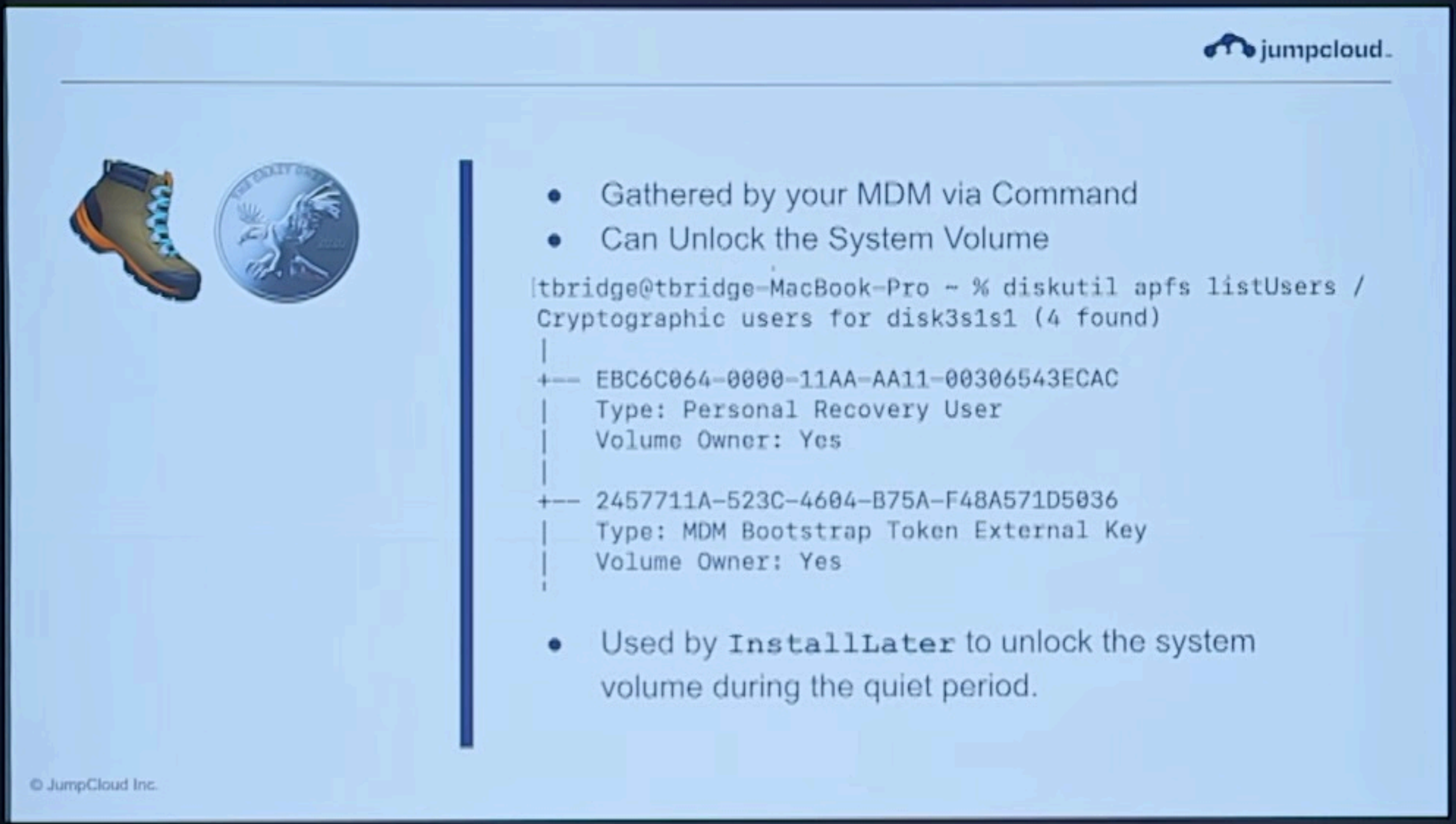
# Bootstrap token in 2 minutes

Arek Dreyer | Senior Product Engineer

6 October 2023



- Gathered by your MDM via Command
- Can Unlock the System Volume

```
tbridge@tbridge-MacBook-Pro ~ % diskutil apfs listUsers /
Cryptographic users for disk3s1s1 (4 found)
|
+-- EBC6C064-0000-11AA-AA11-00306543ECAC
|   Type: Personal Recovery User
|   Volume Owner: Yes
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
|   Type: MDM Bootstrap Token External Key
|   Volume Owner: Yes
|
```

- Used by `InstallLater` to unlock the system volume during the quiet period.

# Explain 2 minutes or less

55 minutes so you can explain it in 2 minutes

Not a session about Kandji

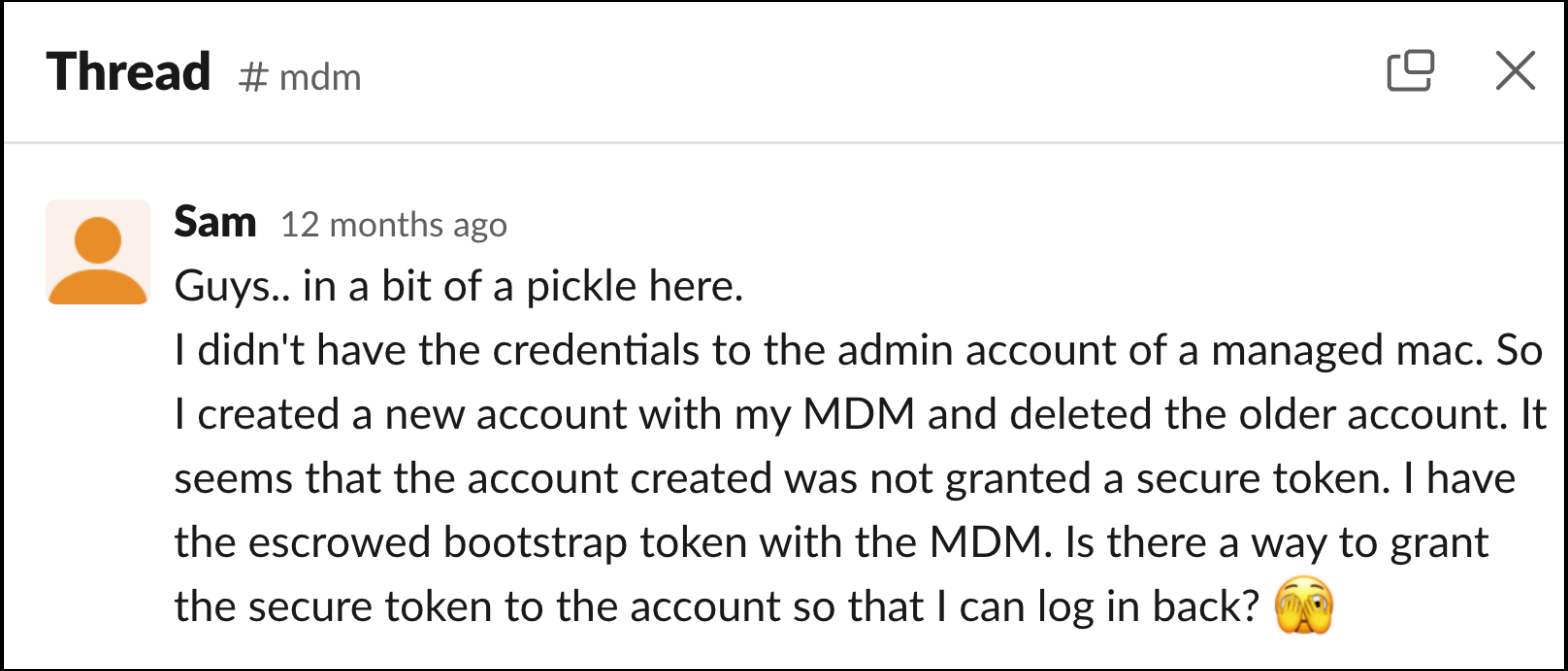
Collection of information from other people

bootstrap token is mostly about secure token

# Tear down the wall between IT and InfoSec.

kandji

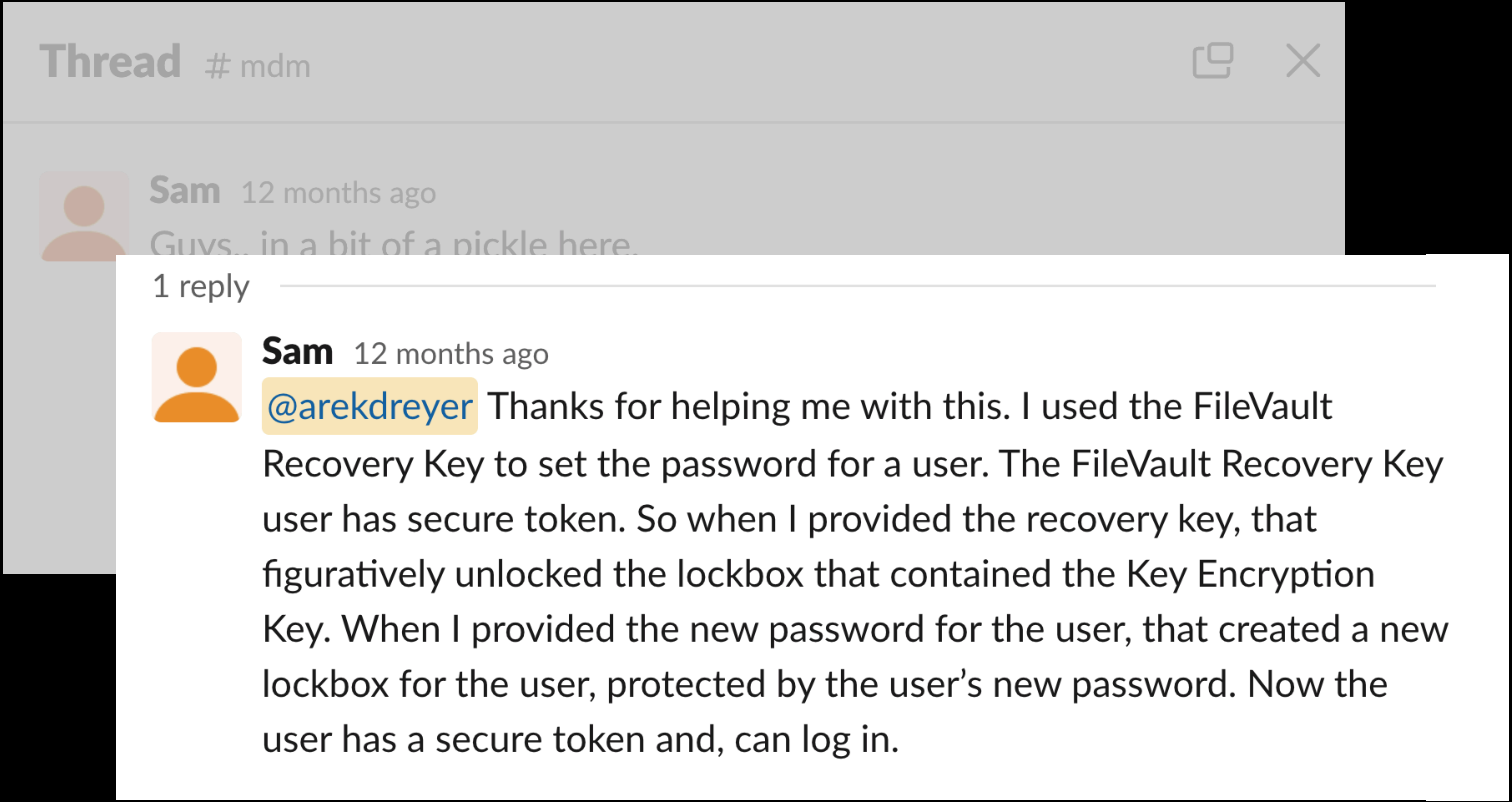
Device Harmony for your Apple fleet.



**Sam** 12 months ago

Guys.. in a bit of a pickle here.

I didn't have the credentials to the admin account of a managed mac. So I created a new account with my MDM and deleted the older account. It seems that the account created was not granted a secure token. I have the escrowed bootstrap token with the MDM. Is there a way to grant the secure token to the account so that I can log in back? 🫣



**Sam** 12 months ago

Guys.. in a bit of a pickle here.

**Sam** 12 months ago

@arekdreyer Thanks for helping me with this. I used the FileVault Recovery Key to set the password for a user. The FileVault Recovery Key user has secure token. So when I provided the recovery key, that figuratively unlocked the lockbox that contained the Key Encryption Key. When I provided the new password for the user, that created a new lockbox for the user, protected by the user's new password. Now the user has a secure token and, can log in.

MacAdmins.org
macadmins.org
MAC ADMINS FOUNDATION
News
Slack
Foundation
Donate
JOIN SLACK NOW

The Mac Admins Slack is a service provided by the Mac Admins Foundation, a 501(c)3 non-profit organization, for the betterment of the Mac Admins Community.

