The Security Framework

Session 704

Dallas De Atley
Manager, Platform Security

These are confidential sessions—please refrain from streaming, blogging, or taking pictures

What You Will Learn

What You Will Learn

- Building blocks of the Security framework

What You Will Learn

- Building blocks of the Security framework
- How to store secrets in the keychain

What You Will Learn

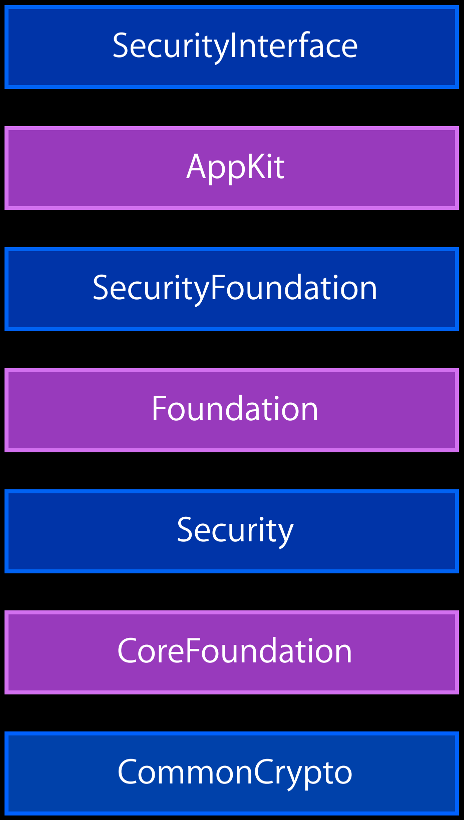
- Building blocks of the Security framework
- How to store secrets in the keychain
- How to secure communication over a network

What You Will Learn

- Building blocks of the Security framework
- How to store secrets in the keychain
- How to secure communication over a network
- How to evaluate a signed object

