2023 JNUC

AUSTIN, TX

Escrow Buddy

A Tool for Escrowing Missing FileVault Recovery Keys

https://tinyurl.com/JNUC23-EB

Elliot Jordan

Senior Client Systems Engineer • Netflix

https://tinyurl.com/JNUC23-EB

Escrow Buddy Logs

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

Jamf FileVault Info

```
Mon Jul 31 20:53:03 PDT 2023
{
  "httpStatus": 404,
  "errors": [
    {
      "code": "INVALID_ID",
      "description": "FileVault information for computer with
given id does not exist",
      "id": "18984",
      "field": null
    }
  ]
}
```

User Experience

Escrow Buddy Logs

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

Jamf FileVault Info

```
Mon Jul 31 20:53:03 PDT 2023
{
  "httpStatus": 404,
  "errors": [
    {
      "code": "INVALID_ID",
      "description": "FileVault information for computer with
given id does not exist",
      "id": "18984",
      "field": null
    }
  ]
}
```

User Experience

Why are my FileVault recovery keys missing?

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

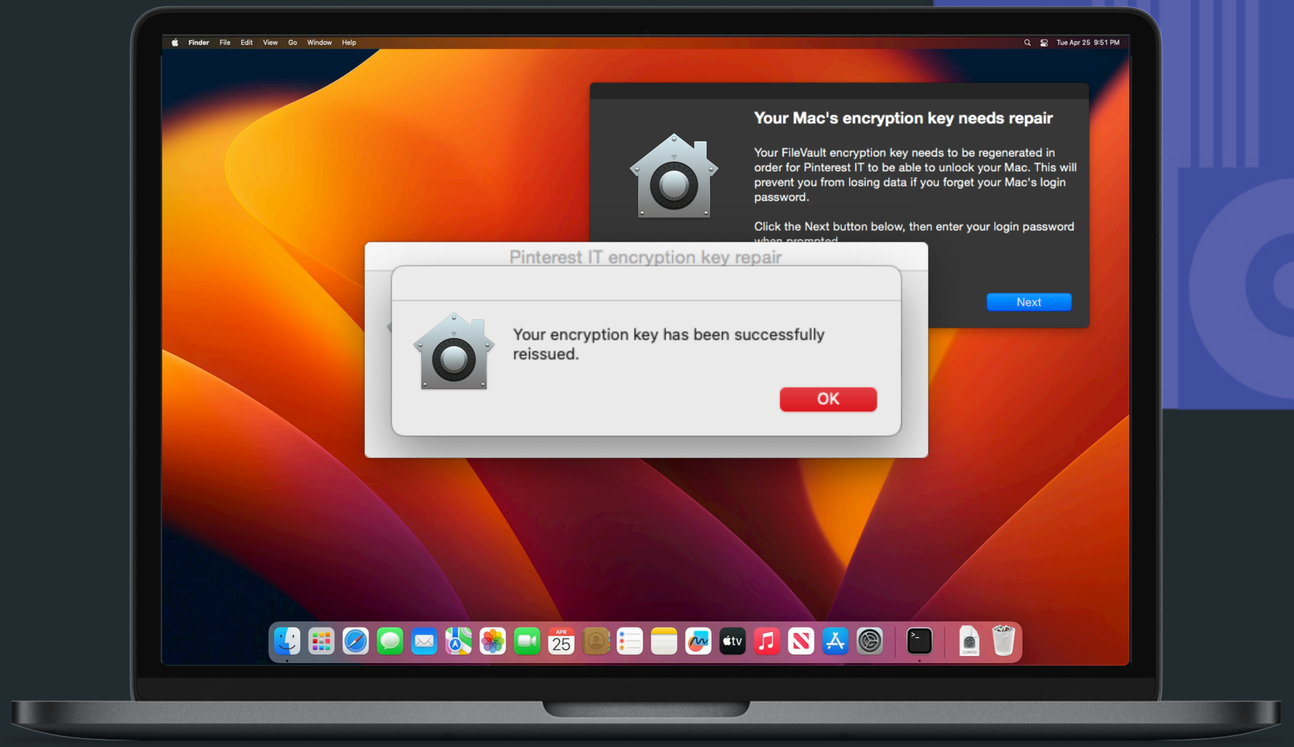
How can I solve missing FileVault recovery keys?

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

The old way

(stop doing this!)