By requesting an invitation to The Mac Admins Slack workspace, you agree to abide by our Code of Conduct.

Already a member of the Mac Admins Slack? Sign in here.

Visit the Mac Admins Github for community projects.

*If you represent a vendor interested in engaging with the Mac Admins community please review our vendor*

of Conduct are adhered to.

Be a valuable postive contributor to this community.

Be respectful of others, ask people to stop if you are bothered; respect privacy; understand this community is primarily not-for-profit, and attempt to resolve issues without Administrators, but if you can't resolve an issue, you can contact the Administrators. If you violate this Code of Conduct, it will be made clear to you, and you may be asked to leave the Mac Admins Slack.

All community members are expected to:

- respect differences in people, their ideas and opinions
- treat one another with dignity and respect
- respect and treat others fairly, regardless of race ancestry, place of origin, colour, ethnic origin, citizenship, religion, gender, sexual orientation, age or disability
- respect the rights of others

# Tools and talk

# A brief trip to Australia

CREDIT SUISSE

Ag
C
T

-00:07:20
1/1
XworldDreyer.mp4
00:00:00
-00:07:20
1/1
seek

veggie blend
immunity hit
beetroot, carrot, orange, pear & ginger
30% less sugar
nudie
2SAN
LYHER
Novel Coronavirus (COVID-19 (Colloidal Gold) for self-testing
SARS-Cov-2 Antigen Rapid Tests for self-testing
5 Tests NASAL
COVID-19 Antigen Test Kit
For in vitro diagnostic use only
Panadol
Rapid
Paracetamol 500 mg
20 caplets
Fast Pain Relief
REMY ROO
Milk Chocolate
ARNOTT'S
TimTam
Original
SUITABLE FOR MICROWAVE OVENS
FOR RE-HEATING PURPOSES ONLY
OPEN

Donate — MacAdmins.org
macadmins.org/donate

## Thank you for supporting the Mac Admins community by donating to the Mac Admins Foundation!

The Mac Admins Foundation is here to support the global community of people who manage Apple devices at large and small scales. Join us by making a gift today and help us maintain affordable access to all community resources and support Mac Admins Foundation programming and initiatives.

Select your donation amount and frequency

What does my donation to the Mac Admins Foundation do? +

Can my company sponsor the Mac Admins Foundation? +

Can I donate via check/ACH to the Mac Admins Foundation? +

Can I donate with Apple Pay/Google Pay? +

Can I donate with PayPal? +

How can I contact the Mac Admins Foundation? +

One more thing about Slack:
#appleseed channel

Pinned by **kish.jayson**

Friday, August 4th ⌄

**kish.jayson** 6:06 AM

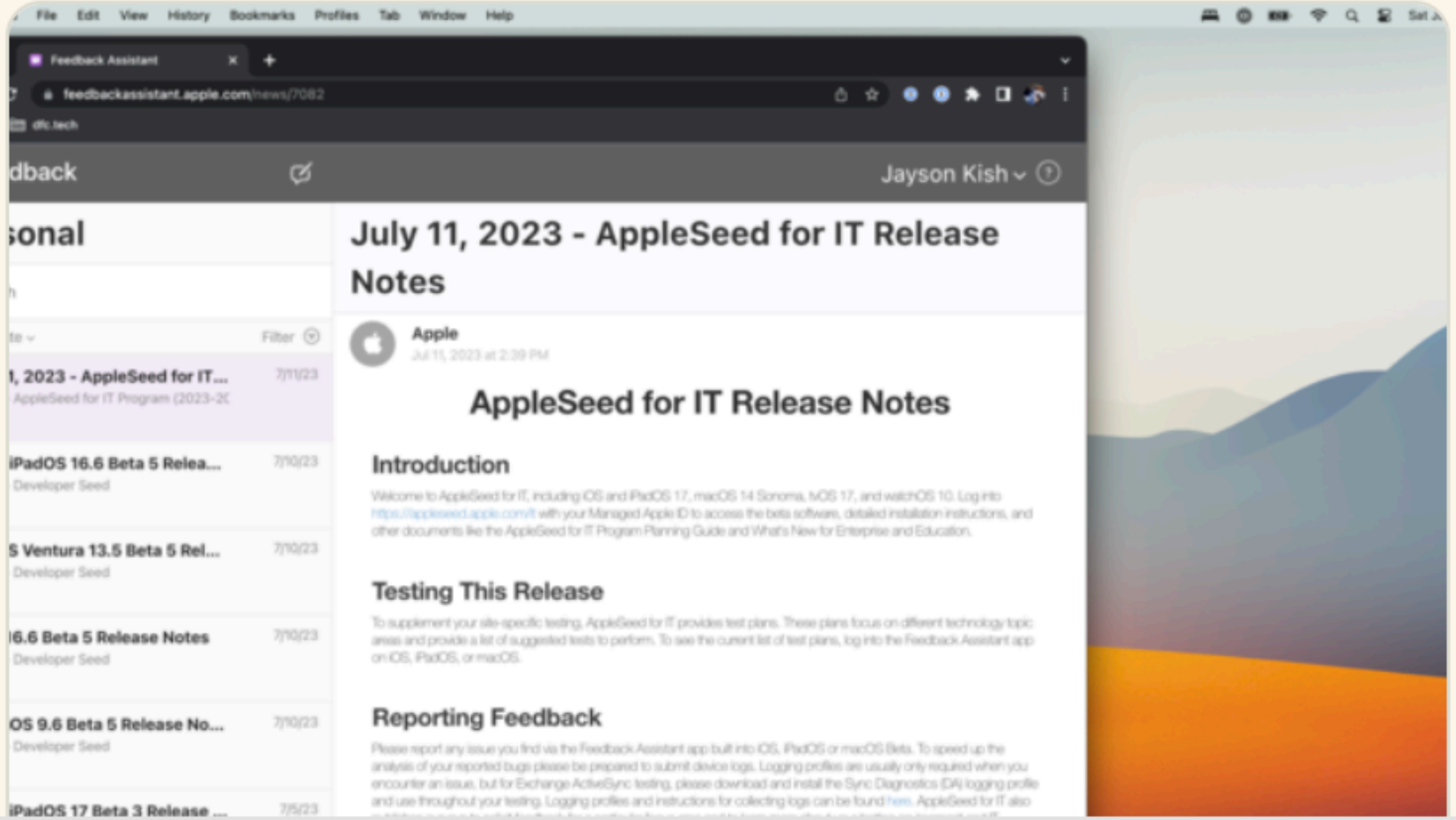
Hi All,

To get access to the sekret channel, please DM one of the custodians listed below an un-cropped screenshot of your Managed Apple ID from Feedback Assistant or Software Update in System Settings (examples below).

@kish.jayson (North America)
@yohan (North America)
@smithjw (Australia)
@hcodfrie (Europe)

Participation in AppleSeed for IT requires a Managed Apple ID provided by your organization from either Apple School Manager or Apple Business Manager. Those enrolled in the Apple Developer Program or Apple Beta Software Program alone do not qualify for access at this time.

3 files ▾


File Edit View History Bookmarks Profiles Tab Window Help
Feedback Assistant
feedbackassistant.apple.com/news/7082
dfc.tech
dback
Jayson Kish
sonal
Filter
1, 2023 - AppleSeed for IT... 7/11/23
AppleSeed for IT Program (2023-20
iPadOS 16.6 Beta 5 Relea... 7/10/23
Developer Seed
S Ventura 13.5 Beta 5 Rel... 7/10/23
Developer Seed
16.6 Beta 5 Release Notes 7/10/23
Developer Seed
OS 9.6 Beta 5 Release No... 7/10/23
Developer Seed
iPadOS 17 Beta 3 Release ... 7/5/23

July 11, 2023 - AppleSeed for IT Release Notes

Apple
Jul 11, 2023 at 2:39 PM

AppleSeed for IT Release Notes

Introduction

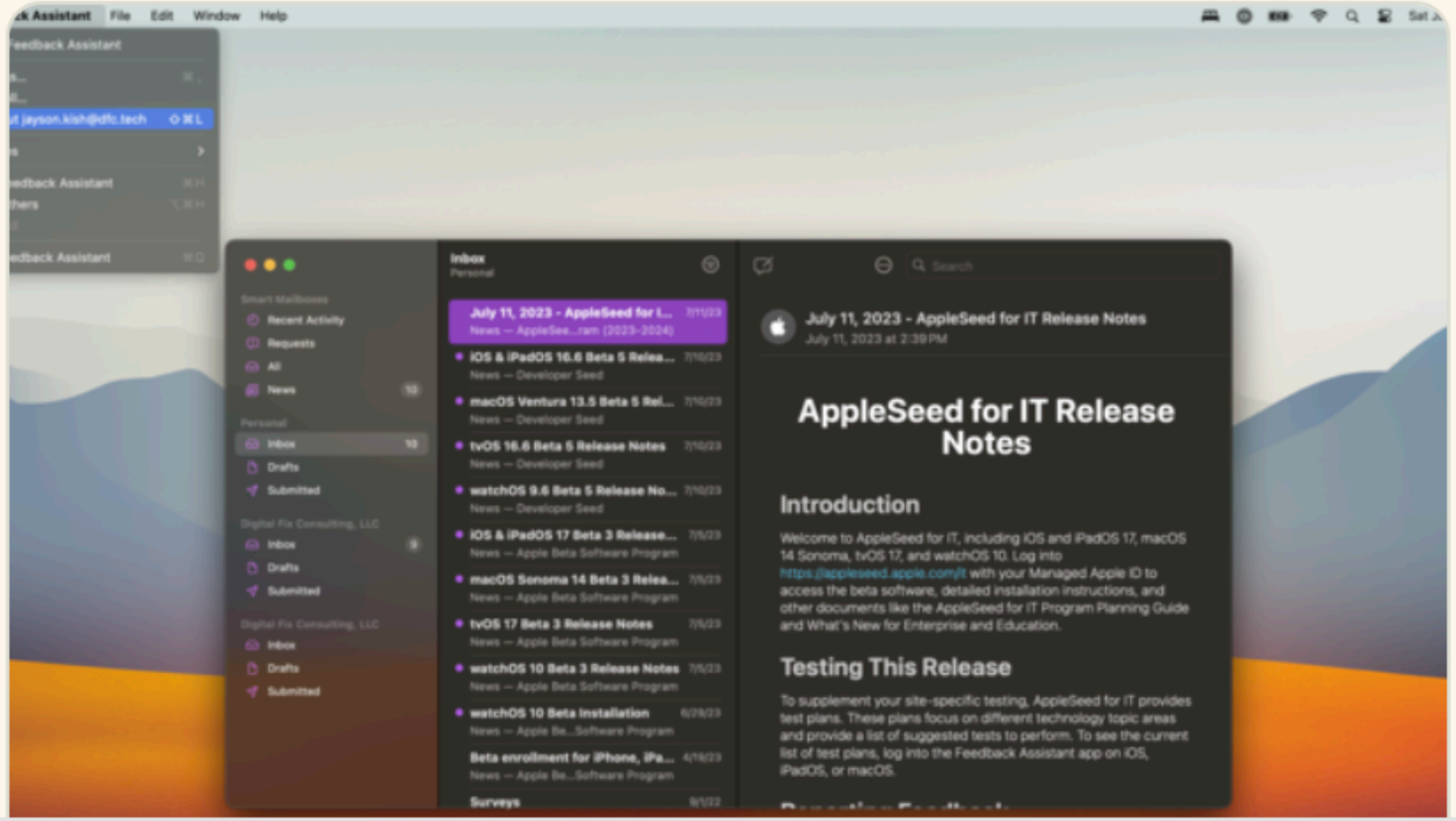
Welcome to AppleSeed for IT, including iOS and iPadOS 17, macOS 14 Sonoma, tvOS 17, and watchOS 10. Log into https://appleseed.apple.com/it with your Managed Apple ID to access the beta software, detailed installation instructions, and other documents like the AppleSeed for IT Program Planning Guide and What's New for Enterprise and Education.

Testing This Release

To supplement your site-specific testing, AppleSeed for IT provides test plans. These plans focus on different technology topic areas and provide a list of suggested tests to perform. To see the current list of test plans, log into the Feedback Assistant app on iOS, iPadOS, or macOS.

