

#WWDC18

# AVContentKeySession Best Practices

Session 507

Anil Katti, AVFoundation Engineer

# Agenda

# Agenda

FairPlay Streaming overview

# Agenda

FairPlay Streaming overview

AVContentKeySession API

# Agenda

FairPlay Streaming overview

AVContentKeySession API

Common pitfalls around key delivery

# Agenda

FairPlay Streaming overview

AVContentKeySession API

Common pitfalls around key delivery

Frequently asked questions

# FairPlay Streaming Overview

# FairPlay Streaming Overview

Introduced in 2015

Protects HLS streams



# FairPlay Streaming Overview

Introduced in 2015

Protects HLS streams

Specifies steps to securely deliver content decryption keys

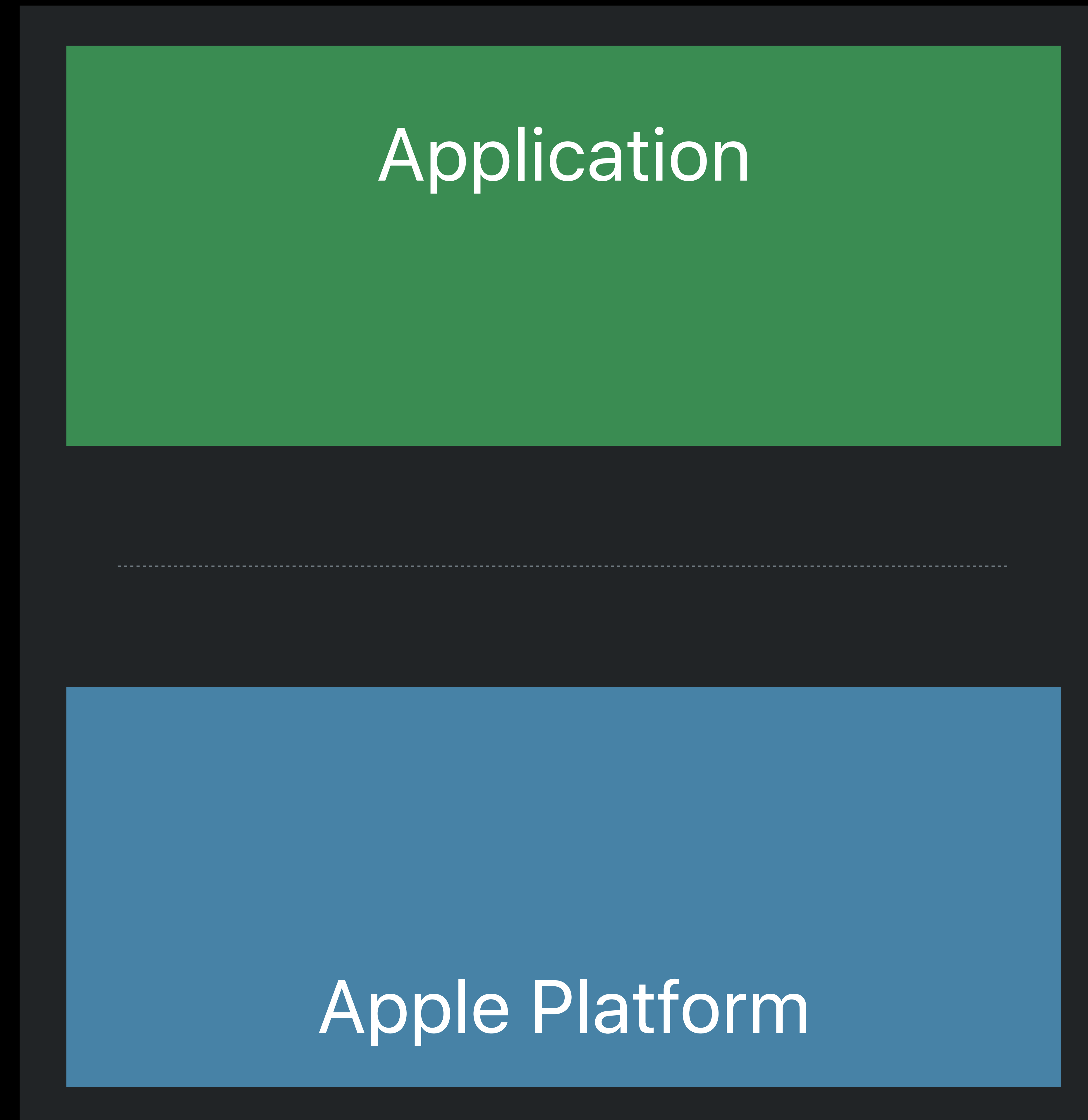
# FairPlay Streaming Overview

# FairPlay Streaming Overview

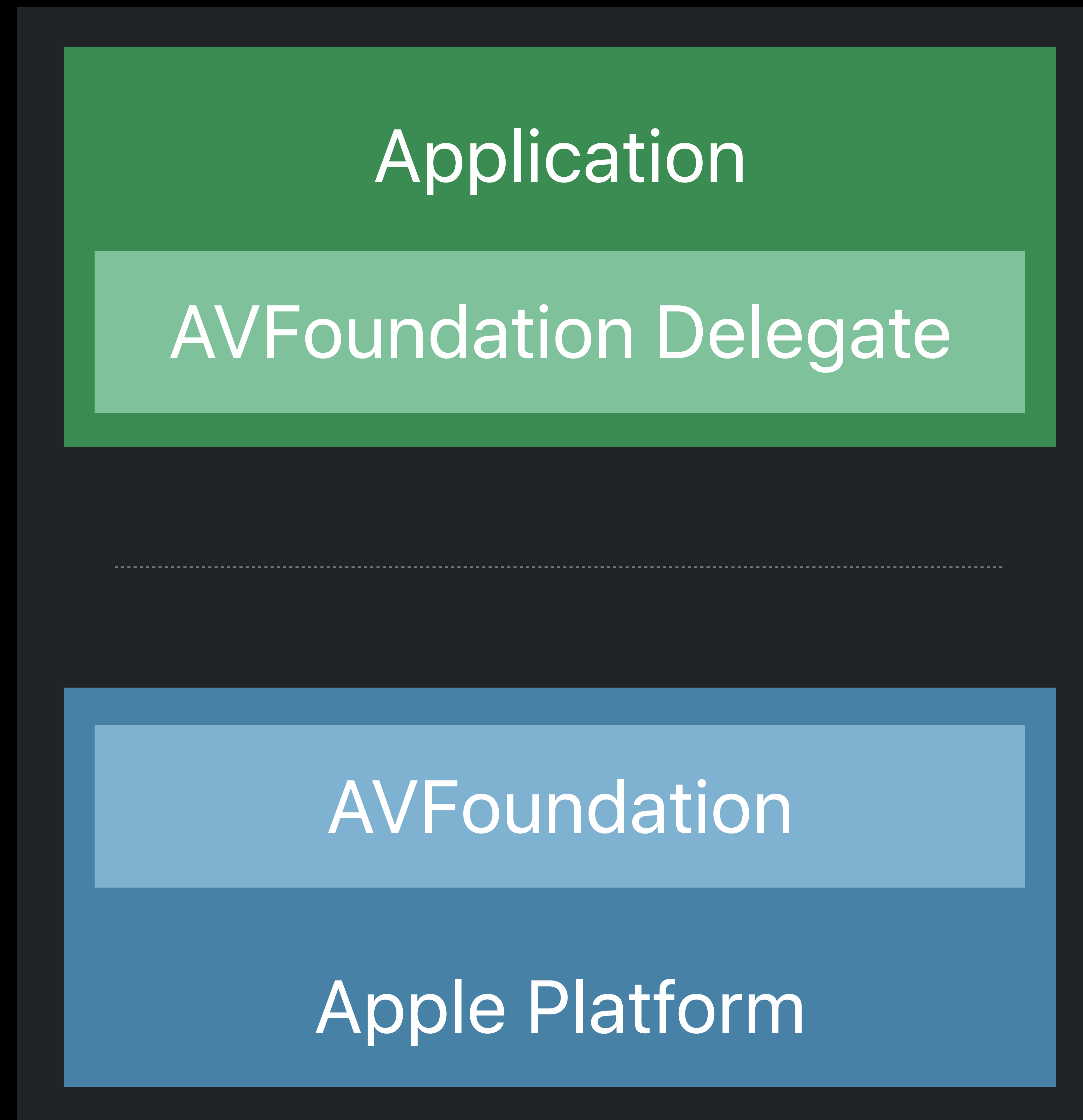


Application

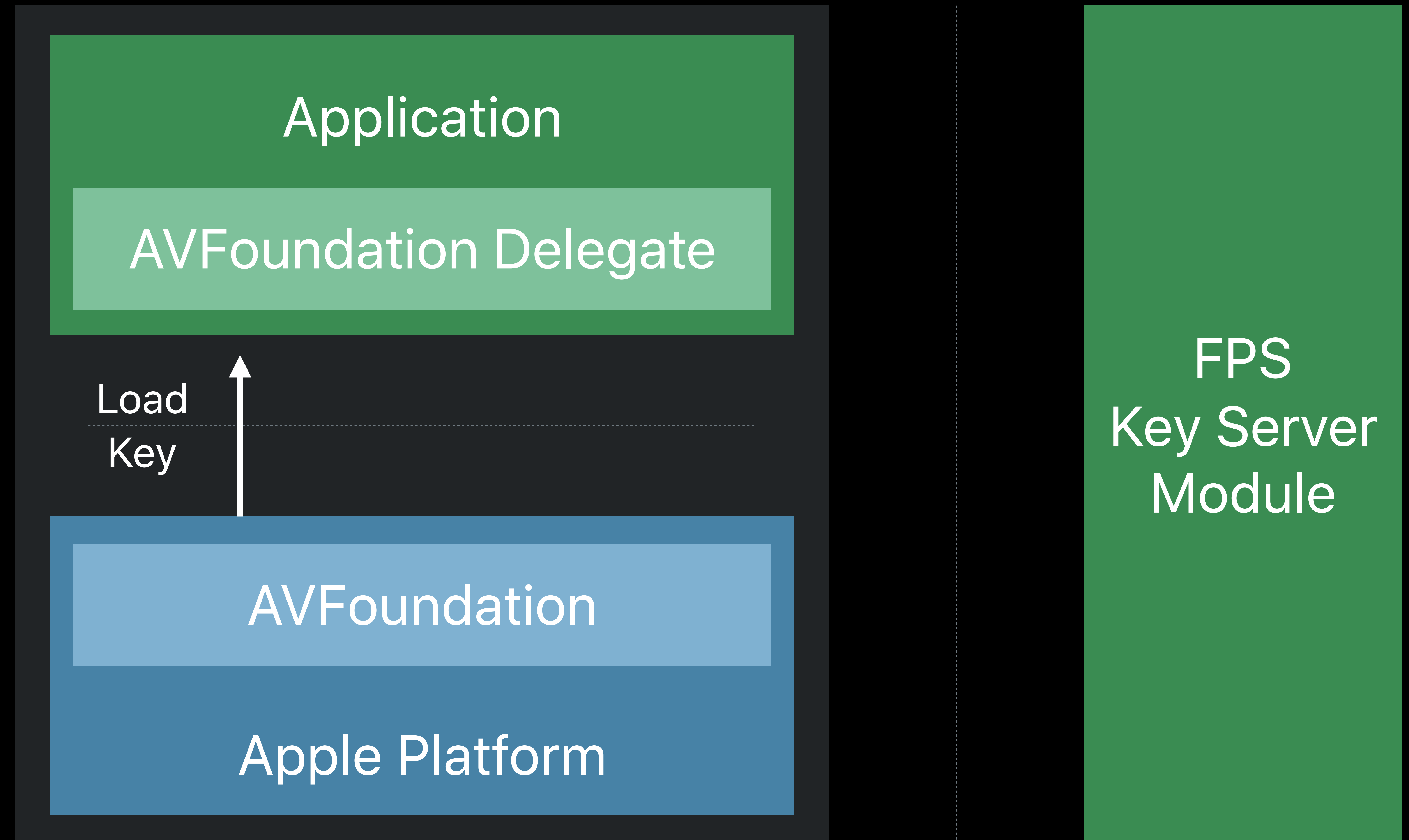
# FairPlay Streaming Overview



# FairPlay Streaming Overview

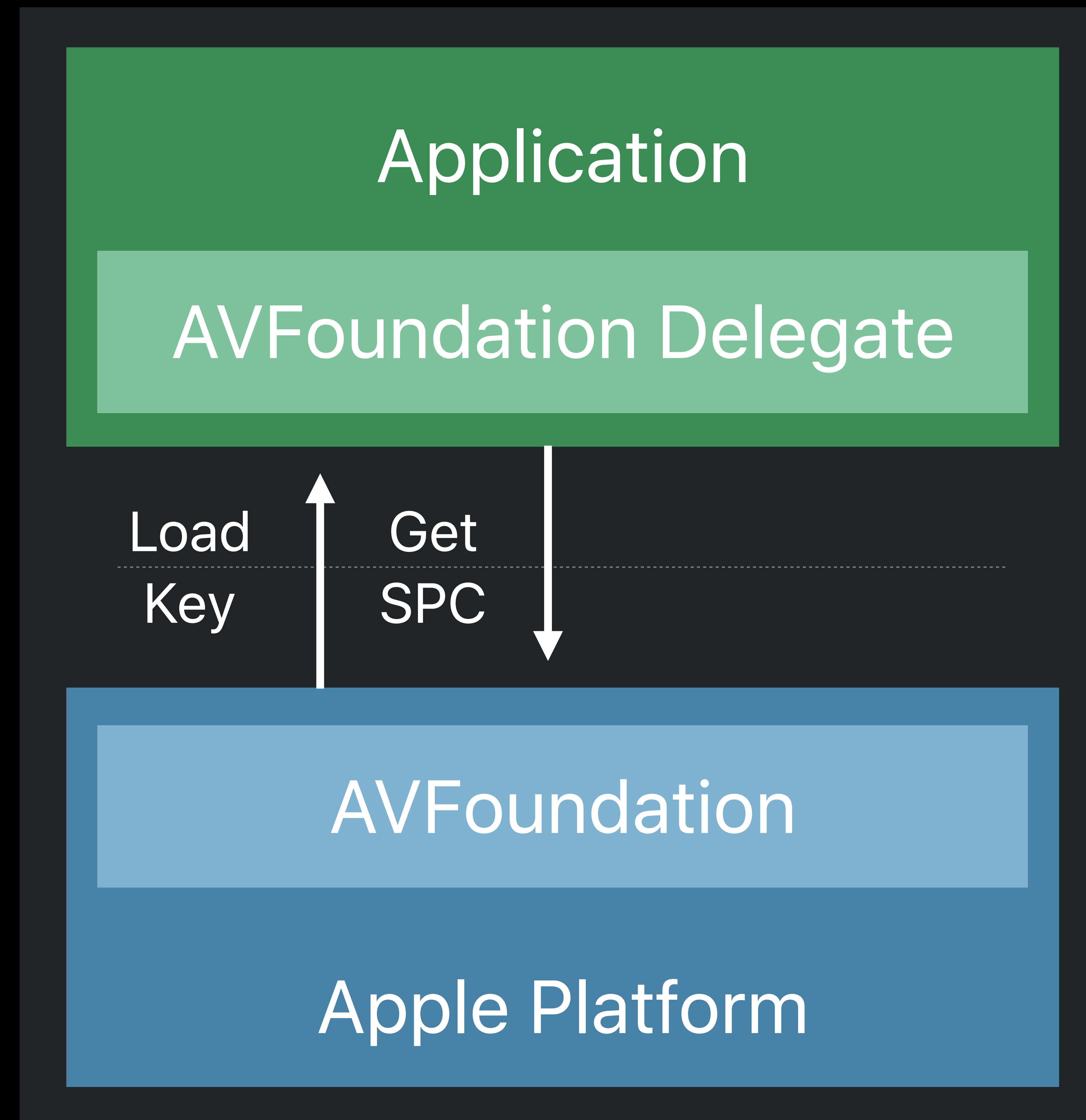


# FairPlay Streaming Overview



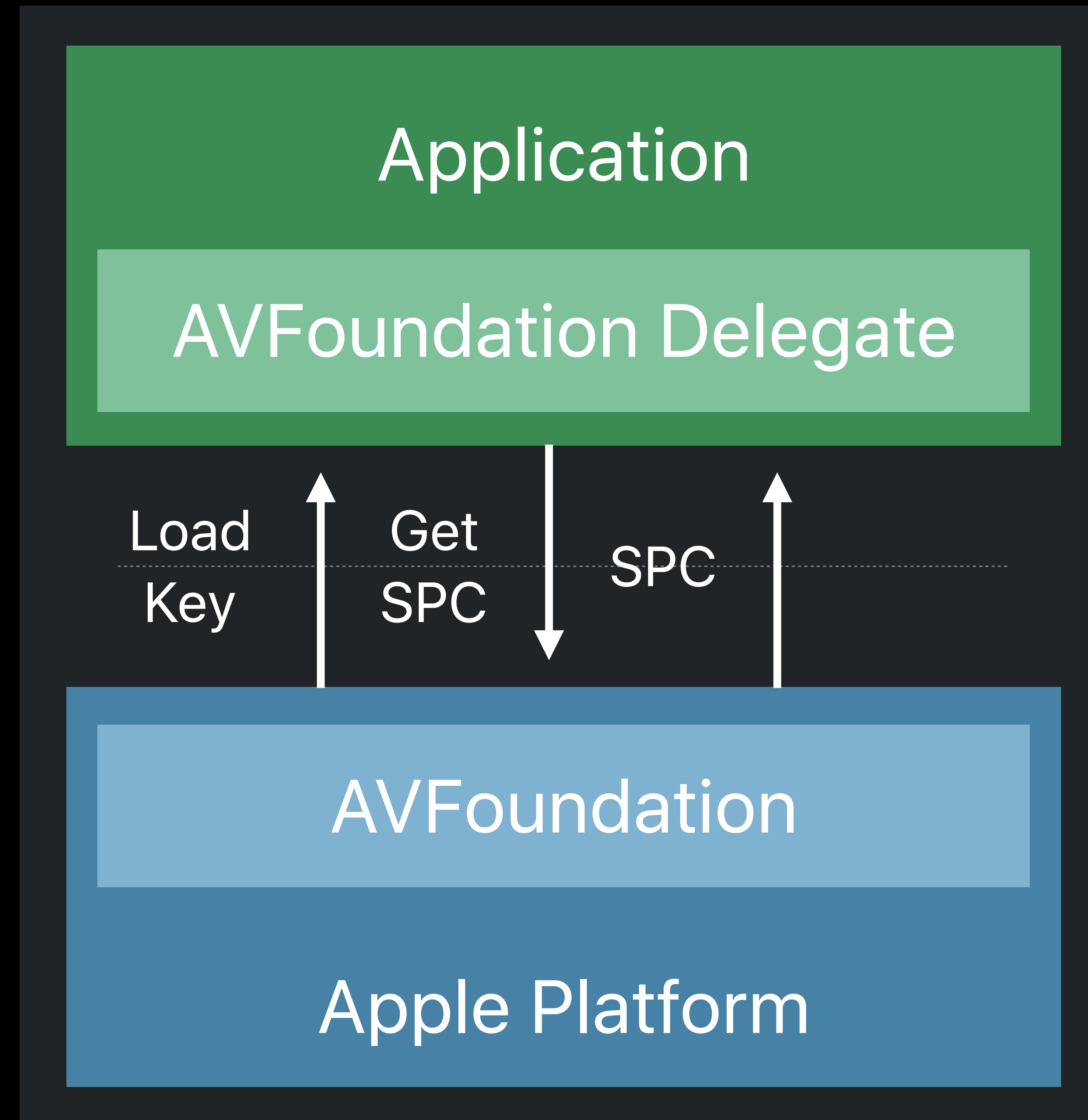
# FairPlay Streaming Overview

SPC = **S**ecure **P**layback **C**ontext  
(Encrypted Key Request)



# FairPlay Streaming Overview

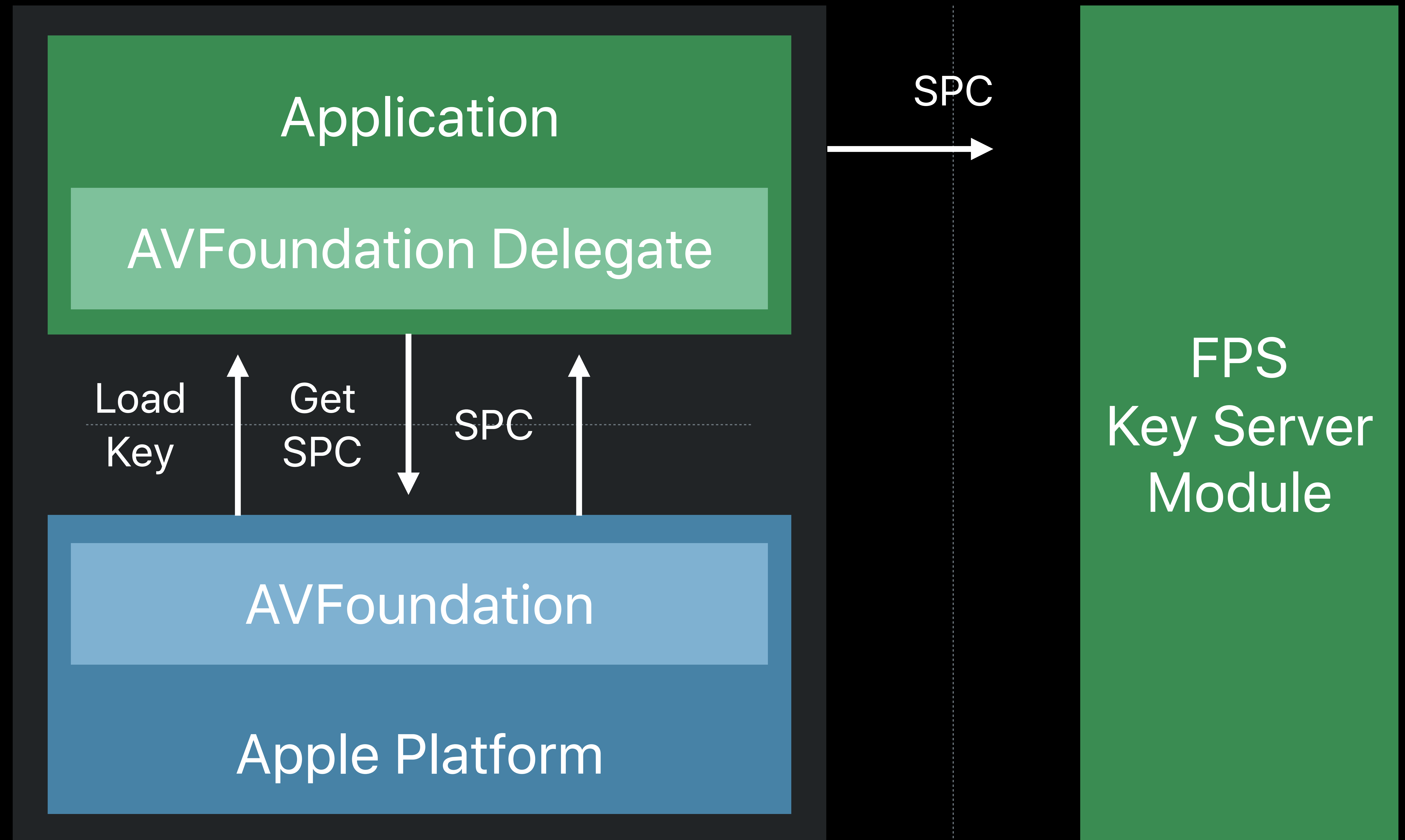
SPC = **S**ecure **P**layback **C**ontext  
(Encrypted Key Request)



