Gatekeeper and Developer ID

Session 702

Perry The Cynic
OS Security Architect

What You Will Learn

- What Gatekeeper is and how it works
- How to control what can install and run on your Mac
- How to sign your app so Macs will accept it by default
- How to debug problems with Gatekeeper and Developer ID
- Code Signing refresher

Code Signing

Refresher

Code Signing in General

Code Signing in General

- A code identification technology

Code Signing in General

- A code identification technology
- Seal code to detect modification after signing

Code Signing in General

- A code identification technology
- Seal code to detect modification after signing
  - Includes bundle resources

Code Signing in General

- A code identification technology
- Seal code to detect modification after signing
  - Includes bundle resources
- Vouch for code with a digital signature

Code Signing in General

- A code identification technology
- Seal code to detect modification after signing
  - Includes bundle resources
- Vouch for code with a digital signature
- Tolerate intended code changes

Code Signing in General

- A code identification technology
- Seal code to detect modification after signing
  - Includes bundle resources
- Vouch for code with a digital signature
- Tolerate intended code changes
- Define and resolve code identity

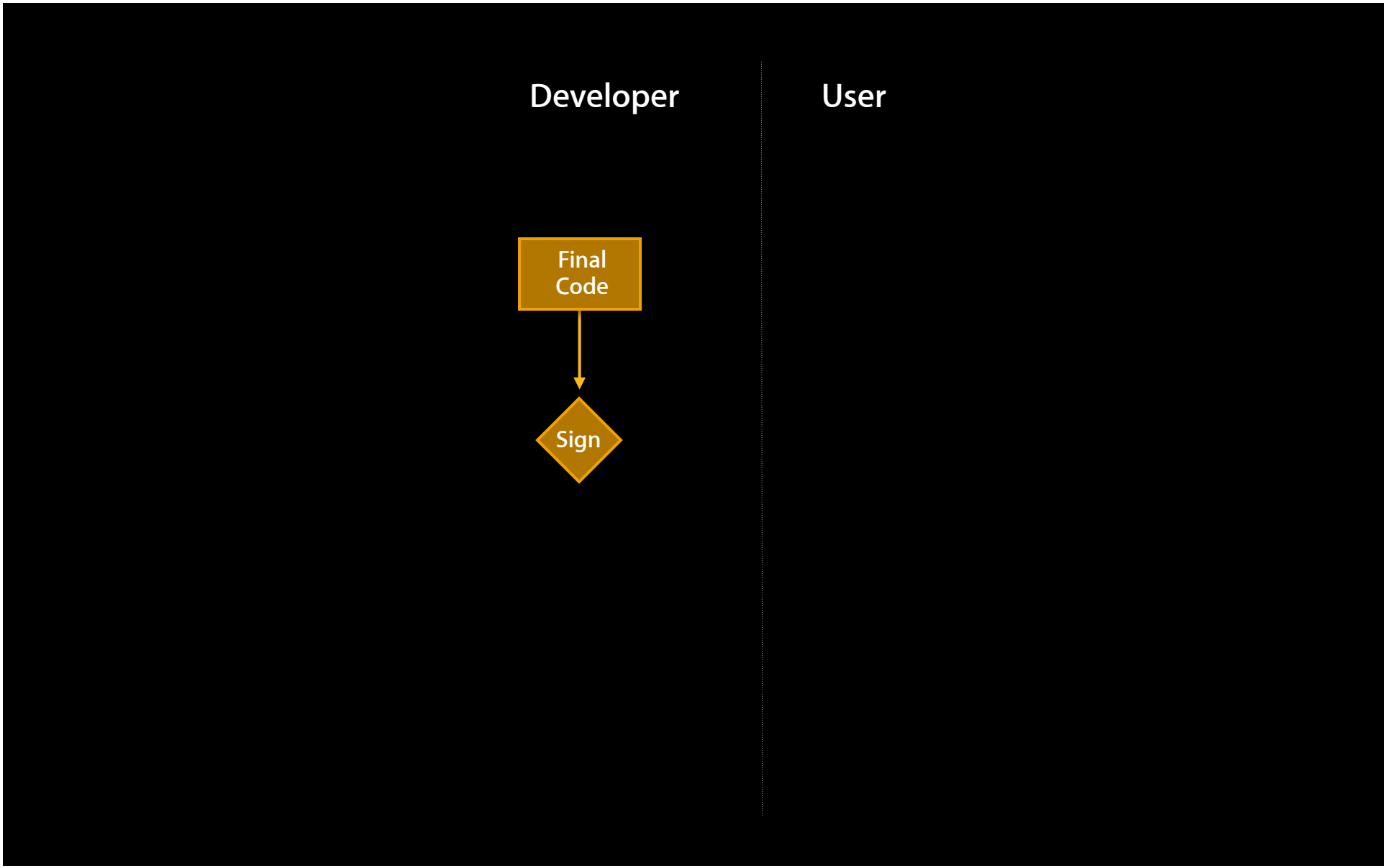
Code Signing in General

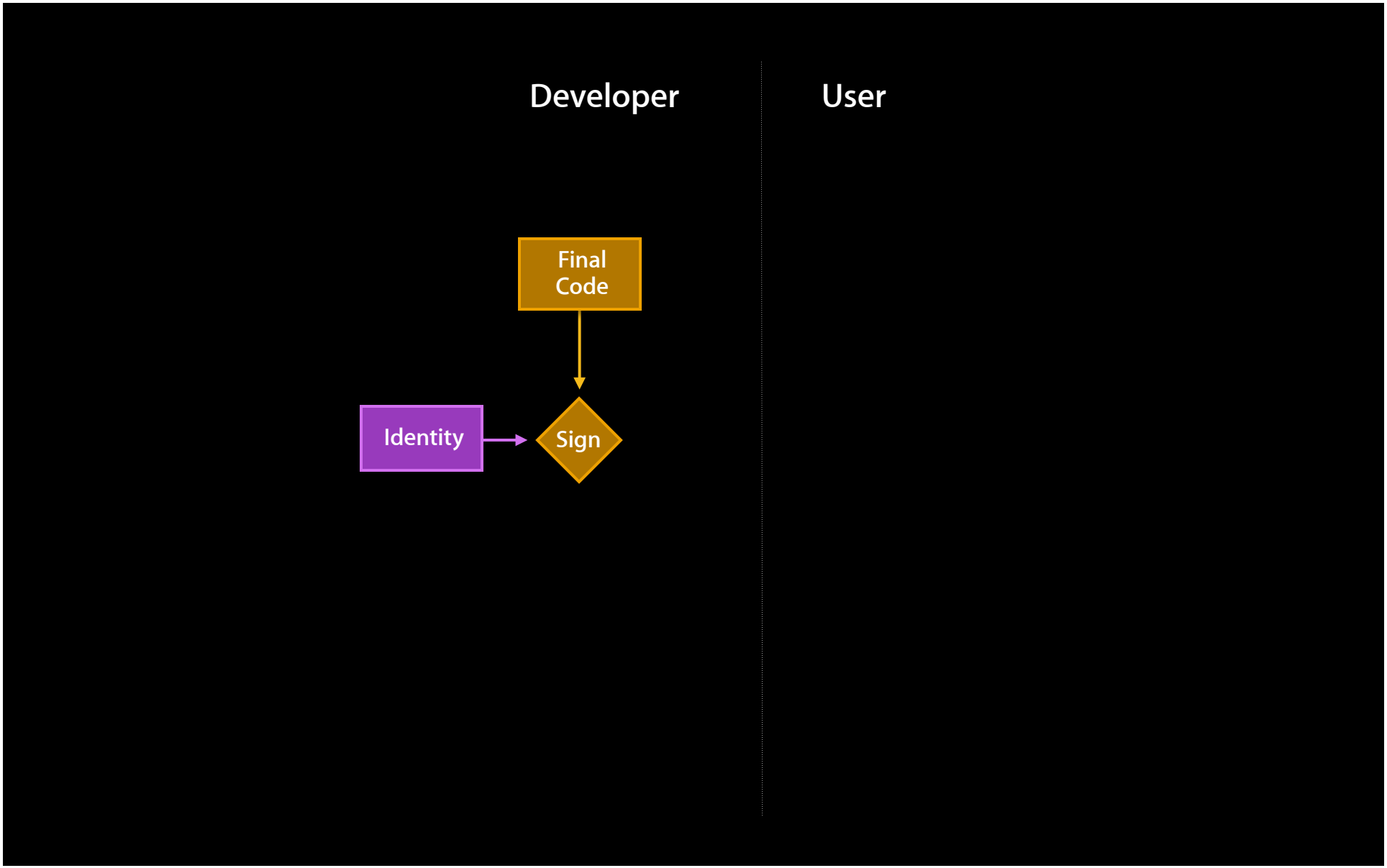
- A code identification technology
- Seal code to detect modification after signing
  - Includes bundle resources
- Vouch for code with a digital signature
- Tolerate intended code changes
- Define and resolve code identity
- Efficient runtime identification and validation