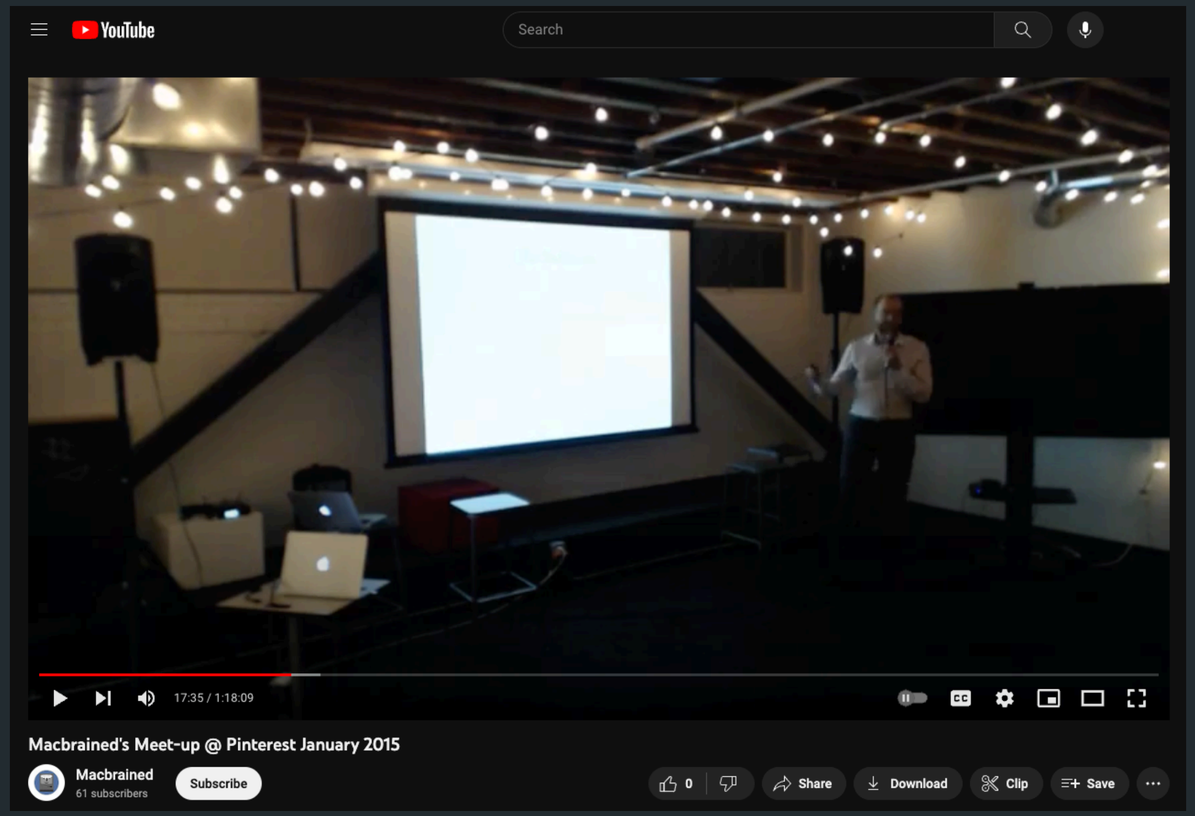
1. Make user aware
2. Prompt for password
3. Trigger **`fdesetup`**
4. Communicate result