Security Frameworks

OS X



SecurityInterface

AppKit

SecurityFoundation

Foundation

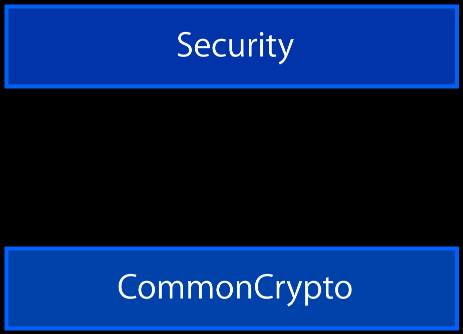
Security

CoreFoundation

CommonCrypto

Security Frameworks

OS X

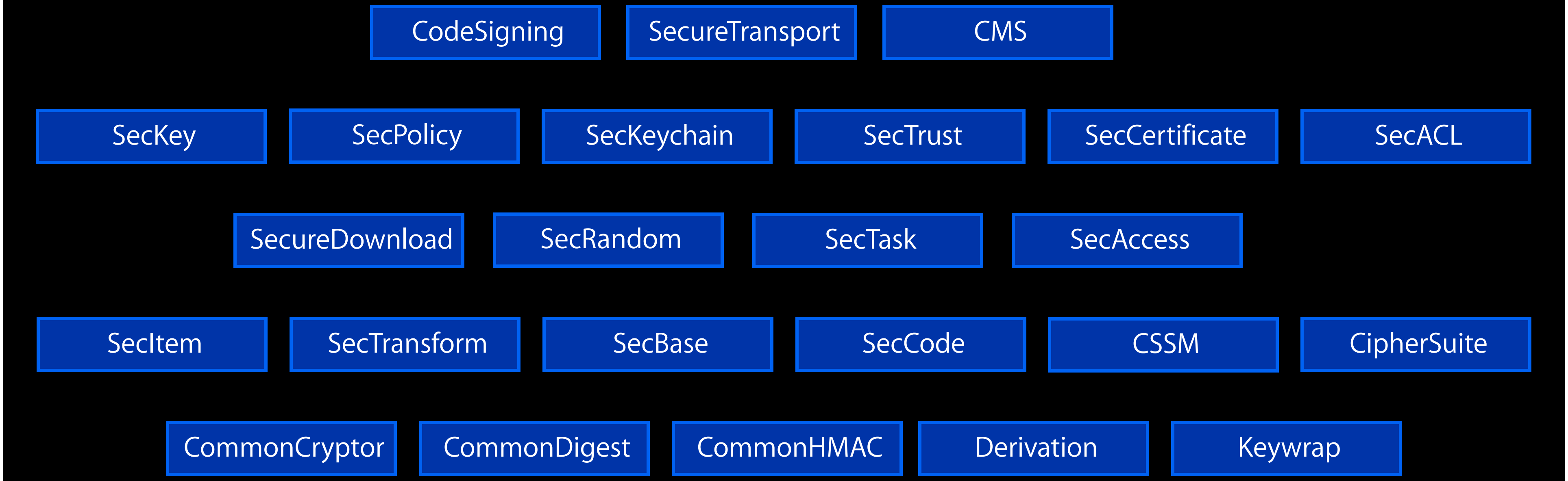


Security

CommonCrypto

Security Framework

OS X



CodeSigning SecureTransport CMS

SecKey SecPolicy SecKeychain SecTrust SecCertificate SecACL

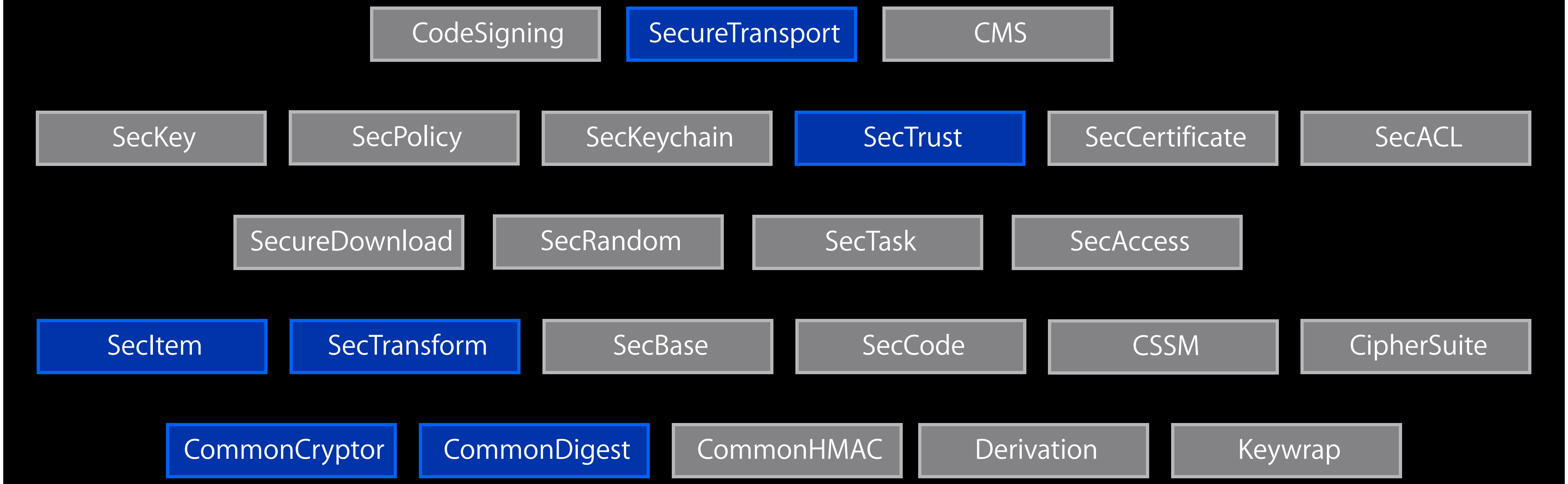
SecureDownload SecRandom SecTask SecAccess

