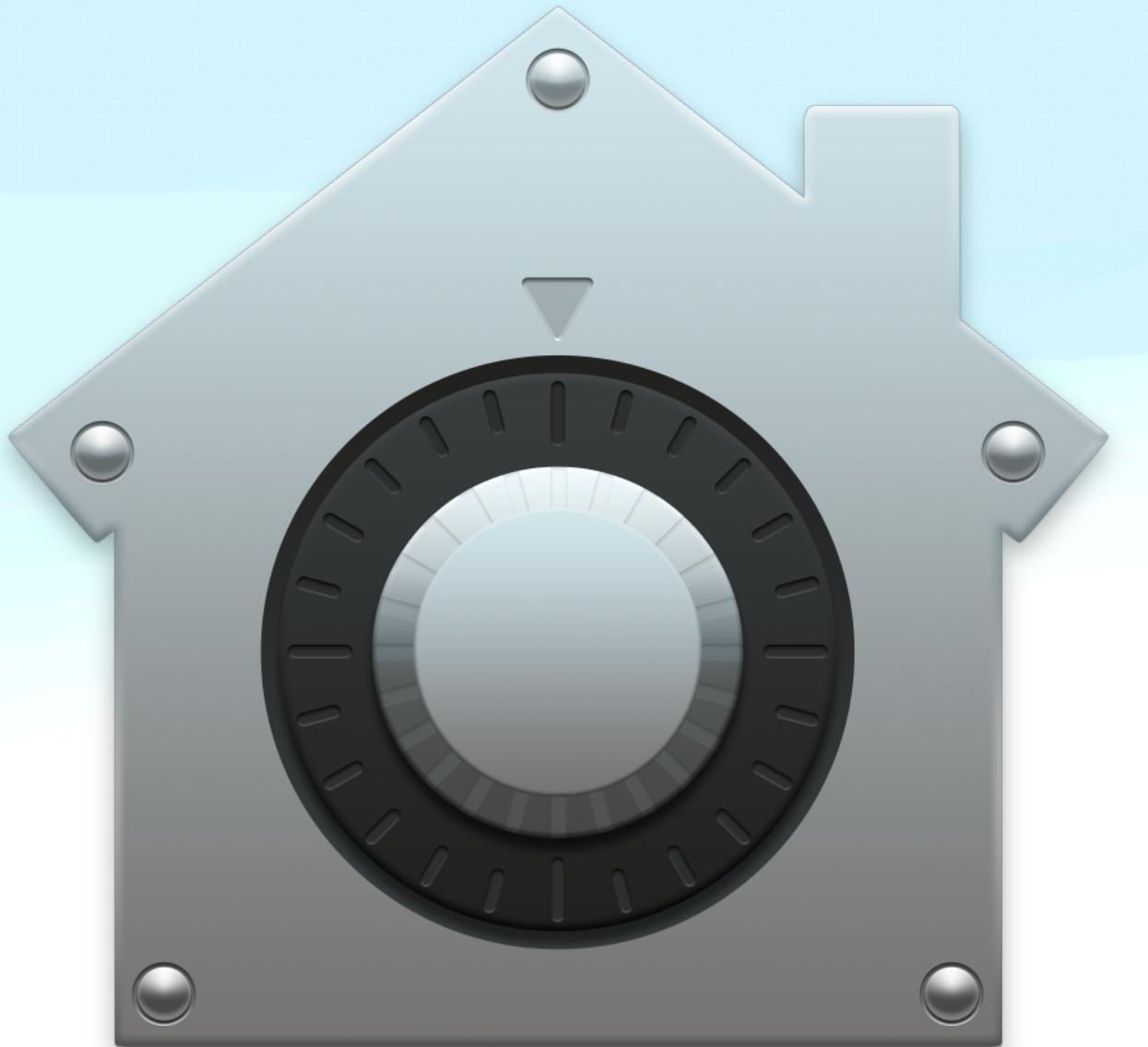


Elliot Jordan

Senior Client Systems Engineer, Netflix

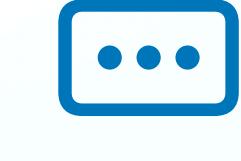


FileVault Basics





FileVault Basics

-  Full disk encryption
-  Protects organization data if a Mac lost/stolen
-  Authorized users' passwords can unlock
-  Personal recovery key (PRK) can unlock
-  PRK can be escrowed to MDM or other storage



Escrow Buddy Log (via SSH)

```
Filtering the log data using "subsystem == "com.netflix.Escrow-Buddy""
```