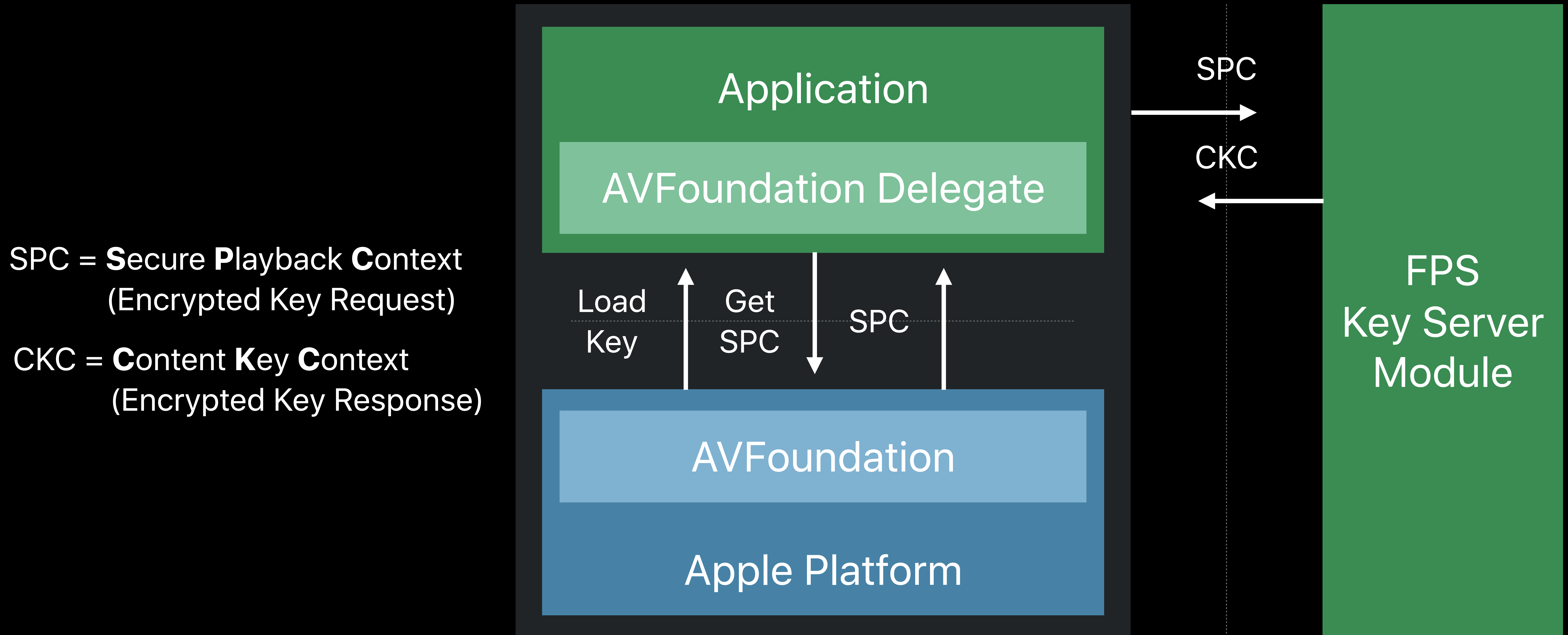


# FairPlay Streaming Overview

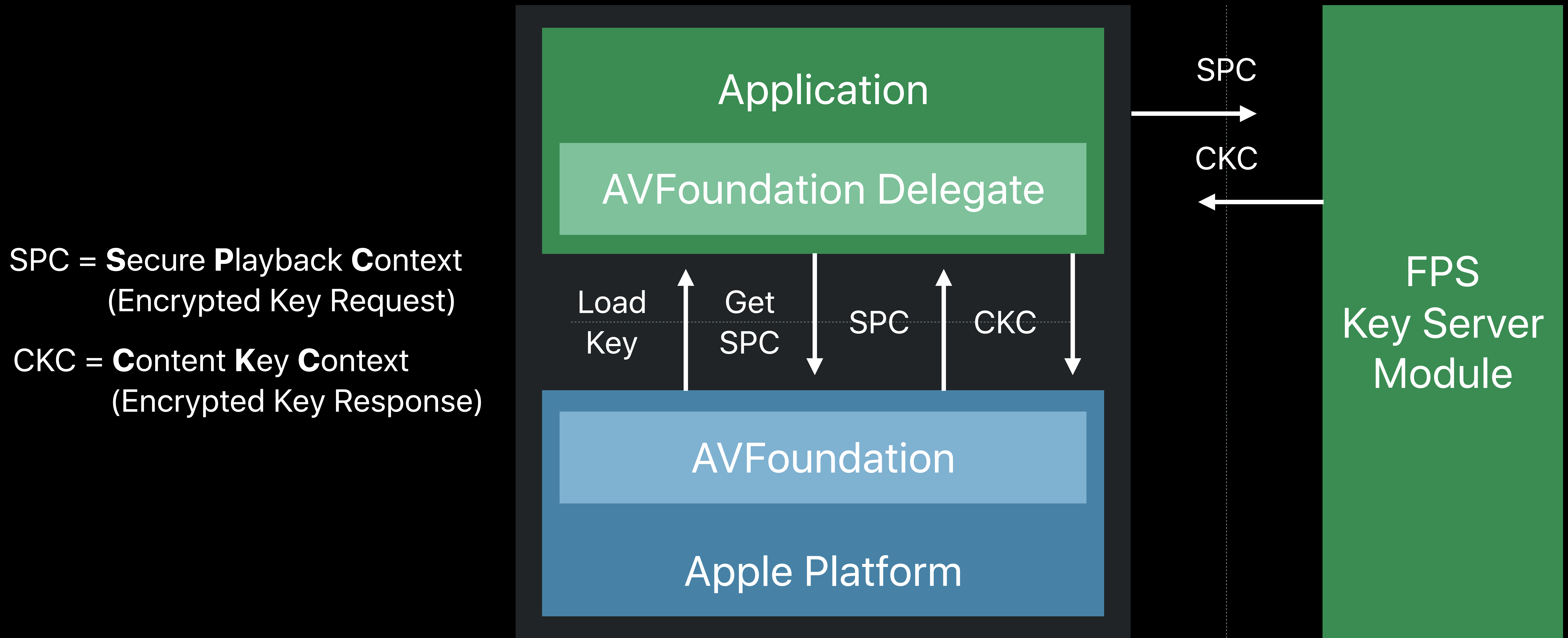
SPC = **S**ecure **P**layback **C**ontext  
(Encrypted Key Request)



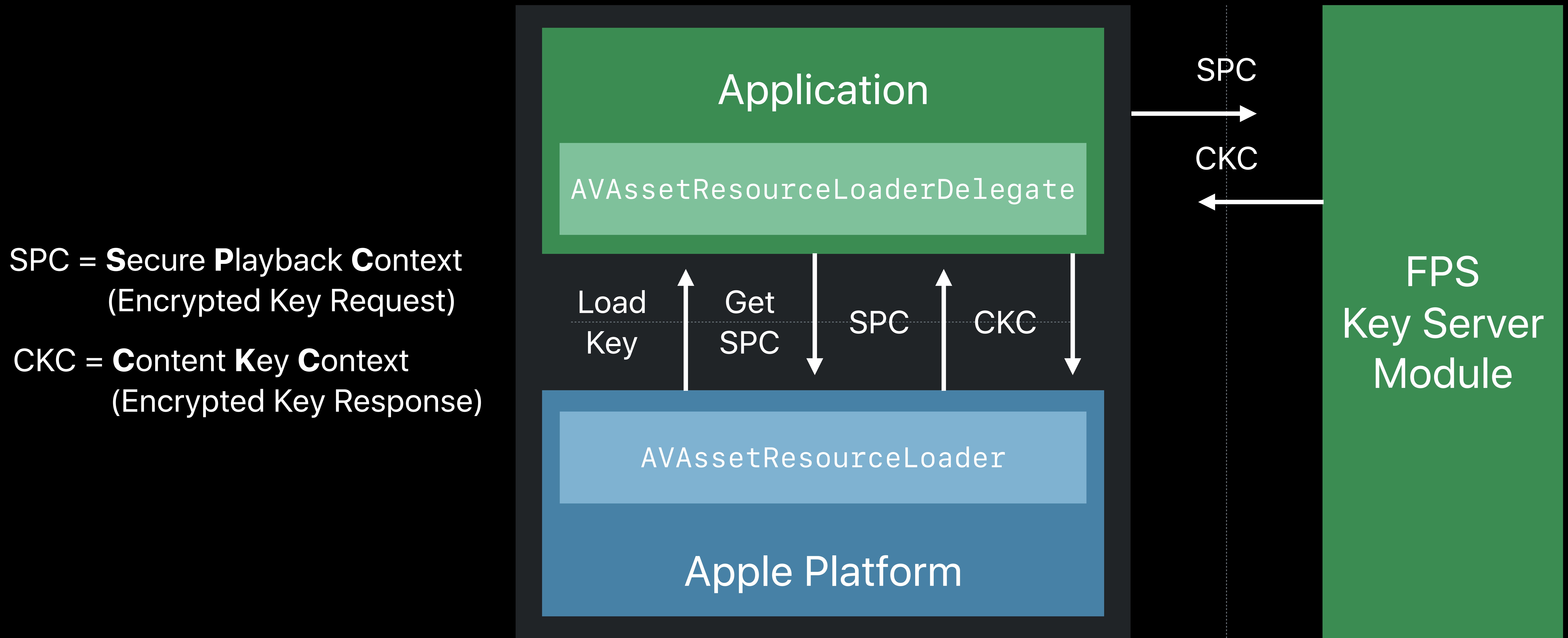
# FairPlay Streaming Overview



# FairPlay Streaming Overview



# FairPlay Streaming Overview



# AVContentKeySession

# AVContentKeySession

Introduced in 2017

# AVContentKeySession

Introduced in 2017

Designed around content decryption keys

# AVContentKeySession

Introduced in 2017

Designed around content decryption keys

- Simplified key loading process



# AVContentKeySession

Introduced in 2017

Designed around content decryption keys

- Simplified key loading process
- Home for new content protection features

# AVContentKeySession

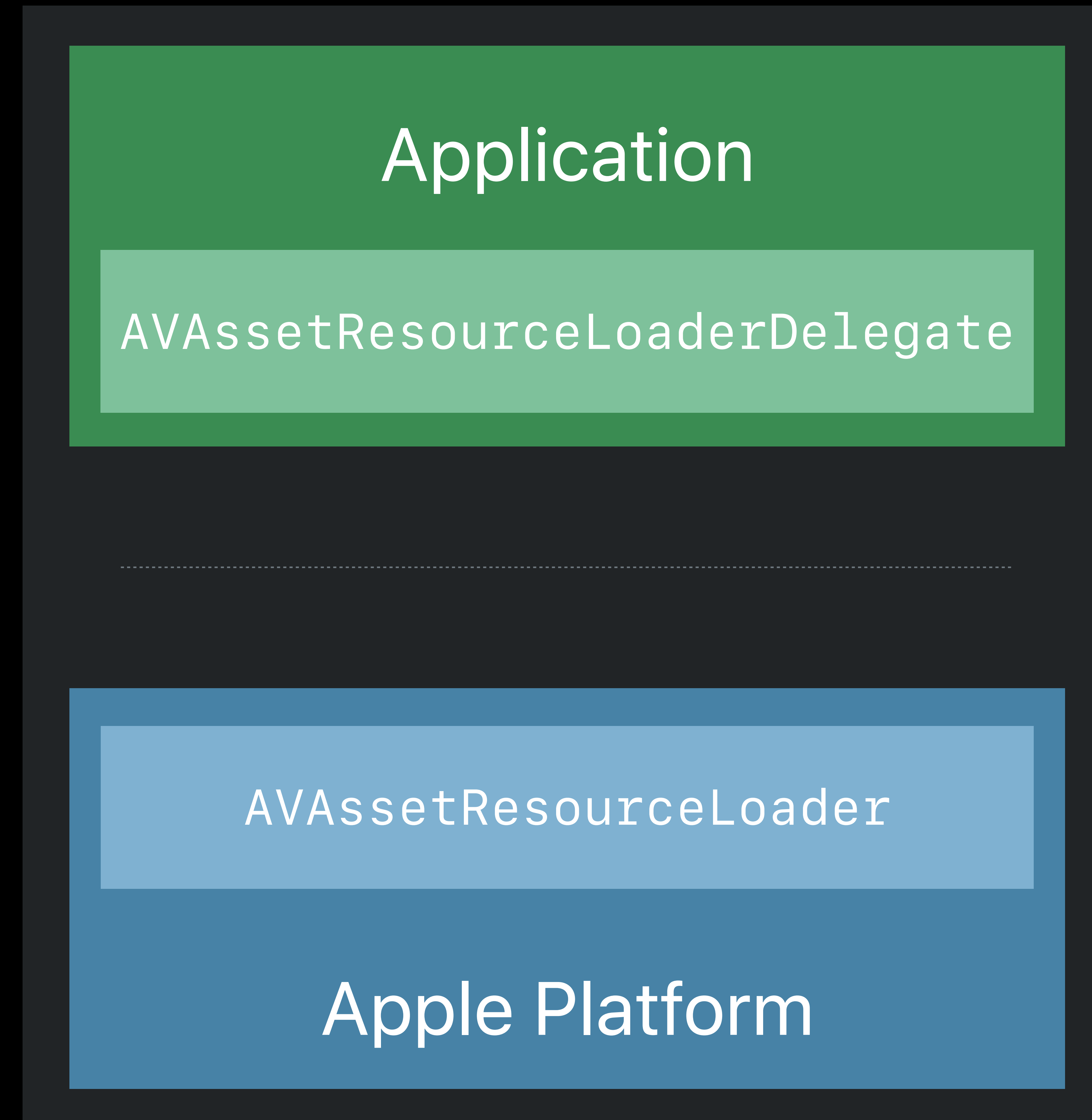
Introduced in 2017

Designed around content decryption keys

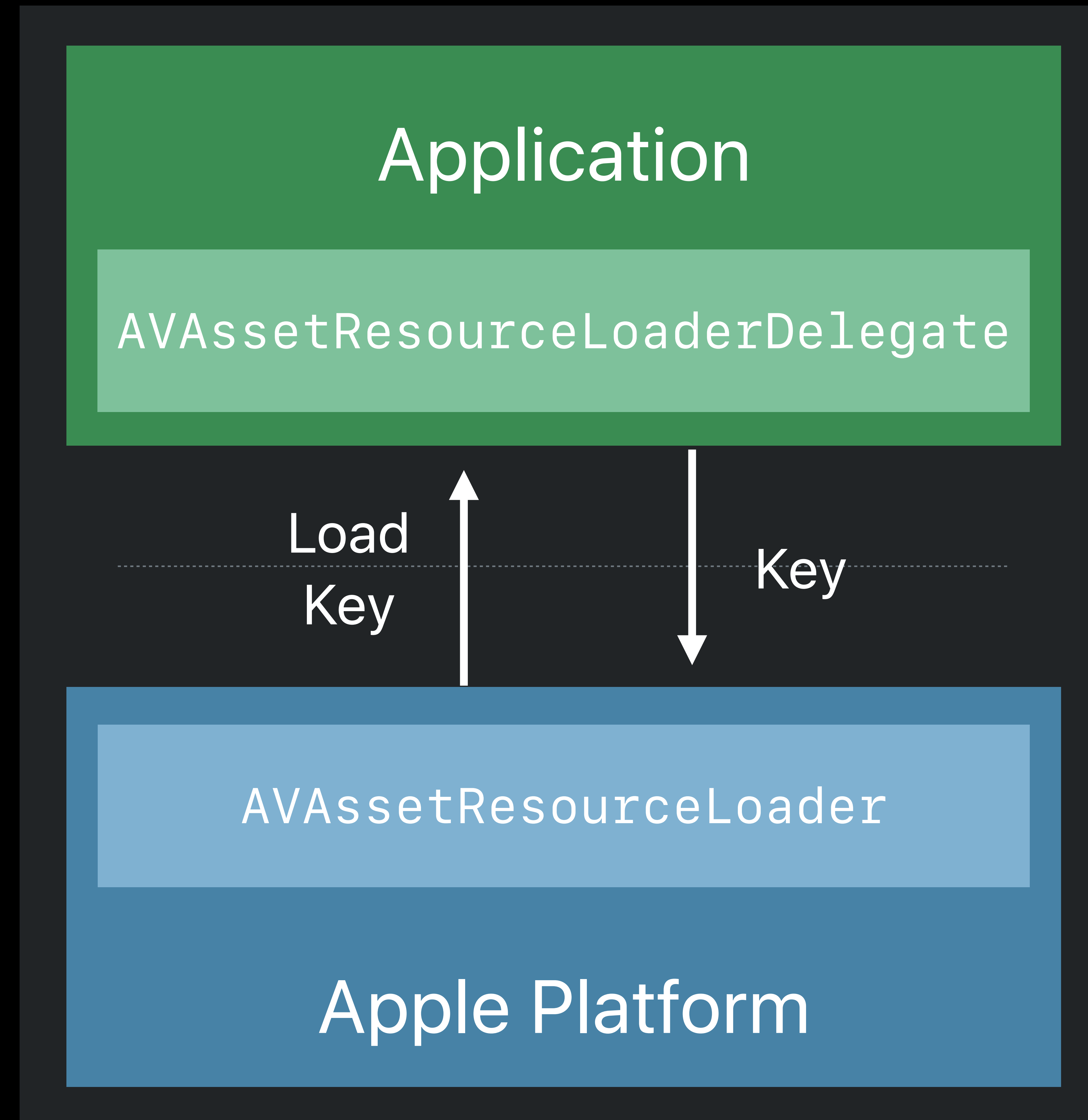
- Simplified key loading process
- Home for new content protection features