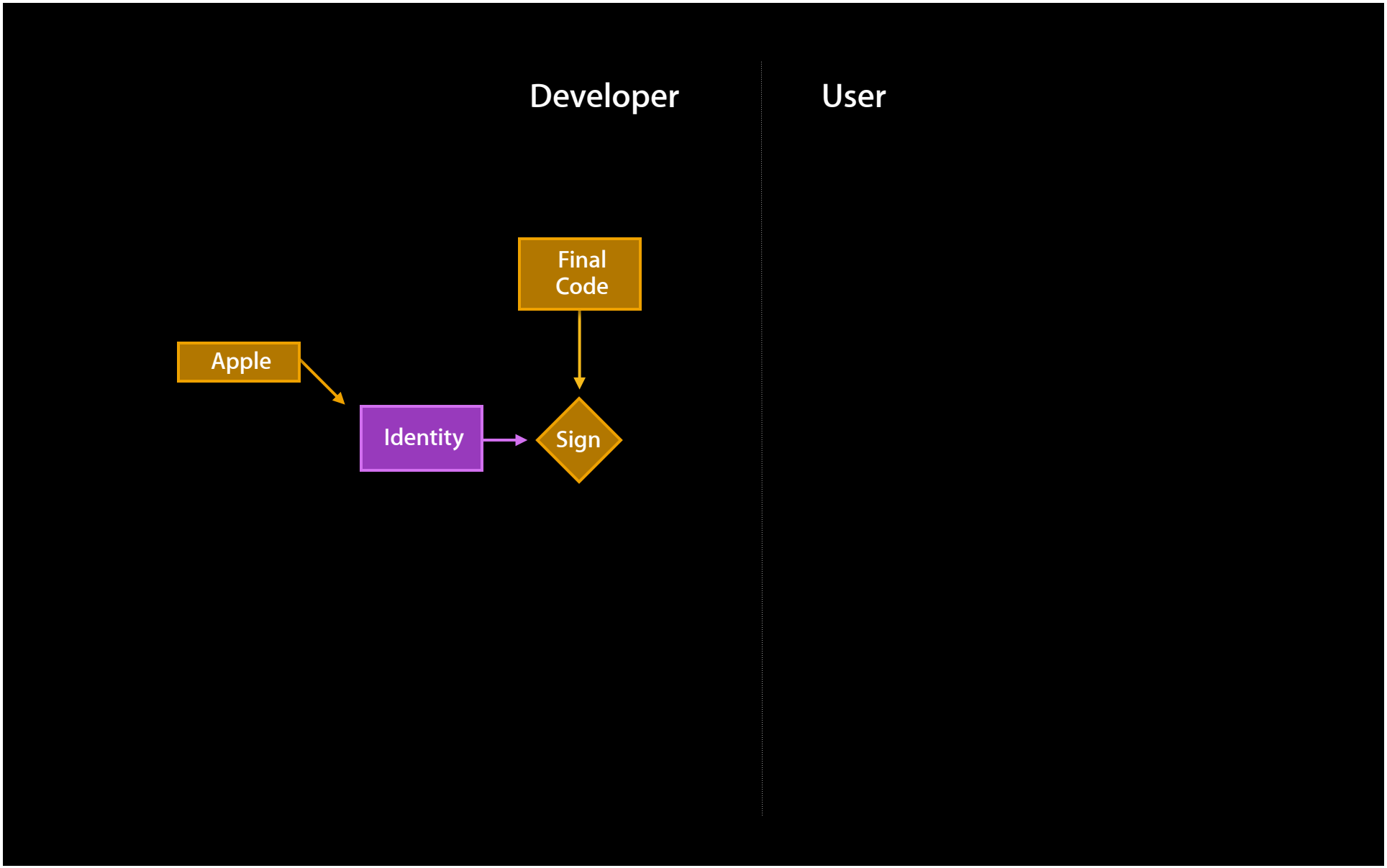
Developer

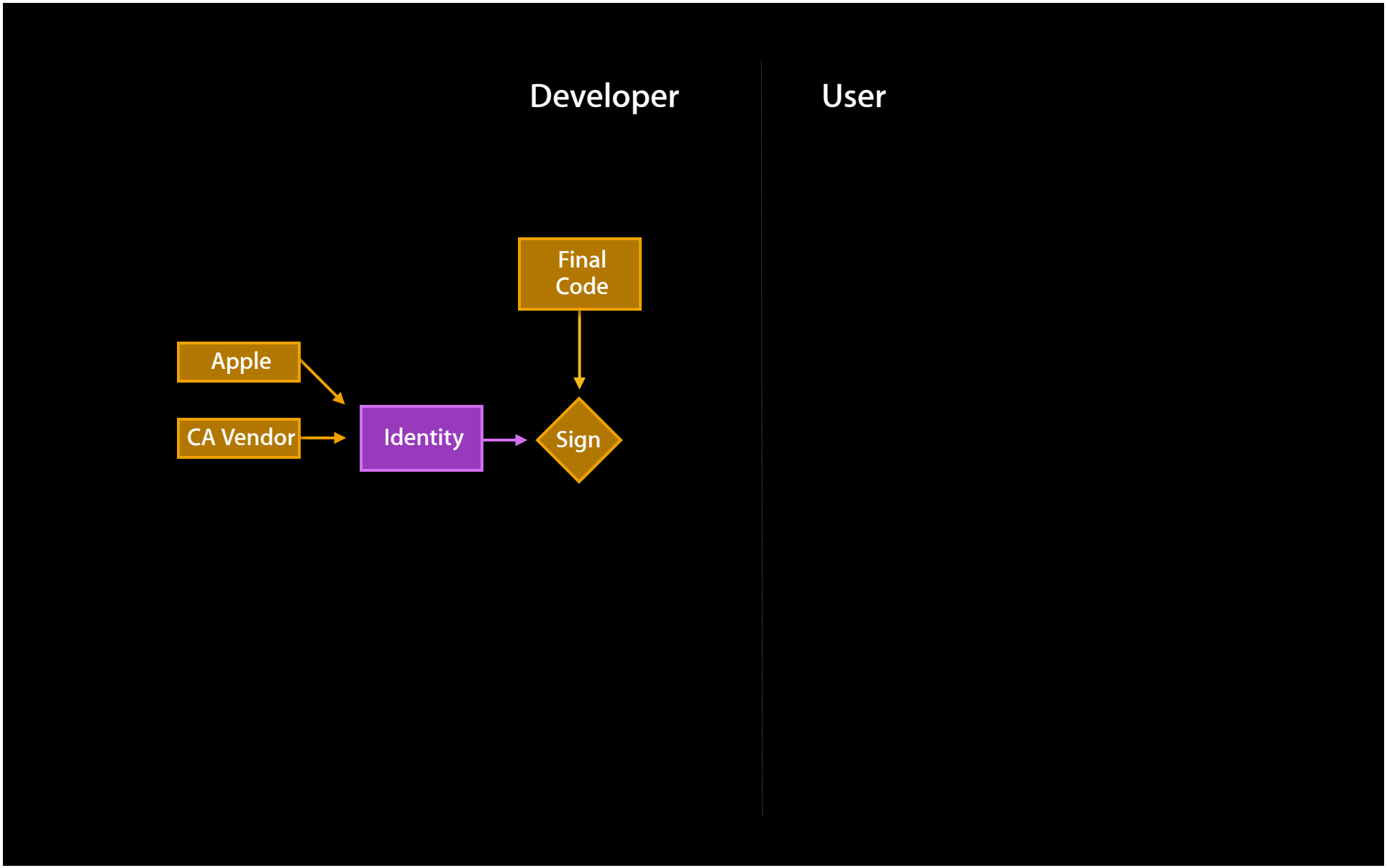
User

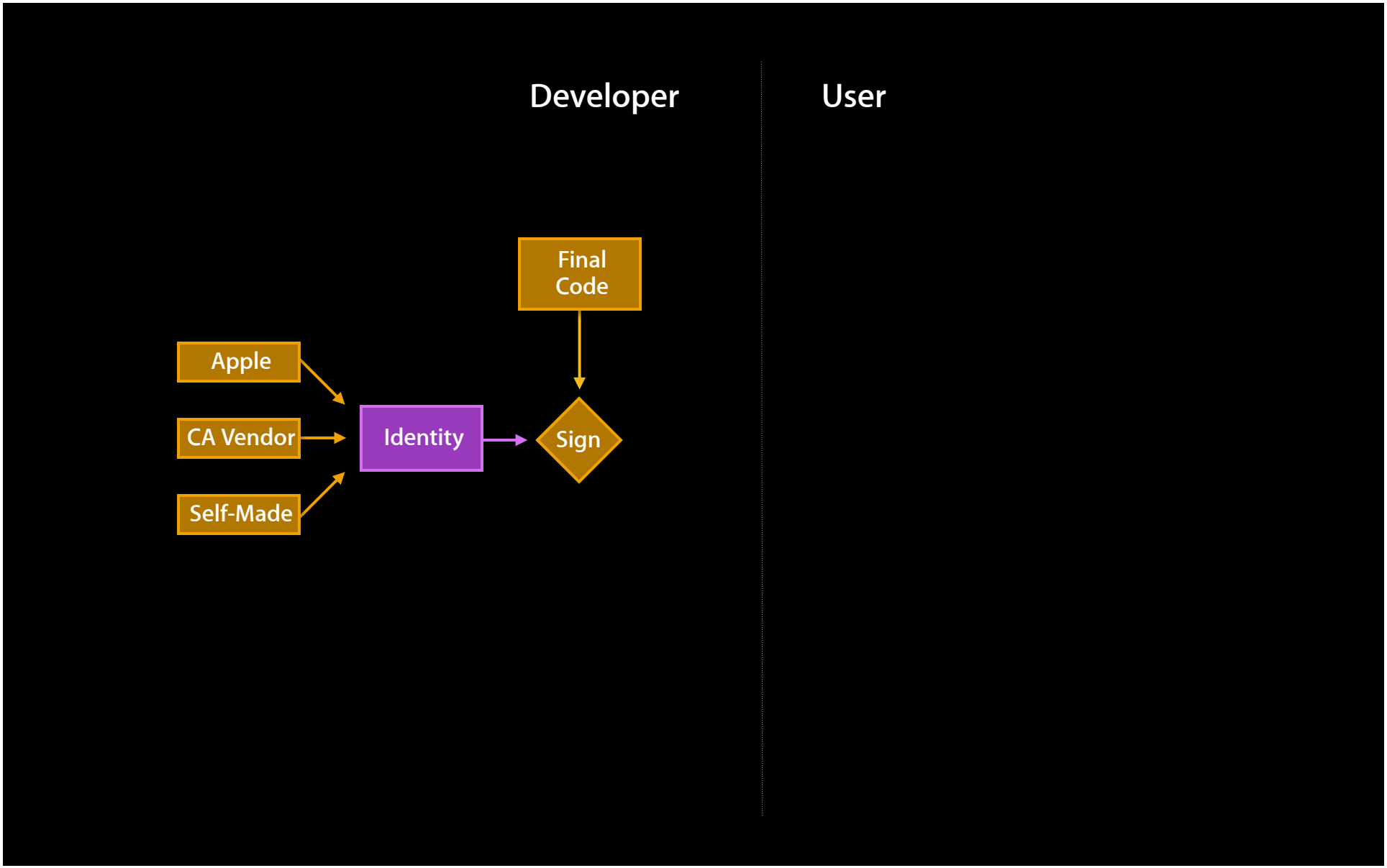

Developer
User
Final
Code

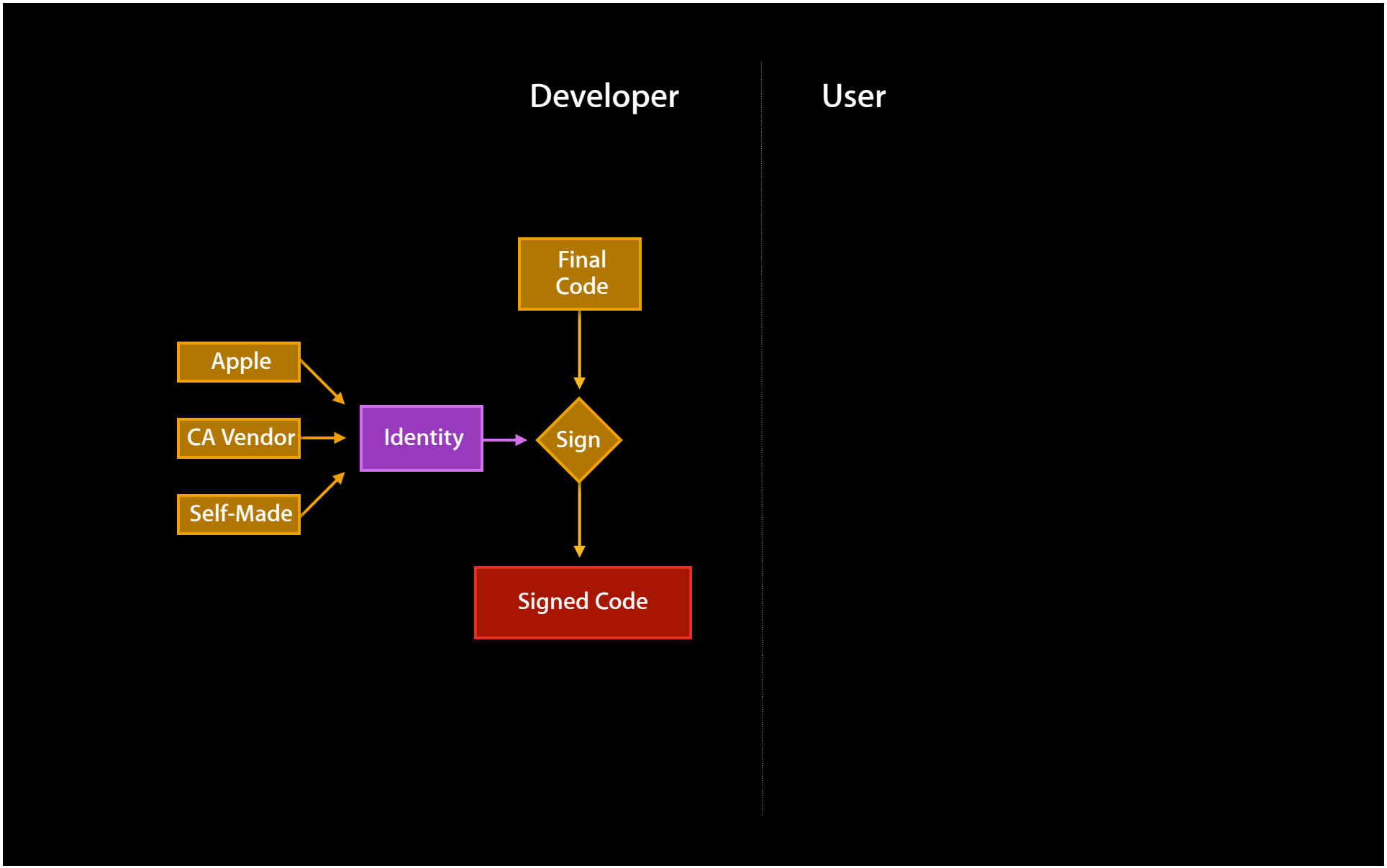

Developer
User
Final Code
Sign

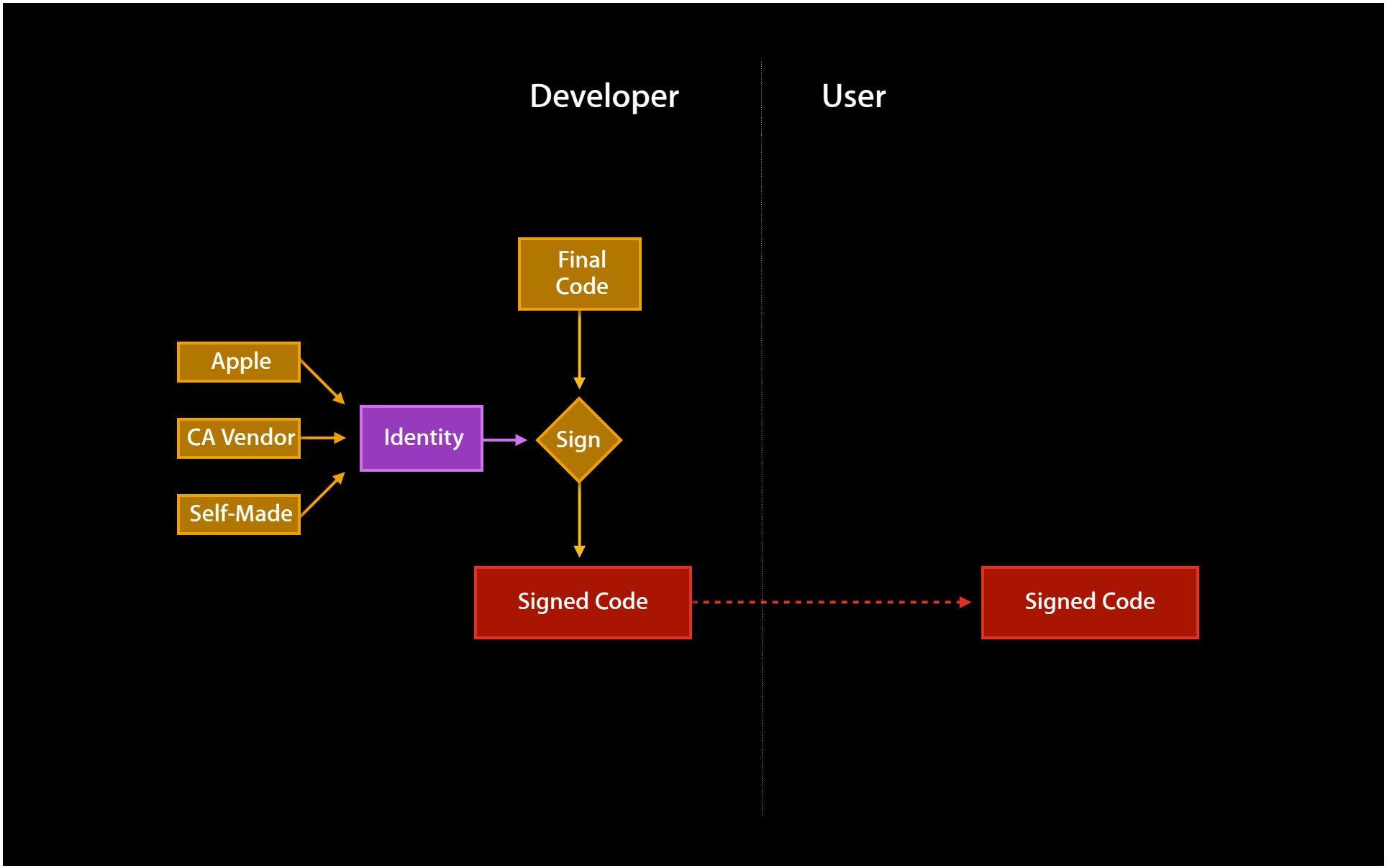

Developer
User
Final Code
Identity
Sign

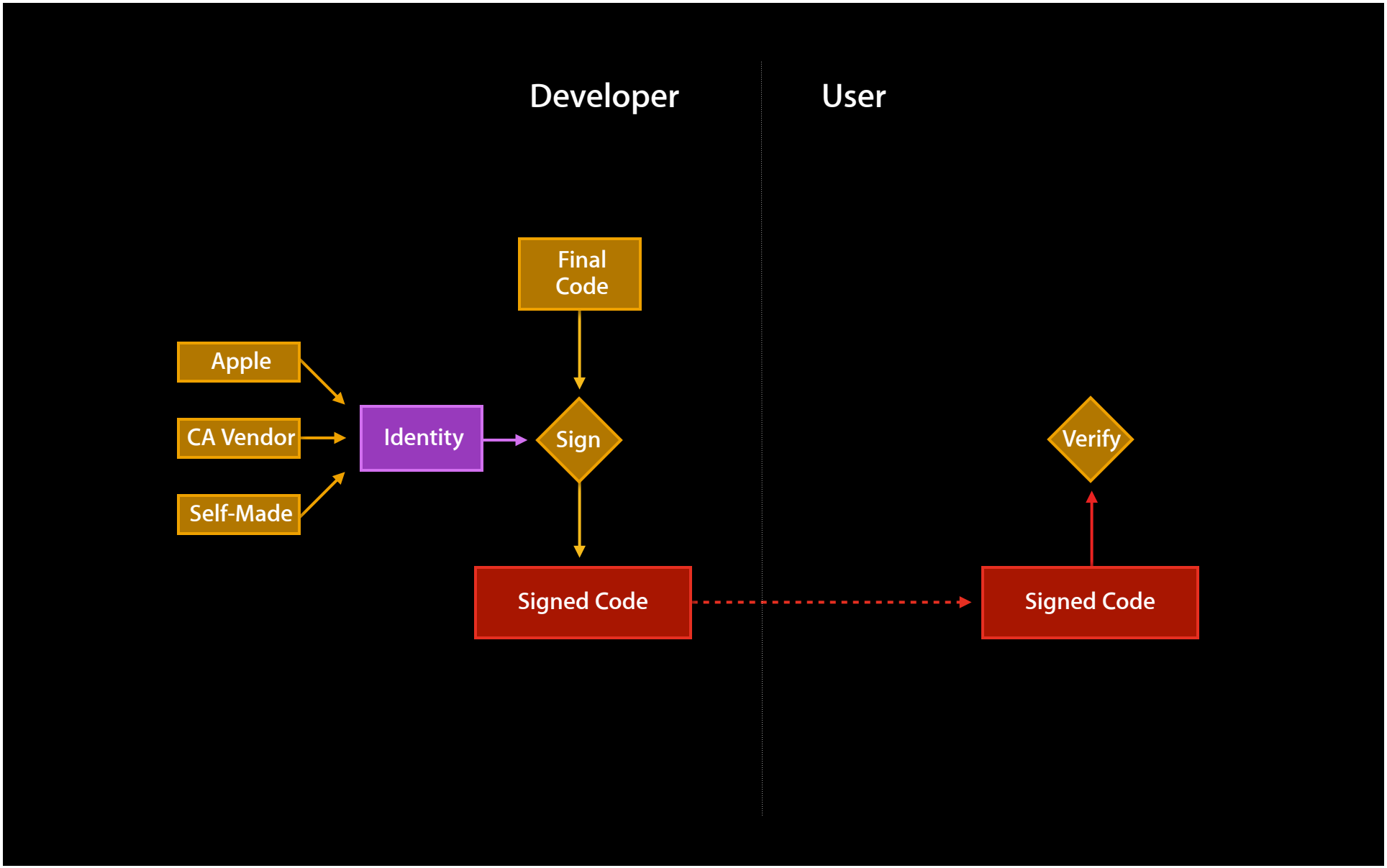

Developer
User
Final Code
Apple
Identity
Sign