Escrow Buddy Logs

(via SSH to target Mac)

```
MDM FileVault Info (via Jamf API)
```

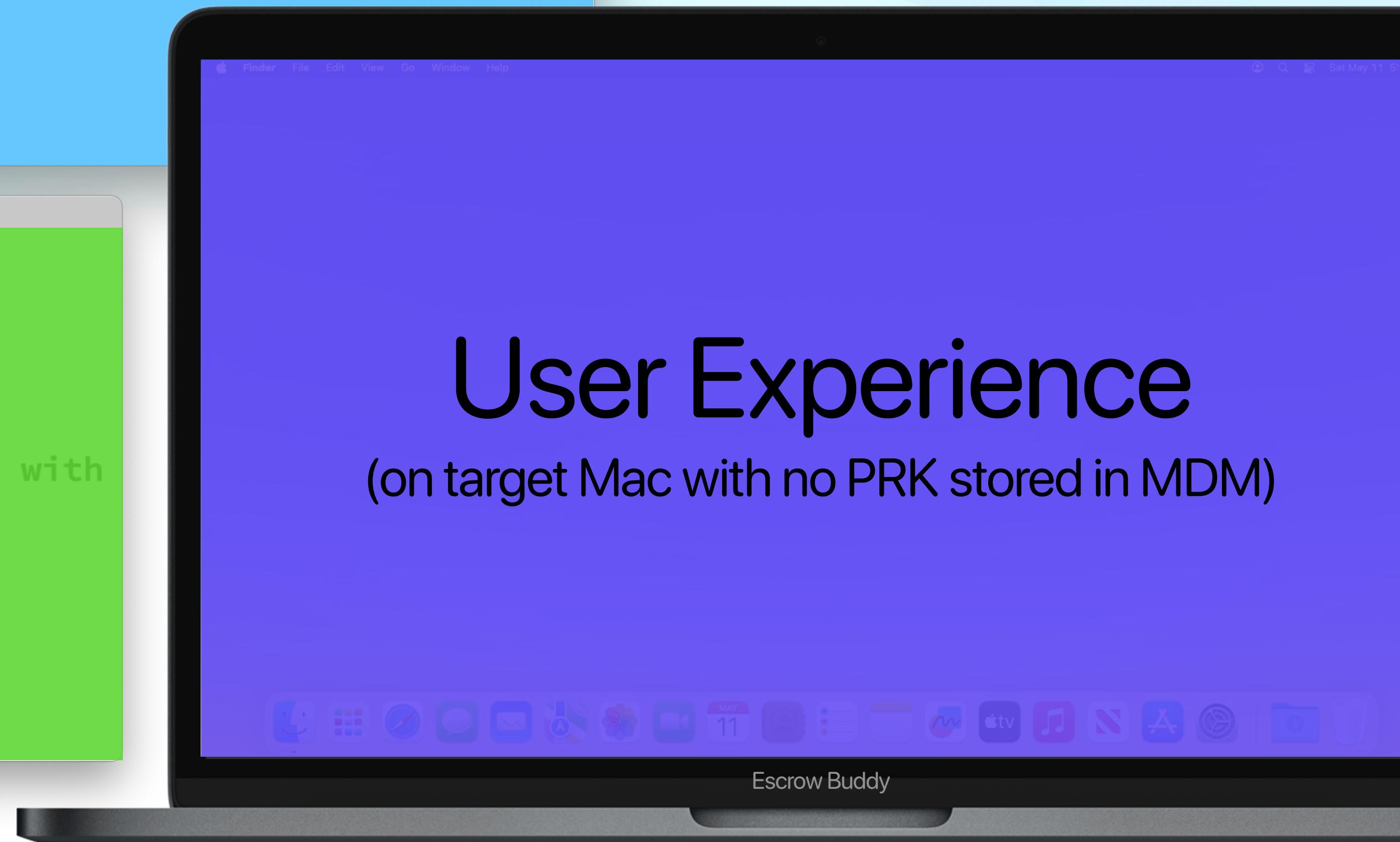
```
2024-05-11 17:13:01
{
  "httpStatus" : 404,
  "errors" : [ {
    "code" : "INVALID_ID",
    "description" : "FileVault information on the computer with given id does not exist",
    "id" : "25026",
    "field" : null
  } ]
}
```

FileVault Info in MDM

(via Jamf API)

User Experience

(on target Mac with no PRK stored in MDM)



Escrow Buddy

Escrow Buddy Log (via SSH)

```
Filtering the log data using "subsystem == "com.netflix.Escrow-Buddy""
```



MDM FileVault Info (via Jamf API)

```
2024-05-11 17:13:50
```

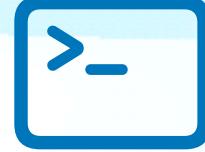
```
{  
  "computerId" : "25026",  
  "name" : "Elliot's Virtual Machine",  
  "personalRecoveryKey" : "8DL9-RNRT-VCWN-ZQ4H-B5E4-VNN8"  
  "bootPartitionEncryptionDetails" : null,  
  "individualRecoveryKeyValidityStatus" : "VALID"  
  "institutionalRecoveryKeyPresent" : false,  
  "diskEncryptionConfigurationName" : ""  
}
```

Escrow Buddy

Why are my FileVault recovery keys missing?