Reporting Feedback

Please report any issue you find via the Feedback Assistant app built into iOS, iPadOS or macOS Beta. To speed up the analysis of your reported bugs please be prepared to submit device logs. Logging profiles are usually only required when you encounter an issue, but for Exchange ActiveSync testing, please download and install the Sync Diagnostics (DA) logging profile and use throughout your testing. Logging profiles and instructions for collecting logs can be found here. AppleSeed for IT also


k Assistant File Edit Window Help
Feedback Assistant
t jayson.kish@dfc.tech ⇧⌘L
edback Assistant
thers
edback Assistant
Inbox
Personal
Smart Mailboxes
Recent Activity
Requests
All
News 10
Personal
Inbox 10
Drafts
Submitted
Digital Fix Consulting, LLC
Inbox 9
Drafts
Submitted
Digital Fix Consulting, LLC
Inbox
Drafts
Submitted
Search
July 11, 2023 - AppleSeed for I... 7/11/23
News — AppleSee...ram (2023-2024)
iOS & iPadOS 16.6 Beta 5 Relea... 7/10/23
News — Developer Seed
macOS Ventura 13.5 Beta 5 Rel... 7/10/23
News — Developer Seed
tvOS 16.6 Beta 5 Release Notes 7/10/23
News — Developer Seed
watchOS 9.6 Beta 5 Release No... 7/10/23
News — Developer Seed
iOS & iPadOS 17 Beta 3 Release... 7/5/23
News — Apple Beta Software Program
macOS Sonoma 14 Beta 3 Relea... 7/5/23
News — Apple Beta Software Program
tvOS 17 Beta 3 Release Notes 7/5/23
News — Apple Beta Software Program
watchOS 10 Beta 3 Release Notes 7/5/23
News — Apple Beta Software Program
watchOS 10 Beta Installation 6/29/23
News — Apple Be...Software Program
Beta enrollment for iPhone, iPa... 4/18/23
News — Apple Be...Software Program
Surveys 9/1/22

July 11, 2023 - AppleSeed for IT Release Notes
July 11, 2023 at 2:39 PM

AppleSeed for IT Release Notes

Introduction

Welcome to AppleSeed for IT, including iOS and iPadOS 17, macOS 14 Sonoma, tvOS 17, and watchOS 10. Log into https://appleseed.apple.com/it with your Managed Apple ID to access the beta software, detailed installation instructions, and other documents like the AppleSeed for IT Program Planning Guide and What's New for Enterprise and Education.

Testing This Release

To supplement your site-specific testing, AppleSeed for IT provides test plans. These plans focus on different technology topic areas and provide a list of suggested tests to perform. To see the current list of test plans, log into the Feedback Assistant app on iOS, iPadOS, or macOS.

# Goal: develop a mental model of secure token

So you can explain it

# Agenda

What else we'll cover today

01 **What's a secure token**

02 **How they are made**

03 **What are they used for**

04 **Where do they live**

What’s a secure token

How are they made

What are they used for

Where do they live

Tyvek
HomeWrap
DUPONT
MADE IN THE USA
Call 1-800-448-9835 tyvek.com/homewrap
ZIP System
FLASHING TAPE
WARNING
procom
2419

Tyvek
HomeWrap
THE HOME DEPOT
DUPONT

eWrap
DUPONT
Tyvek
HomeWrap
THE HOME DEPOT
Master Lock
Push Button Set-Your-Own Combination

Master Lock
Push Button
Set-Your-Own Combination
P8A278

1
abc 2
def 3
ghi 4
jkl 5
mno 6
pqrs 7
tuv 8
wxyz 9
#
0
*
C
Master Lock

Secure token is *kind of* like a lockbox

# Secure token

It’s like a lockbox

Secure token is a feature

A secure token is a thing

**We’ll define it later**

What’s a secure token

**How are they made**

What are they used for

Where do they live

# Volume encryption with FileVault in macOS

Mac computers offer FileVault, a built-in encryption capability, to secure all data at rest. FileVault uses the AES-XTS data encryption algorithm to protect full volumes on internal and removable storage devices.

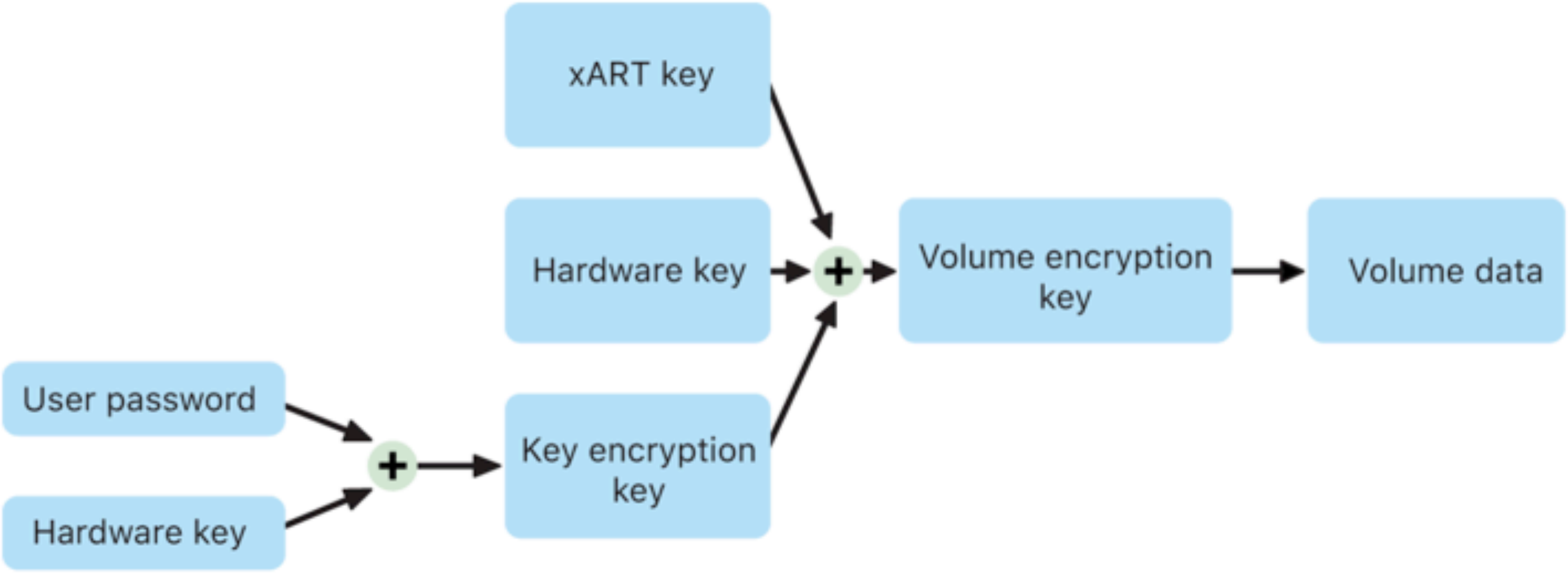
FileVault on a Mac with Apple silicon is implemented using Data Protection Class C with a volume key. On a Mac with the Apple T2 Security Chip as well as a Mac with Apple silicon, encrypted internal storage devices directly connected to the Secure Enclave leverage its hardware security capabilities as well as that of the AES engine. After a user turns on FileVault on a Mac, their credentials are required during the boot process.

## Internal storage with FileVault turned on

Without valid login credentials or a cryptographic recovery key, the internal APFS volumes remain encrypted and are protected from unauthorized access even if the physical storage device is removed and connected to another computer. In macOS 10.15, this includes both the system volume and the data volume. Starting in macOS 11, the system volume is protected by the signed system volume (SSV) feature, but the data volume remains protected by encryption. Internal volume encryption on a Mac with Apple silicon as well as those with the T2 chip is implemented by constructing and managing a hierarchy of keys, and builds on the hardware encryption technologies built into the chip. This hierarchy of keys is designed to simultaneously achieve four goals:

- Require the user's password for decryption
- Protect the system from a brute-force attack directly against storage media removed from Mac
- Provide a swift and secure method for wiping content via deletion of necessary cryptographic material

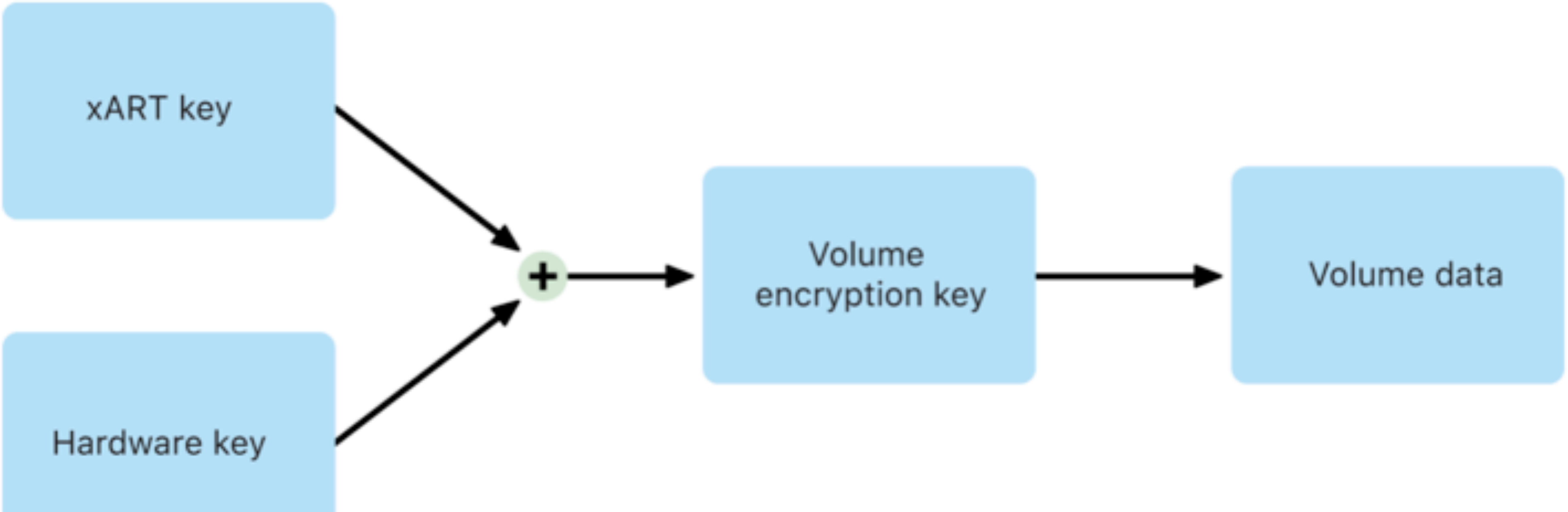
- Provide a swift and secure method for wiping content via deletion of necessary cryptographic material
- Enable users to change their password (and in turn the cryptographic keys used to protect their files) without requiring reencryption of the entire volume



On a Mac with Apple silicon and those with the T2 chip, all FileVault key handling occurs in the Secure Enclave; encryption keys are never directly exposed to the Intel CPU. All APFS volumes are created with a volume encryption key by default. Volume and metadata contents are encrypted with this volume encryption key, which is wrapped with the class key. The class key is protected by a combination of the user’s password and the hardware UID when FileVault is turned on.

## Internal storage with FileVault turned off

If FileVault isn’t turned on in a Mac with Apple silicon or a Mac with the T2 chip during the initial Setup Assistant process, the volume is still encrypted but the volume encryption key is protected only by the hardware UID in the Secure Enclave.



xART key
Hardware key
+
Volume encryption key
Volume data

# How a secure token is born

It’s really easy

(unless you have a weird workflow)

You log in

With your password

# Log in

Subhead lorem ipsum

It’s kind of like setting up a lock box

The following is important

You need the user’s cleartext password in order to make that first lockbox

The house key is now in the lockbox

The lockbox is protected by your passphrase

There are no unprotected versions of the key

But next user also needs access to the key

Need to unlock the first user’s lockbox in order to get the key

Need the cleartext password to unlock the first lockbox

The key is copied and placed into the second user’s lockbox

The second user’s lockbox is protected by the second user’s passcode.

The same key is in two different lockboxes. Each lockbox is protected by a different user's key.

Passwords aren’t stored on disk.

Instead, macOS uses wrapping.

Apple-File-System-Reference.pdf
Page 1 of 181
Search
Apple-File-System-Refer...
Apple File System Reference
Developer
1
Contents
2

# Apple File System Reference

Apple File System supports encryption in the data structures used for containers, volumes, and files. When a volume is encrypted, both its file-system tree and the contents of files in that volume are encrypted.

Depending on the device's capabilities, Apple File System uses either hardware or software encryption, which impacts encryption process and the meaning of several data structures. Hardware encryption is used for internal storage on devices that support it, including macOS (with T2 security chip) and iOS devices. Software encryption is used for external storage, and for internal storage on devices that don't support hardware encryption. When hardware encryption is in use, only the kernel can interact with internal storage.

> **Important**
>
> This document describes only software encryption.