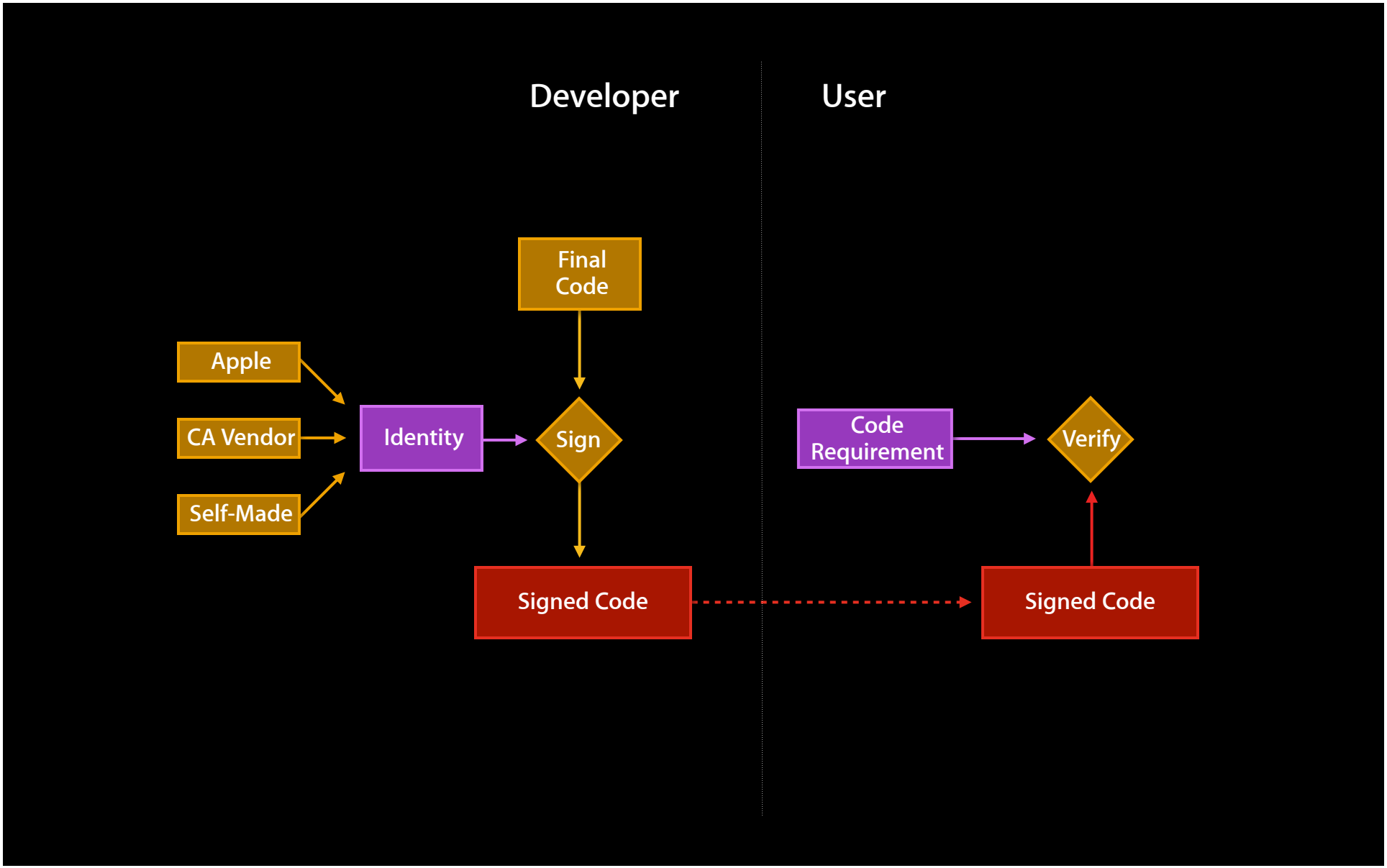

Developer
User
Final Code
Apple
CA Vendor
Identity
Sign

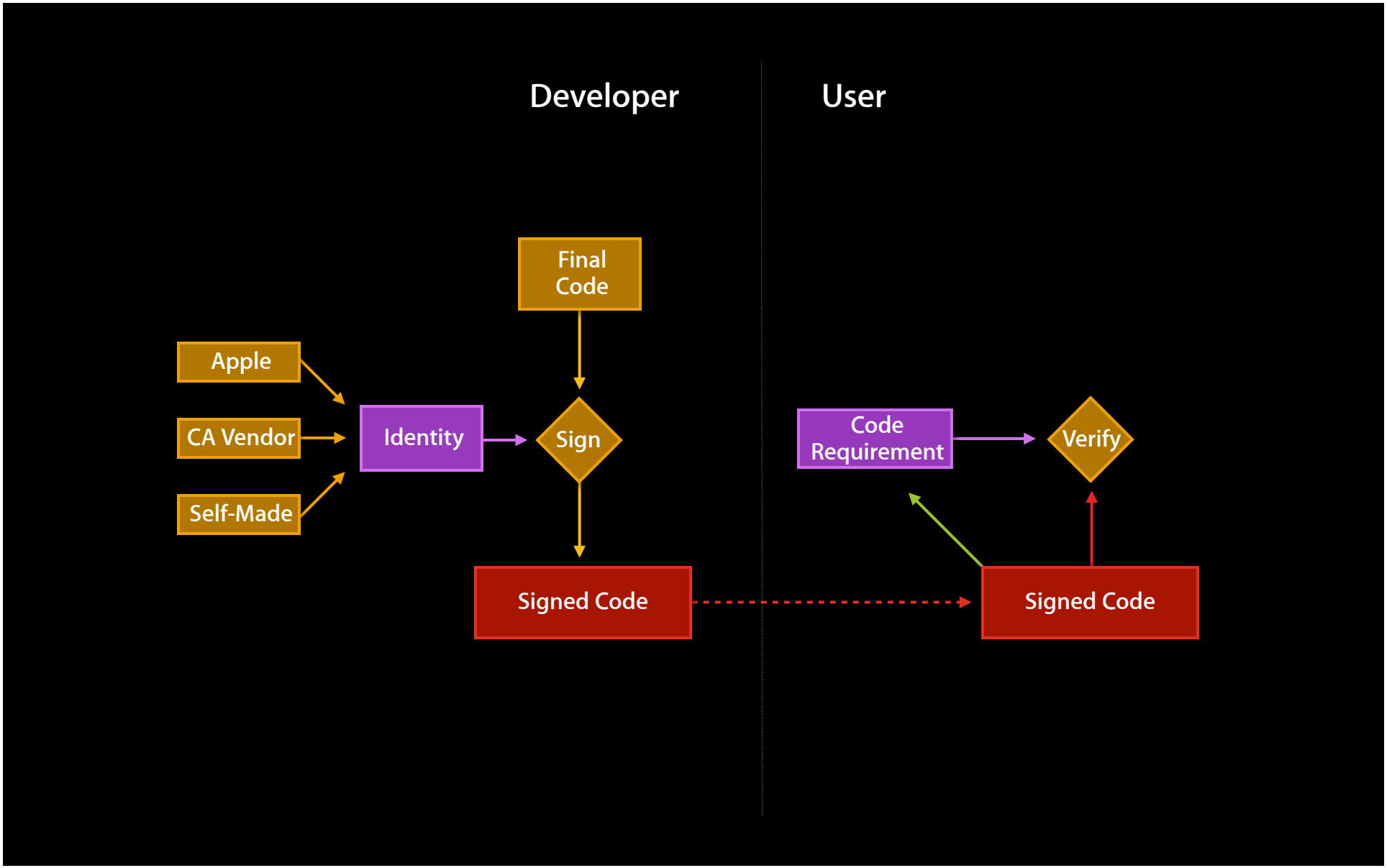

Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign

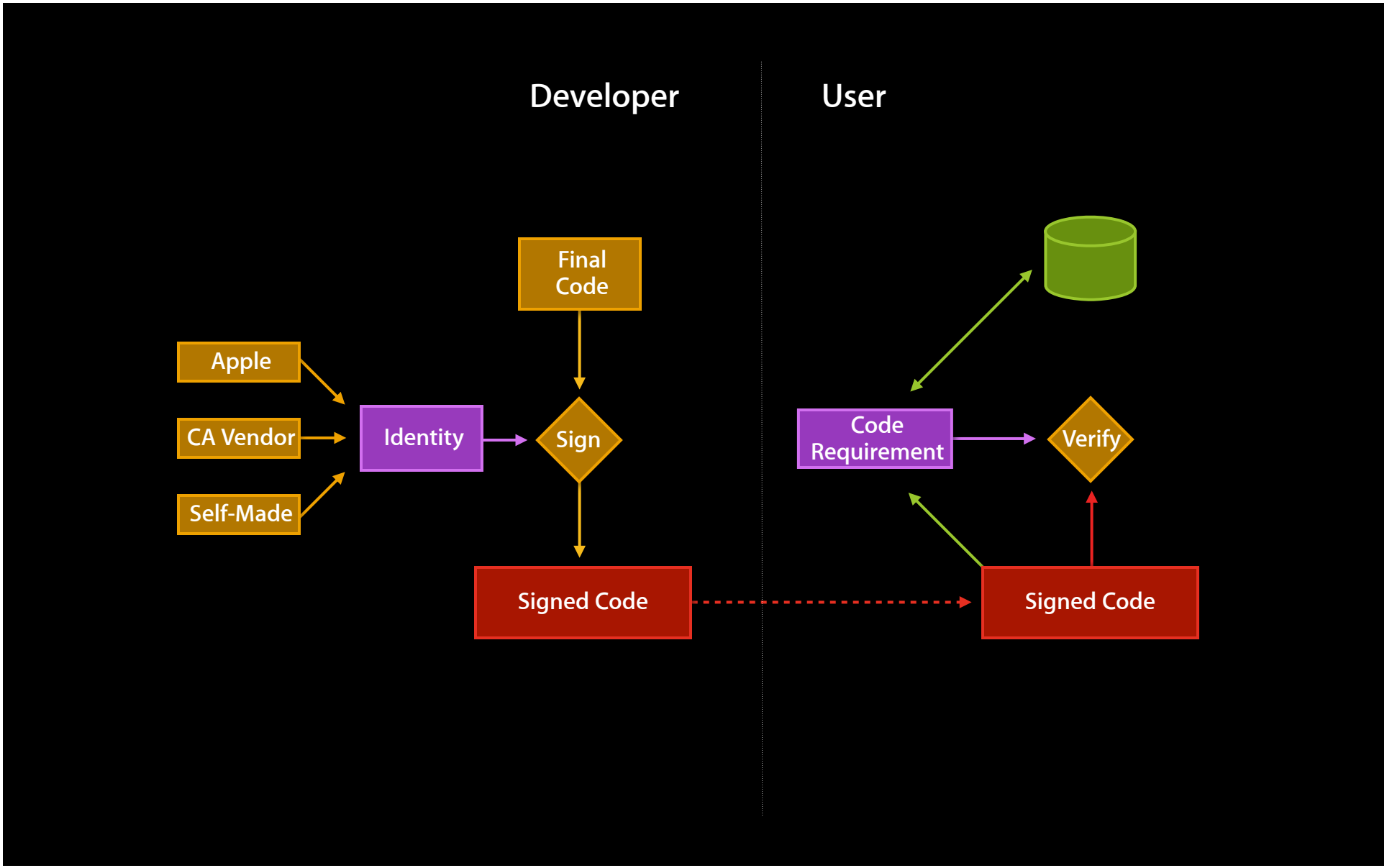

Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Signed Code

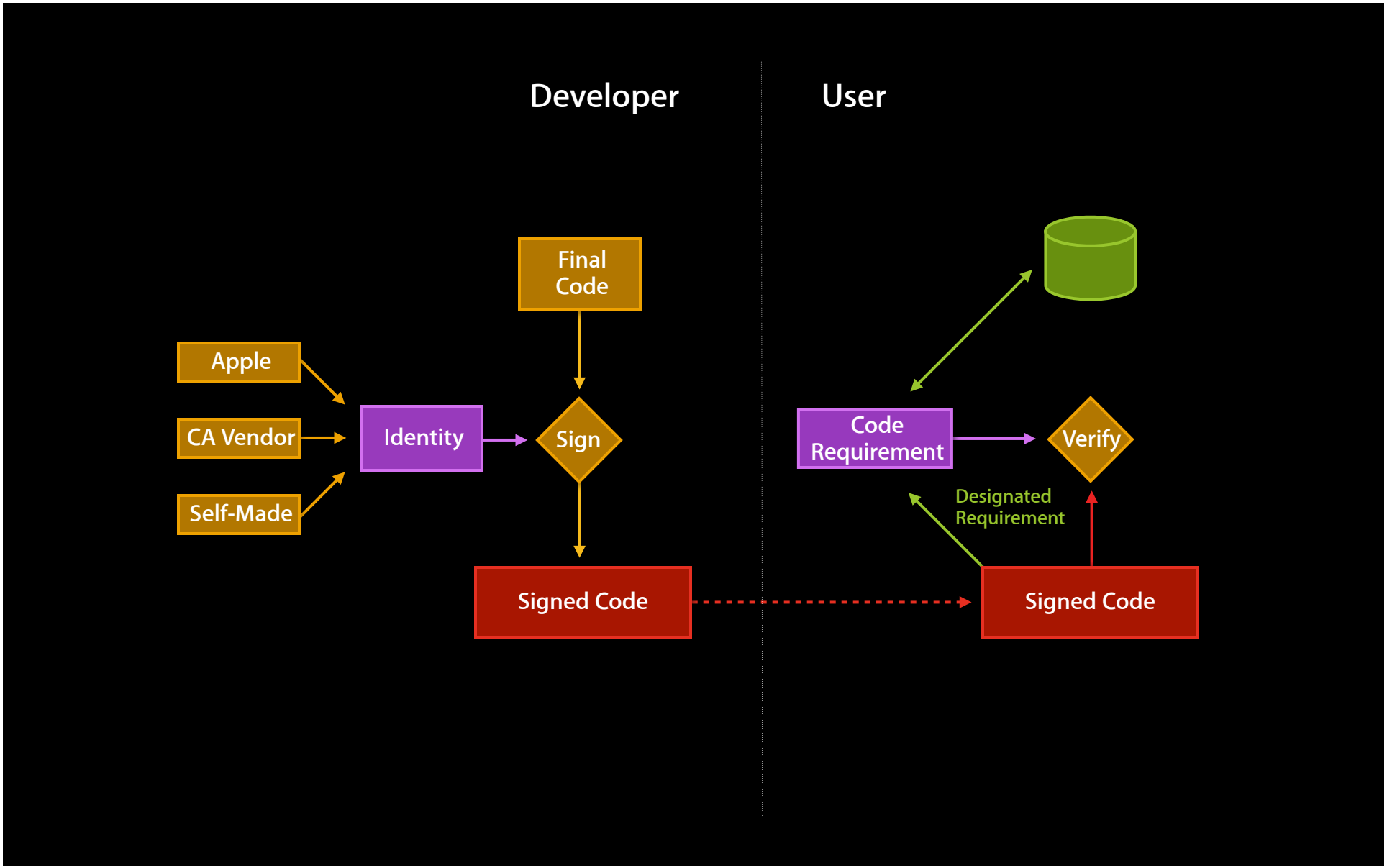

Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Signed Code
Signed Code