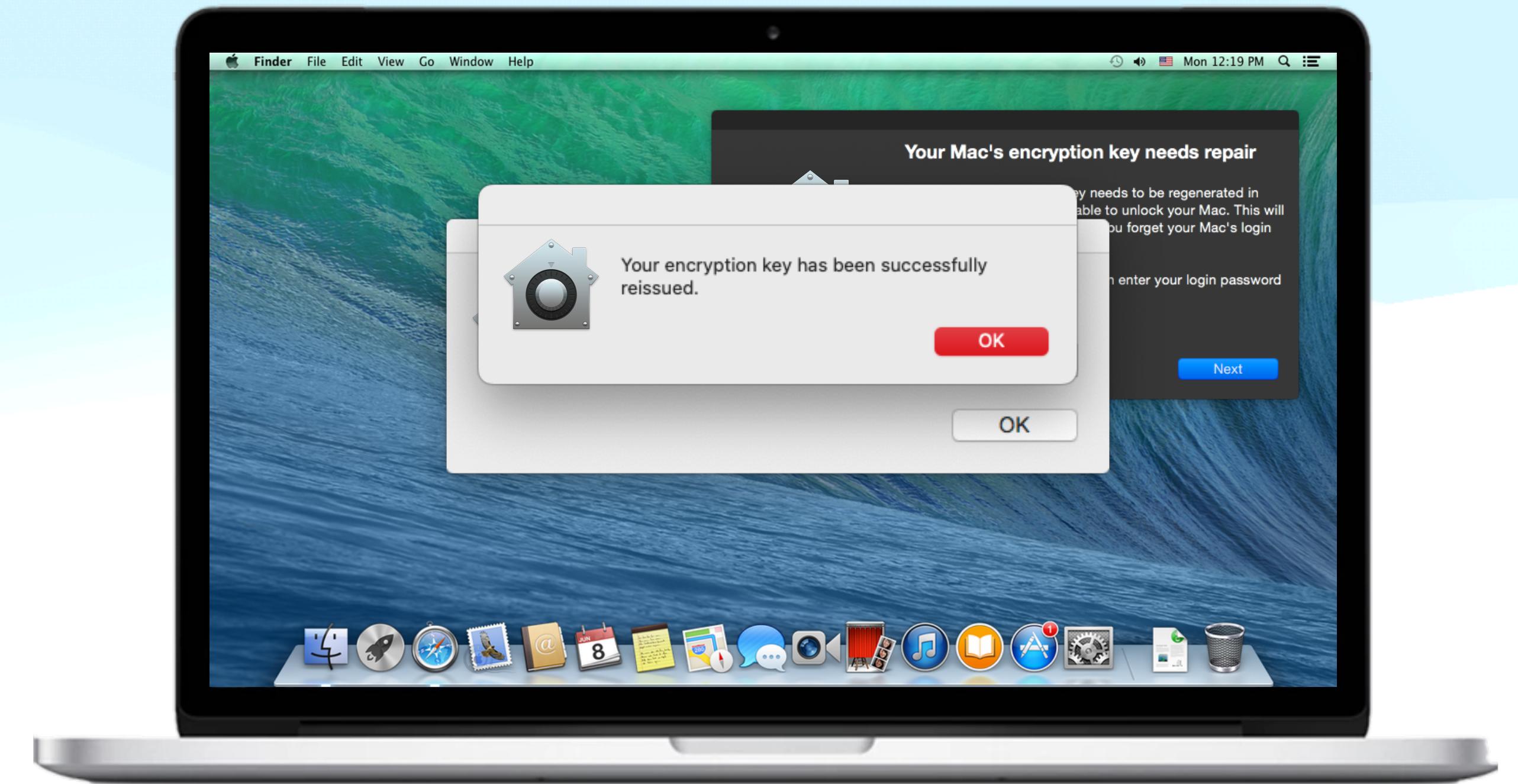
-  Migration from another MDM
-  Encrypted before enrollment
-  Escrow profile misconfigured
-  Data loss or corruption

How can I solve missing FileVault recovery keys?

-  Toggle FileVault off/on
-  Manually use `fdesetup`
-  Automate `fdesetup`

The old way (stop doing this!)