The keys used to access file data are stored on disk in a wrapped state. You access these keys through a chain of key-unwrapping operations. The *volume encryption key* (VEK) is the default key used to access encrypted content on the volume. The *key encryption key* (KEK) is used to unwrap the VEK. The KEK is unwrapped in one of several ways:

- **User password.** The user enters their password, which is used to unwrap the KEK.
- **Personal recovery key.** This key is generated when the drive is formatted and is saved by the user on a paper printout. The string on that printout is used to unwrap the KEK.
- **Institutional recovery key.** This key is enabled by the user in Settings and allows the corresponding corporate master key to unwrap the KEK.
- **iCloud recovery key.** This key is used by customers working with Apple Support, and isn't described in this document.

For example, to access a file given the user's password on a volume that uses per-volume encryption, the chain of key unwrapping and data decryption consists of the following high-level operations:

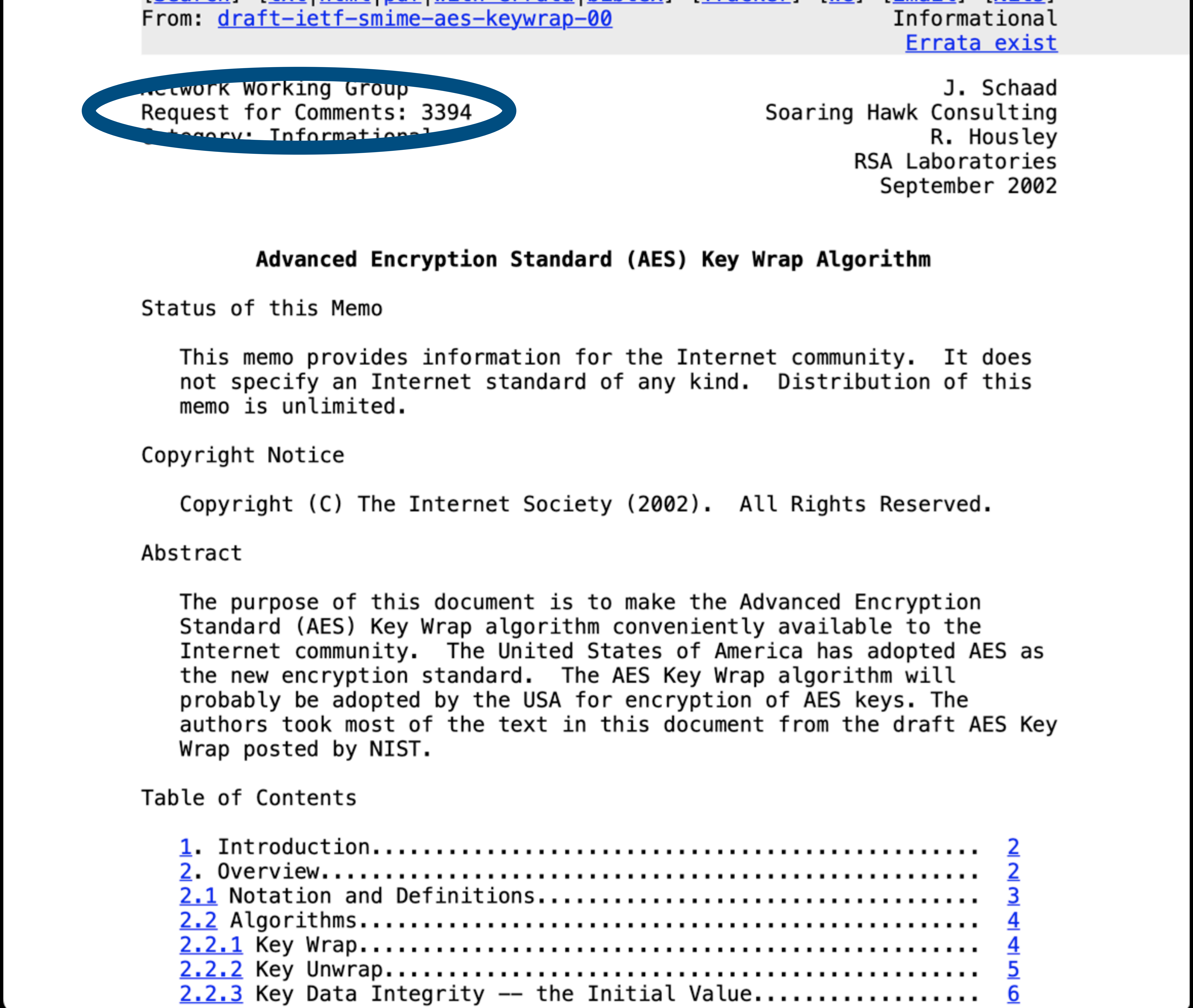
1. Unwrap the KEK using the user's password.

133
134
135
136

use per-file encryption require hardware encryption, and the steps below describe only software encryption.

To obtain the unwrapped VEK for a volume, do the following:

1. Locate the container's keybag using the `nx_keylocker` field of `nx_superblock_t`.
2. Unwrap the container's keybag using the container's UUID, according to the algorithm described in RFC 3394.
3. Find an entry in the container's keybag whose UUID matches the volume's UUID and whose tag is `KB_TAG_VOLUME_KEY`. The key data for that entry is the wrapped VEK for this volume.
4. Find an entry in the container's keybag whose UUID matches the volume's UUID and whose tag is `KB_TAG_VOLUME_UNLOCK_RECORDS`. The key data for that entry is the location of the volume's keybag.
5. Unwrap the volume's keybag using the volume's UUID according to the algorithm described in RFC 3394.
6. Find an entry in the volume's keybag whose UUID matches the user's Open Directory UUID and whose tag is `KB_TAG_VOLUME_UNLOCK_RECORDS`. The key data for that entry is the wrapped KEK for this volume.
7. Unwrap the KEK using the user's password, and then unwrap the VEK using the KEK, both according to the algorithm described in RFC 3394.



[Search] [txt|html|pdf|with errata|bibtex] [Tracker] [WG] [Email] [Nits]

From: draft-ietf-smime-aes-keywrap-00 Informational

Errata exist

Network Working Group
Request for Comments: 3394
Category: Informational

J. Schaad
Soaring Hawk Consulting
R. Housley
RSA Laboratories
September 2002

## Advanced Encryption Standard (AES) Key Wrap Algorithm

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

The purpose of this document is to make the Advanced Encryption Standard (AES) Key Wrap algorithm conveniently available to the Internet community. The United States of America has adopted AES as the new encryption standard. The AES Key Wrap algorithm will probably be adopted by the USA for encryption of AES keys. The authors took most of the text in this document from the draft AES Key Wrap posted by NIST.

Table of Contents

datatracker.ietf.org

## 2. Overview

The AES key wrap algorithm is designed to wrap or encrypt key data. The key wrap operates on blocks of 64 bits. Before being wrapped, the key data is parsed into n blocks of 64 bits.

The only restriction the key wrap algorithm places on n is that n be at least two. (For key data with length less than or equal to 64 bits, the constant field used in this specification and the key data form a single 128-bit codebook input making this key wrap unnecessary.) The key wrap algorithm accommodates all supported AES key sizes. However, other cryptographic values often need to be wrapped. One such value is the seed of the random number generator for DSS. This seed value requires n to be greater than four. Undoubtedly other values require this type of protection. Therefore, no upper bound is imposed on n.

# Two possibilities

Success = a key!

Failure = data that is not a key

**RFC3304 decrypt attempt by applying cleartext passcode**

# What’s really inside the lockbox

The analogy of a key inside a lockbox isn’t quite right

# Strained Analogy

Secure token = lockbox

Passcode = combo for lockbox

What’s inside = intermediate key

# Intermediate Key

That can be used to create multiple other keys

It’s a key encryption key (KEK)

So a key encryption key (KEK)
is inside your lockbox

# Secure token

Apple File System (APFS) in macOS 10.13 or later changes how FileVault encryption keys are generated. In previous versions of macOS on CoreStorage volumes, the keys used in the FileVault encryption process were created when a user or organization turned on FileVault on a Mac. In macOS on APFS volumes, encryption keys are generated either during user creation, setting the first user's password, or during the first login by a user of the Mac. This implementation of the encryption keys, when they're generated, and how they're stored are all part of a feature known as *Secure token*. Specifically, a secure token is a wrapped version of a key encryption key (KEK) protected by a user's password.

When deploying FileVault on APFS, the user can continue to:

- Use existing tools and processes, such as a personal recovery key (PRK) that can be stored with a mobile device management (MDM) solution for escrow
- Create and use an institutional recovery key (IRK)
- Defer enablement of FileVault until a user logs in to or out of the Mac

In macOS 11 or later, setting the initial password for the very first user on the Mac results in that user being granted a secure token. In some workflows, that may not be the

# Key Encryption Key

Like an access pass

Or a token that grants access to other specific keys

Since the KEK is a token

And that token is secured

It’s a secured token

Hence the term secure token

# Let’s look at the Volume encryption key (VEK)

## Token involved with unsealing your protected data

Your KEK wraps the VEK

Your KEK also wraps your OIK

# OIK allows you to

Modify startup security settings (LocalPolicy) for your specific install of macOS

Authorize updates and upgrades

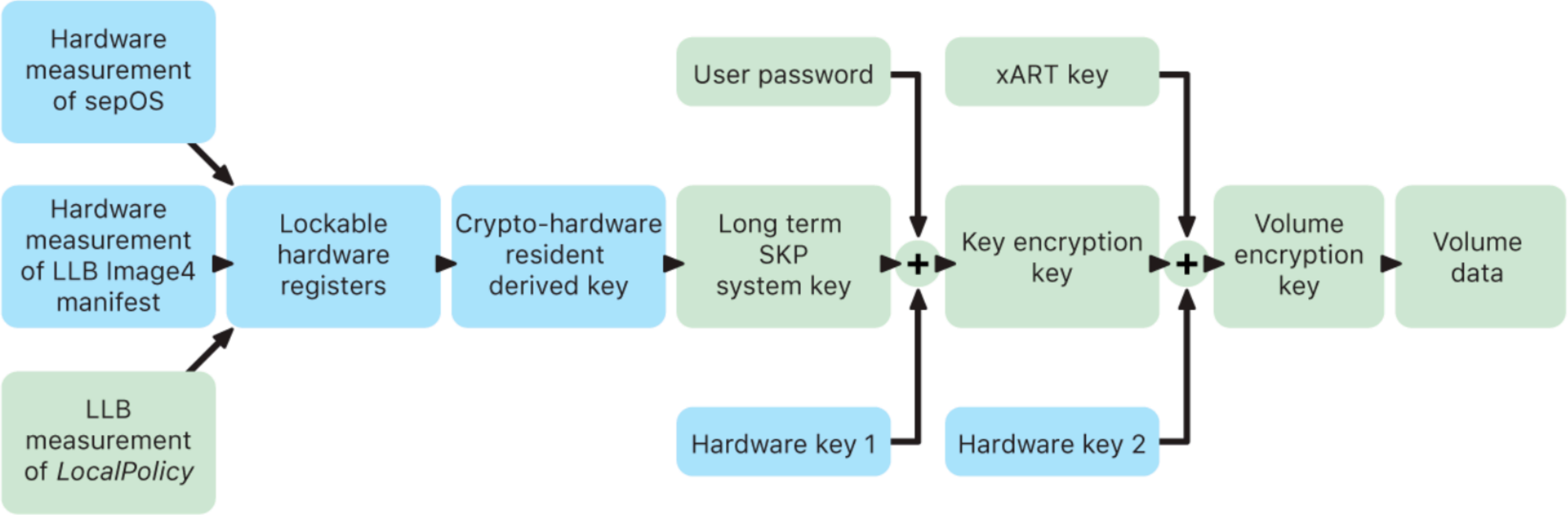
Authorize EACAS

More

## Owner identity key (OIK)

xART key
Hardware key
+
Volume encryption key
Volume data

xART key
Hardware key
Volume encryption key
Volume data
User password
Hardware key
Key encryption key
+
+


Hardware measurement of sepOS
Hardware measurement of LLB Image4 manifest
LLB measurement of *LocalPolicy*
Lockable hardware registers
Crypto-hardware resident derived key
User password
Long term SKP system key
Hardware key 1
+
xART key
Key encryption key
Hardware key 2
+
Volume encryption key
Volume data