Great adoption - helps optimize key delivery

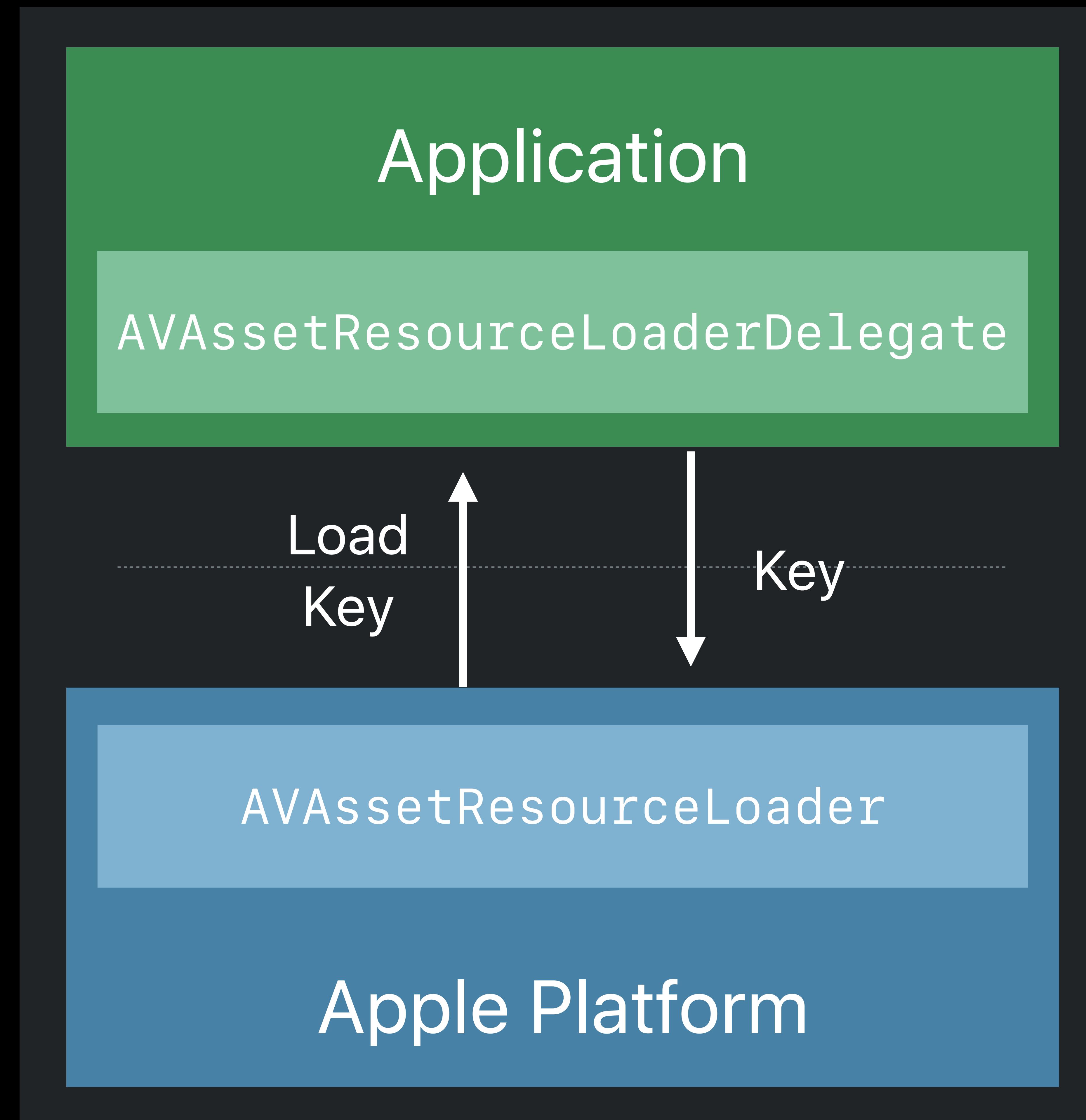
# AVAssetResourceLoader



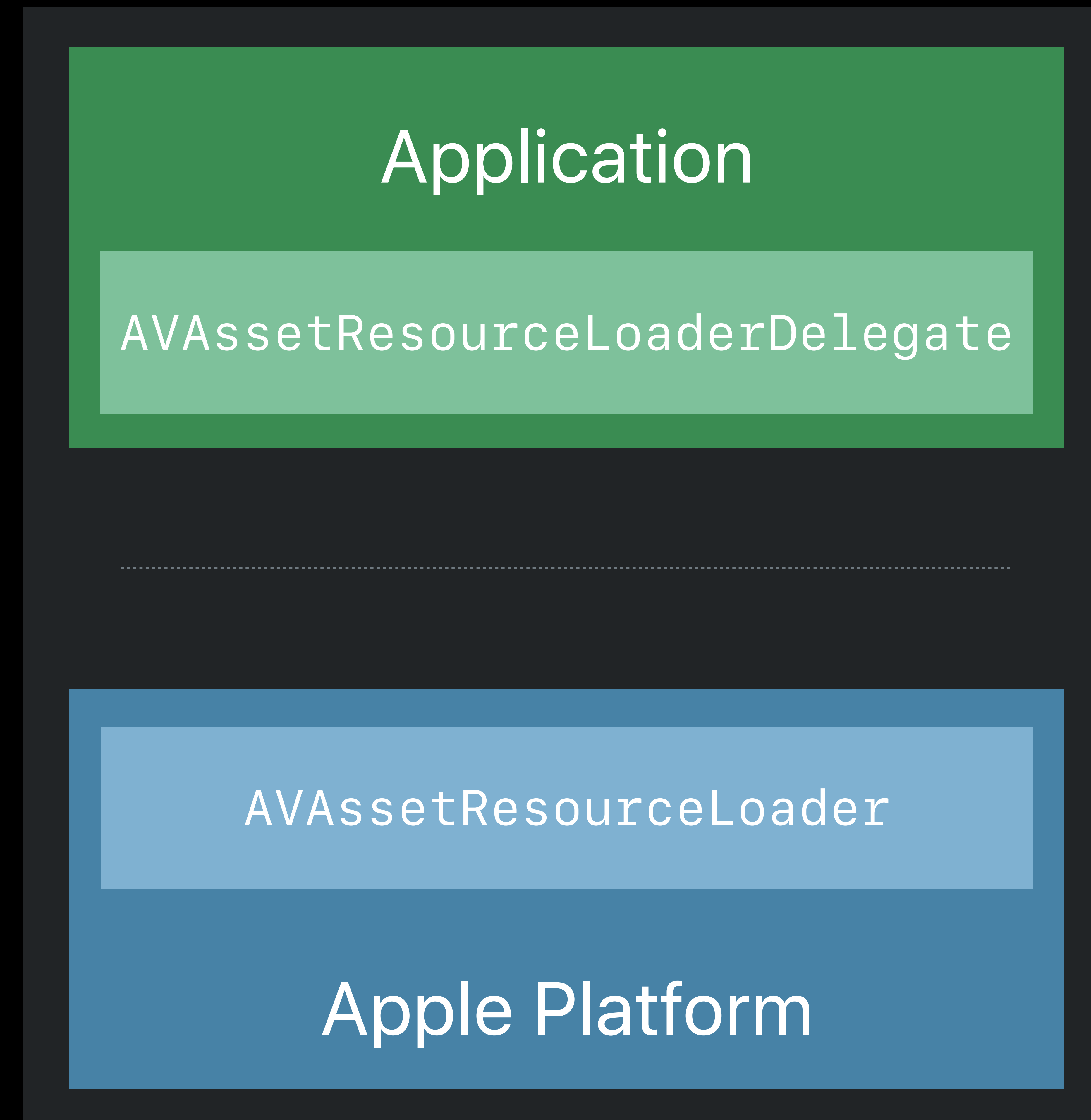
# AVAssetResourceLoader



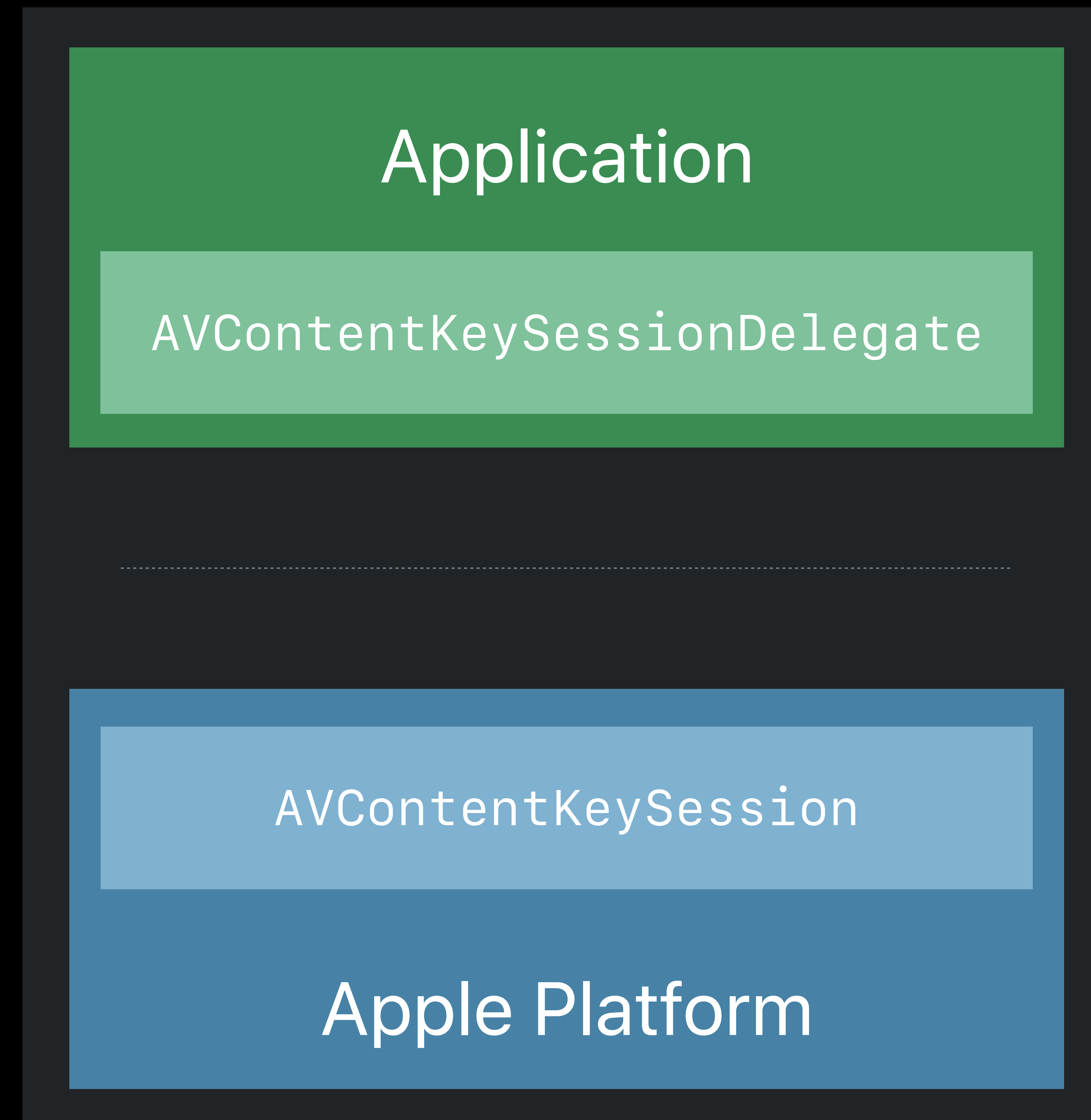
# AVAssetResourceLoader



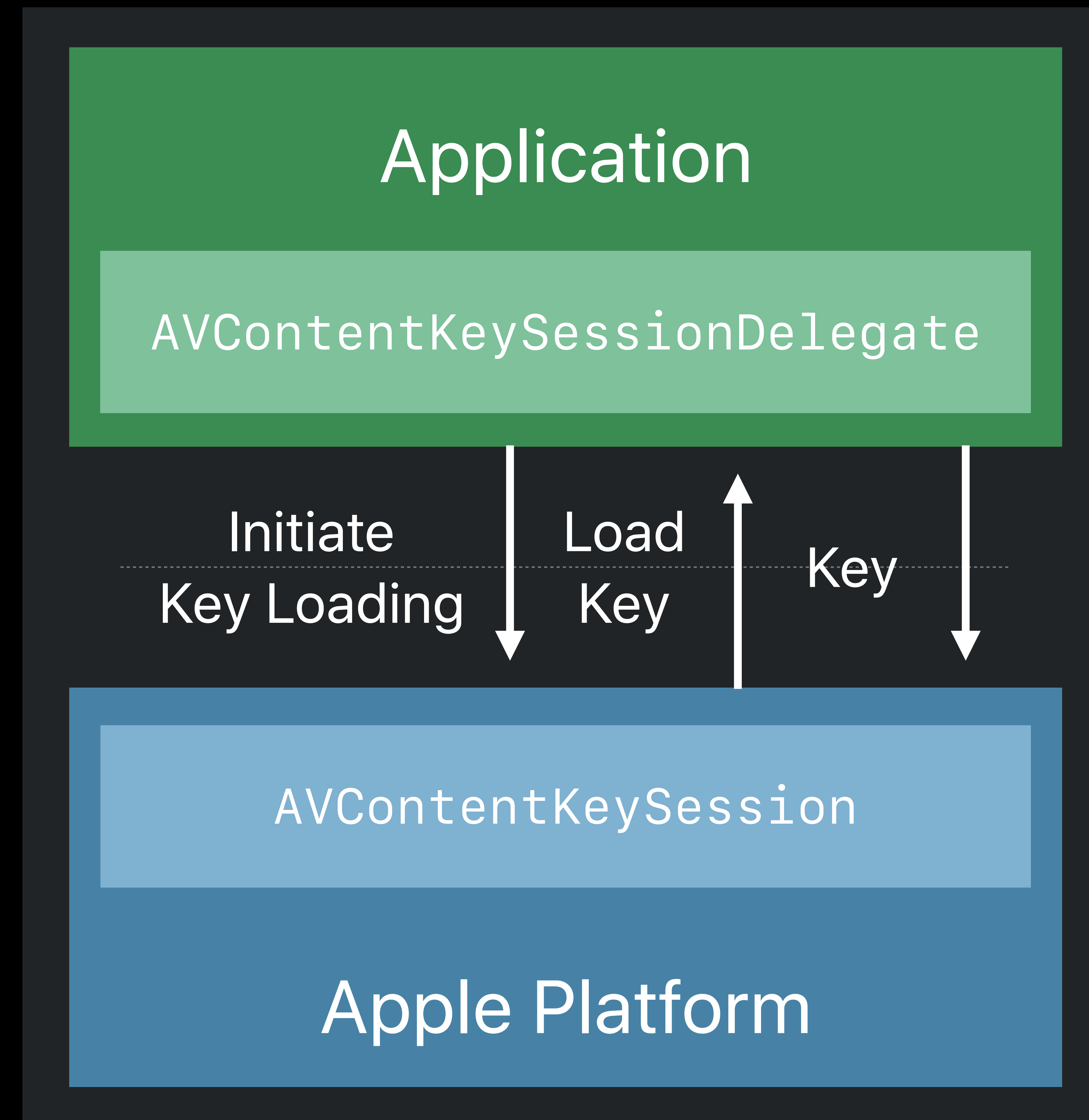
# AVContentKeySession



# AVContentKeySession



# AVContentKeySession





# How Do I Reduce Playback Startup Delay?

# How Do I Reduce Playback Startup Delay?

Preload keys that you predict might be used

# How Do I Reduce Playback Startup Delay?

Preload keys that you predict might be used

Batch up key requests - reduce round-trips to key server

# How Do I Reduce Playback Startup Delay?

Preload keys that you predict might be used

Batch up key requests - reduce round-trips to key server

```
//Initiate Key Loading Process
contentKeySession.processContentKeyRequest(withIdentifier: "skd://myKey", initializationData:
nil, options: nil)

//Delegate Callback
func contentKeySession(_ session: AVContentKeySession,
                        didProvide keyRequest: AVContentKeyRequest)
```

# How Do I Reduce Playback Startup Delay?

Preload keys that you predict might be used

Batch up key requests - reduce round-trips to key server

```
//Initiate Key Loading Process
contentKeySession.processContentKeyRequest(withIdentifier: "skd://myKey", initializationData:
nil, options: nil)
```

```
//Delegate Callback
func contentKeySession(_ session: AVContentKeySession,
didProvide keyRequest: AVContentKeyRequest)
```

**Could A Key Be Requested Again?**

# Could A Key Be Requested Again?

Yes

# Could A Key Be Requested Again?

Yes

New keys might be required for decryption (AirPlay, Lightning Digital AV Adapter)



# Could A Key Be Requested Again?

Yes

New keys might be required for decryption (AirPlay, Lightning Digital AV Adapter)

Always be prepared to answer redundant key requests

# How Do I Preload All Keys?

# How Do I Preload All Keys?

Need key identifier to load key