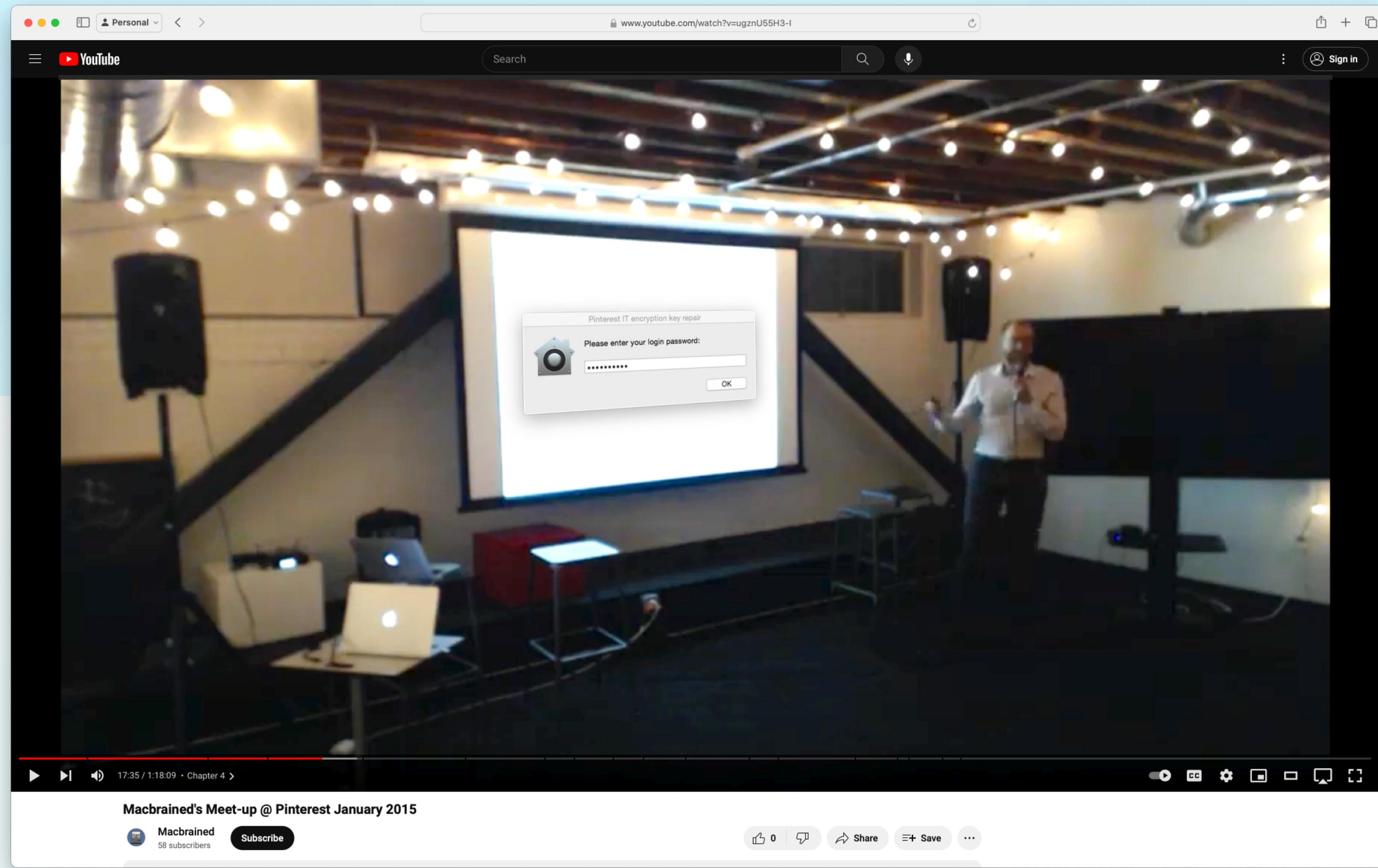
1. Make user aware
2. Prompt for password
3. Trigger fdesetup
4. Communicate result



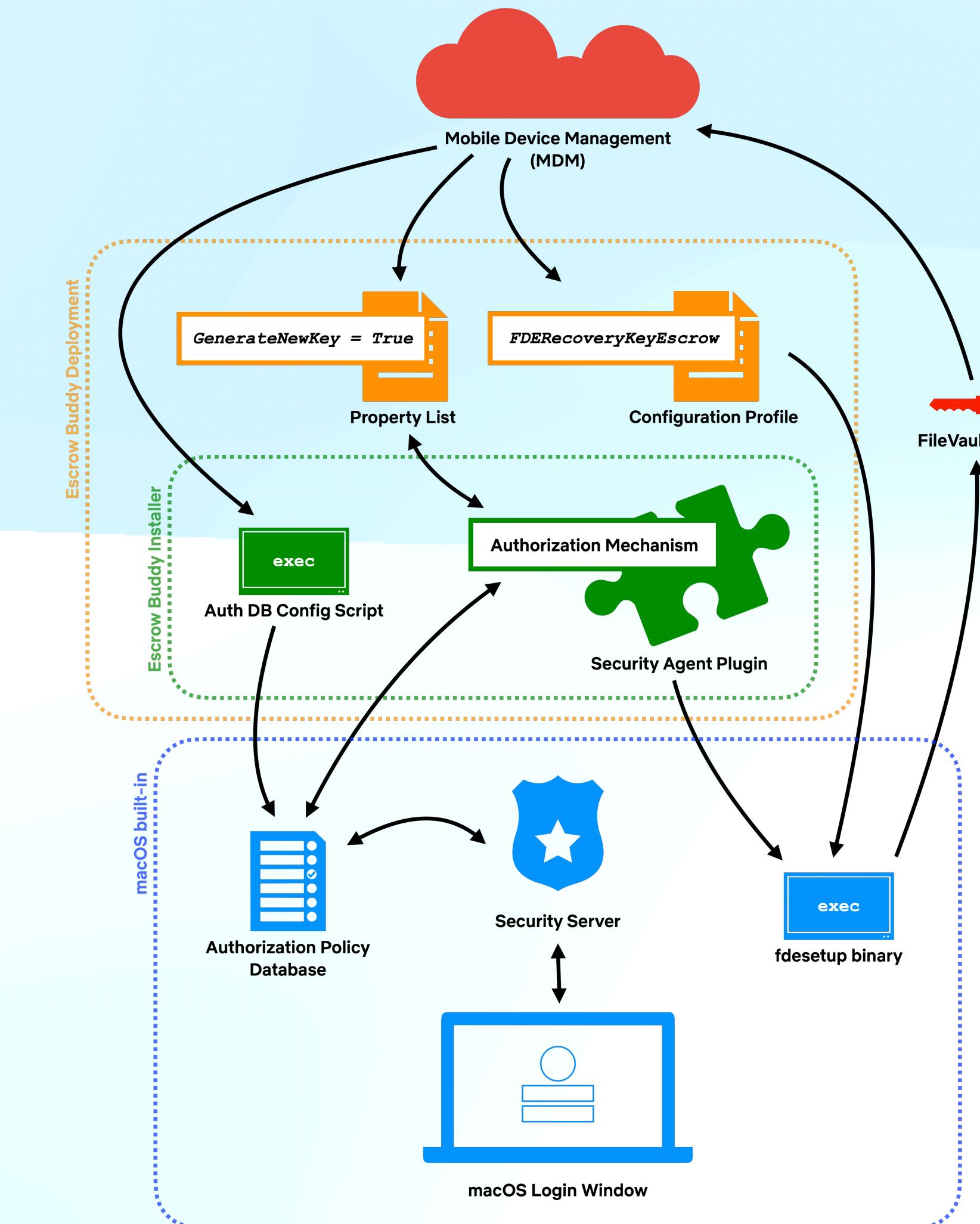
🔗 <https://github.com/homebysix/jss-filevault-reissue>