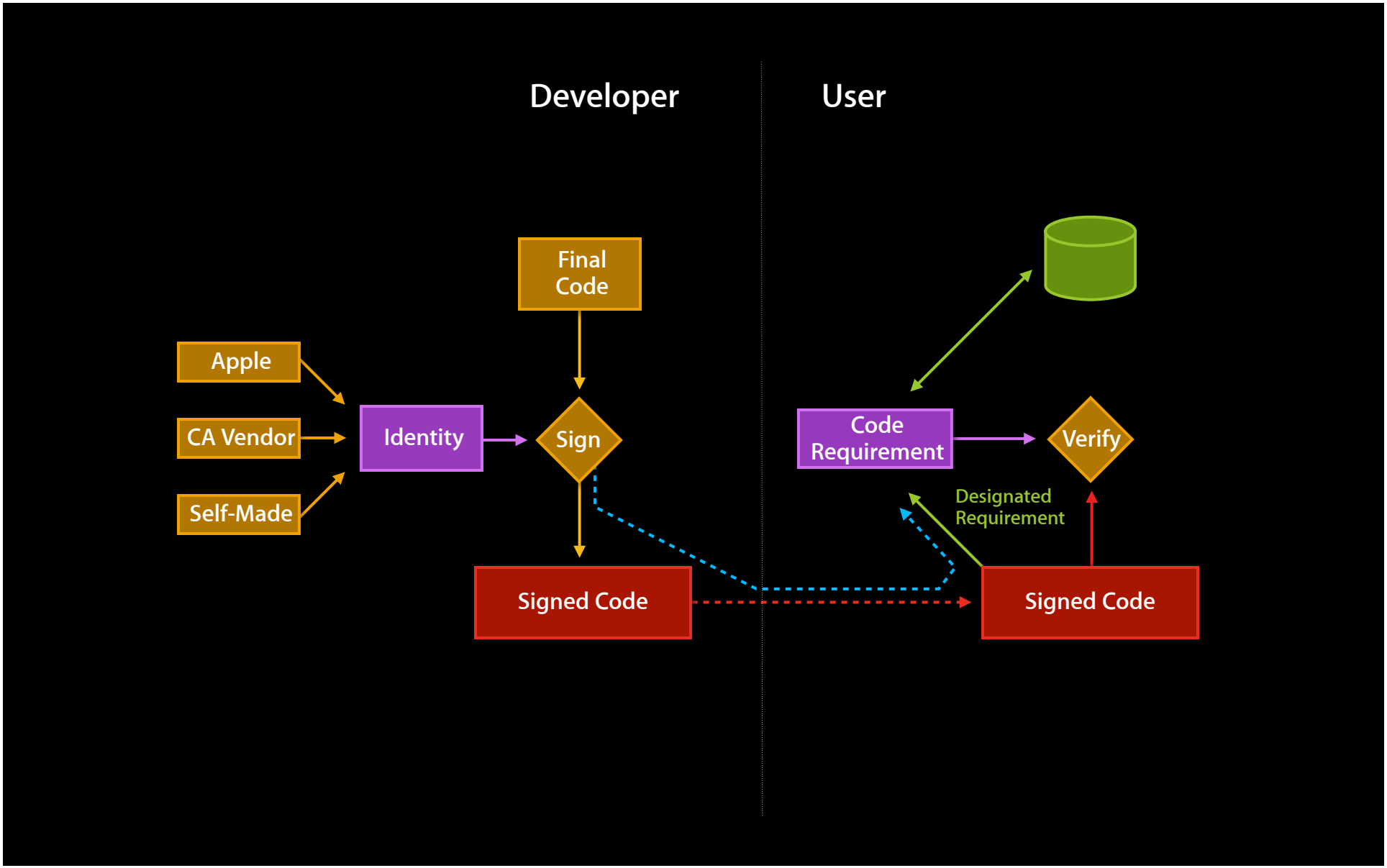

Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Verify
Signed Code
Signed Code

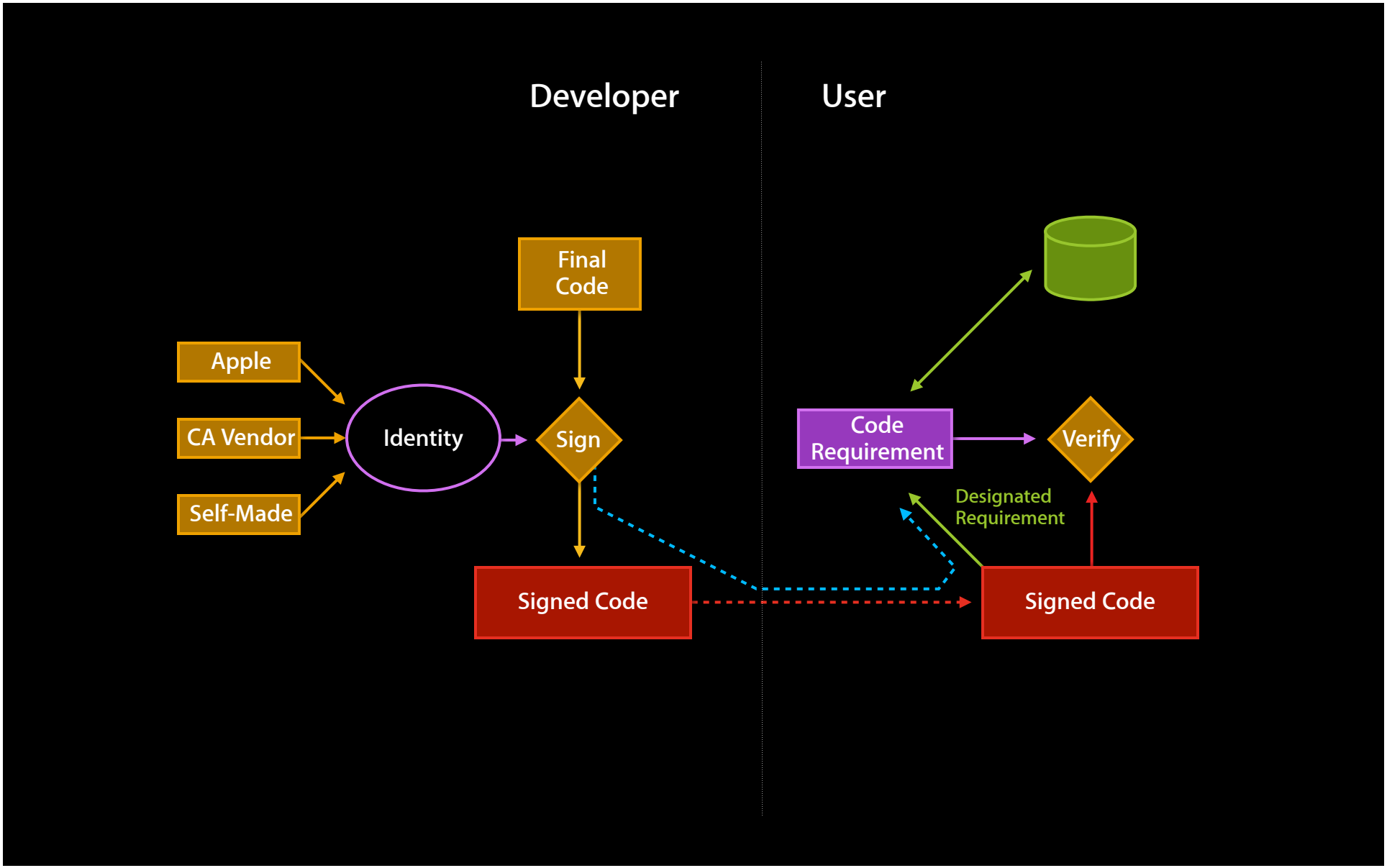

Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Code Requirement
Verify
Signed Code
Signed Code

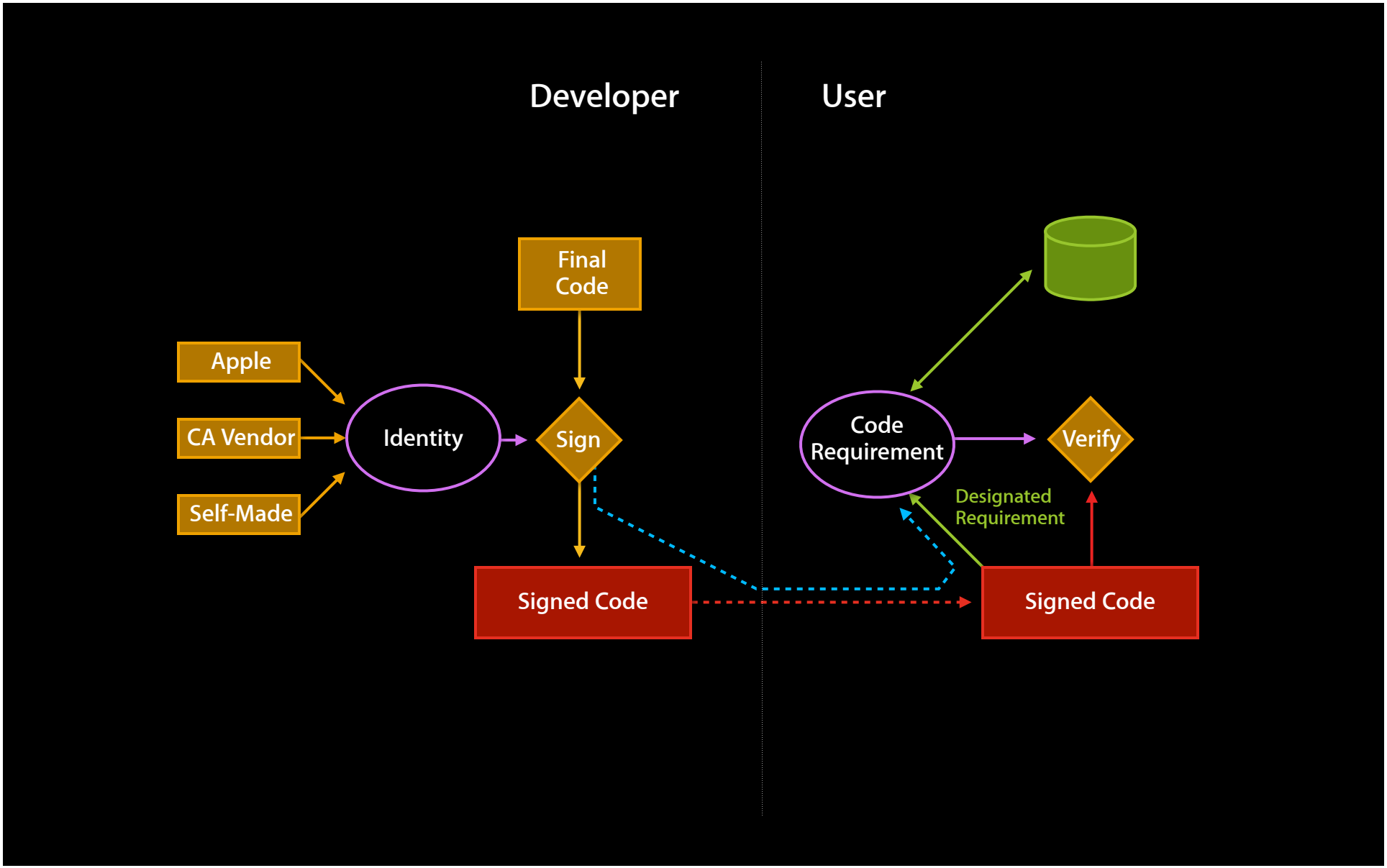

Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Code Requirement
Verify
Signed Code
Signed Code


Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Signed Code
Code Requirement
Verify
Signed Code


Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Signed Code
Code Requirement
Verify
Designated Requirement
Signed Code


Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Code Requirement
Verify
Designated Requirement
Signed Code
Signed Code


Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Signed Code
Code Requirement
Verify
Designated Requirement
Signed Code


Developer
User
Final Code
Apple
CA Vendor
Self-Made
Identity
Sign
Signed Code
Code Requirement
Verify
Designated Requirement
Signed Code

Code Requirement Examples

Code Requirement Examples

- Mail.app

  anchor apple and identifier com.apple.mail

Code Requirement Examples

- Mail.app

  anchor apple and identifier com.apple.mail

- Self-made certificate

  anchor H"3b8ca...3e0fe7" and identifier "com.your.program"

Code Requirement Examples

- Mail.app

  anchor apple and identifier com.apple.mail

- Self-made certificate

  anchor H"3b8ca...3e0fe7" and identifier "com.your.program"

- May use the iCloud password

  anchor apple and info["Application-Group"] = "dot-mac"

Code Requirement Examples

- Mail.app

  anchor apple and identifier com.apple.mail

- Self-made certificate

  anchor H"3b8ca...3e0fe7" and identifier "com.your.program"

- May use the iCloud password

  anchor apple and info["Application-Group"] = "dot-mac"

- Mac App Store

  anchor apple generic and identifier com.your.program and certificate leaf[field.
  1.2.840.113635.100.6.1.9]

Code Requirement Examples

- Mail.app

  anchor apple and identifier com.apple.mail

- Self-made certificate

  anchor H"3b8ca...3e0fe7" and identifier "com.your.program"

- May use the iCloud password

  anchor apple and info["Application-Group"] = "dot-mac"

- Mac App Store

  anchor apple generic and identifier com.your.program and certificate leaf[field.
  1.2.840.113635.100.6.1.9]

- Developer ID

  anchor apple generic and identifier com.your.program and (certificate leaf[field.
  1.2.840.113635.100.6.1.9] or certificate 1[field.1.2...6.2.6] and certificate leaf[field.1.2...6.1.13] and
  certificate leaf[subject.OU] = XYR4B7AAFB)

Developer ID

Доверяй, но проверяй

Mac Developer Program

Mac Developer Program

- Supports development for Macintosh

Mac Developer Program

- Supports development for Macintosh
- $99/year

Mac Developer Program

- Supports development for Macintosh
- $99/year
- Issues Development and Distribution certificates

Mac Developer Program

- Supports development for Macintosh
- $99/year
- Issues Development and Distribution certificates
- For distribution through the Mac App Store

Developer ID

Developer ID

- Part of the Mac Developer program

Developer ID

- Part of the Mac Developer program
- No additional cost

Developer ID

- Part of the Mac Developer program
- No additional cost
- Issues separate "Developer ID" certificates

Developer ID

- Part of the Mac Developer program
- No additional cost
- Issues separate "Developer ID" certificates
- For distribution outside the Mac App Store

Comparison

Comparison

Mac App Store	Developer ID

Comparison

	Mac App Store	Developer ID
Distribution	By Apple (Mac App Store)	Direct (up to you)

Comparison

	Mac App Store	Developer ID
Distribution	By Apple (Mac App Store)	Direct (up to you)
Rules	Program License Agreement, schedules 1+2, App Store approval	Program License Agreement

Comparison

	Mac App Store	Developer ID
Distribution	By Apple (Mac App Store)	Direct (up to you)
Rules	Program License Agreement, schedules 1+2, App Store approval	Program License Agreement
Certificates	Development + Distribution	“Developer ID”

Comparison

	Mac App Store	Developer ID
Distribution	By Apple (Mac App Store)	Direct (up to you)
Rules	Program License Agreement, schedules 1+2, App Store approval	Program License Agreement
Certificates	Development + Distribution	“Developer ID”
App Sandbox	Required	Not required (but recommended)

Comparison

	Mac App Store	Developer ID
Distribution	By Apple (Mac App Store)	Direct (up to you)
Rules	Program License Agreement, schedules 1+2, App Store approval	Program License Agreement
Certificates	Development + Distribution	“Developer ID”
App Sandbox	Required	Not required (but recommended)
Code Identity	Coordinated	

Comparison

Certificate flow

Comparison

Certificate flow

Mac App Store

Developer ID

Comparison

Certificate flow

Mac App Store

Developed App

Developer ID

Comparison

Certificate flow

Mac App Store

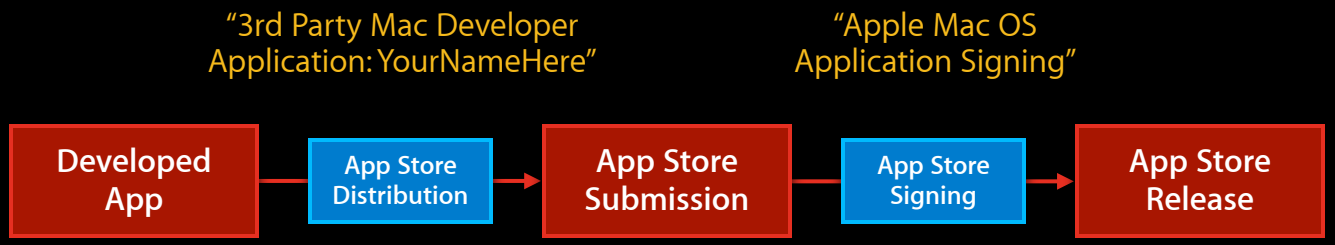
"3rd Party Mac Developer Application: YourNameHere"

Developer ID

Comparison

Certificate flow

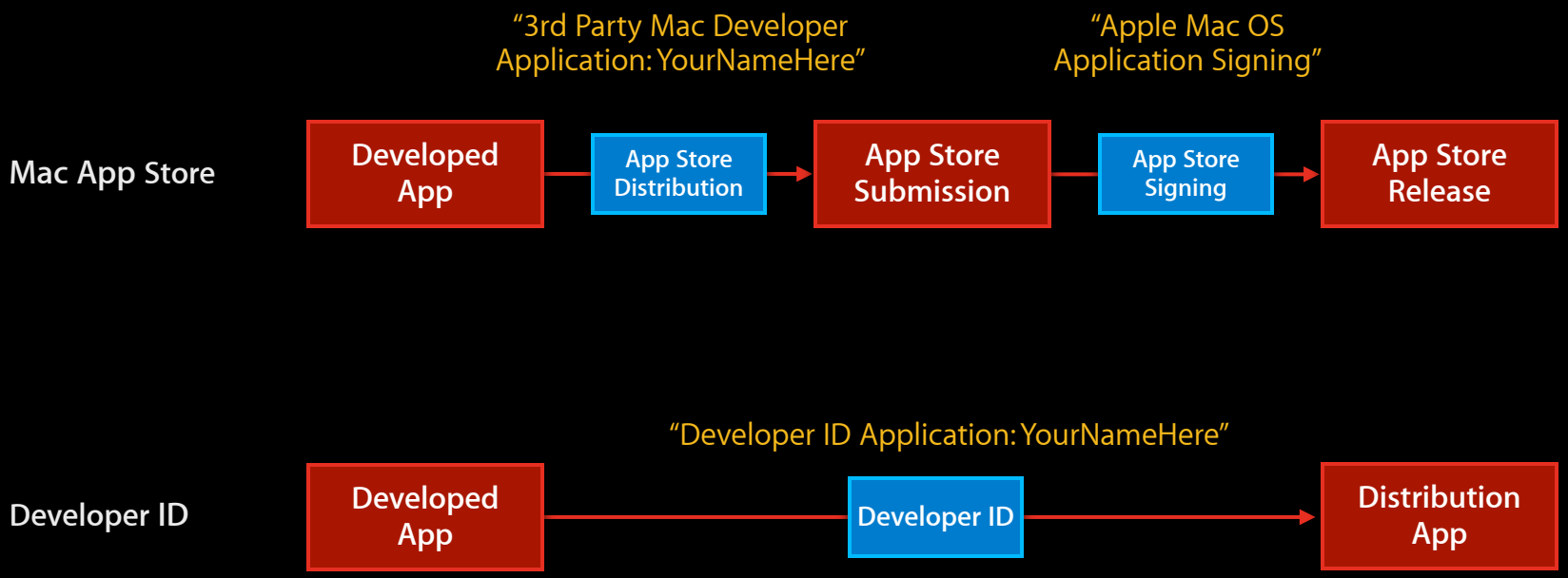
Mac App Store



Developer ID

Comparison

Certificate flow



Using Developer ID

Using Developer ID

- Use Xcode 4.3+

Using Developer ID

- Use Xcode 4.3+
- Archive to Developer ID

Using Developer ID

- Use Xcode 4.3+
- Archive to Developer ID
- Takes care of obtaining and managing certificates

Using Developer ID

- Use Xcode 4.3+
- Archive to Developer ID
- Takes care of obtaining and managing certificates
- Takes care of generating proper Designated Requirements

Using Developer ID

- Use Xcode 4.3+
- Archive to Developer ID
- Takes care of obtaining and managing certificates
- Takes care of generating proper Designated Requirements
- Use `codesign(1)` only as last resort

Demo

Managing Your Keys

Managing Your Keys

- Nobody else has your private keys

Managing Your Keys

- Nobody else has your private keys
  - Not even Apple

Managing Your Keys

- Nobody else has your private keys
  - Not even Apple
- Back them up

Managing Your Keys

- Nobody else has your private keys
  - Not even Apple
- Back them up
- Use Xcode export/import to copy them

Managing Your Keys

- Nobody else has your private keys
  - Not even Apple
- Back them up
- Use Xcode export/import to copy them
- Developer ID keys belong to your entire team

Managing Your Keys

- Nobody else has your private keys
  - Not even Apple
- Back them up
- Use Xcode export/import to copy them
- Developer ID keys belong to your entire team
- Keep your keys secret

Managing Your Keys

- Nobody else has your private keys
  - Not even Apple
- Back them up
- Use Xcode export/import to copy them
- Developer ID keys belong to your entire team
- Keep your keys secret
- Report loss or compromise (product-security@apple.com)

Transition to Developer ID

Transition to Developer ID

- From unsigned code

Transition to Developer ID

- From unsigned code
- From Mac App Store

Transition to Developer ID

- From unsigned code
- From Mac App Store
- From third-party signature

Gatekeeper

What's on *your* Mac?

Download Quarantine

Download Quarantine

- A “tag” attached to files

Download Quarantine

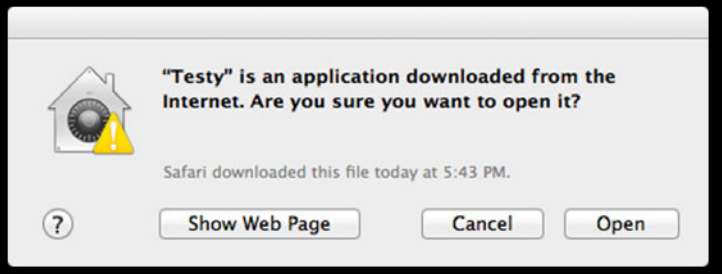
- A “tag” attached to files
- Applied by downloading apps

Download Quarantine

- A “tag” attached to files
- Applied by downloading apps
- Preserved by copy, archives, disk images

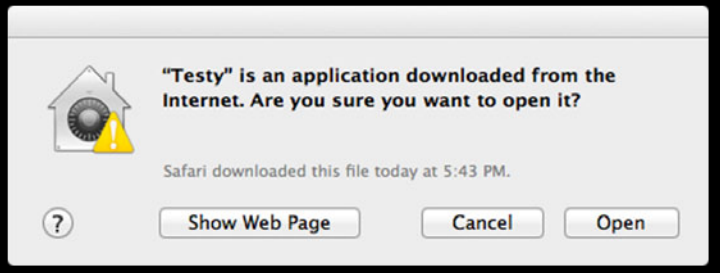
Download Quarantine

- A “tag” attached to files
- Applied by downloading apps
- Preserved by copy, archives, disk images
- Confirmation dialog



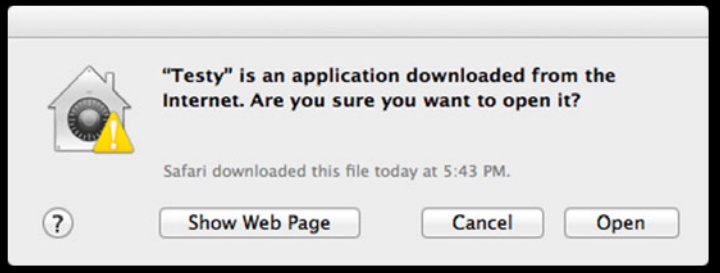
Download Quarantine

- A “tag” attached to files
- Applied by downloading apps
- Preserved by copy, archives, disk images
- Confirmation dialog
- Not applied to prior content



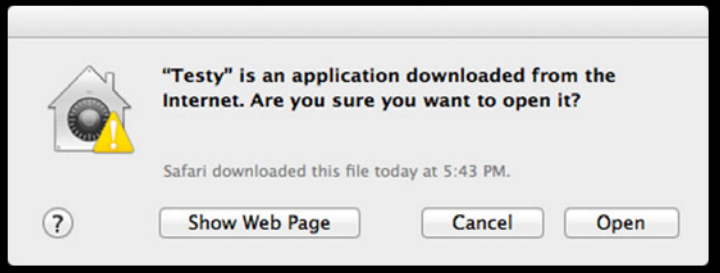
Download Quarantine

- A “tag” attached to files
- Applied by downloading apps
- Preserved by copy, archives, disk images
- Confirmation dialog
- Not applied to prior content
- Not applied to local files



Download Quarantine

- A “tag” attached to files
- Applied by downloading apps
- Preserved by copy, archives, disk images
- Confirmation dialog
- Not applied to prior content
- Not applied to local files
  - That includes most remote file systems



Malware Detection

Malware Detection

- Pattern matching

Malware Detection

- Pattern matching
- Frequent updates

Malware Detection

- Pattern matching
- Frequent updates
- Warning with extreme prejudice

The Traditional Way

- Descriptions of known-bad programs
- Everything else is allowed
- Problem: Evasion

The Gatekeeper Way

- Descriptions of identified programs
- Everything else is denied
- Problem: Catch all the good ones

Gatekeeper

Gatekeeper

- System facility

Gatekeeper

- System facility
- Rule-driven

Gatekeeper

- System facility
- Rule-driven
- Based on signatures and Code Requirements

Gatekeeper

- System facility
- Rule-driven
- Based on signatures and Code Requirements
- Highly configurable

Gatekeeper

- System facility
- Rule-driven
- Based on signatures and Code Requirements
- Highly configurable
- Applied to downloads