# How Do I Preload All Keys?

Need key identifier to load key

Obtain all key identifiers out-of-band

# How Do I Preload All Keys?

Need key identifier to load key

Obtain all key identifiers out-of-band

Advertise session keys ( `EXT-X-SESSION-KEY` ) in master m3u8

- Initiate preloading `urlAsset.resourceLoader.preloadsEligibleContentKeys = true`

# How Do I Preload All Keys?

Need key identifier to load key

Obtain all key identifiers out-of-band

Advertise session keys ( `EXT-X-SESSION-KEY` ) in master m3u8

- Initiate preloading `urlAsset.resourceLoader.preloadsEligibleContentKeys = true`

# How Can My Live Streams Avoid The Thundering Herd?

# How Can My Live Streams Avoid The Thundering Herd?

Disperse key request events



# How Can My Live Streams Avoid The Thundering Herd?

Disperse key request events

Clients rotate keys at the same time -> impulse load on key server

# How Can My Live Streams Avoid The Thundering Herd?

Disperse key request events

Clients rotate keys at the same time -> impulse load on key server

Load keys before EXT-X-KEY tag appears

# How Can My Live Streams Avoid The Thundering Herd?

Disperse key request events

Clients rotate keys at the same time -> impulse load on key server

Load keys before EXT-X-KEY tag appears

Scale live offering by load balancing key loading requests

# How Can My Live Streams Avoid The Thundering Herd?

Disperse key request events

Clients rotate keys at the same time -> impulse load on key server

Load keys before EXT-X-KEY tag appears

Scale live offering by load balancing key loading requests

# What Is Offline Rentals?

# What Is Offline Rentals?

Define two expiration durations on offline FairPlay Streaming keys

# What Is Offline Rentals?

Define two expiration durations on offline FairPlay Streaming keys

- Storage duration



Expires in 30 days



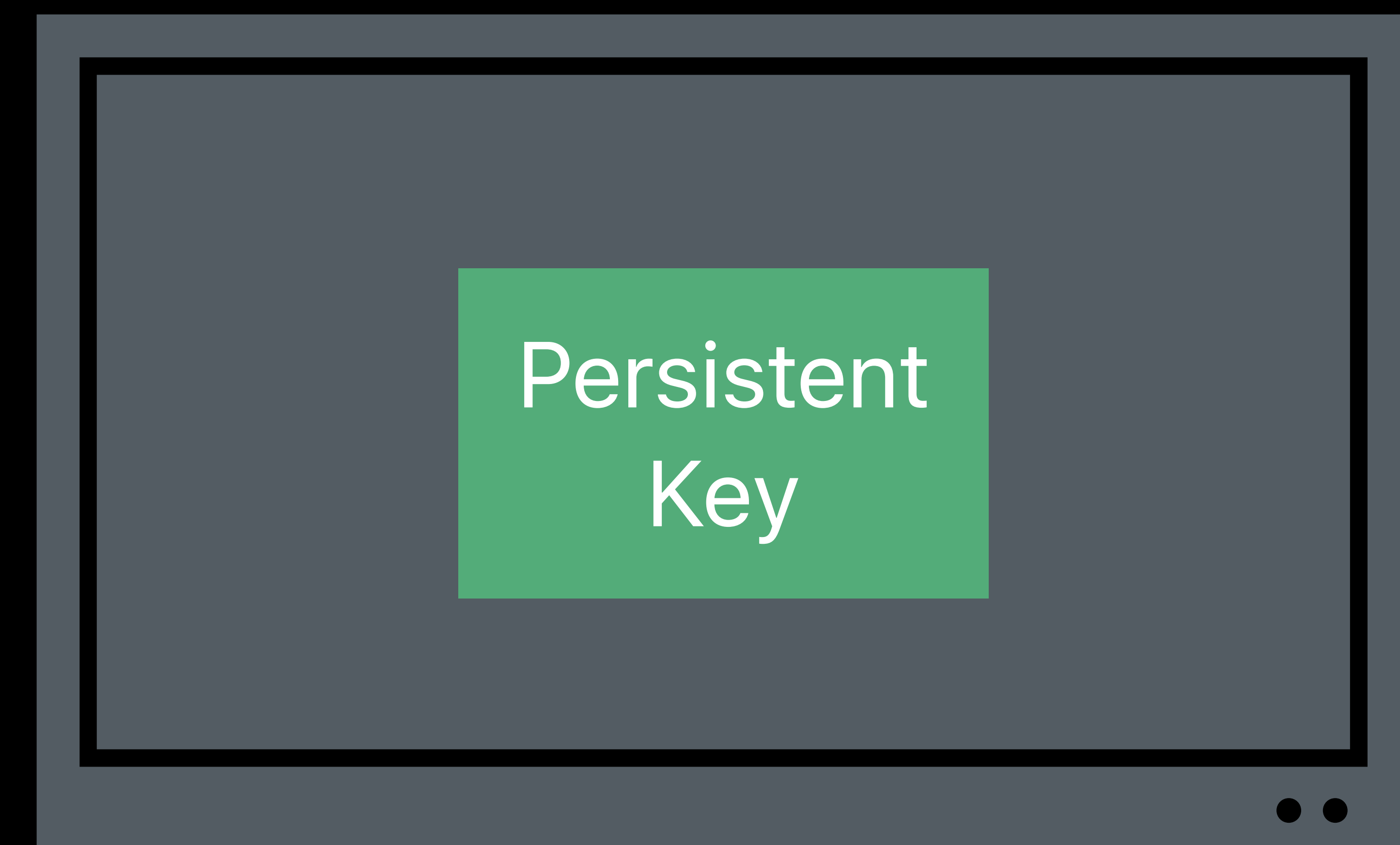
# What Is Offline Rentals?