The new way is better...

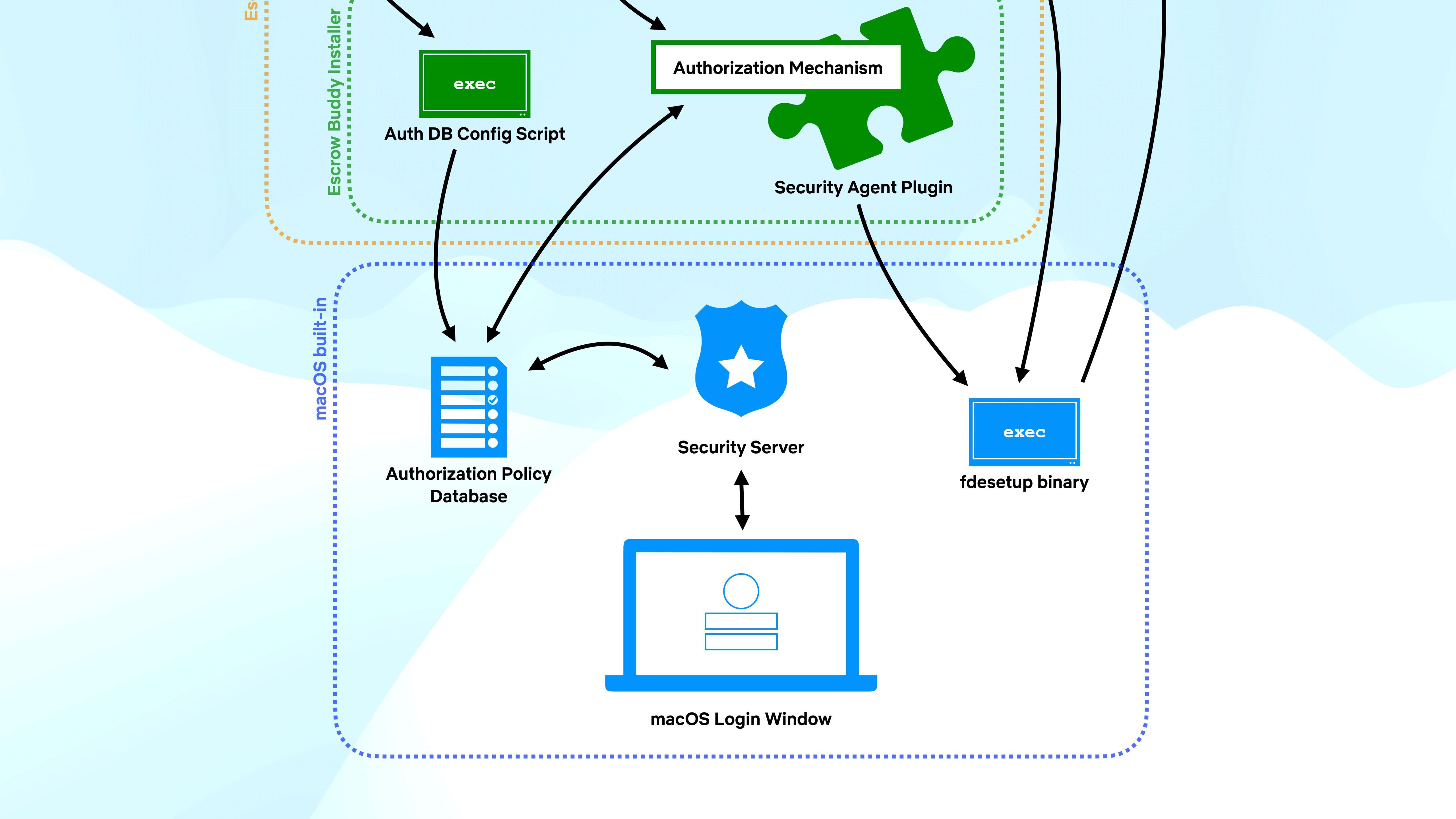
(take it from the guy who popularized the old way)