What’s a secure token

How are they made

What are they used for

Where do they live

## But first a quick break from tokens

Patrick’s ChatGPT jokes were funny
Greg’s session was super interesting
BUT

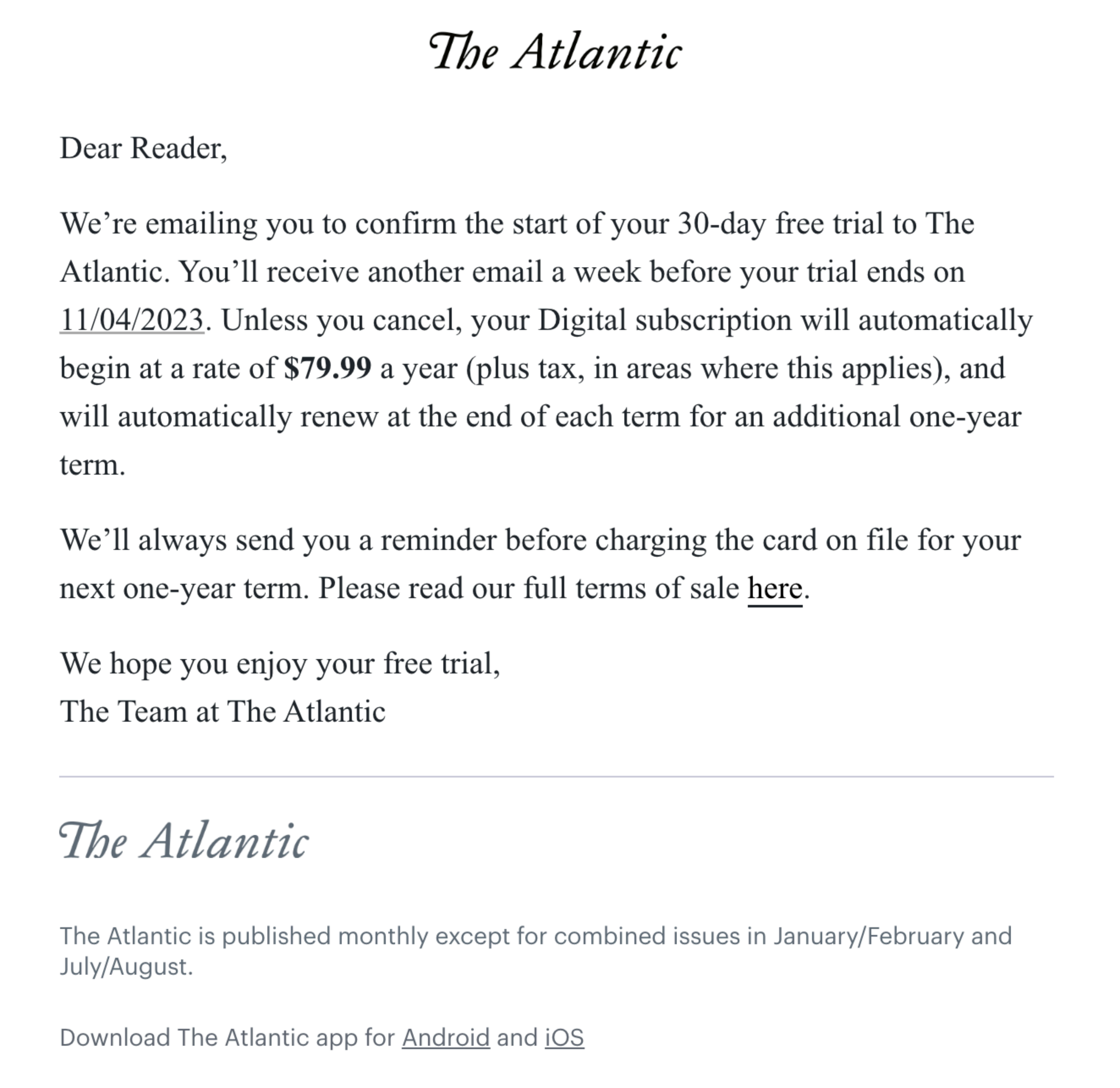
INDUSTRY & ADVOCACY NEWS

# You Just Found Out Your Book Was Used to Train AI. Now What?

This week, many authors discovered that their books were used without permission to train AI systems. Here's what you need to know if your books are in the Books3 dataset, as well as actions you can take now to speak out in defense of your rights.

*Artificial Intelligence*

September 27, 2023



The Atlantic

Dear Reader,

We’re emailing you to confirm the start of your 30-day free trial to The Atlantic. You’ll receive another email a week before your trial ends on 11/04/2023. Unless you cancel, your Digital subscription will automatically begin at a rate of **$79.99** a year (plus tax, in areas where this applies), and will automatically renew at the end of each term for an additional one-year term.

We’ll always send you a reminder before charging the card on file for your next one-year term. Please read our full terms of sale here.

We hope you enjoy your free trial,
The Team at The Atlantic

The Atlantic

The Atlantic is published monthly except for combined issues in January/February and July/August.

Download The Atlantic app for Android and iOS

You Just Found Out Your Book Was Used to Train AI. Now What? - The Authors Gu...
The Atlantic
These 183,000 Books Are Fueling the Biggest Fight in Publishing and Tech - The A...
Popular
Latest
Newsletters
The Atlantic
Saved Stories
My Account
Give a Gift

Before you begin, please note several caveats: Some books appear multiple times, reflecting different editions, translations, abridgments, or annotations. Because of inconsistencies in the spelling of author names, the search may not return books that are, in fact, in Books3. It may also deliver a jumble of odd formatting: A query for *Agatha Christie* will also return books labeled *Agatha Christie* and *Christie Agatha*, for example. And because of possible errors in the book-identification process, which involves detecting an ISBN within the text of the books and using a book database to find their author and title, there is a very small chance of false positives.

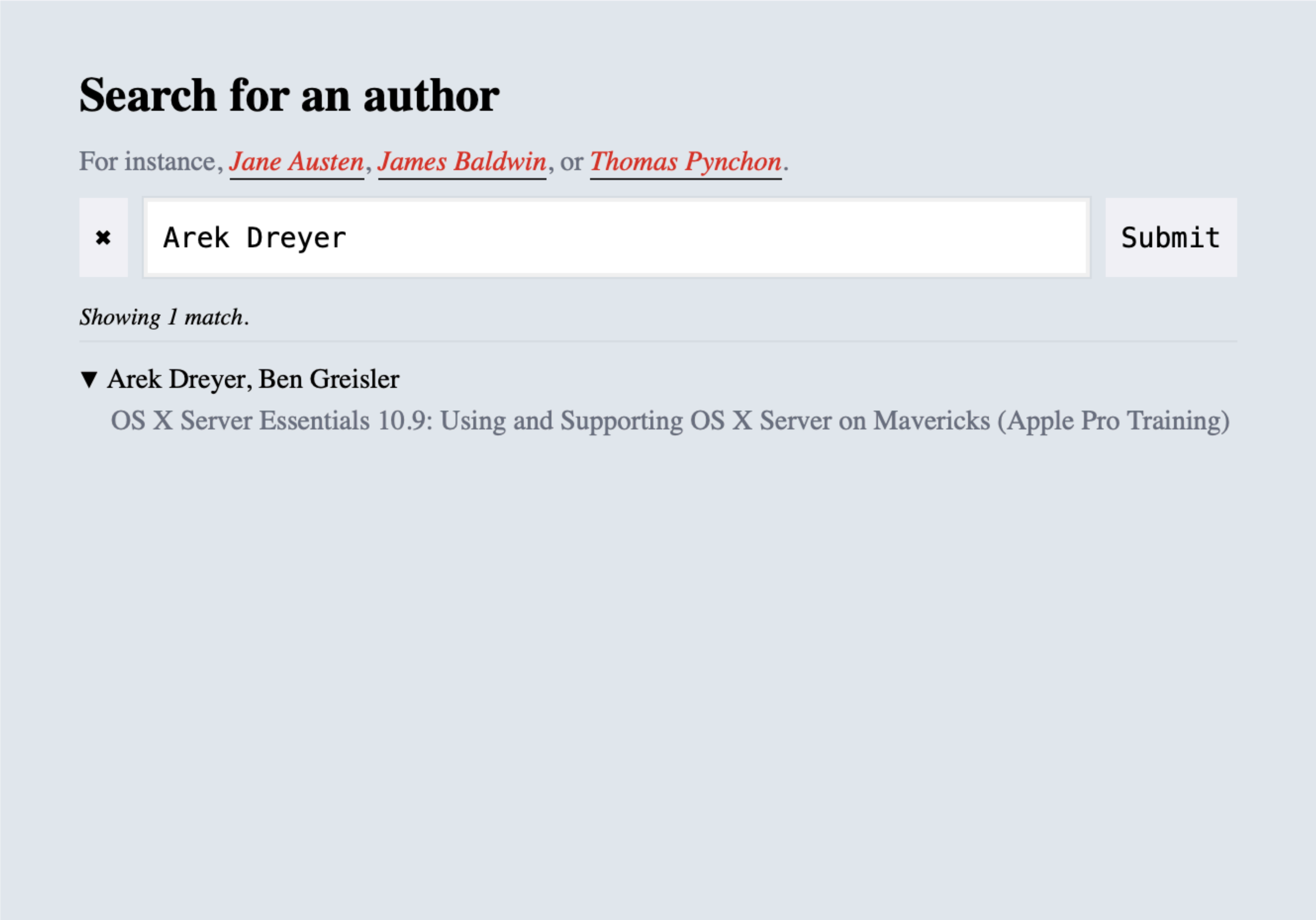
## Search for an author

For instance, *Jane Austen*, *James Baldwin*, or *Thomas Pynchon*.

✖ Arek Dreyer Submit

*Showing 1 match.*

▶ Arek Dreyer, Ben Greisler



# Search for an author

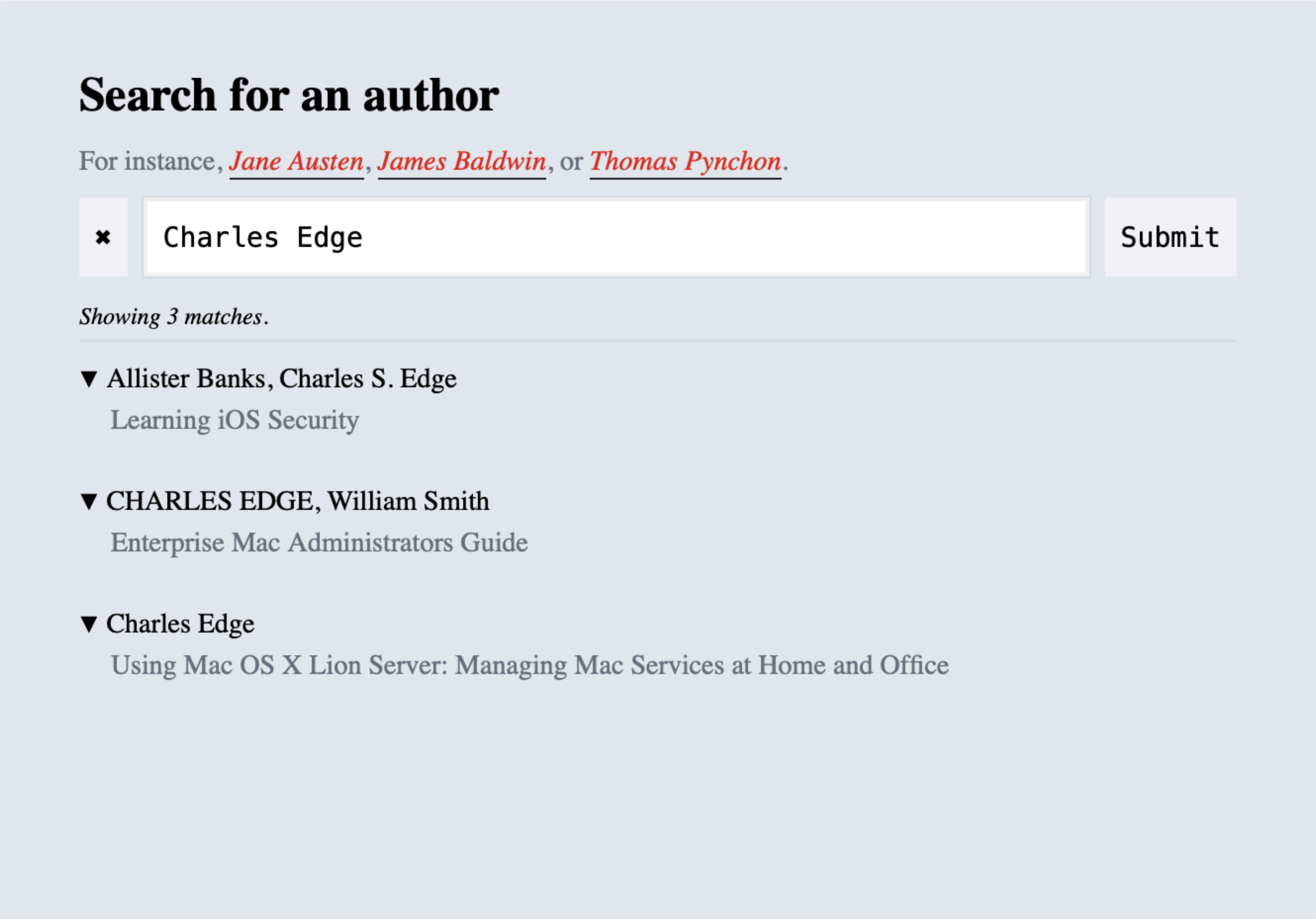
For instance, *Jane Austen*, *James Baldwin*, or *Thomas Pynchon*.