Demo

Affected Subjects

Affected Subjects

- Applications and other code

Affected Subjects

- Applications and other code
- Flat Installer packages

Affected Subjects

- Applications and other code
- Flat Installer packages
- Dangerous documents

Affected Subjects

- Applications and other code
- Flat Installer packages
- Dangerous documents
- XIP Archives (.xip)

XIP Archives

- New archive file format
- Signed with installer certificates
- Create and sign using command line
- Extract by opening (double-clicking)

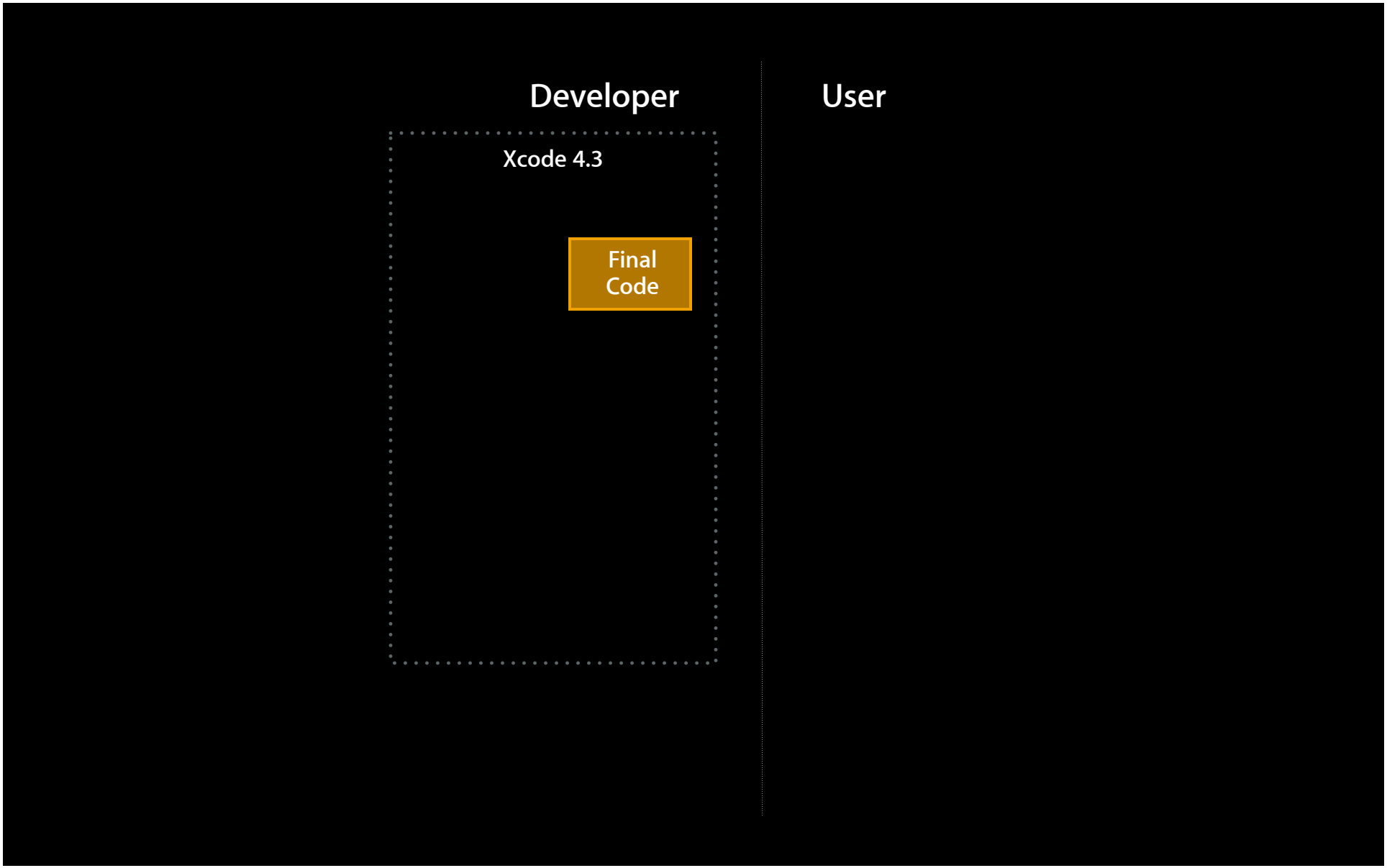
Rules

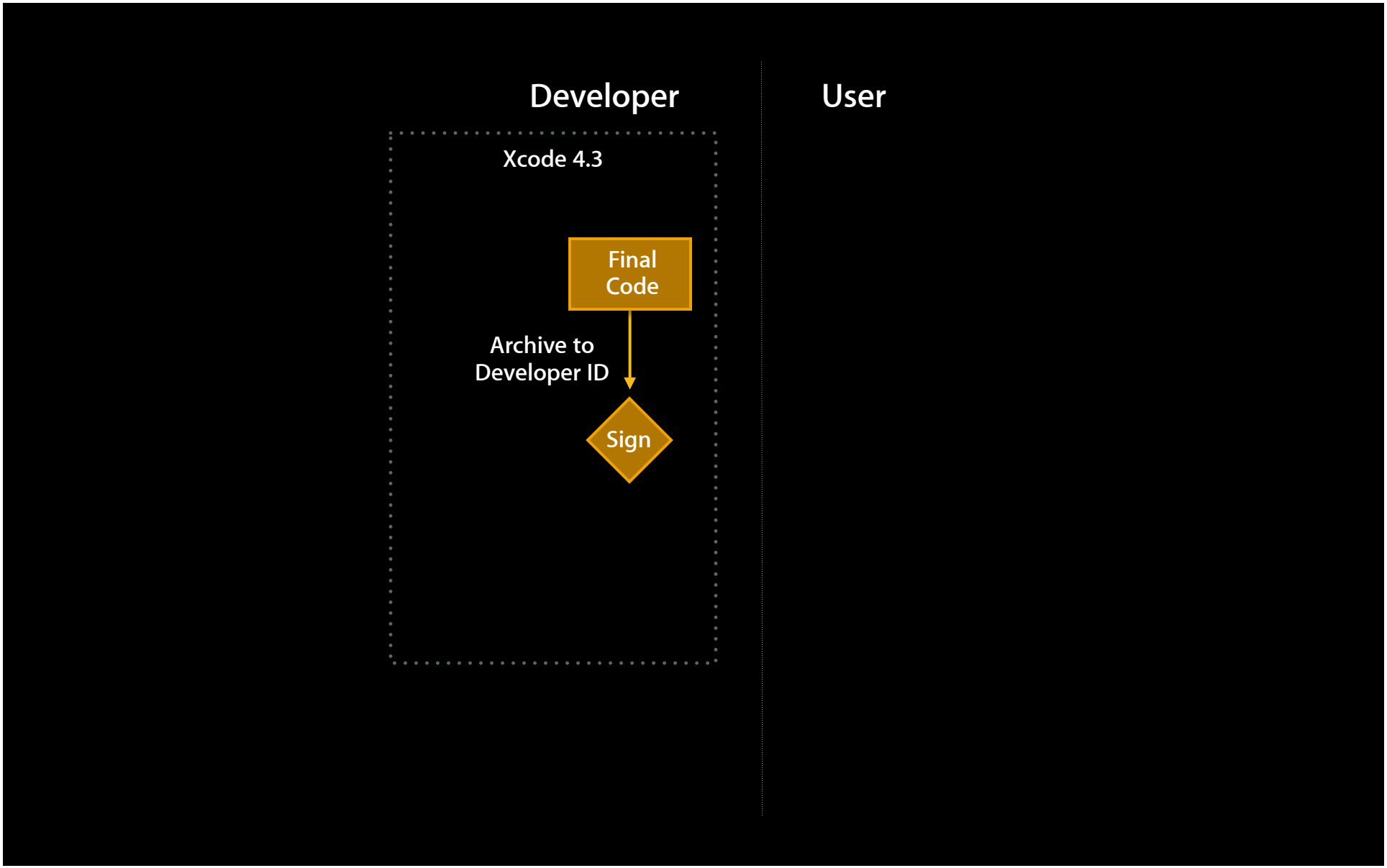
- Matched by Code Requirements
- Typed (execution, installation, …)
- Can be prioritized, labelled, disabled, expired, annotated, searched, …
- Outcomes cached systemwide