SecItem SecTransform SecBase SecCode CSSM CipherSuite

CommonCryptor CommonDigest CommonHMAC Derivation Keywrap

Security Framework

OS X



CodeSigning SecureTransport CMS

SecKey SecPolicy SecKeychain SecTrust SecCertificate SecACL

SecureDownload SecRandom SecTask SecAccess

SecItem SecTransform SecBase SecCode CSSM CipherSuite

CommonCryptor CommonDigest CommonHMAC Derivation Keywrap

Technologies

Technologies

- Crypto

Technologies

- Crypto
- Keychain

Technologies

- Crypto
- Keychain
- Secure Transport

Technologies

- Crypto
- Keychain
- Secure Transport
- Trust Evaluation

Cryptography

Cryptography

- CommonCrypto

Cryptography

- CommonCrypto
- Designed for performance

Cryptography

- CommonCrypto
- Designed for performance
    - Processor specific optimizations

Cryptography

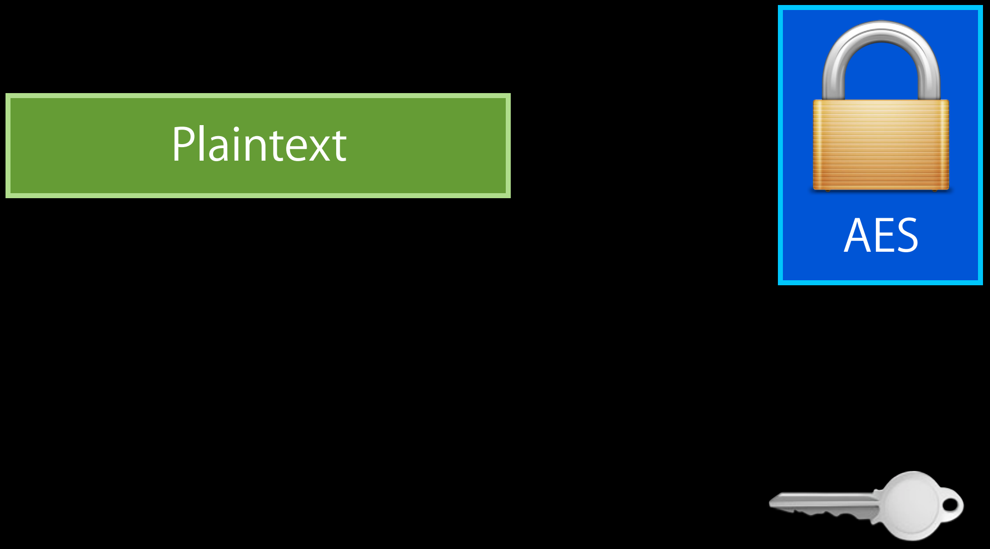
- CommonCrypto
- Designed for performance
  - Processor specific optimizations
- State of the art algorithms

Cryptography

- CommonCrypto
- Designed for performance
  - Processor specific optimizations
- State of the art algorithms
  - FIPS 140-2 as defined by NIST