Arek Dreyer

*Showing 1 match.*

▼ Arek Dreyer, Ben Greisler

OS X Server Essentials 10.9: Using and Supporting OS X Server on Mavericks (Apple Pro Training)



## Search for an author

For instance, *Jane Austen*, *James Baldwin*, or *Thomas Pynchon*.

*Showing 3 matches.*

▼ Allister Banks, Charles S. Edge

Learning iOS Security

▼ CHARLES EDGE, William Smith

Enterprise Mac Administrators Guide

▼ Charles Edge

Using Mac OS X Lion Server: Managing Mac Services at Home and Office

What’s a secure token

How are they made

**What are they used for**

Where do they live

# What are they used for

- Sometimes just an access token
- Sometimes cryptographic element to sign things

# Intel based Mac

Prove you have the ability to change settings in recoveryOS

You have to be an admin (which you can change if you have root access)

You MUST have secure token

**Sometimes just an access token**

# Mac with Apple silicon

Apple changed the way you can modify boot settings

**Sometimes cryptographical element**

# Differences

Intel based Mac: NVRAM for entire Mac

Mac with Apple silicon: LocalPolicy for each install of macOS

**Sometimes cryptographical element**

# LocalPolicy

- Collection of boot settings for each install of macOS
- Cryptographically signed by the OIK

# After you change LocalPolicy

- Use your secure token to access the OIK
- Use the OIK to sign the LocaPolicy
- If the LocalPolicy isn’t signed the Mac won’t boot.

# Secure tokens are important

- encryption
- data protection

# Quick review

- After the first secure token is created, there are no more unprotected copies of the Volume encryption key (VEK)
- Making another secure token is like copying a key
- VEK is an example of a specific purpose key that gets wrapped by the KEK
- Your passcode opens only your secure token, to your access token (KEK), to access one of the many specific purpose keys like the VEK

# When you shut down your Mac

- You locked your startup volume

# Then these are not accessible

- All the data on the startup volume
- Internal directory info
- External directory info (AD, OD, IdP)
- MDM enrollment

# Locked but Mac has network available

- For Mac witih Apple silicon
- Even though you might have heard otherwise
- FileVault login window has a Wi-Fi connection indicator
- But the OS is not running and management is not available
- I wonder what the future holds here

# But there is some metadata outside

- Information about accounts that have secure token
- By default Mac displays an icon for every user
- For Mac with Apple silicon you can display fields instead

# If a Mac with FileVault starts

- No users available from external directory that don’t already exist on the Mac
- So they can’t log in

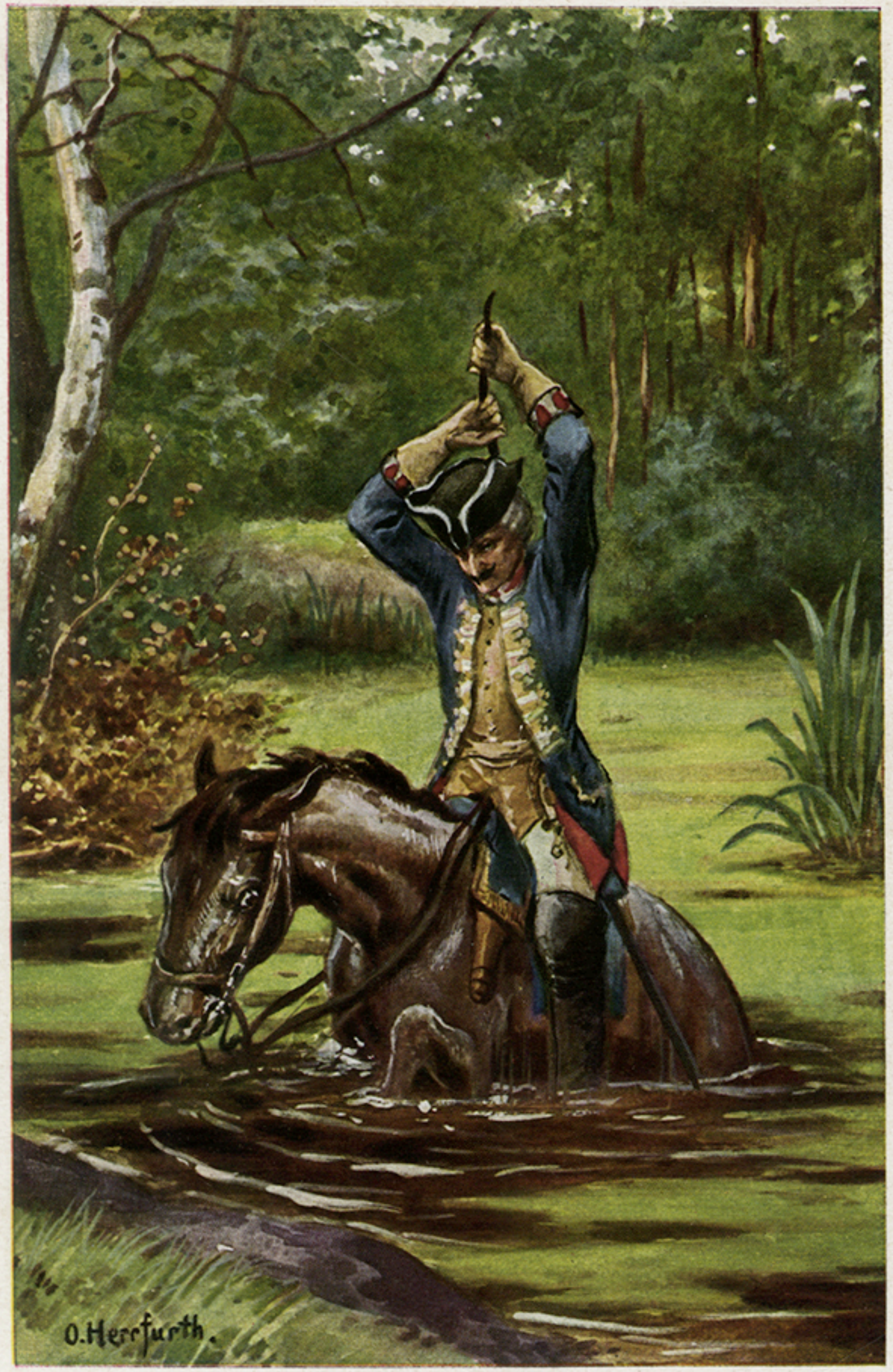
# Even if you could provide a new login

- That user couldn’t log in
- Because they don’t have a secure token
- Because making a new secure token is like copying a key

# Lifeline for mobile accounts in 10.15

- Bootstrap token

# A slight language diversion



Münchhauſen

O. Herrfurth pinx

https://flickr.com/photos/69184488@N06/

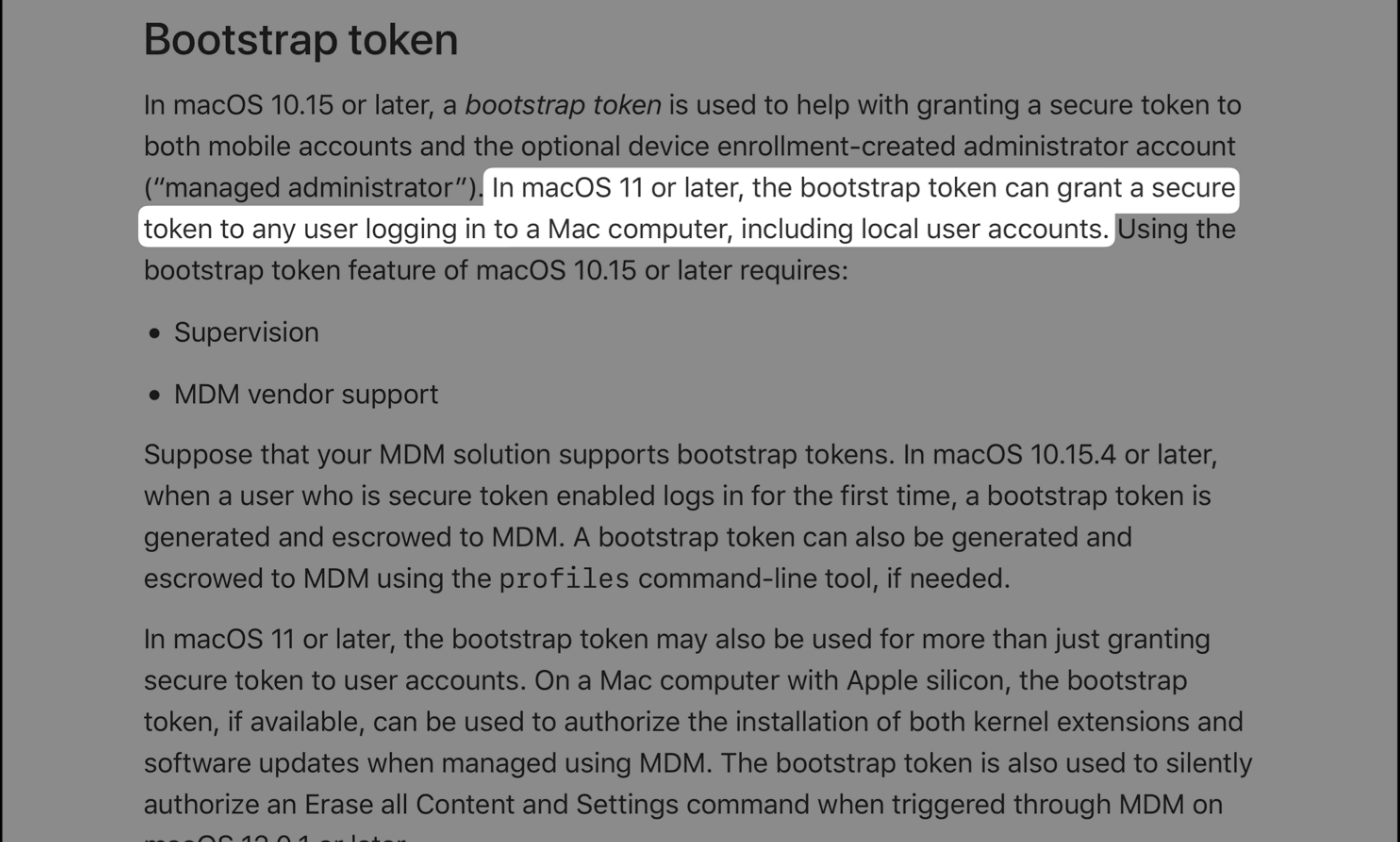
# Bootstrap token

In macOS 10.15 or later, a *bootstrap token* is used to help with granting a secure token to both mobile accounts and the optional device enrollment-created administrator account (“managed administrator”). In macOS 11 or later, the bootstrap token can grant a secure token to any user logging in to a Mac computer, including local user accounts. Using the bootstrap token feature of macOS 10.15 or later requires:

- Supervision
- MDM vendor support

Suppose that your MDM solution supports bootstrap tokens. In macOS 10.15.4 or later, when a user who is secure token enabled logs in for the first time, a bootstrap token is generated and escrowed to MDM. A bootstrap token can also be generated and escrowed to MDM using the `profiles` command-line tool, if needed.

In macOS 11 or later, the bootstrap token may also be used for more than just granting secure token to user accounts. On a Mac computer with Apple silicon, the bootstrap token, if available, can be used to authorize the installation of both kernel extensions and software updates when managed using MDM. The bootstrap token is also used to silently authorize an Erase all Content and Settings command when triggered through MDM on macOS 12.0.1 or later.



## Bootstrap token

In macOS 10.15 or later, a *bootstrap token* is used to help with granting a secure token to both mobile accounts and the optional device enrollment-created administrator account (“managed administrator”). In macOS 11 or later, the bootstrap token can grant a secure token to any user logging in to a Mac computer, including local user accounts. Using the bootstrap token feature of macOS 10.15 or later requires:

- Supervision
- MDM vendor support

Suppose that your MDM solution supports bootstrap tokens. In macOS 10.15.4 or later, when a user who is secure token enabled logs in for the first time, a bootstrap token is generated and escrowed to MDM. A bootstrap token can also be generated and escrowed to MDM using the `profiles` command-line tool, if needed.

In macOS 11 or later, the bootstrap token may also be used for more than just granting secure token to user accounts. On a Mac computer with Apple silicon, the bootstrap token, if available, can be used to authorize the installation of both kernel extensions and software updates when managed using MDM. The bootstrap token is also used to silently authorize an Erase all Content and Settings command when triggered through MDM on macOS 12.0.1 or later.