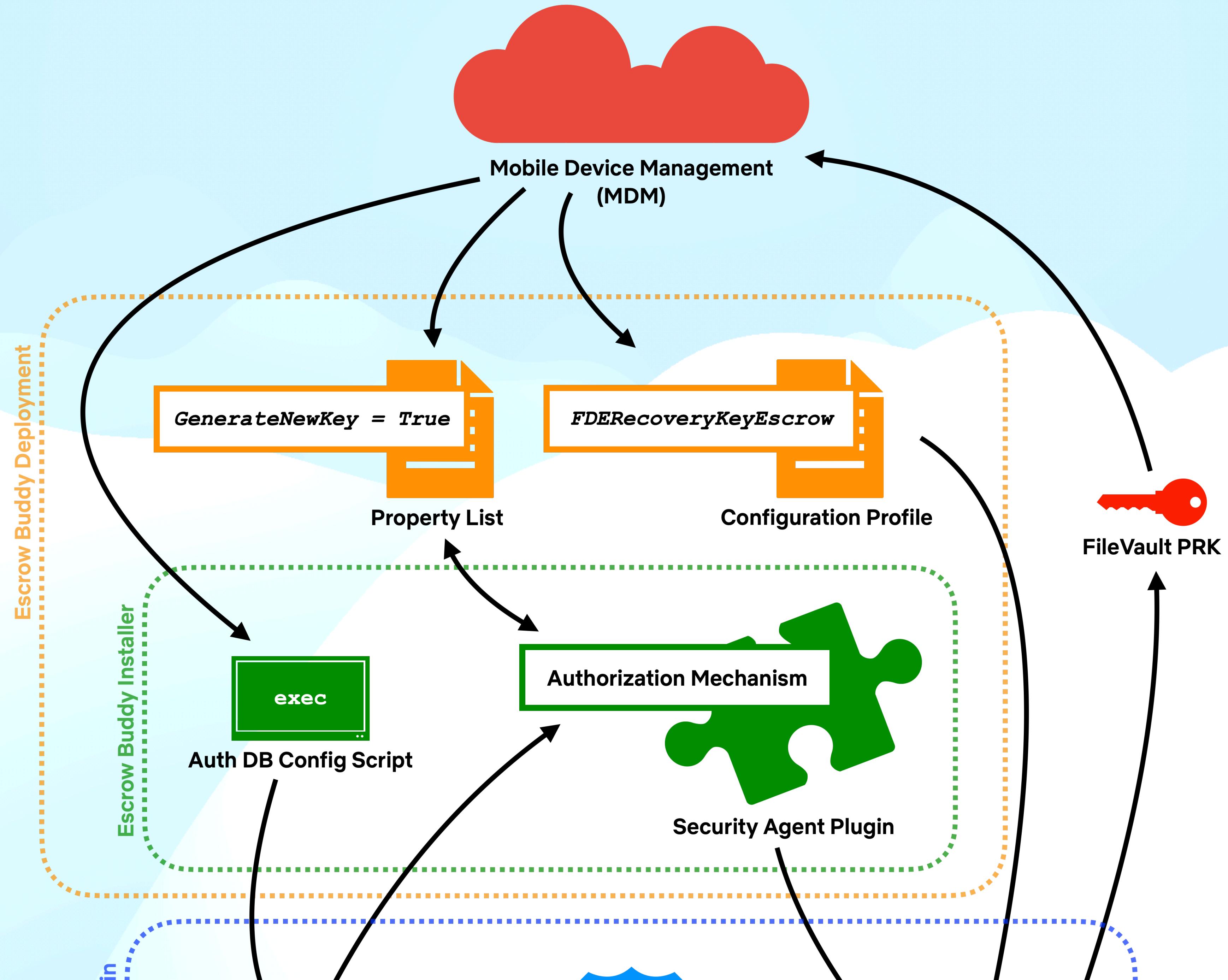


The new way: authorization plugin



- Leverages macOS login
- Secure credential access
- No unfamiliar prompts!





Crypt did it first!

Crypt is an authorization plugin that will enforce FileVault 2, and then submit it to an instance of Crypt Server.



Lesser-known feature:
Standalone regeneration of
FileVault keys upon login

The screenshot shows a GitHub repository page for 'grahamgilbert / crypt' (Public). The repository has 6 issues, 2 pull requests, and 47 forks. The README file is the active tab, showing the following content:

Crypt

WARNING: As this has the potential for stopping users from logging in, extensive testing should take place before deploying into production.

Crypt is an authorization plugin that will enforce FileVault 2, and then submit it to an instance of [Crypt Server](#). Crypt supports macOS 13 and above. For versions below 13.0, please use version 4.1.0. For versions below 11.0, please use version 4.0.0. For versions below 10.12 please use version 2 and below.

When using Crypt with macOS 10.15 and higher, you will also need to deploy a PPC TCC profile via user approved MDM to allow Crypt to enable FileVault. [An example can be found here](#).

Features

- Uses native authorization plugin so FileVault enforcement cannot be skipped.
- Escrow is delayed until there is an active user, so FileVault can be enforced when the Mac is offline.
- Administrators can specify a series of username that should not have to enable FileVault (IT admin, for example).

Configuration

Preferences can be set either in `/Library/Preferences/com.grahamgilbert.crypt.plist` or via MCX / Profiles. An example profile can be found [here](#).

The right sidebar contains sections for About, Releases (14), Packages, and Contributors (19), along with various repository statistics.