Cryptography

Symmetric Encryption

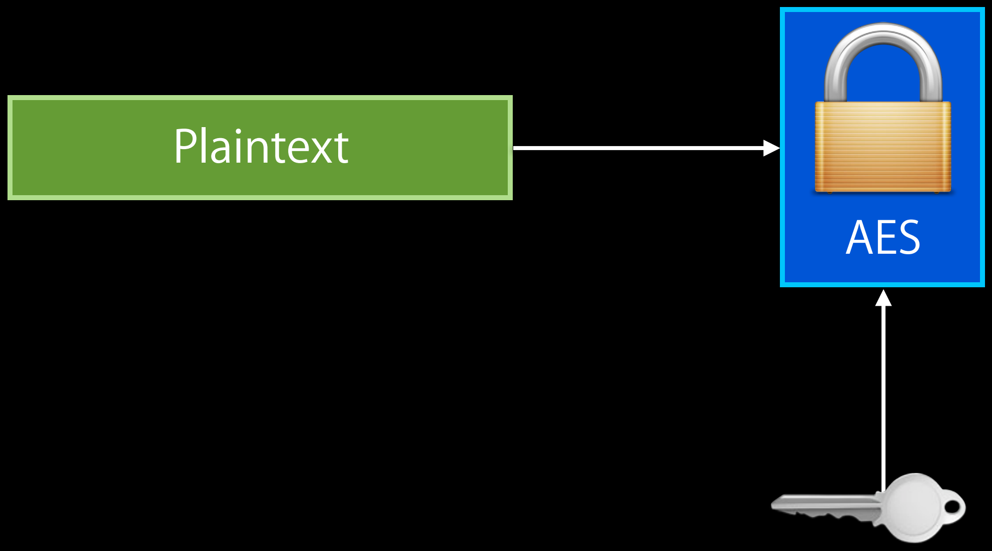


Plaintext

AES

Cryptography

Symmetric Encryption

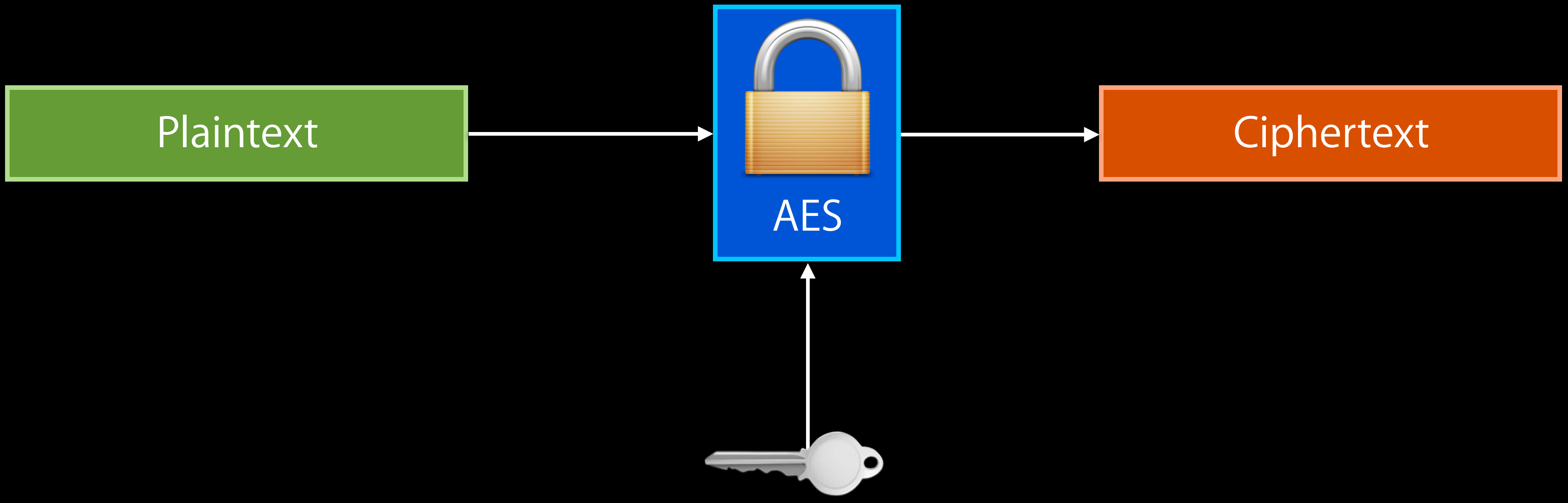


Plaintext

AES

Cryptography

Symmetric Encryption