Define two expiration durations on offline FairPlay Streaming keys

- Storage duration
- Playback duration



Expires in 24 hours





# What Is Offline Rentals?

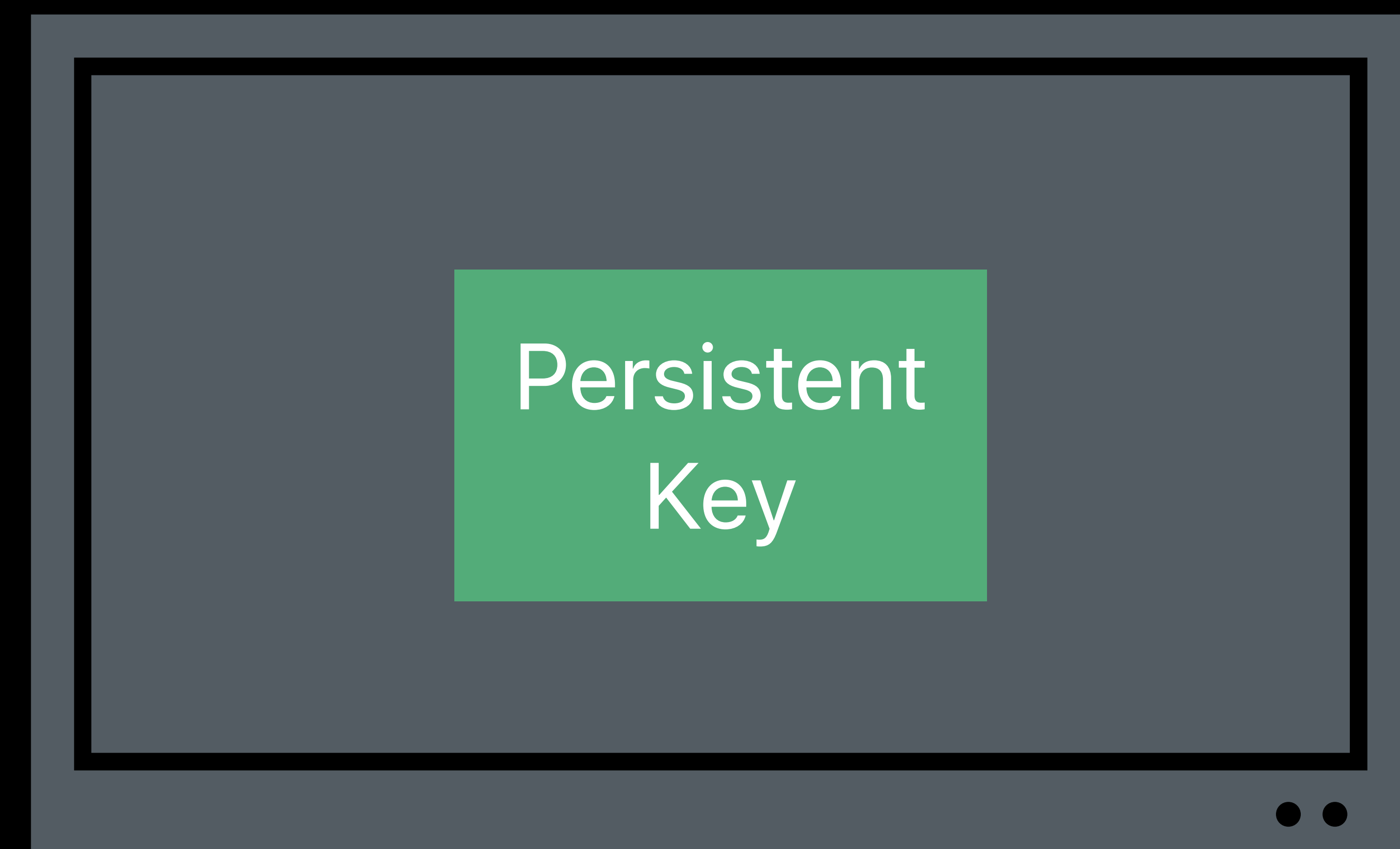
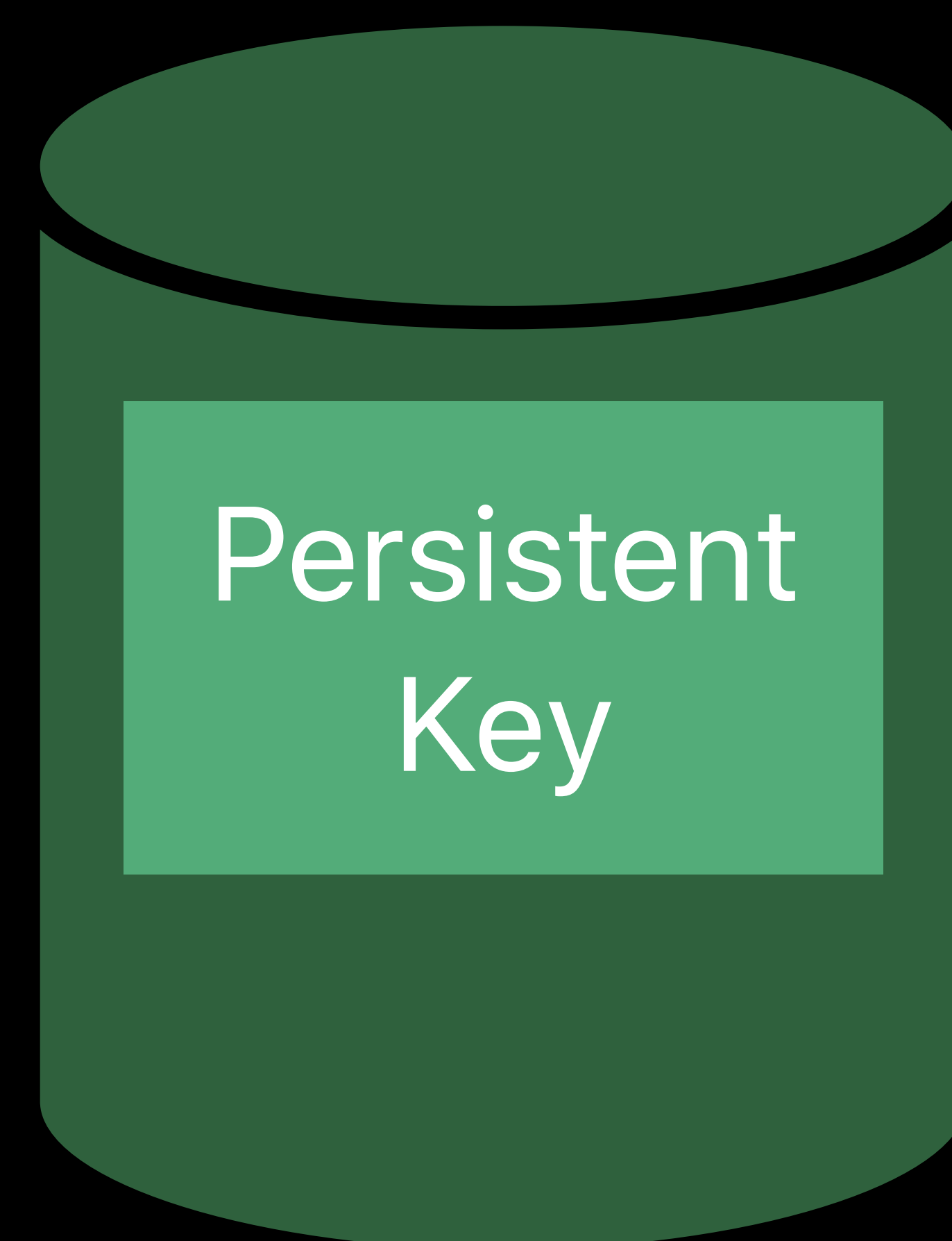
Define two expiration durations on offline FairPlay Streaming keys

- Storage duration
- Playback duration

Expiration durations are enforced even when the device is offline



Expires in 24 hours



# How Do I Do Offline Rentals?

# How Do I Do Offline Rentals?

## Use Offline Key TLLV

**Table 7-1 Offline Key TLLV**

Field name	Byte range	Description
TLLV tag	0-7	An 8-byte value of 0x6375d9727060218c.

# How Do I Do Offline Rentals?

## Use Offline Key TLLV

- Signaled in CKC used while requesting persistent key

**Table 7-1 Offline Key TLLV**

Field name	Byte range	Description
TLLV tag	0-7	An 8-byte value of 0x6375d9727060218c.

# How Do I Do Offline Rentals?

# How Do I Do Offline Rentals?

```
//Requesting persistent key from AVPersistableContentKeyRequest  
let persistentKey = try persistableKeyRequest.persistableContentKey(fromKeyVendorResponse:  
ckcData, options: nil)
```

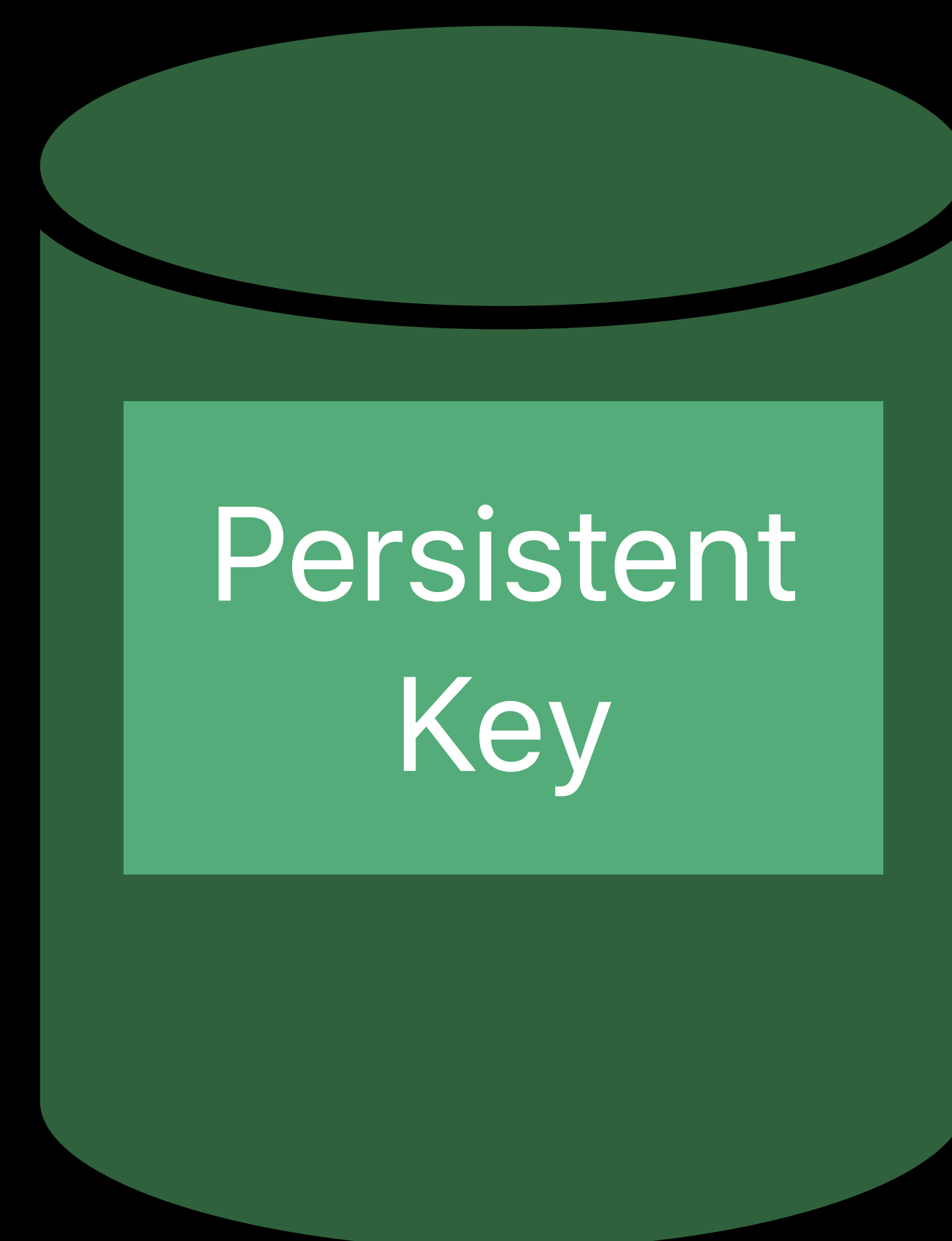
# How Do I Do Offline Rentals?

```
//Requesting persistent key from AVPersistableContentKeyRequest  
let persistentKey = try persistableKeyRequest.persistableContentKey(fromKeyVendorResponse:  
ckcData, options: nil)
```

Persistent  
Key

# How Do I Do Offline Rentals?

```
//Requesting persistent key from AVPersistableContentKeyRequest  
let persistentKey = try persistableKeyRequest.persistableContentKey(fromKeyVendorResponse:  
ckcData, options: nil)
```



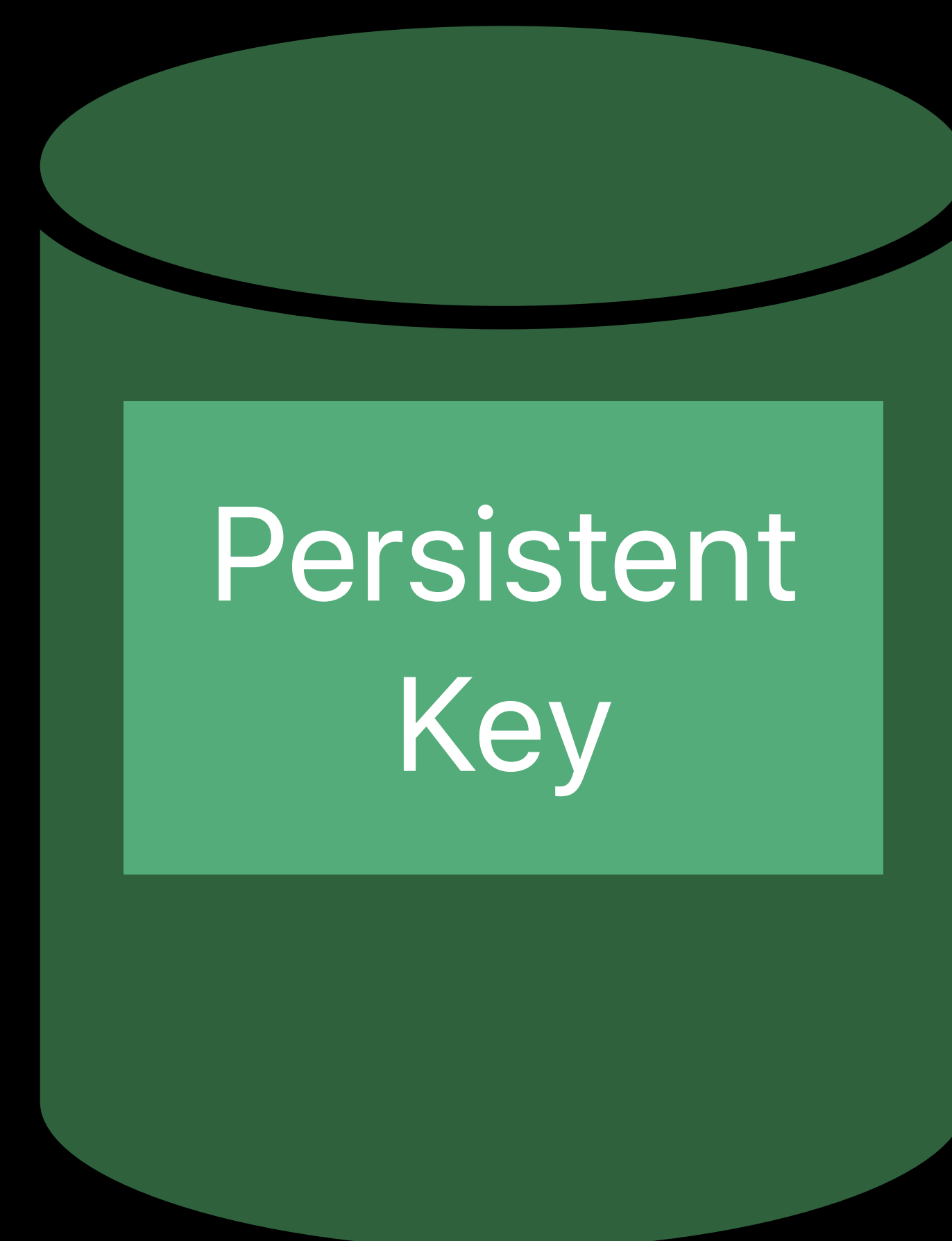


# How Do I Do Offline Rentals?

```
//Requesting persistent key from AVPersistableContentKeyRequest  
let persistentKey = try persistableKeyRequest.persistableContentKey(fromKeyVendorResponse:  
ckcData, options: nil)
```