In macOS 10.15 or later, a *bootstrap token* is used to help with granting a secure token to both mobile accounts and the optional device enrollment-created administrator account (“managed administrator”). In macOS 11 or later, the bootstrap token can grant a secure token to any user logging in to a Mac computer, including local user accounts. Using the bootstrap token feature of macOS 10.15 or later requires:

- Supervision
- MDM vendor support

Suppose that your MDM solution supports bootstrap tokens. In macOS 10.15.4 or later, when a user who is secure token enabled logs in for the first time, a bootstrap token is generated and escrowed to MDM. A bootstrap token can also be generated and escrowed to MDM using the `profiles` command-line tool, if needed.

In macOS 11 or later, the bootstrap token may also be used for more than just granting secure token to user accounts. On a Mac computer with Apple silicon, the bootstrap token, if available, can be used to authorize the installation of both kernel extensions and software updates when managed using MDM. The bootstrap token is also used to silently authorize an Erase all Content and Settings command when triggered through MDM on macOS 12.0.1 or later.

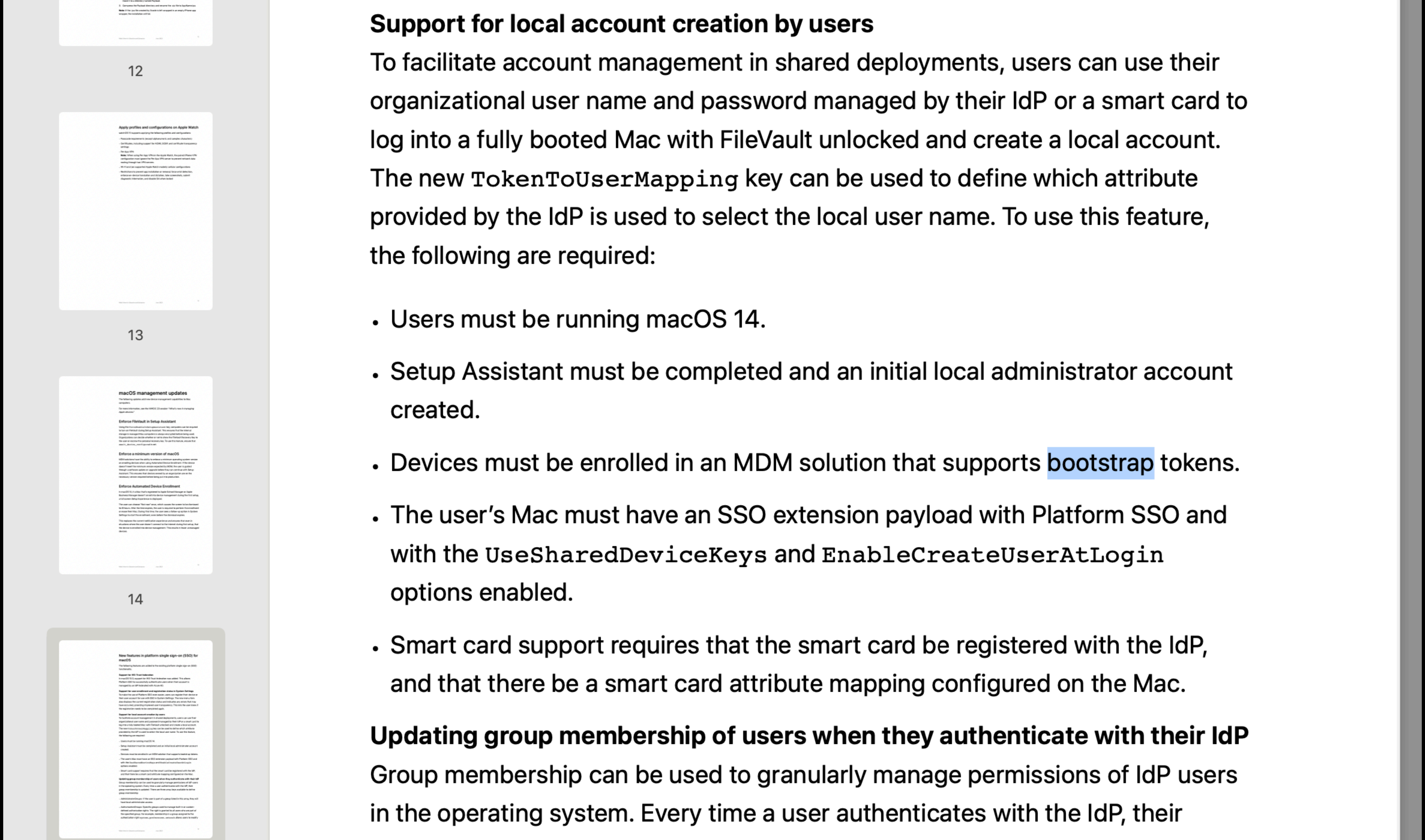
**Page 15** 1 match

• Devices must be enrolled in an MDM solution that support…

# What's New for Education and Enterprise

## WWDC

June 2023 (v1.0)



### Support for local account creation by users

To facilitate account management in shared deployments, users can use their organizational user name and password managed by their IdP or a smart card to log into a fully booted Mac with FileVault unlocked and create a local account. The new `TokenToUserMapping` key can be used to define which attribute provided by the IdP is used to select the local user name. To use this feature, the following are required:

- Users must be running macOS 14.
- Setup Assistant must be completed and an initial local administrator account created.
- Devices must be enrolled in an MDM solution that supports bootstrap tokens.
- The user's Mac must have an SSO extension payload with Platform SSO and with the `UseSharedDeviceKeys` and `EnableCreateUserAtLogin` options enabled.
- Smart card support requires that the smart card be registered with the IdP, and that there be a smart card attribute mapping configured on the Mac.

### Updating group membership of users when they authenticate with their IdP

Group membership can be used to granularly manage permissions of IdP users in the operating system. Every time a user authenticates with the IdP, their

# Do you want to talk about labs?

FileVault isn’t recommended when you don’t know who is going to log in after restart

# fdesetup authrestart

😭 Undocumented time limit

🫣 Restart script needs plaintext password

😵‍💫 Breaks after power loss

🤔 Similar to not turning FileVault on

## Why not be clever

What’s a secure token

How are they made

What are they used for

**Where do they live**

There in a keybag!

# Magic keybag

On the house

Not in the house

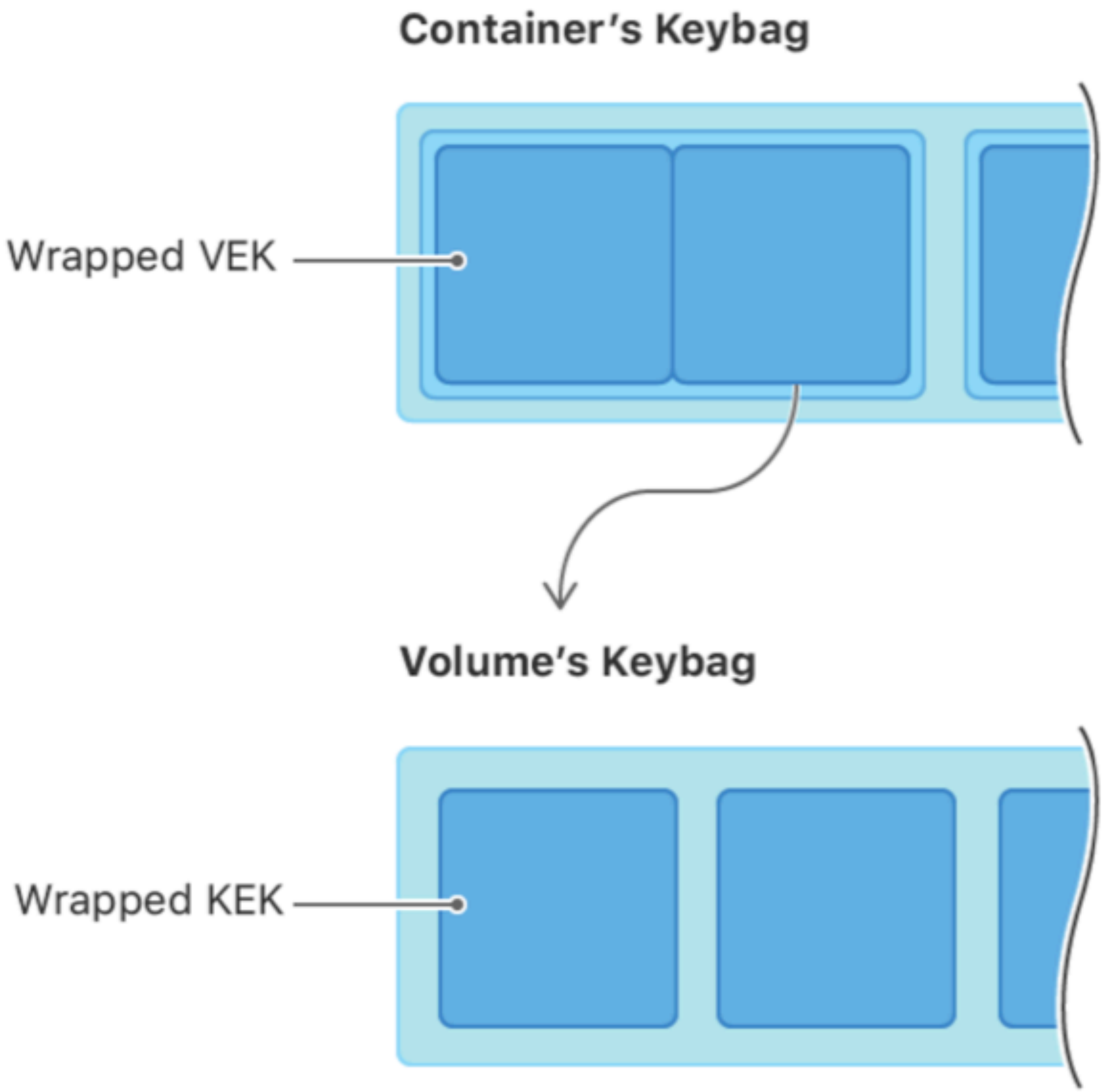
In a location everyone knows

## Back to the analogy

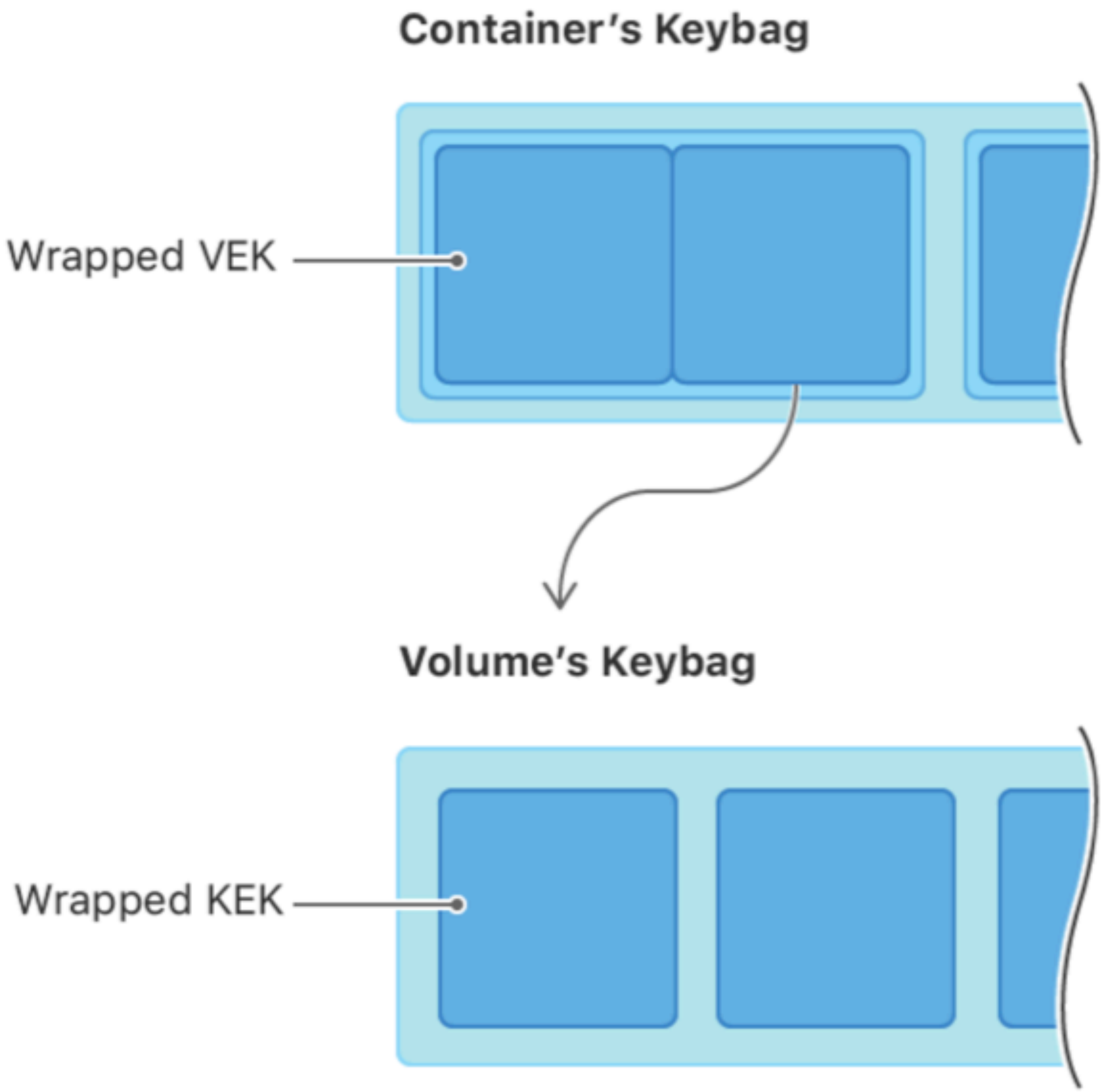
133

134

135



Keybags are encrypted using the UUID of the container or volume, which makes it possible to quickly and securely destroy the contents of an encrypted volume by changing or deleting the UUID. For a volume, destroying the UUID by securely erasing a volume superblock makes the corresponding keybag unreadable, which in turn makes the encrypted content of that volume inaccessible. For a container superblock, you need to destroy all of the copies of that block in the checkpoint descriptor area and the copy at block zero.