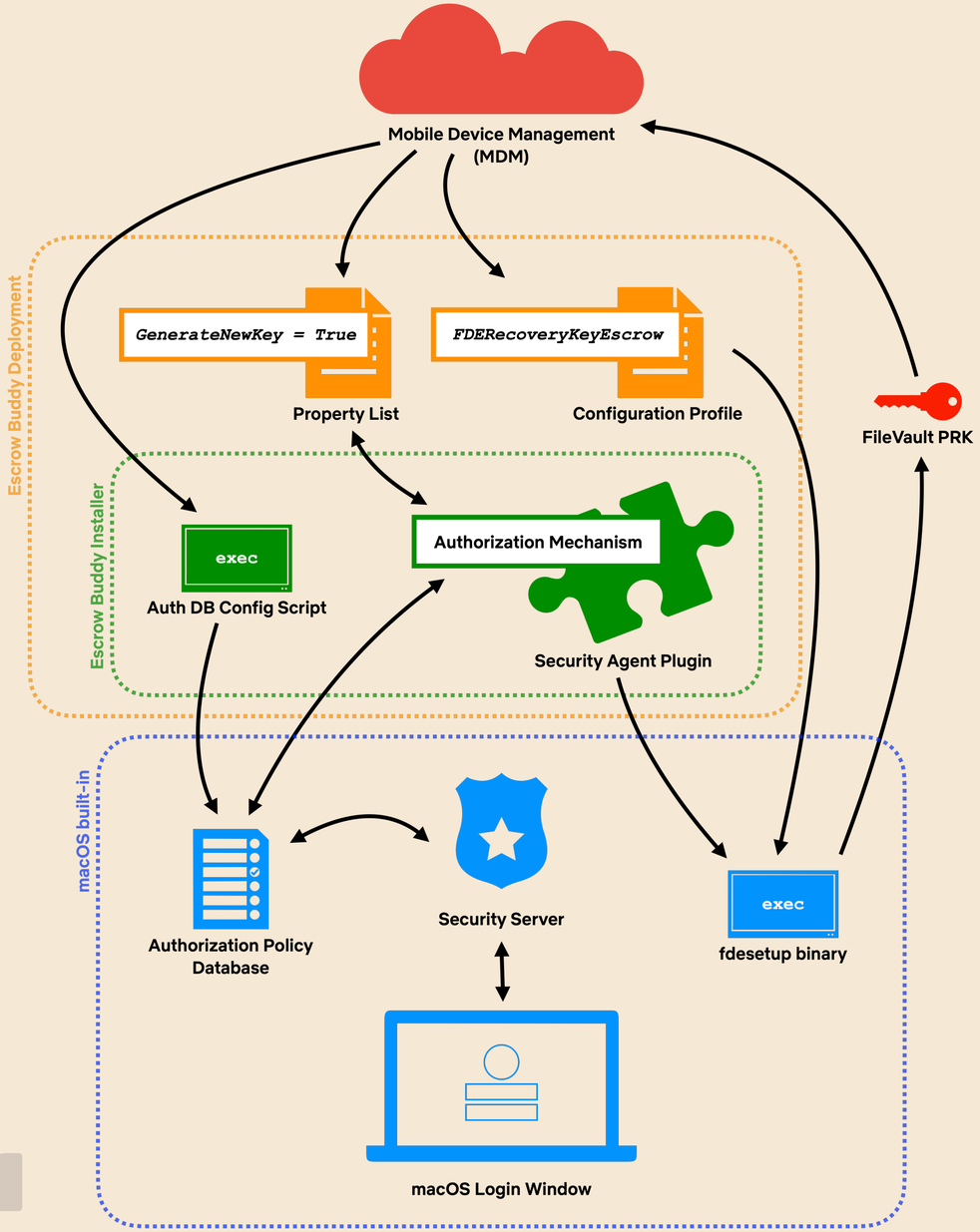


~~https://github.com/homebysix/jss-filevault-reissue~~

The new way is better...