Expires in 30 days

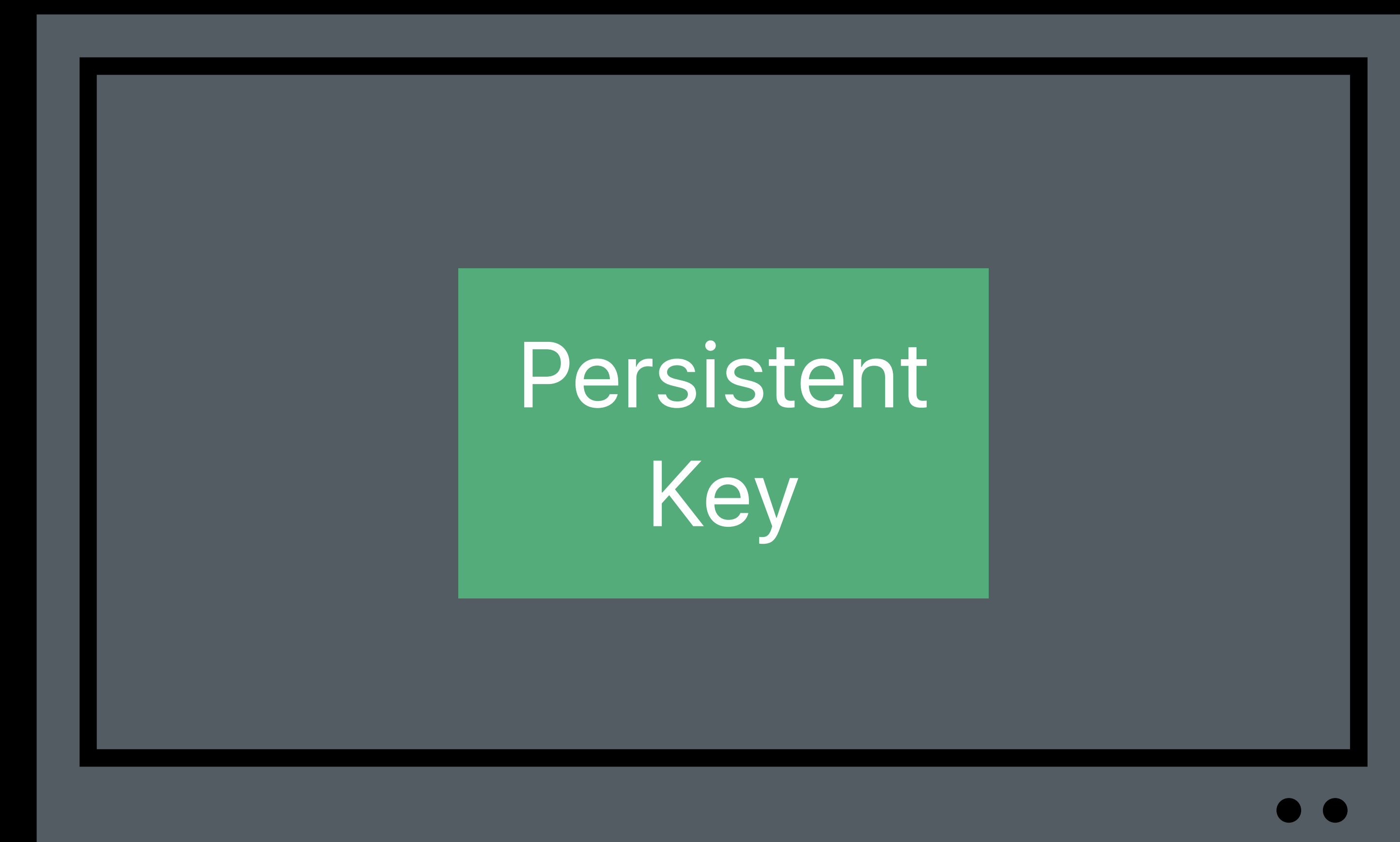
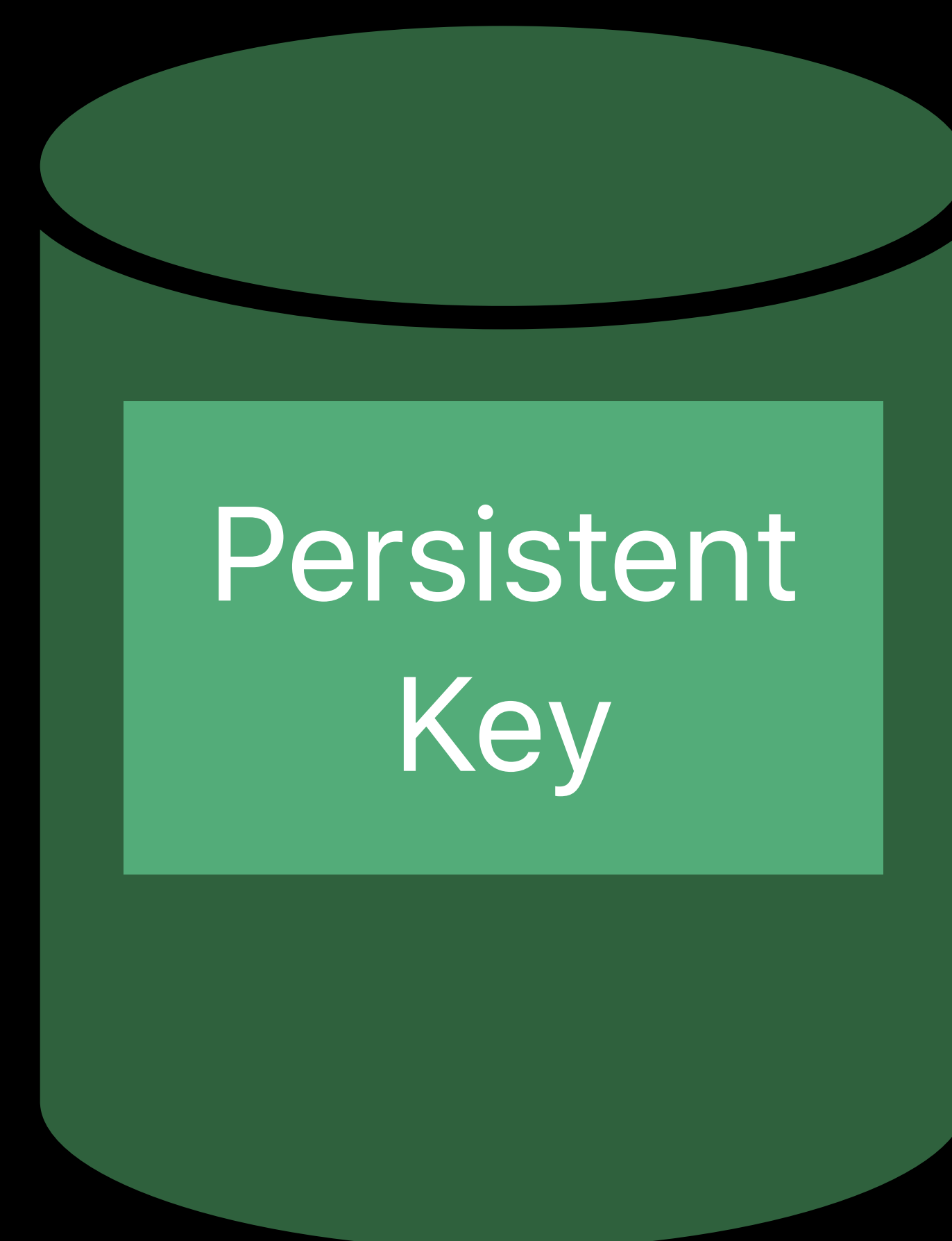


# How Do I Do Offline Rentals?

```
//Requesting persistent key from AVPersistableContentKeyRequest  
let persistentKey = try persistableKeyRequest.persistableContentKey(fromKeyVendorResponse:  
ckcData, options: nil)
```



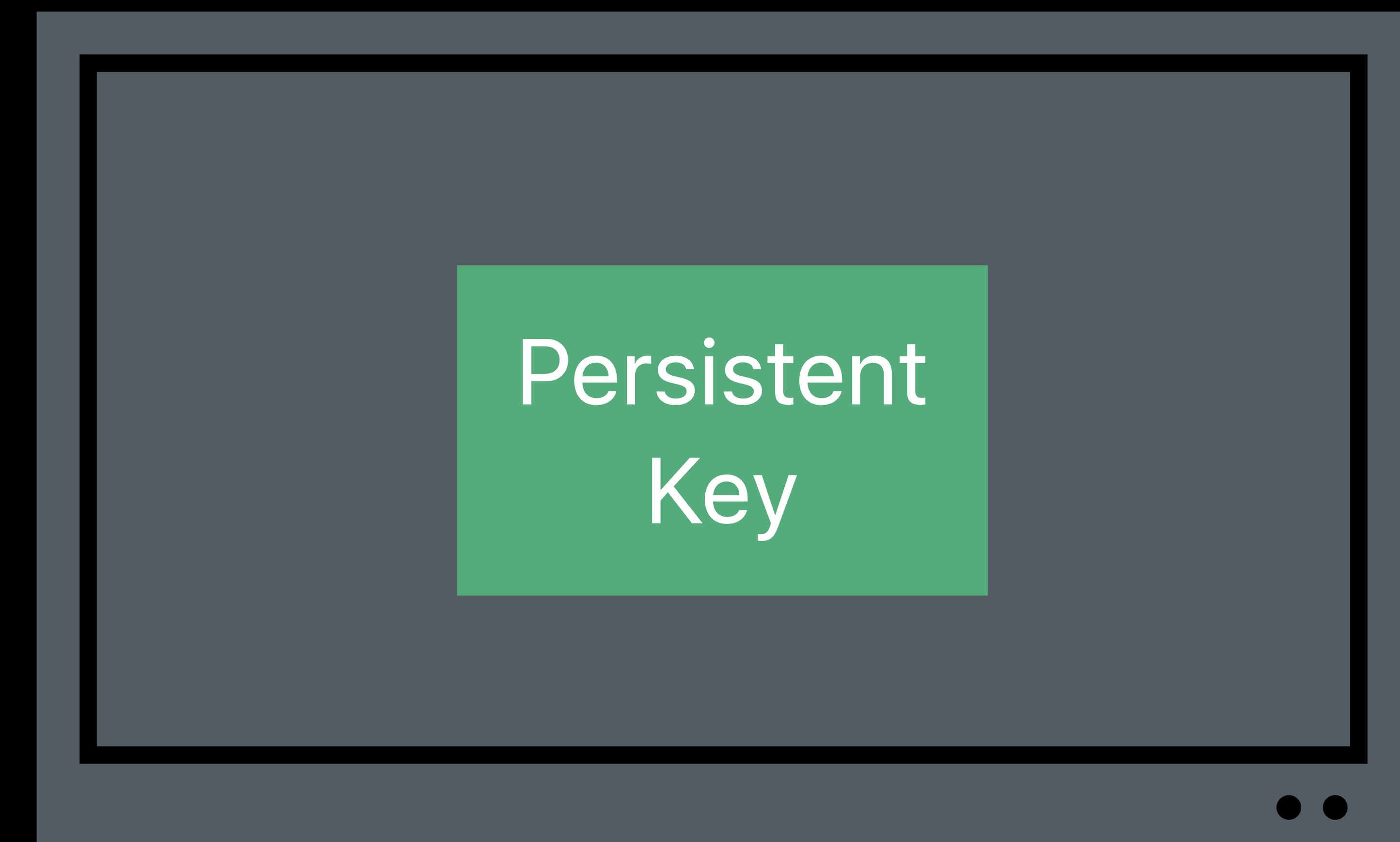
Expires in 30 days



# How Do I Do Offline Rentals?



Expires in 30 days

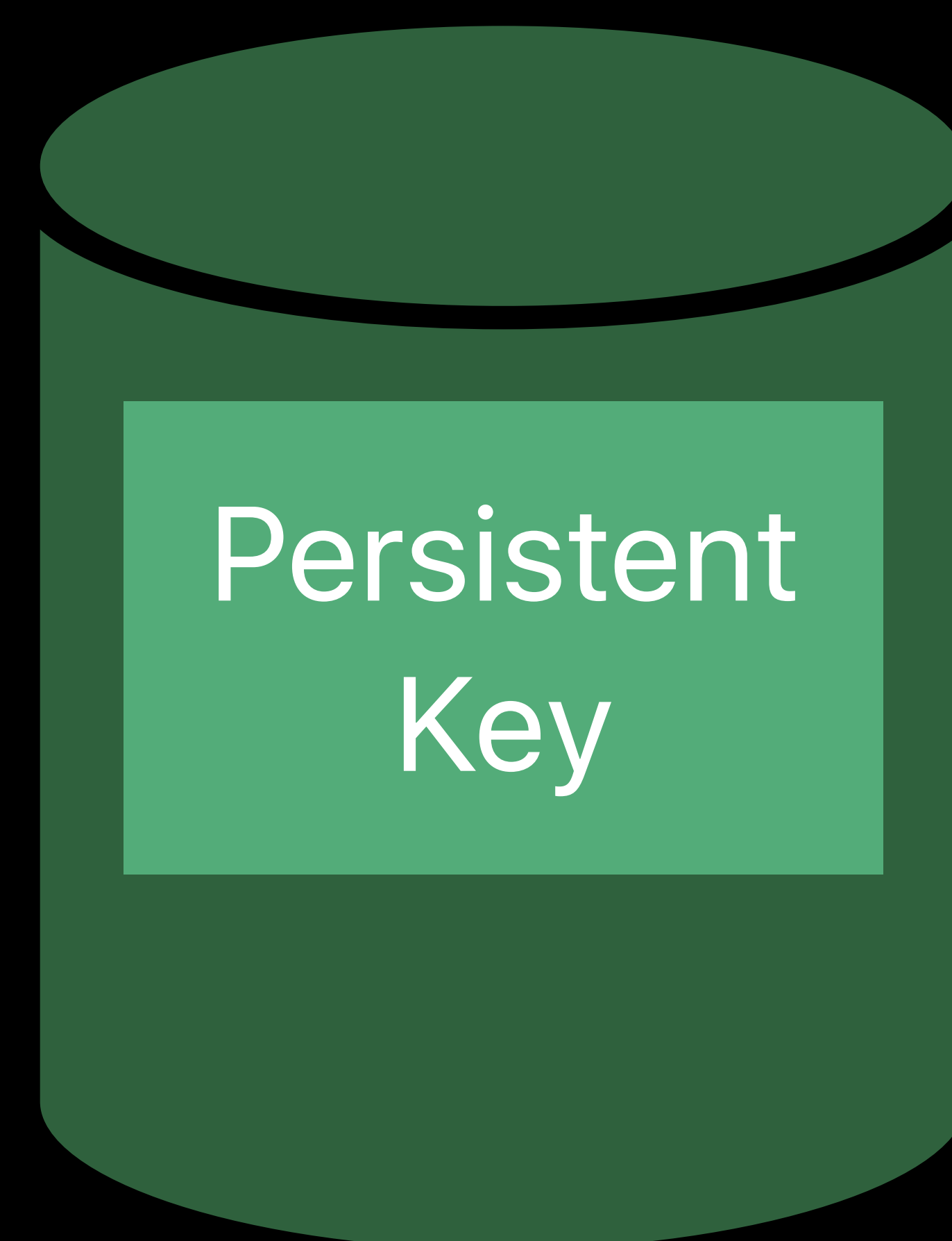


# How Do I Do Offline Rentals?

```
//Delegate Callback  
func contentKeySession(_ session: AVContentKeySession,  
    didUpdatePersistableContentKey persistableContentKey: Data,  
    forKeyIdentifier keyIdentifier: Any)
```