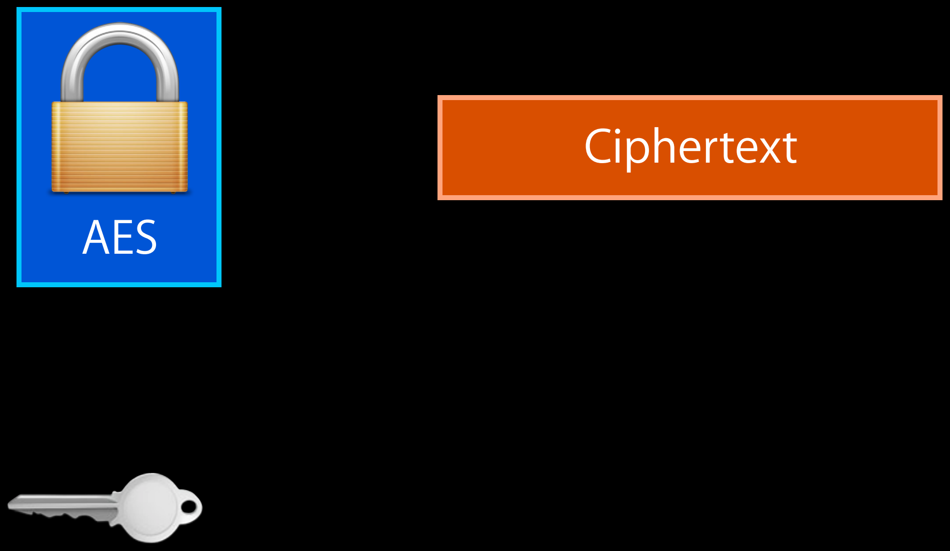
Plaintext

AES

Ciphertext

Cryptography

Symmetric Decryption

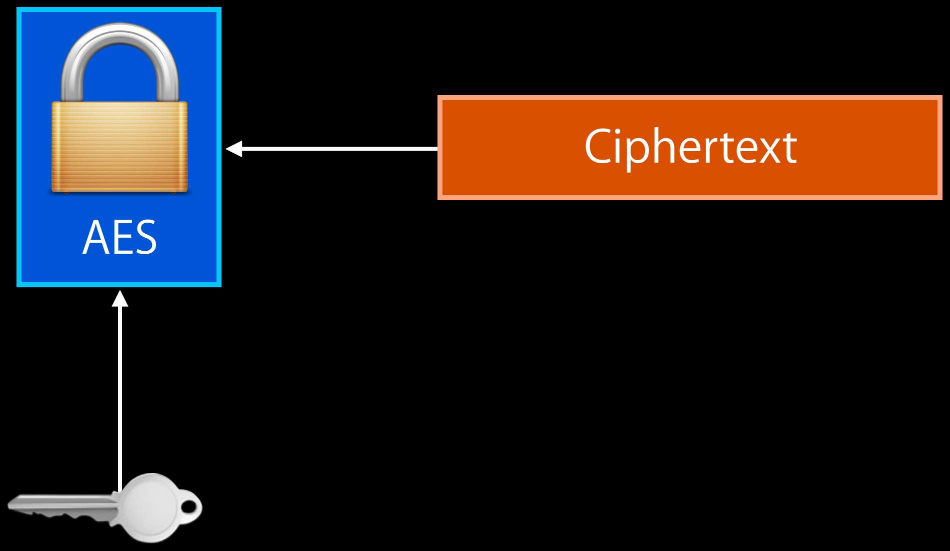


AES

Ciphertext

Cryptography

Symmetric Decryption

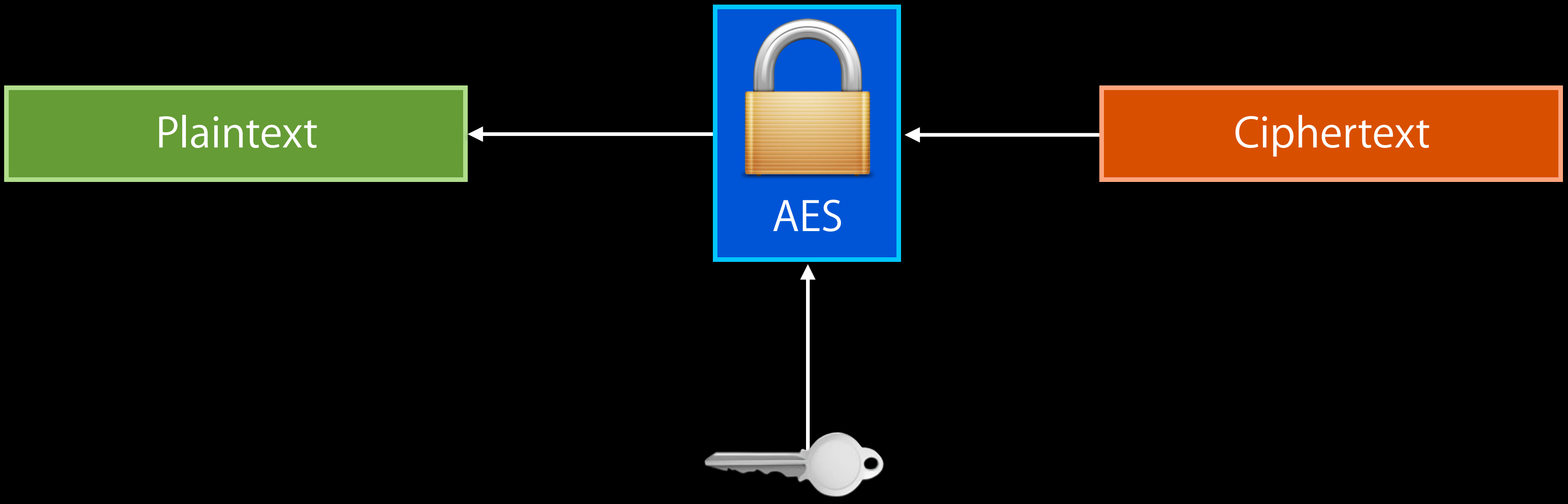