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

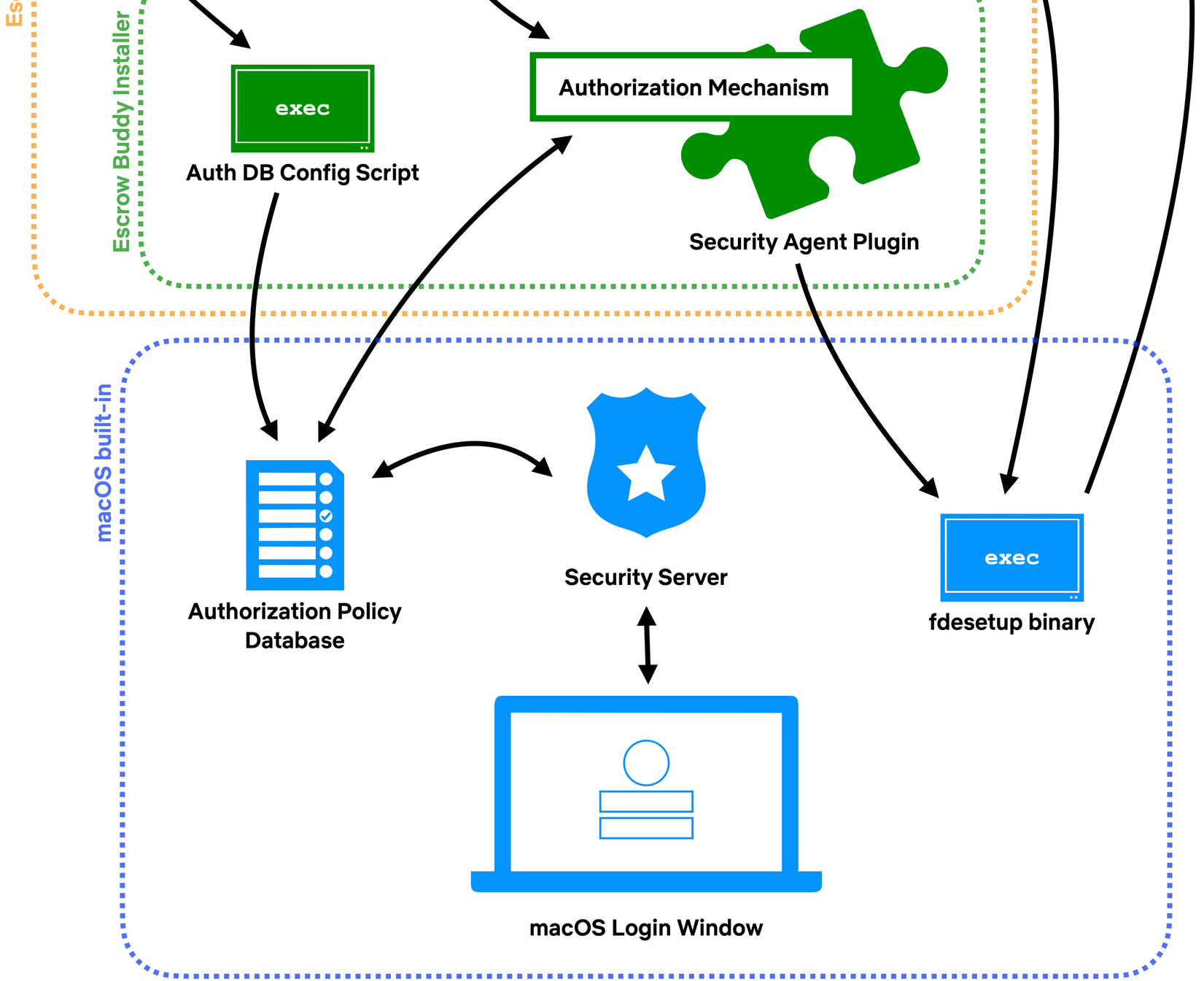


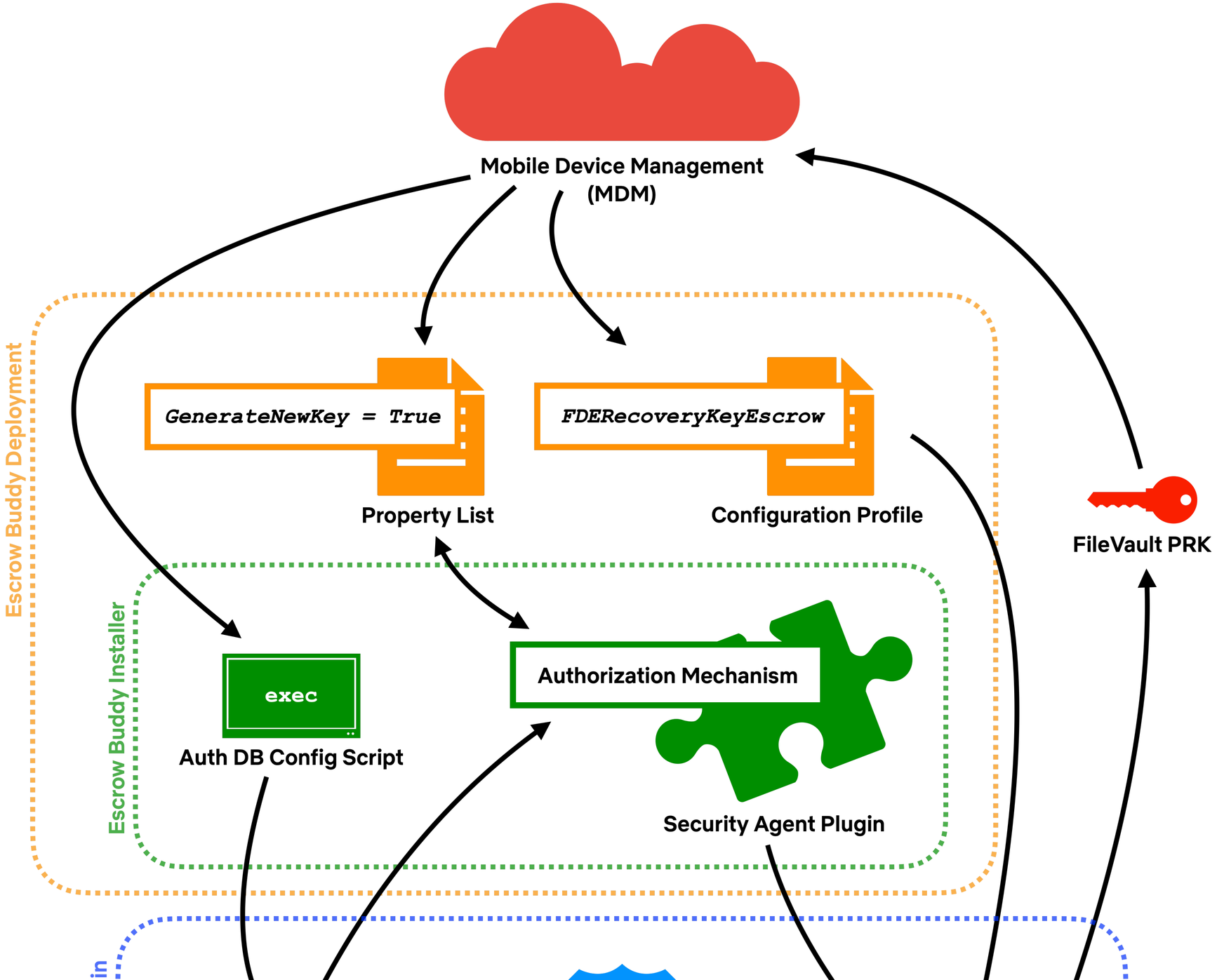


The new way:

authorization plugin

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


Escrow Buddy Installer
exec
Auth DB Config Script
Authorization Mechanism
Security Agent Plugin
macOS built-in
Authorization Policy Database
Security Server
exec
fdesetup binary
macOS Login Window