Keybags are encrypted using the UUID of the container or volume, which makes it possible to quickly and securely destroy the contents of an encrypted volume by changing or deleting the UUID. For a volume, destroying the UUID by securely erasing a volume superblock makes the corresponding keybag unreadable, which in turn makes the encrypted content of that volume inaccessible. For a container superblock, you need to destroy all of the copies of that block in the checkpoint descriptor area and the copy at block zero.

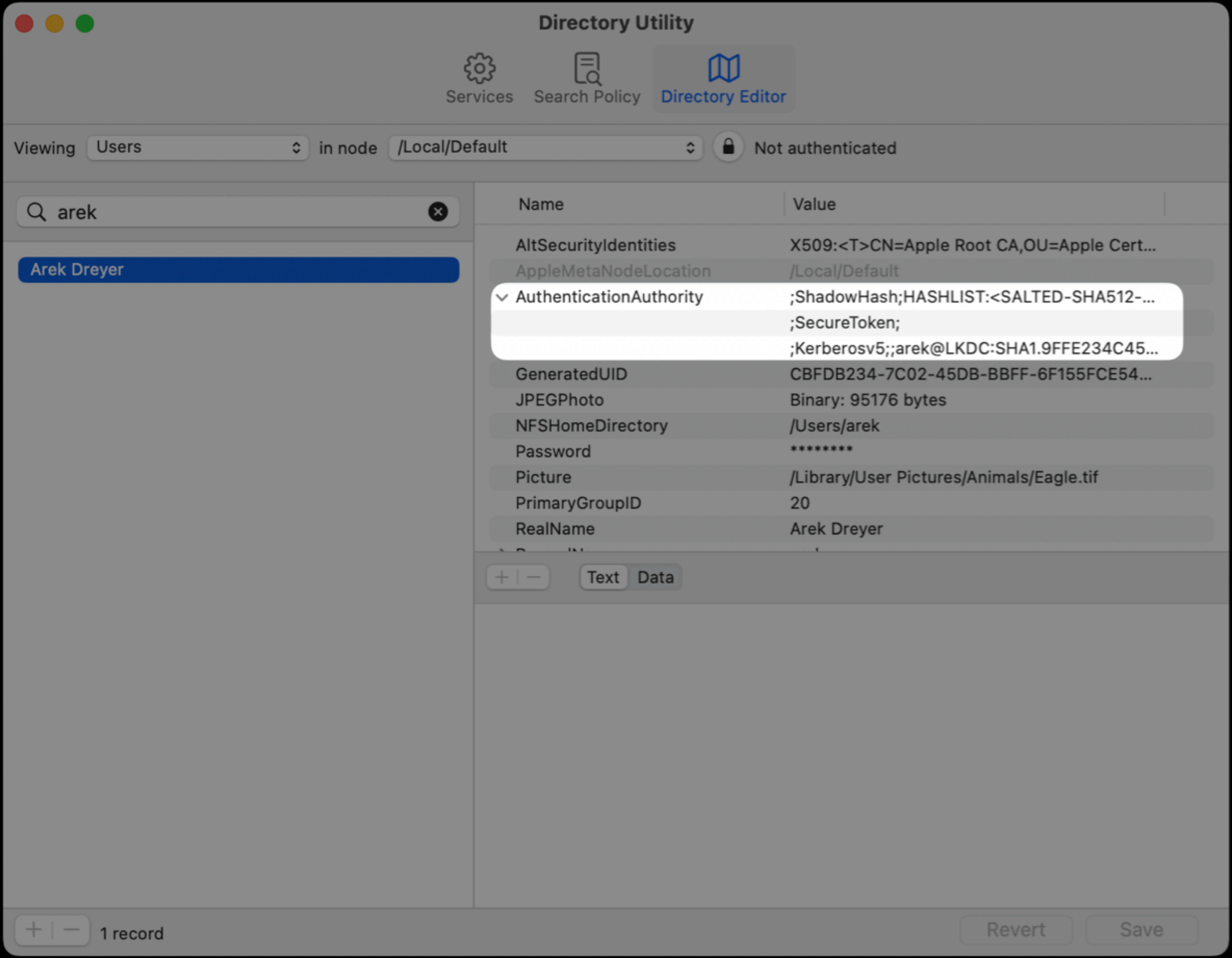
But there’s no Keybag Utility

So how do you deal with them

# So how do you deal with them

- Some information in the directory node
- Our old friend Directory Utility
- Or dscl
- Mac directory info is stored as plists files
- /var/db/dslocal/nodes/Default

Our old friend Directory Utility (or dscl)



Viewing Users in node /Local/Default Not authenticated

arek

Arek Dreyer

| Name | Value |
|---|---|
| AltSecurityIdentities | X509:<T>CN=Apple Root CA,OU=Apple Cert... |
| AppleMetaNodeLocation | /Local/Default |
| AuthenticationAuthority | ;ShadowHash;HASHLIST:<SALTED-SHA512-... |
| | ;SecureToken; |
| | ;Kerberosv5;;arek@LKDC:SHA1.9FFE234C45... |
| GeneratedUID | CBFDB234-7C02-45DB-BBFF-6F155FCE54... |
| JPEGPhoto | Binary: 95176 bytes |
| NFSHomeDirectory | /Users/arek |
| Password | ******** |
| Picture | /Library/User Pictures/Animals/Eagle.tif |
| PrimaryGroupID | 20 |
| RealName | Arek Dreyer |

1 record

| | |
|---|---|
| AltSecurityIdentities | X509:<T>CN=Apple Root CA,OU=Apple Cert... |
| AppleMetaNodeLocation | /Local/Default |
| AuthenticationAuthority | ;ShadowHash;HASHLIST:<SALTED-SHA512-... |
| | ;SecureToken; |
| | ;Kerberosv5;;arek@LKDC:SHA1.9FFE234C45... |
| GeneratedUID | CBFDB234-7C02-45DB-BBFF-6F155FCE54... |
| JPEGPhoto | Binary: 95176 bytes |
| NFSHomeDirectory | /Users/arek |
| Password | ******** |
| Picture | /Library/User Pictures/Animals/Eagle.tif |
| PrimaryGroupID | 20 |
| RealName | Arek Dreyer |

# It’s just a hint

;SecureToken;

It’s not the token itself

If you delete, parts of OS might have a hard time understanding you have secure token

**The info in the directory record**

Adding or removing `;SecureToken;` to a directory record doesn’t mean much

You could erase every single file in the APFS Data volume including directory info and your secure tokens would still exist

How do I know I have a secure token?

diskutil knows how to read keybag info!

arek — -zsh — 80×24

```
arek@[redacted] ~ % diskutil apfs listCryptousers /
Cryptographic users for disk3s1s1 (3 found)
|
+-- CBFDB234-7C02-45DB-BBFF-6F155FCE54B2
|    Type: Local Open Directory User
|    Volume Owner: Yes
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
|    Type: MDM Bootstrap Token External Key
|    Volume Owner: Yes
|
+-- EBC6C064-0000-11AA-AA11-0030654 3ECAC
     Type: Personal Recovery User
     Volume Owner: Yes

arek@[redacted] ~ % 
```

arek — -zsh — 94×24

```
arek@[redacted] ~ % sudo fdesetup list --extended
Password:
ESCROW  UUID                                                         TYPE USER
        CBFDB234-7C02-45DB-BBFF-6F155FCE54B2                      OS User arek
        2457711A-523C-4604-B75A-F48A571D5036                 Bootstrap Token
        EBC6C064-0000-11AA-AA11-00306543ECAC        Personal Recovery Record
arek@[redacted] ~ %
```

# Changed GUID

You still need that user's passphrase in order to unlock their lockbox

**What happens if you do silly things**

# Damaged GUID

Yikes!

It’s not clear to OS who owns the secure token and which password should be used to unlock it.

**What happens if you do silly things**

# Prevention steps

It’s hard to delete the last user that has secure token

System Settings won’t allow it

Some CLI tools won’t allow it

But you’re clever

**macOS tries really hard to keep you from doing bad things**

# Unexpected things

Unrecommended flows in recoveryOS

**More clever together!**

# Don’t do these

❌ Don’t create a throwaway account with Setup Assistant then forget the password.

❌ Don’t force the password of the last secure token enabled account

❌ Don’t delete all your users

Really

# Using PRK to reset password in recoveryOS is OK!

For many organization it’s preferred

# PRK and KEK

PRK has access to the KEK so Mac can:

✅ Safely destroy old lockbox protected by the forgotten password

✅ Create a new lockbox by wrapping the KEK with the cleartext passcode that you provide as the new passcode

**reset password in recoveryOS**

On a new Mac that automatically creates an managed administrator account:

when does that account get a secure token?

# Not until someone types it

- The MDM command to create the account contains the hash of the password, not the cleartext password.
- The cleartext password is required to create the secure token
- This poses a challenge for a LAPS-type solution for a Mac after restart

# Need OIK to change boot settings

- For Mac with Apple silicon
- Need the password of a secure token user
  - to get access to the OIK
    - to sign any changes to boot settings
      - like update or upgrade

# If there’s a bootstrap token

- You Mac can ask its MDM solution for the bootstrap token
  - to access the OIK
    - so your MDM solution can force an update without a user typing password

# If you lose all the keys

You have to start over

# Bootstrap token before macOS 10.14

# Bootstrap token as of macOS 10.14

# Here we go

# Bootstrap token

- A feature of macOS
- Requires MDM solution that supports it
- Requires Apple School Manager or Apple Business Manager

# Bootstrap token allows Mac to:

- Obtain a secure token
- Approve kernel extensions
- Approve software updates without a user entering their password
- Approve Erase All Content and Settings from an MDM Erase command
- Use declarative device management for macOS updates
- Create a new account at a FileVault unlocked login window w/ PSSO

# As a feature, secure token is the

- implementation of encryption keys
  - for securing the APFS startup volume
  - when they're generated
  - and how they're stored

# As an object, a secure token is a

- wrapped version of a key encryption key
  - protected by a user’s password
- Secure tokens live in a keybag
  - a chunk of data written to the internal volume
    - accessible even when FileVault is on

# A user with a secure token can:

- Create new secure tokens
- Access the VEK for FileVault after a restart
- Access the OIK for updates and such

# The first secure token is made by

- wrapping the KEK with the first user’s cleartext password
    - which removes the KEK from being unprotected
- Subsequent secure tokens are made by unwrapping another secure token
    - to get access to the KEK
        - then wraps the KEK with the new user’s password

# All new features of MDM

- Will be declarative device management
- In order to use DDM for software updates, the MDM solution must support bootstrap token

# Platform SSO is

- an app extension from an app provided by your Identity Provider
    - which enables users to sign in once at the login window and then automatically sign in to apps and websites
        - and absolutely does not handle creating the first local user account

# Platform SSO features for Sonoma are:

- User enrollment and registration status in System Settings
- Local account creation by users
- Update group membership of users when they authenticate with their IdP
- Use non-local IdP user accounts at authorization prompts

# In order for PSSO to create a new user

- Mac must be:
  - enrolled in an MDM solution that supports bootstrap token
    - fully booted with macOS 14
      - with setup Assistant completed
        - with existing local account created
          - with FileVault unlocked

# bootstrap token recap

- Helps an MDM solution
  - obtain a secure token
    - to create new users’ secure tokens and change LocalPolicy
- and the Mac can silently install updates, approve kernel extensions, and EACAS
- and use declarative device management to update macOS
- and allow PlatformSSO to create a new user at the login window

# That was bootstrap token

# Thank you