AES

Ciphertext

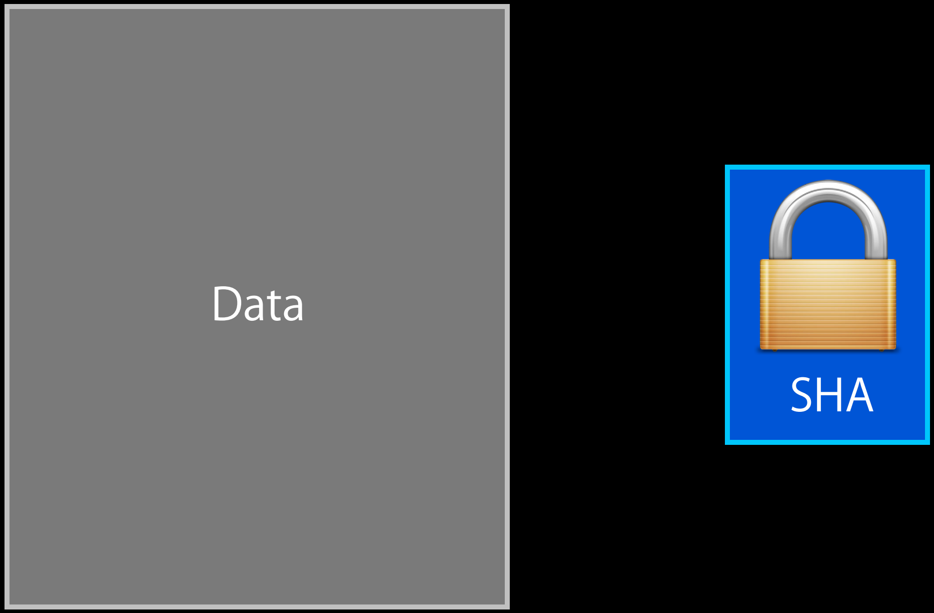
Cryptography

Symmetric Decryption



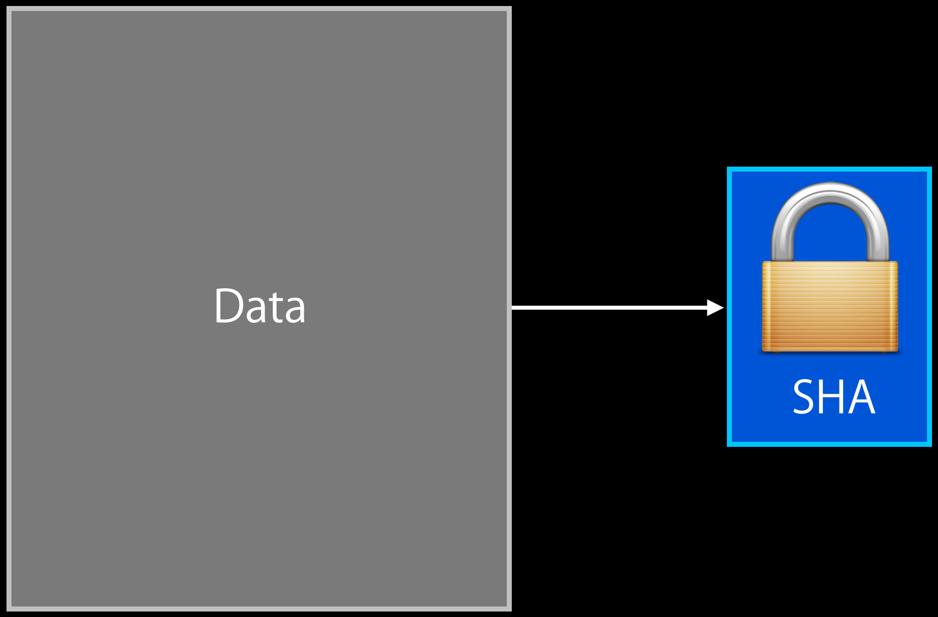
Cryptography

Message Digest



Cryptography

Message Digest

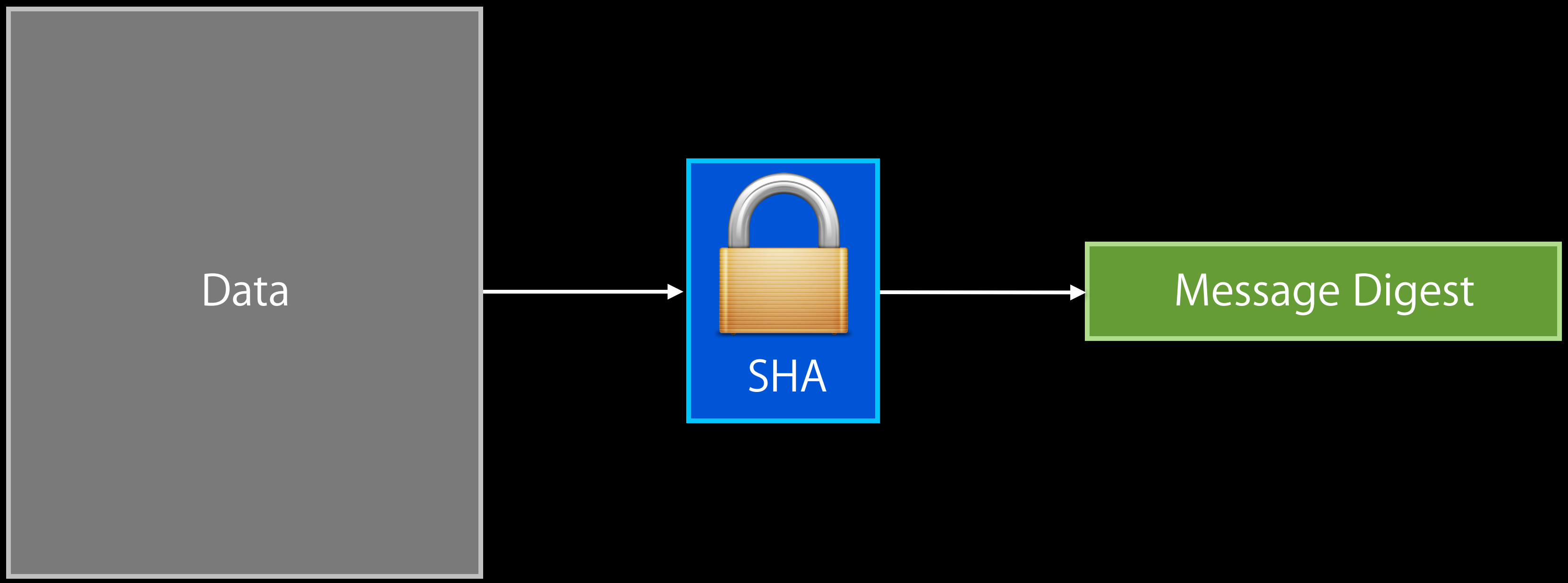