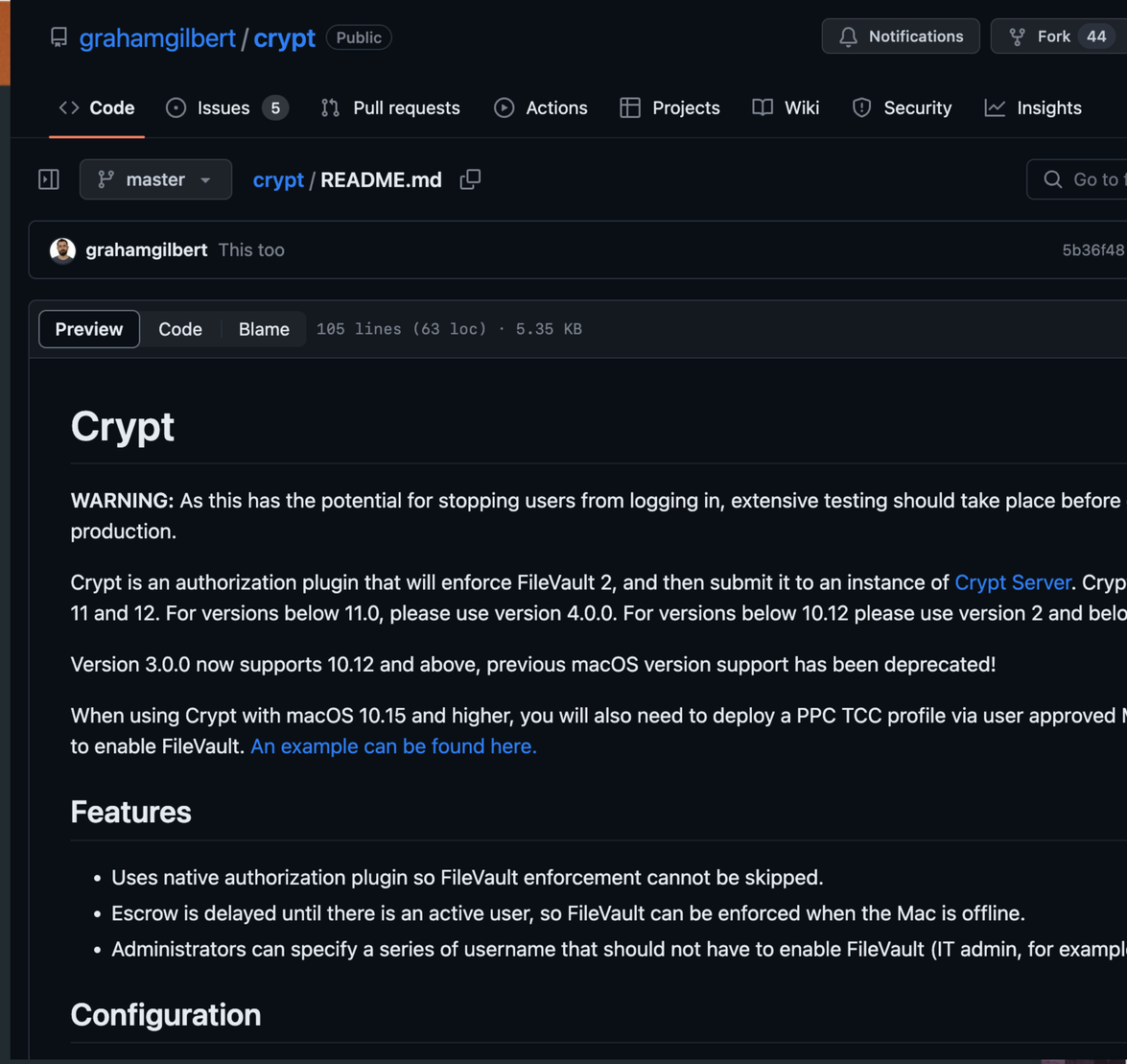

Mobile Device Management
(MDM)
Escrow Buddy Deployment
GenerateNewKey = True
Property List
FDERecoveryKeyEscrow
Configuration Profile
FileVault PRK
Escrow Buddy Installer
exec
Auth DB Config Script
Authorization Mechanism
Security Agent Plugin

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.)