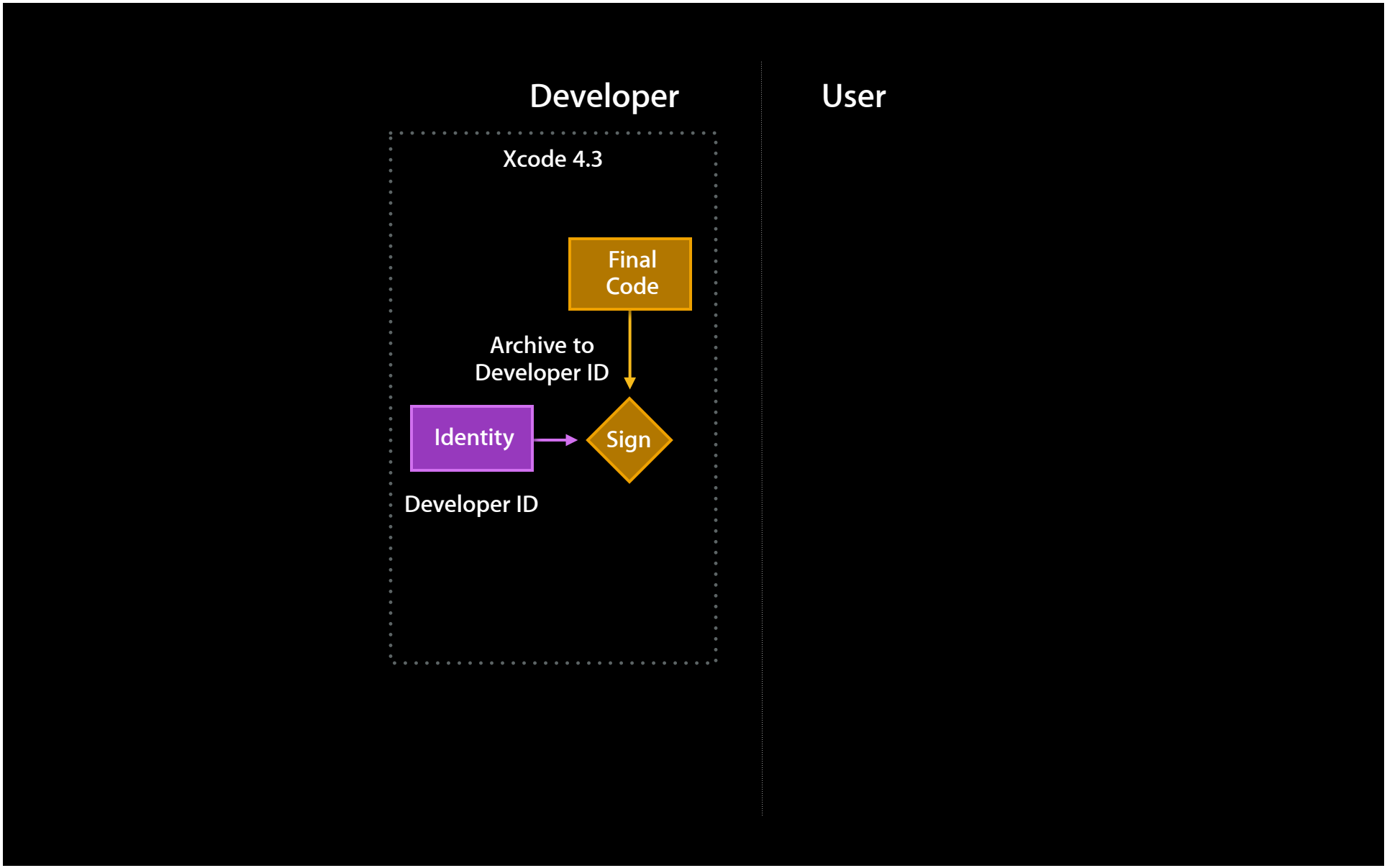
Developer

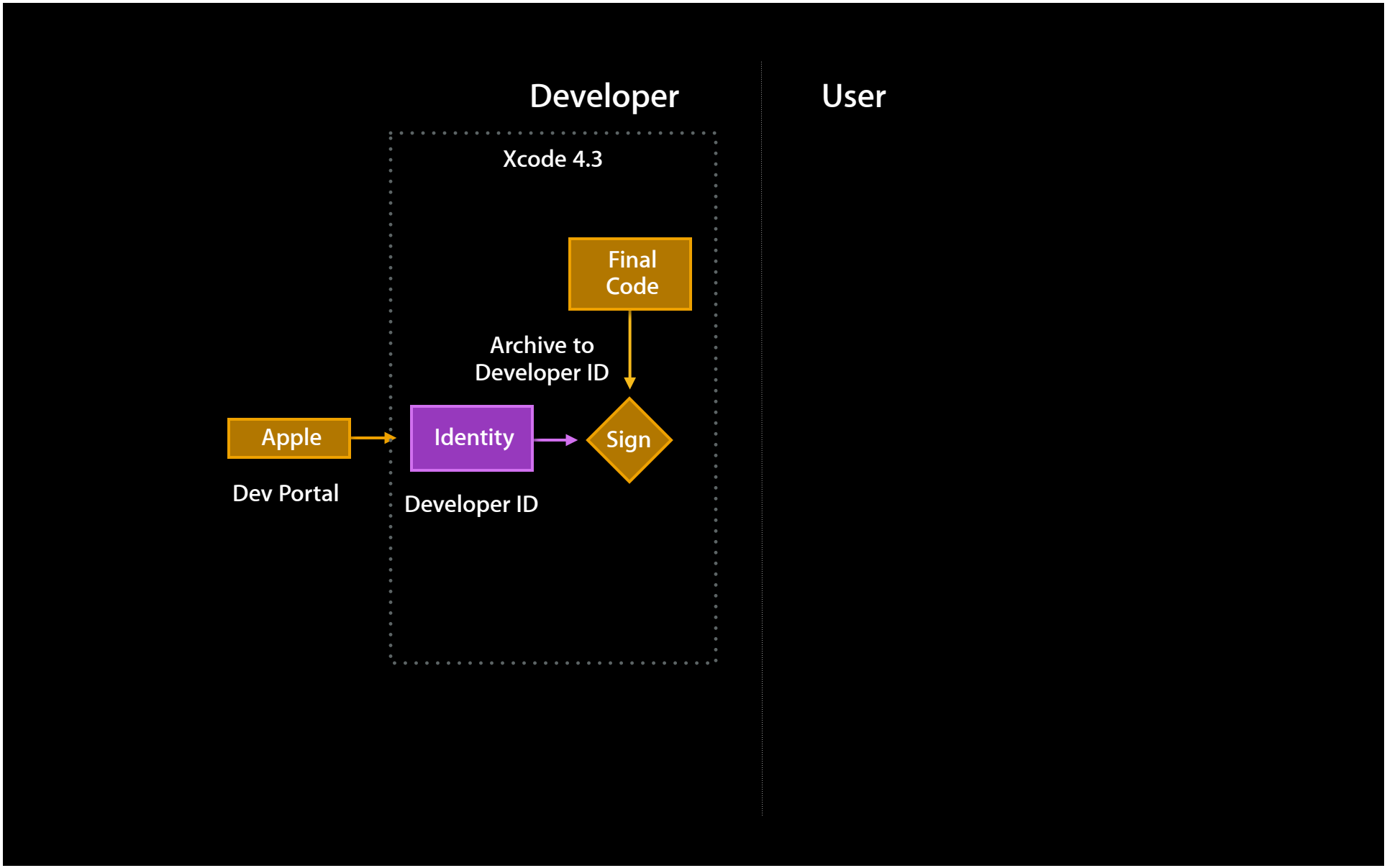
User

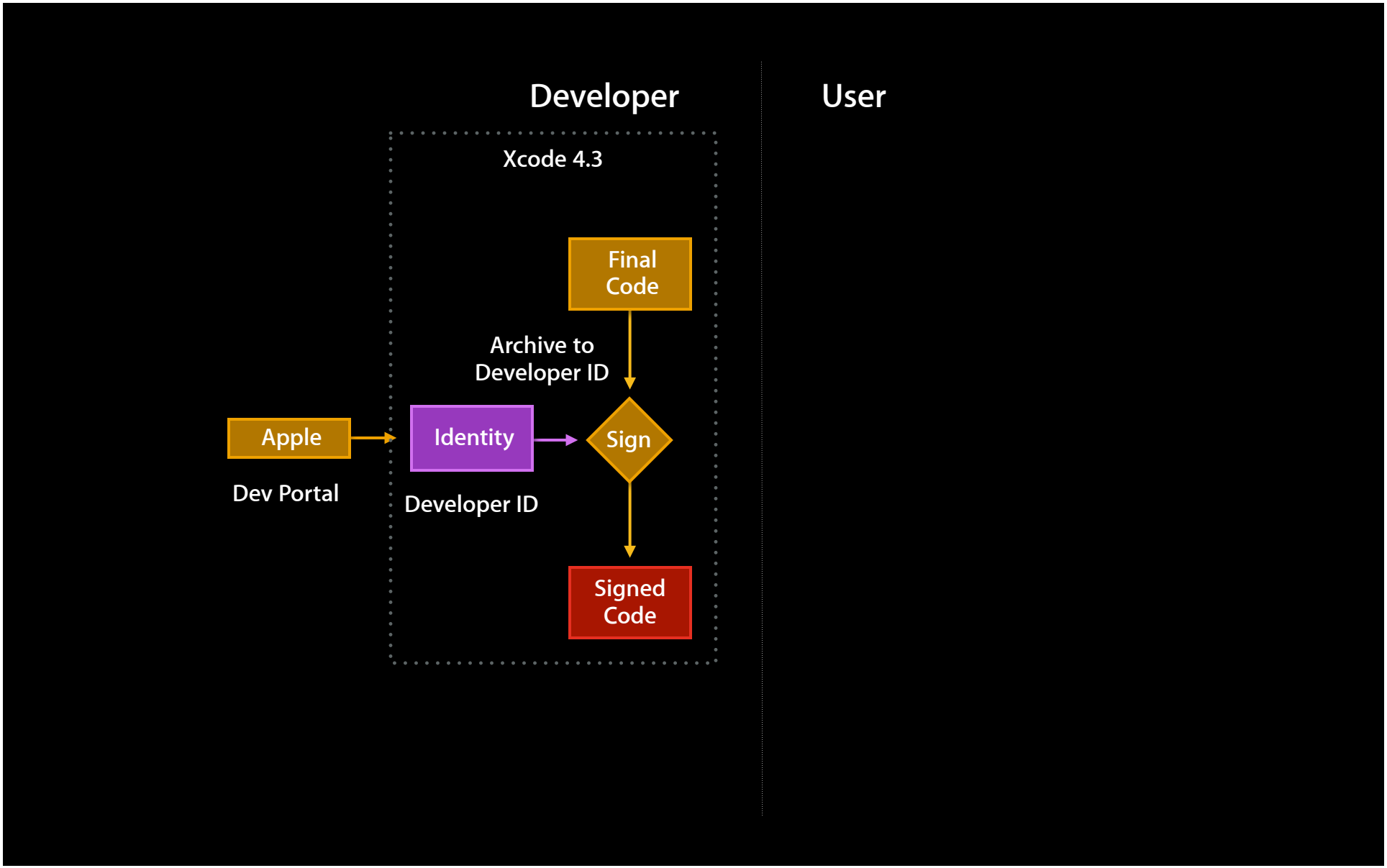

Developer
User
Final
Code

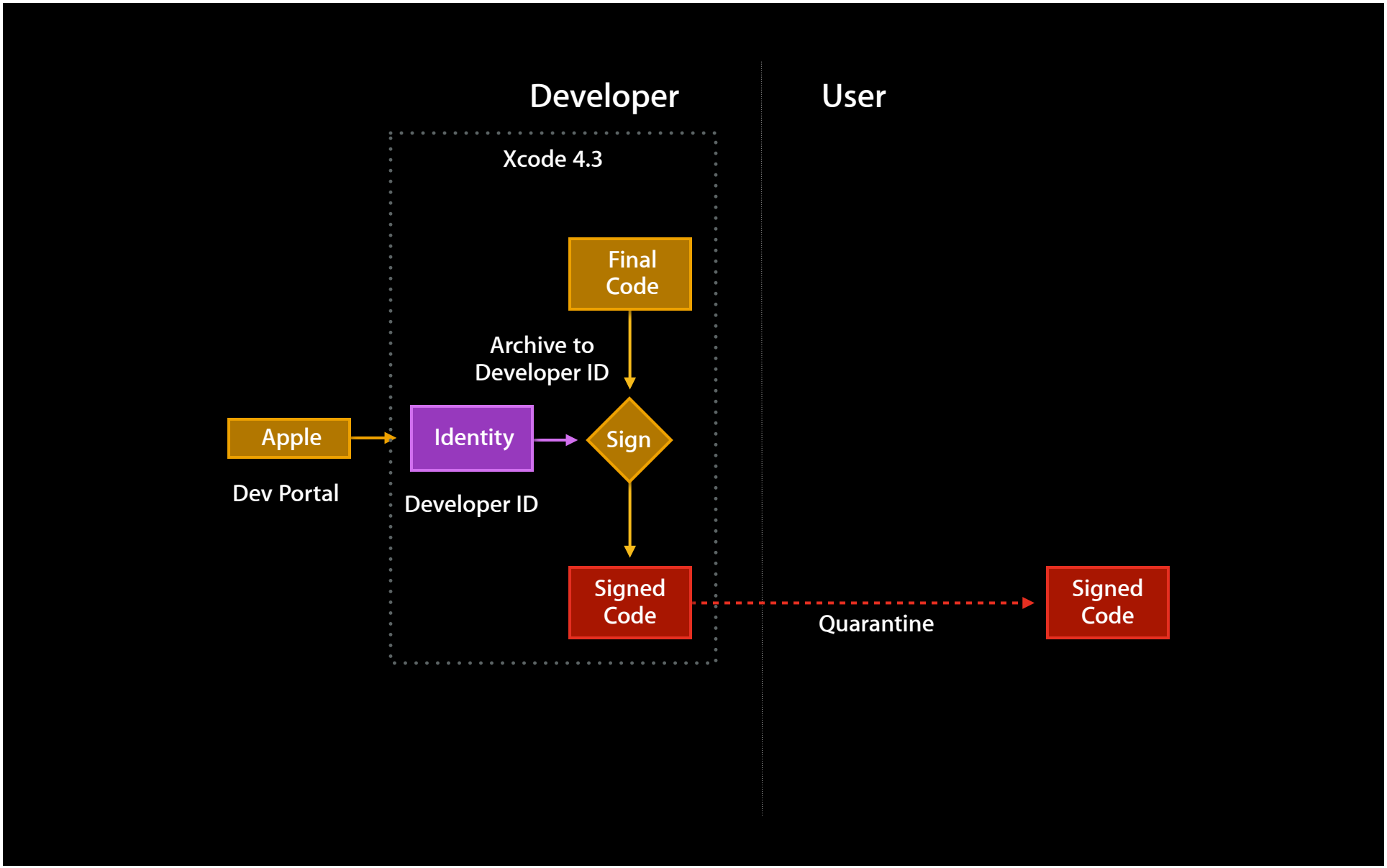

Developer
User
Xcode 4.3
Final
Code

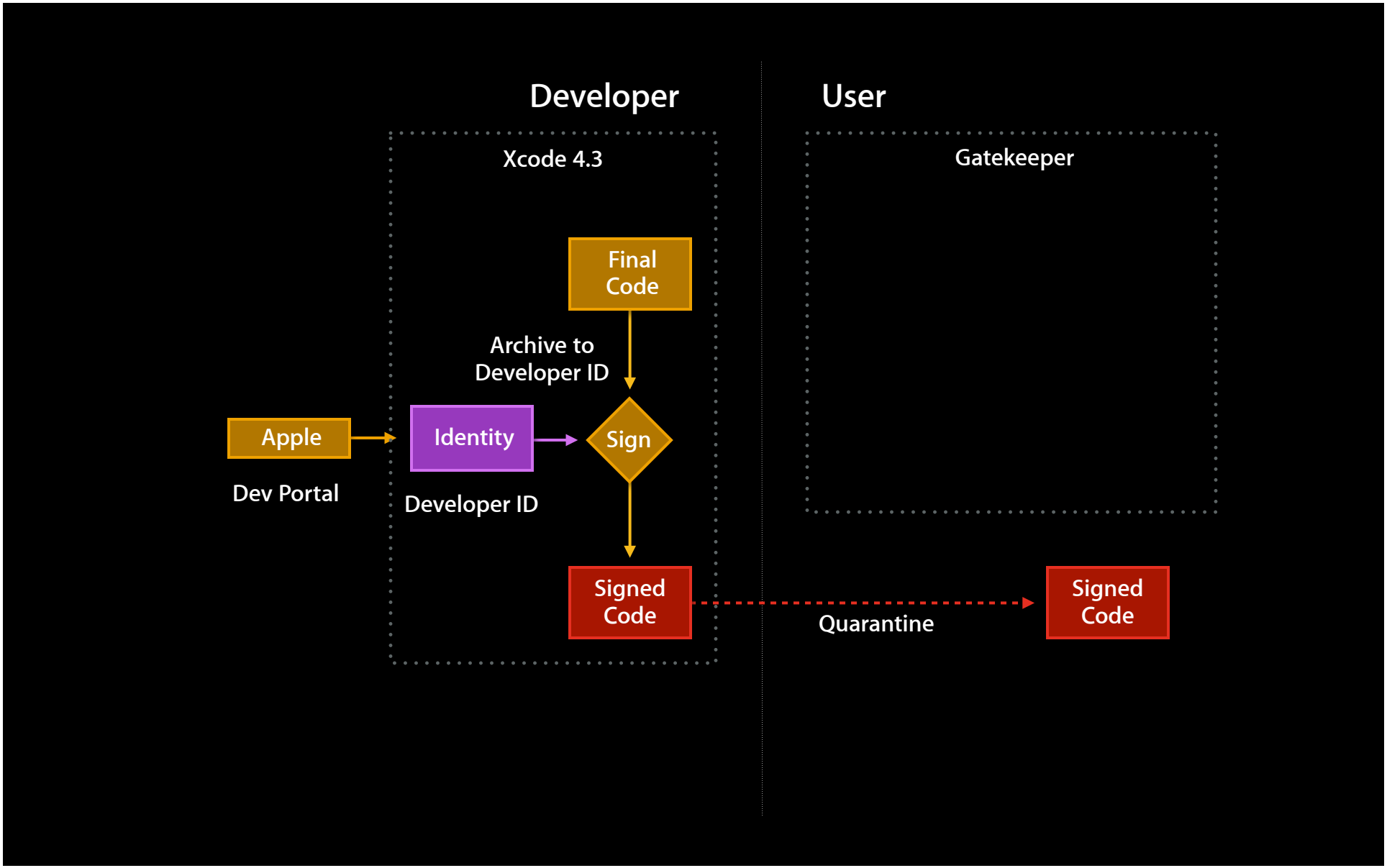

Developer
User
Xcode 4.3
Final Code
Archive to Developer ID
Sign

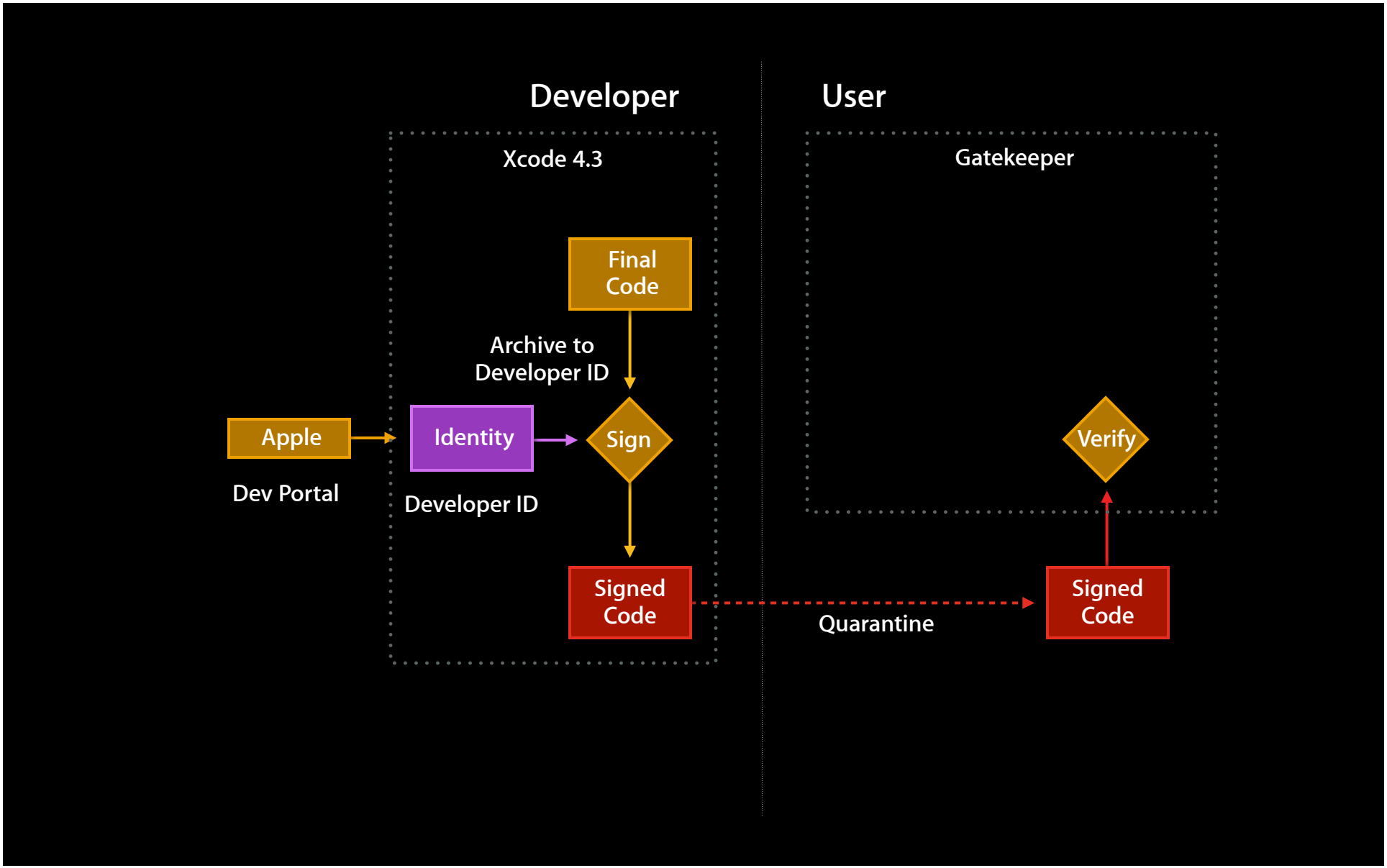

Developer
User
Xcode 4.3
Final Code
Archive to Developer ID
Identity
Sign
Developer ID