Expires in 30 days

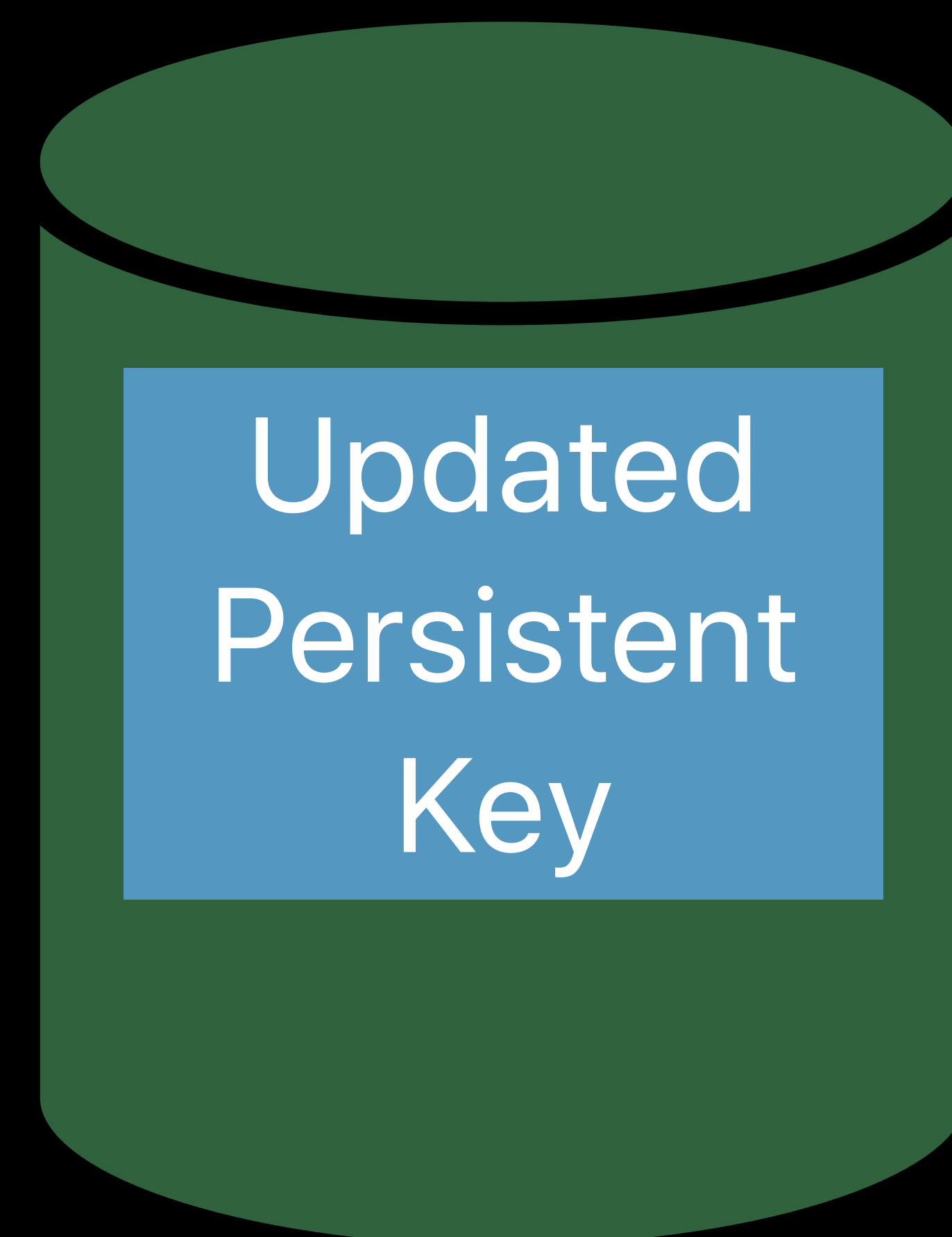


# How Do I Do Offline Rentals?

```
//Delegate Callback  
func contentKeySession(_ session: AVContentKeySession,  
    didUpdatePersistableContentKey persistableContentKey: Data,  
    forContentKeyIdentifier keyIdentifier: Any)
```



Expires in 30 days

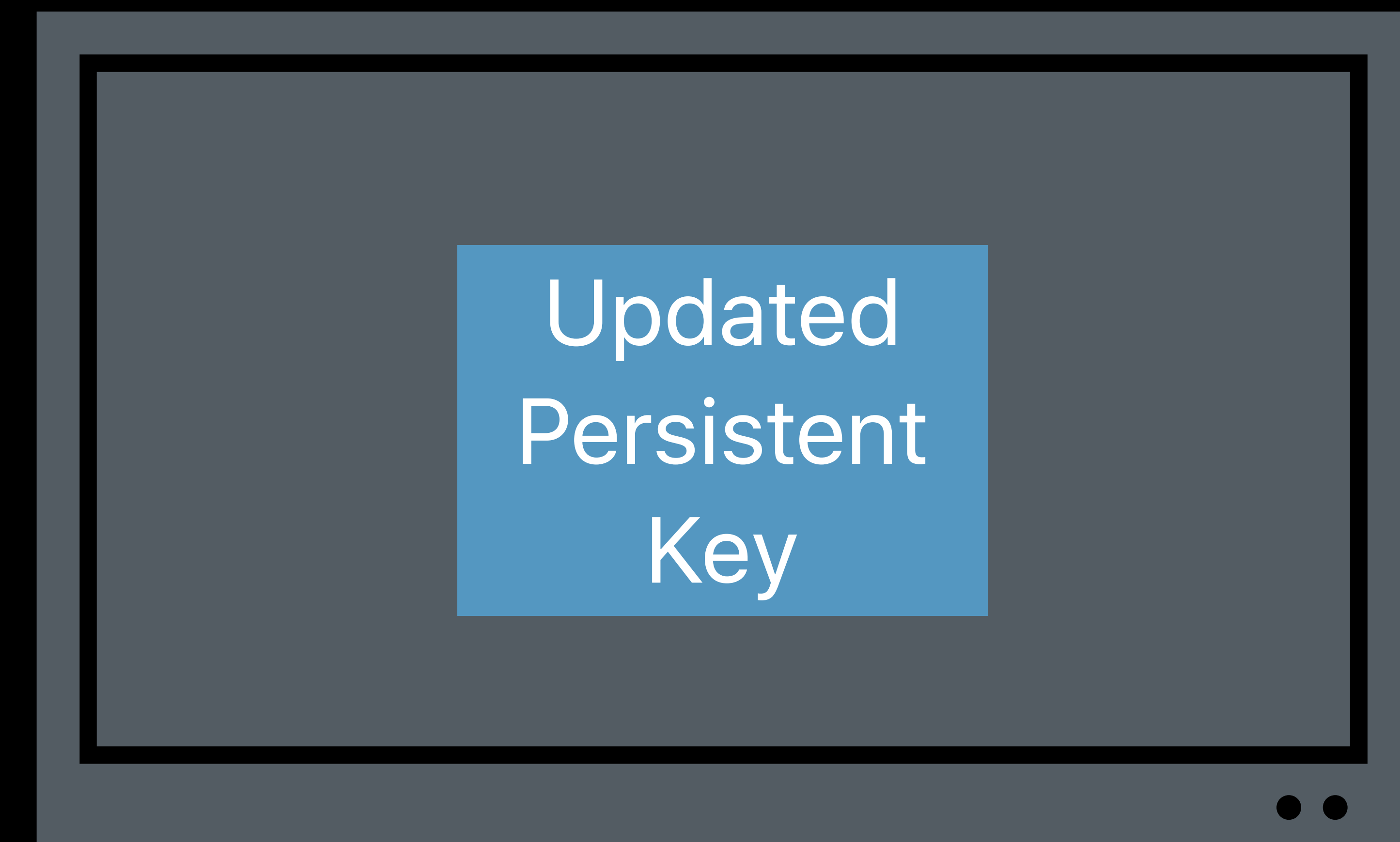


# How Do I Do Offline Rentals?

```
//Delegate Callback  
func contentKeySession(_ session: AVContentKeySession,  
    didUpdatePersistableContentKey persistableContentKey: Data,  
    forKeyIdentifier keyIdentifier: Any)
```



Expires in 24 hours



# How Do I Handle Errors While Loading Keys?

# How Do I Handle Errors While Loading Keys?

When something fails...



# How Do I Handle Errors While Loading Keys?

When something fails...

- Report error to AVFoundation

```
//Setting error on an AVContentKeyRequest  
contentKeyRequest.processContentKeyResponseError(error)  
  
//Setting error on an AVAssetResourceLoadingRequest  
resourceLoadingRequest.finishLoading(with: error)
```

# How Do I Handle Errors While Loading Keys?

When something fails...

- Report error to AVFoundation

```
//Setting error on an AVContentKeyRequest  
contentKeyRequest.processContentKeyResponseError(error)  
  
//Setting error on an AVAssetResourceLoadingRequest  
resourceLoadingRequest.finishLoading(with: error)
```

- Monitor error logs and address root-cause

# How Do I Handle Errors While Loading Keys?

When something fails...

- Report error to AVFoundation

```
//Setting error on an AVContentKeyRequest  
contentKeyRequest.processContentKeyResponseError(error)  
  
//Setting error on an AVAssetResourceLoadingRequest  
resourceLoadingRequest.finishLoading(with: error)
```

- Monitor error logs and address root-cause

# Common Pitfalls While Delivering Keys

# Common Pitfalls While Delivering Keys

Taking too long to provide key response

- Player times out waiting for key response

# Common Pitfalls While Delivering Keys

Taking too long to provide key response

- Player times out waiting for key response
- Deliver keys as soon as possible

# Common Pitfalls While Delivering Keys

Taking too long to provide key response

- Player times out waiting for key response
- Deliver keys as soon as possible
- Survey `playerItem.accessLogs()`

# Common Pitfalls While Delivering Keys



# Common Pitfalls While Delivering Keys

Using same keys across variants with different HDCP requirements

- HDCP requirement is signaled inside key response

# Common Pitfalls While Delivering Keys

Using same keys across variants with different HDCP requirements

- HDCP requirement is signaled inside key response
- Use multiple key identifiers

# Common Pitfalls While Delivering Keys

# Common Pitfalls While Delivering Keys

Using persistent keys to answer all key loading requests

- Persistent keys cannot be shared across devices (AirPlay)

# Common Pitfalls While Delivering Keys

Using persistent keys to answer all key loading requests

- Persistent keys cannot be shared across devices (AirPlay)
- Make sure key loading request accepts persistent keys

# Common Pitfalls While Delivering Keys

Using persistent keys to answer all key loading requests

- Persistent keys cannot be shared across devices (AirPlay)
- Make sure key loading request accepts persistent keys
- Minor API changes in iOS 11.2+

**Is Persistent Key Accepted As Response?**

# Is Persistent Key Accepted As Response?

## Using AVContentKeySession

```
do {  
    try contentKeyRequest.respondByRequestingPersistableContentKeyRequestAndReturnError()  
} catch {  
    //Fallback to provide online FairPlay Streaming key from key server  
}
```



**Is Persistent Key Accepted As Response?**

# Is Persistent Key Accepted As Response?

## Using AVAssetResourceLoader

```
if let contentType = resourceLoadingRequest.contentInformationRequest?.allowedContentTypes,
    !contentType.contains(AVStreamingKeyDeliveryPersistentContentType) {
    //Fallback to provide online FairPlay Streaming key from key server
}
```

# Summary

# Summary

AVContentKeySession API

# Summary

AVContentKeySession API

How to improve playback startup?

# Summary

AVContentKeySession API

How to improve playback startup?

How to scale live streaming?

# Summary

AVContentKeySession API

How to improve playback startup?

How to scale live streaming?

How to do offline rentals?

# Summary

AVContentKeySession API

How to improve playback startup?

How to scale live streaming?

How to do offline rentals?

How to handle failures while loading keys?



# Summary

AVContentKeySession API

How to improve playback startup?

How to scale live streaming?

How to do offline rentals?

How to handle failures while loading keys?

How to avoid common pitfalls while delivering keys?

# More Information

<https://developer.apple.com/wwdc18/507>

 **WWDC18**