<https://github.com/grahamgilbert/crypt/>

Escrow Buddy makes it simple

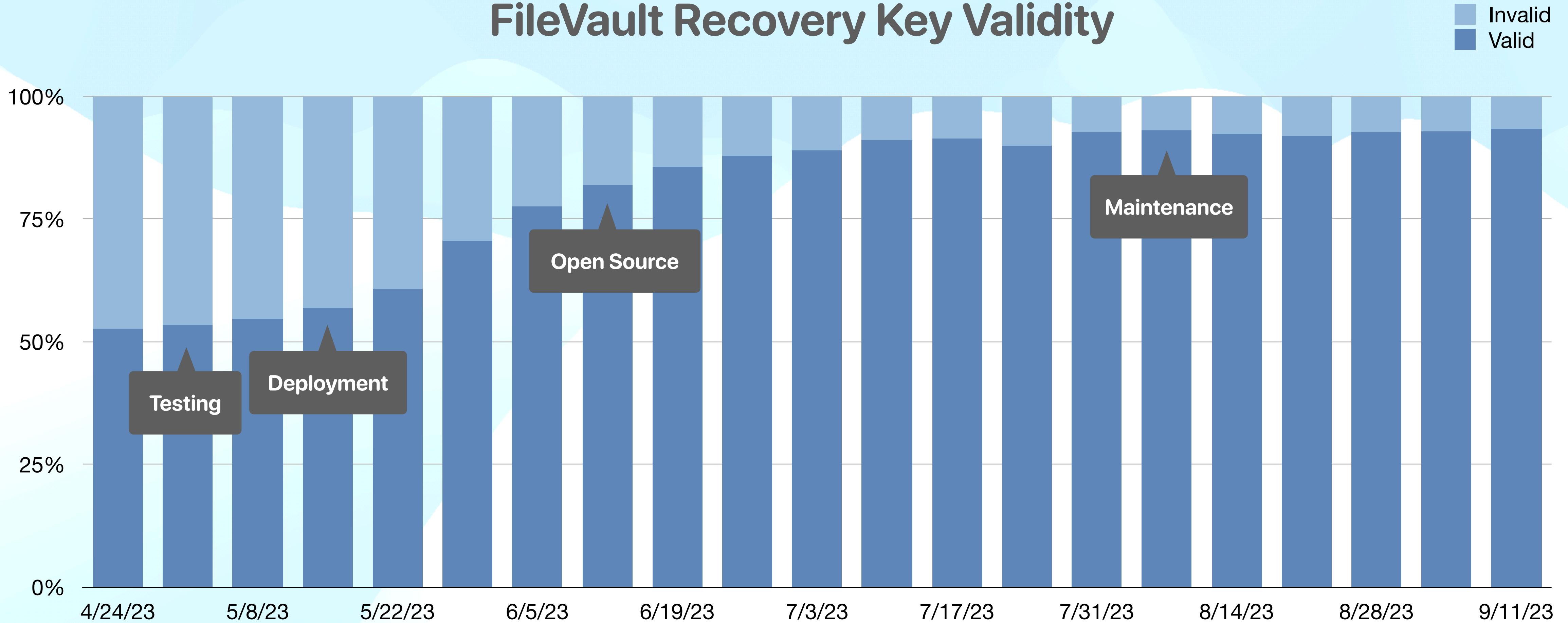
- ✓ Checks for FDERecoveryEscrow payload
- ✓ Generates new FileVault keys upon login
- ✓ Nothing else