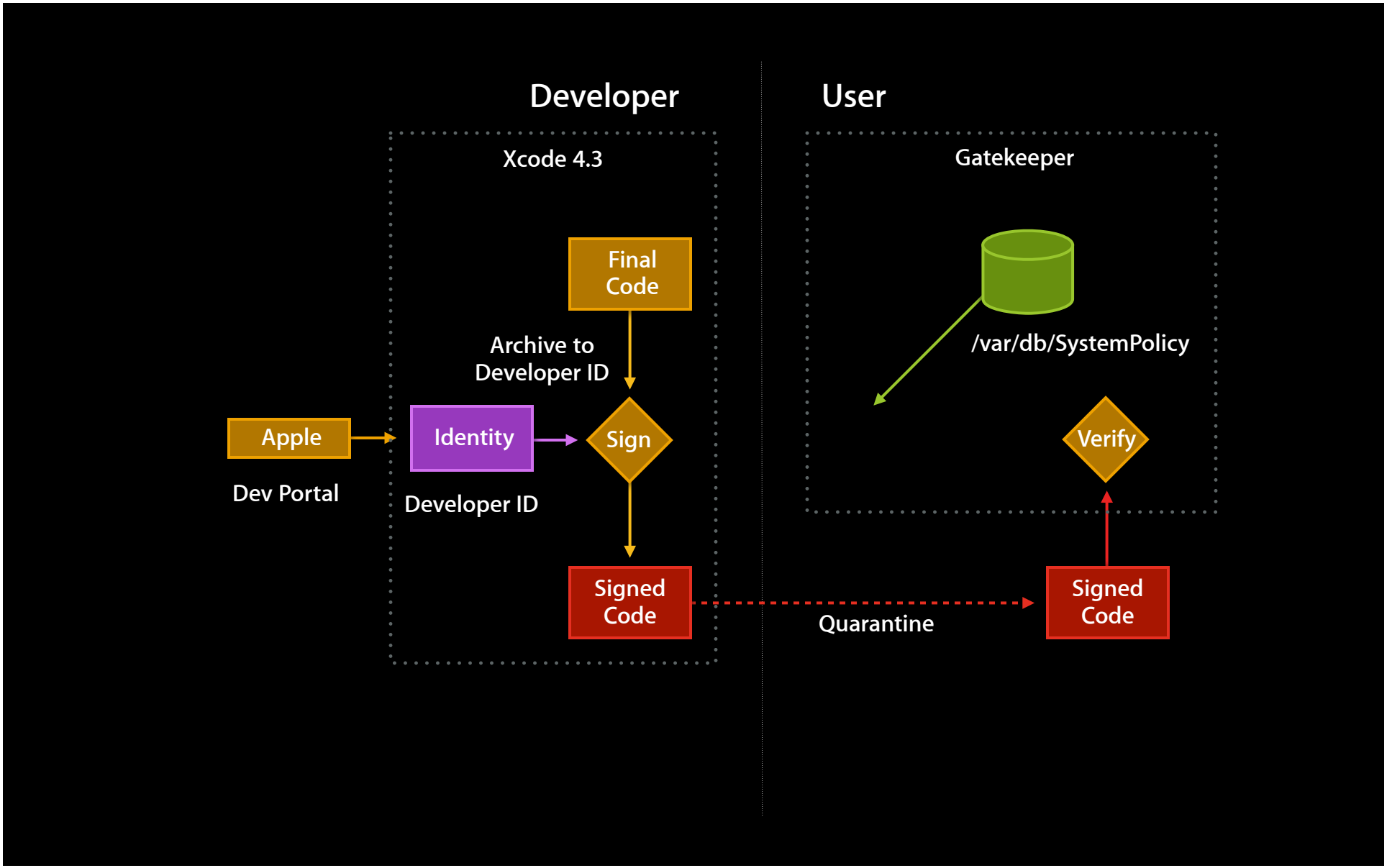

Developer
User
Xcode 4.3
Final Code
Archive to Developer ID
Apple
Identity
Sign
Dev Portal
Developer ID

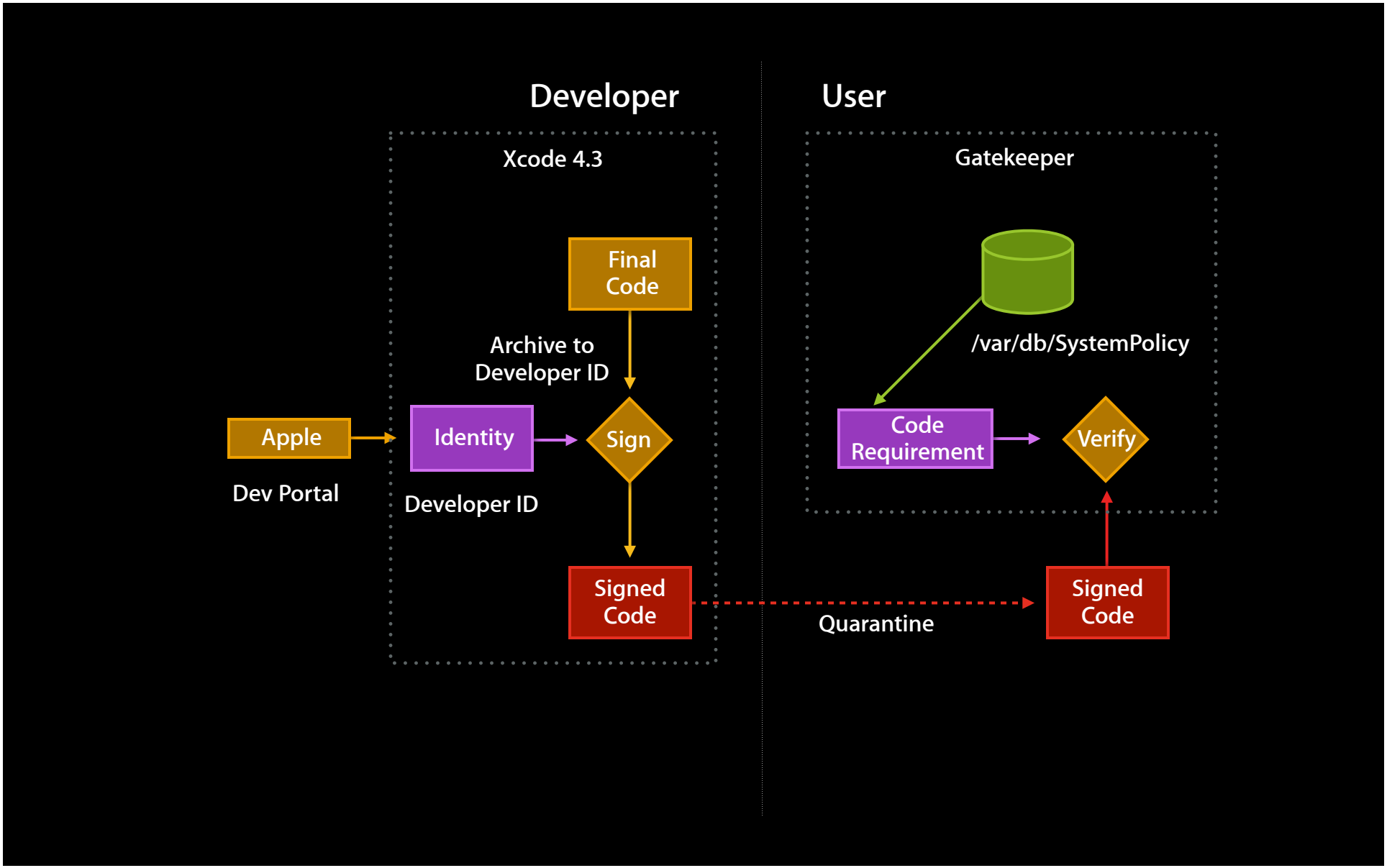

Developer
User
Xcode 4.3
Final Code
Archive to Developer ID
Apple
Identity
Sign
Dev Portal
Developer ID
Signed Code


Developer
User
Xcode 4.3
Final Code
Archive to Developer ID
Apple
Identity
Sign
Dev Portal
Developer ID
Signed Code
Quarantine
Signed Code


Developer
User
Xcode 4.3
Gatekeeper
Final Code
Archive to Developer ID
Apple
Identity
Sign
Dev Portal
Developer ID
Signed Code
Quarantine
Signed Code


Developer
User
Xcode 4.3
Gatekeeper
Final Code
Archive to Developer ID
Apple
Identity
Sign
Verify
Dev Portal
Developer ID
Signed Code
Signed Code
Quarantine


Developer
User
Xcode 4.3
Gatekeeper
Final Code
Archive to Developer ID
/var/db/SystemPolicy
Apple
Identity
Sign
Verify
Dev Portal
Developer ID
Signed Code
Signed Code
Quarantine


Developer
User
Xcode 4.3
Gatekeeper
Final Code
Archive to Developer ID
/var/db/SystemPolicy
Apple
Identity
Sign
Code Requirement
Verify
Dev Portal
Developer ID
Signed Code
Signed Code
Quarantine

Rule Deployment

Rule Deployment

- Default (System, Mac App Store, Developer ID)

Rule Deployment

- Default (System, Mac App Store, Developer ID)
- Individual exceptions (administrator)

Rule Deployment

- Default (System, Mac App Store, Developer ID)
- Individual exceptions (administrator)
- Configuration profiles (OS X Server)

Rule Deployment

- Default (System, Mac App Store, Developer ID)
- Individual exceptions (administrator)
- Configuration profiles (OS X Server)
- Workgroup Manager (OS X Server)

Rule Deployment

- Default (System, Mac App Store, Developer ID)
- Individual exceptions (administrator)
- Configuration profiles (OS X Server)
- Workgroup Manager (OS X Server)
- Local rule changes (administrator: `spctl`)

Supported Systems

Supported Systems

- Mountain Lion (enabled by default)

Supported Systems

- Mountain Lion (enabled by default)
- Lion 10.7.4+ (disabled and hidden by default)

End-to-End Test

- Download via Safari
  - Or mail an attachment and save
- Double-click it in the Finder
- Watch what happens

Terminal Tools

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
$ spctl --add --label MyTest ~/Downloads/Frob.app
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
$ spctl --add --label MyTest ~/Downloads/Frob.app

$ man codesign   # Examine code signatures
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
$ spctl --add --label MyTest ~/Downloads/Frob.app

$ man codesign   # Examine code signatures
$ codesign --verify --verbose=3 ~/Downloads/Frob.app
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
$ spctl --add --label MyTest ~/Downloads/Frob.app

$ man codesign   # Examine code signatures
$ codesign --verify --verbose=3 ~/Downloads/Frob.app
$ codesign --display --verbose=3 ~/Downloads/Frob.app
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
$ spctl --add --label MyTest ~/Downloads/Frob.app

$ man codesign   # Examine code signatures
$ codesign --verify --verbose=3 ~/Downloads/Frob.app
$ codesign --display --verbose=3 ~/Downloads/Frob.app

$ man csreq      # manipulate and test code requirements
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
$ spctl --add --label MyTest ~/Downloads/Frob.app

$ man codesign   # Examine code signatures
$ codesign --verify --verbose=3 ~/Downloads/Frob.app
$ codesign --display --verbose=3 ~/Downloads/Frob.app

$ man csreq      # manipulate and test code requirements

$ productsign --sign identity input.pkg output.pkg
```

Terminal Tools

```
$ man spctl      # Direct access to System Policy Assessor
$ spctl --assess ~/Downloads/Frob.app
$ spctl --add --label MyTest ~/Downloads/Frob.app

$ man codesign   # Examine code signatures
$ codesign --verify --verbose=3 ~/Downloads/Frob.app
$ codesign --display --verbose=3 ~/Downloads/Frob.app

$ man csreq      # manipulate and test code requirements

$ productsign --sign identity input.pkg output.pkg
$ xip --sign identity inputs... output
```

More Information

Paul Danbold
Core OS Evangelist
danbold@apple.com

Documentation
Developer ID and Gatekeeper
http://developer.apple.com/resources/developer-id/

Apple Developer Forums
http://devforums.apple.com

Related Sessions

The Security Framework	Nob Hill Tuesday 2:00PM
Building, Archiving, and Submitting Your App	Pacific Heights Thursday 4:30PM
The OS X App Sandbox (Repeat)	Nob Hill Friday 10:15AM

Labs

Security Lab	Core OS Lab B Tuesday 3:15PM
Xcode Lab	Developer Tools Lab B Tuesday 2:00PM
Security Lab (For Early Risers)	Core OS Lab B Thursday 9:00AM

Summary

- Gatekeeper helps the user control what runs on their Mac
- Developer ID helps you identify your code for those users
- Gatekeeper is on by default in Mountain Lion
  - Can be enabled in Lion if the user wishes
- Developer ID signed code will be allowed by default

Q&A


WWDC2012