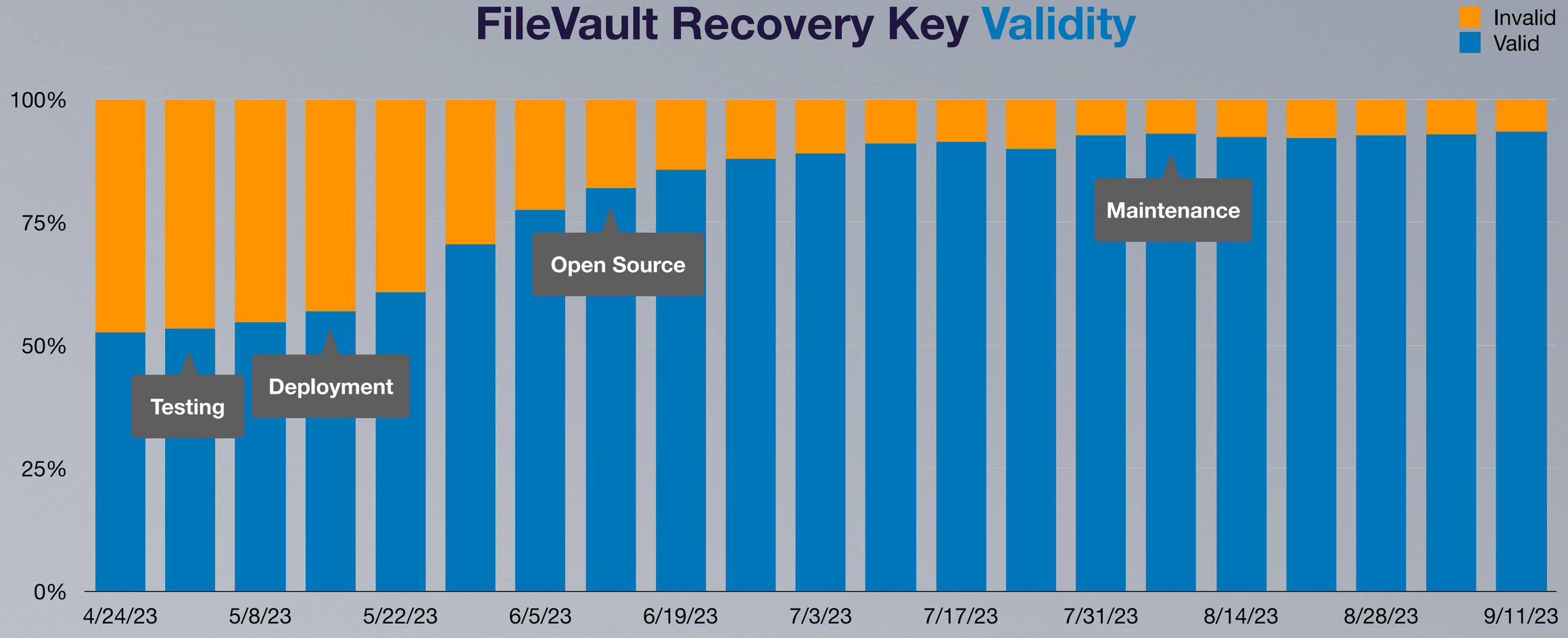
https://github.com/grahamgilbert/crypt/

Escrow Buddy

makes it simple

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

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



Our Success Story

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

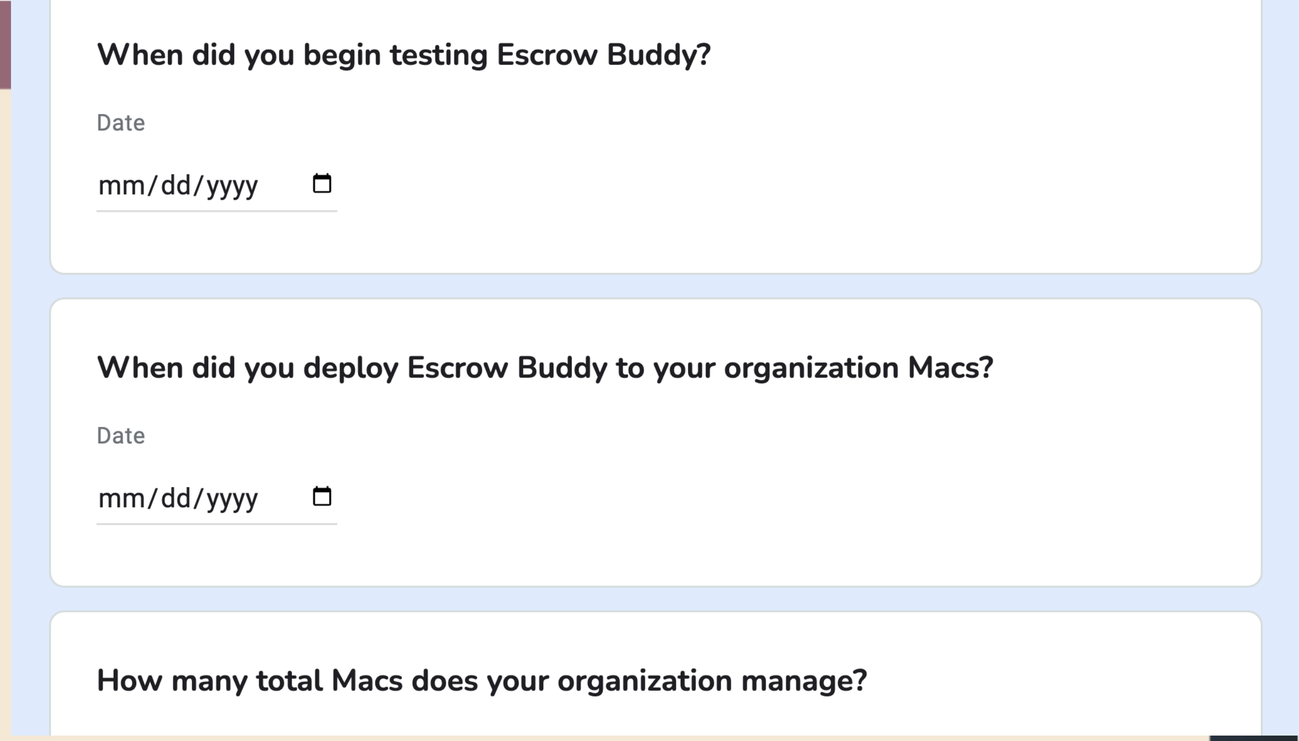
https://github.com/macadmins/escrow-buddy/wiki/Jamf

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

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

https://tinyurl.com/JNUC23-EB

Thank you for listening!

https://tinyurl.com/JNUC23-EB