<https://github.com/macadmins/escrow-buddy/>

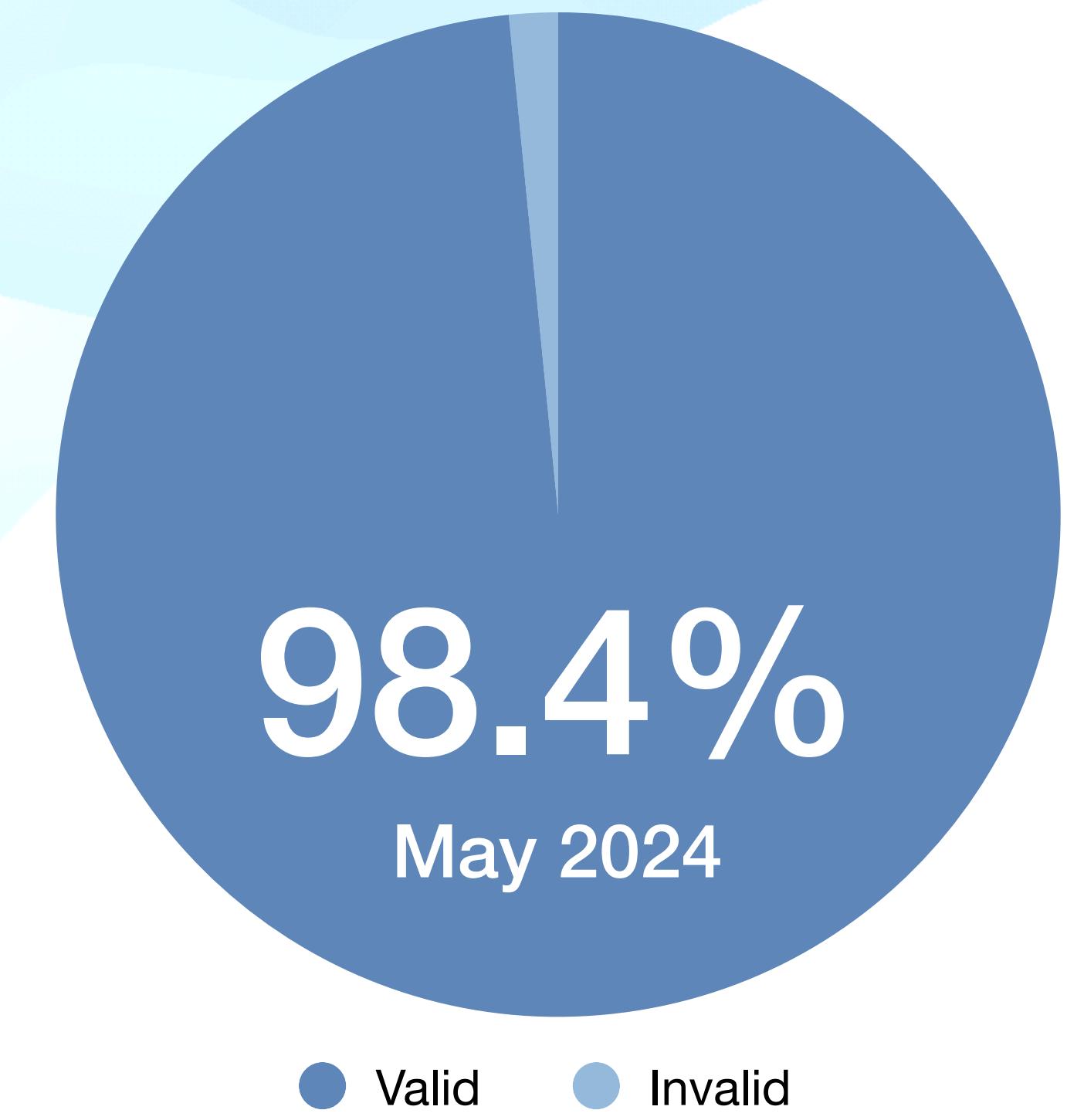
Our Success Story

FileVault Recovery Key Validity

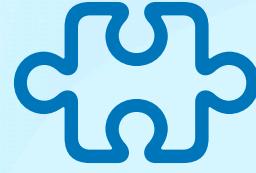


Our Success Story

FileVault Recovery Key Validity



Deploying Escrow Buddy from your MDM

-  Works with any MDM that can deploy pkgs
-  Community-contributed setup instructions for
 - Addigy
 - Jamf
 - Intune
 - Kandji
 - Mosyle
 - WorkspaceONE

 <https://github.com/macadmins/escrow-buddy/wiki/Examples>

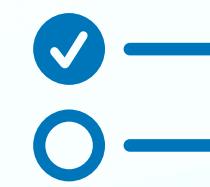
Example: Basic deployment with Jamf



Package: Escrow Buddy



Smart Group: FileVault PRK Missing or Invalid



Policy: Install and configure Escrow Buddy

Wiki <https://github.com/macadmins/escrow-buddy/wiki/Jamf>
HCS Guide <https://tinyurl.com/2systu46>

Advanced workflow options

↗ Separate installation/configuration

↔ Recidivism detection

█ Automatic key rotation

❗ Logout notification

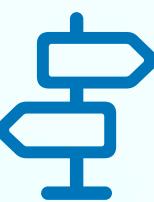
Escrowing quickly after key generation

/Library/LaunchDaemons/com.elliottjordan.FileVaultPRKWatcher.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Comment</key>
    <string>Details: https://www.elliottjordan.com/posts/filevault-escrow-daemon/</string>
    <key>Label</key>
    <string>com.elliottjordan.FileVaultPRKWatcher</string>
    <key>ProgramArguments</key>
    <array>
        <string>/usr/local/bin/jamf</string>
        <string>recon</string>
    </array>
    <key>WatchPaths</key>
    <array>
        <string>/var/db/FileVaultPRK.dat</string>
    </array>
</dict>
</plist>
```

🔗 <https://www.elliottjordan.com/posts/filevault-escrow-daemon/>

Tips and troubleshooting

-  Reading logs
 -  Testing with new macOS versions
 -  Tracking success over time
 -  Managing authorization database entries
-  <https://github.com/macadmins/escrow-buddy/wiki/>

Escrow Buddy Usage Survey

 Consider submitting our anonymous survey after you deploy

 Collected data will help us prioritize potential future work

When did you begin testing Escrow Buddy?

Date

mm/dd/yyyy

When did you deploy Escrow Buddy to your organization Macs?

Date

mm/dd/yyyy

How many total Macs does your organization manage?

 <https://tinyurl.com/eb-usage>

Mac Admins Open Source

 Solving problems broadly

 Signed/notarized releases

 Community stewardship



 <https://youtu.be/REyEYsgz5MI>

Takeaways

-  Check your FileVault key validity
-  Consider using Escrow Buddy to remediate
-  Stop prompting users for their passwords whenever possible





Links and References:
<https://tinyurl.com/MacADUK-EB>



Thank you!