Data

SHA

Cryptography

Message Digest



Data

SHA

Message Digest

Cryptography

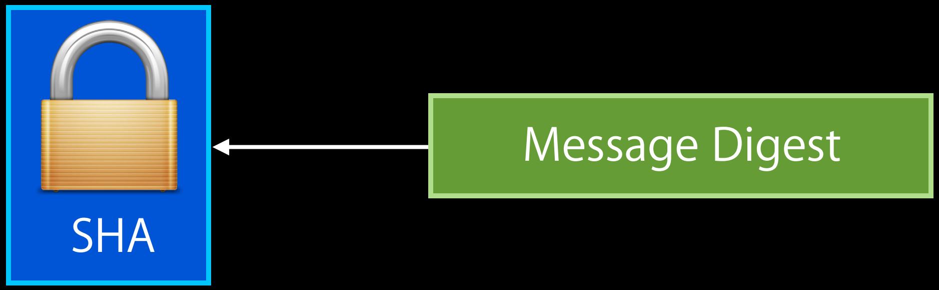
Message Digest

SHA

Message Digest

Cryptography

Message Digest

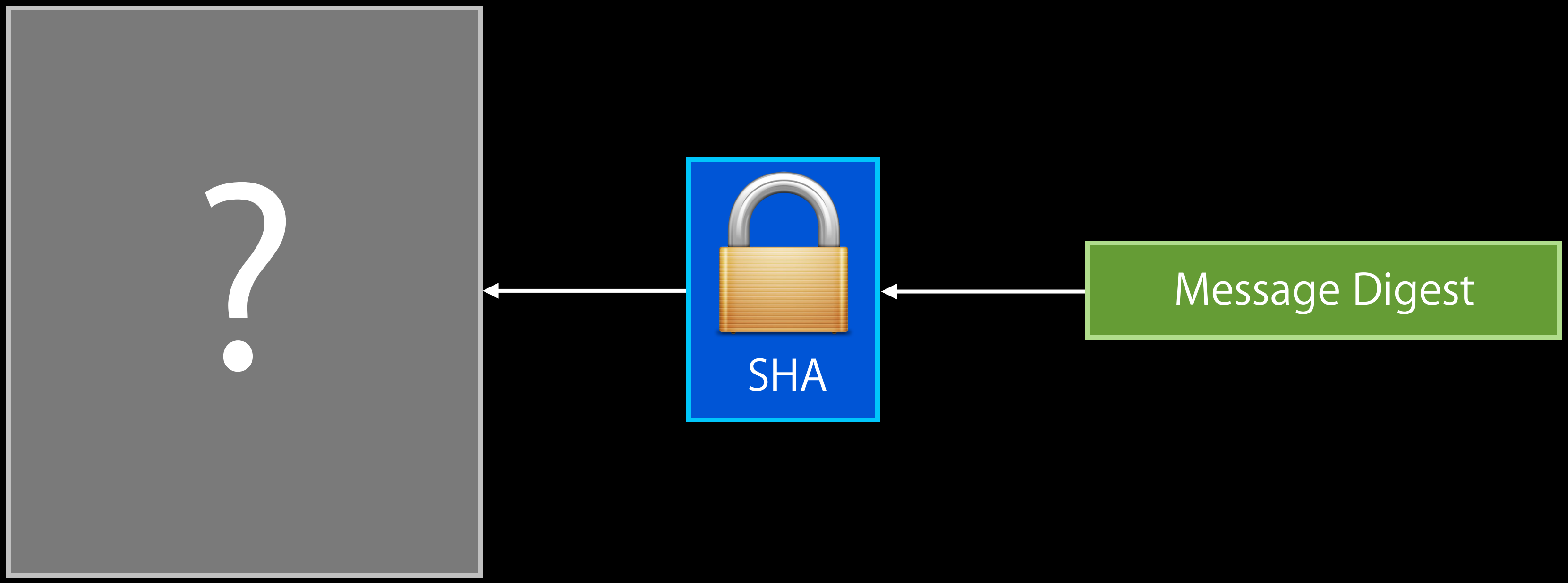


SHA

Message Digest

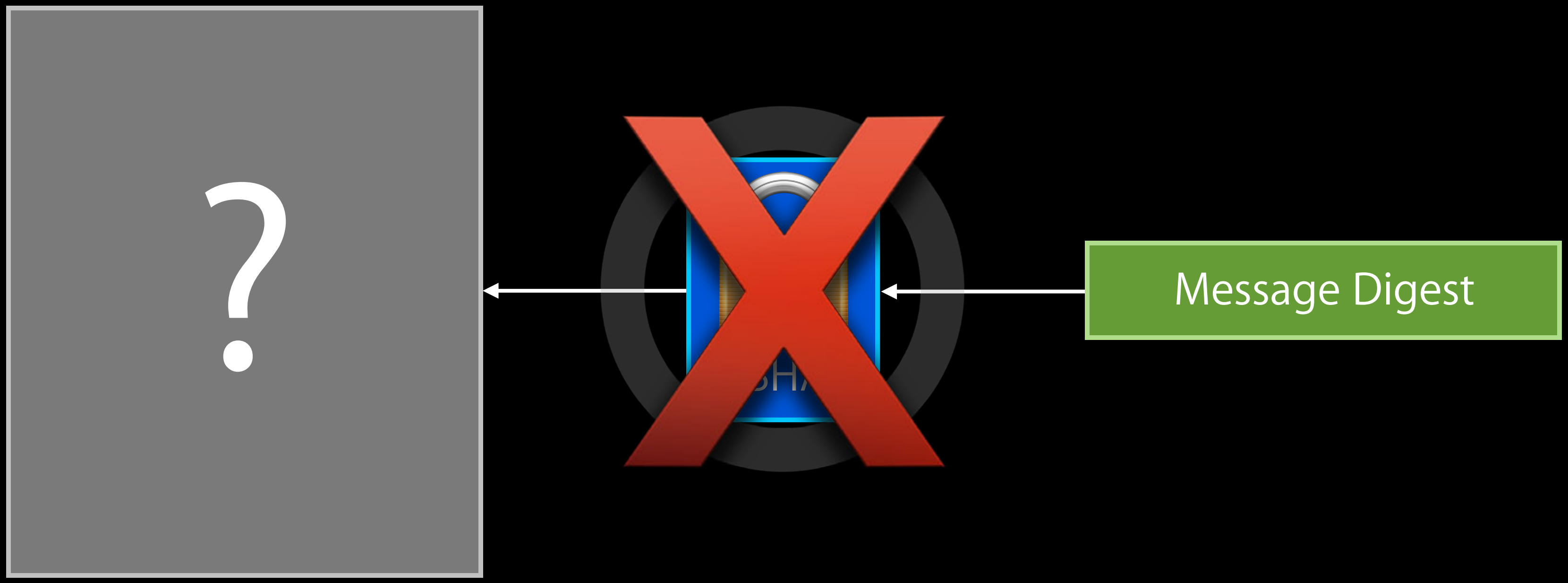
Cryptography

Message Digest



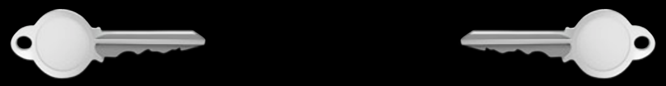
Cryptography

Message Digest



Cryptography

Public Key Cryptography

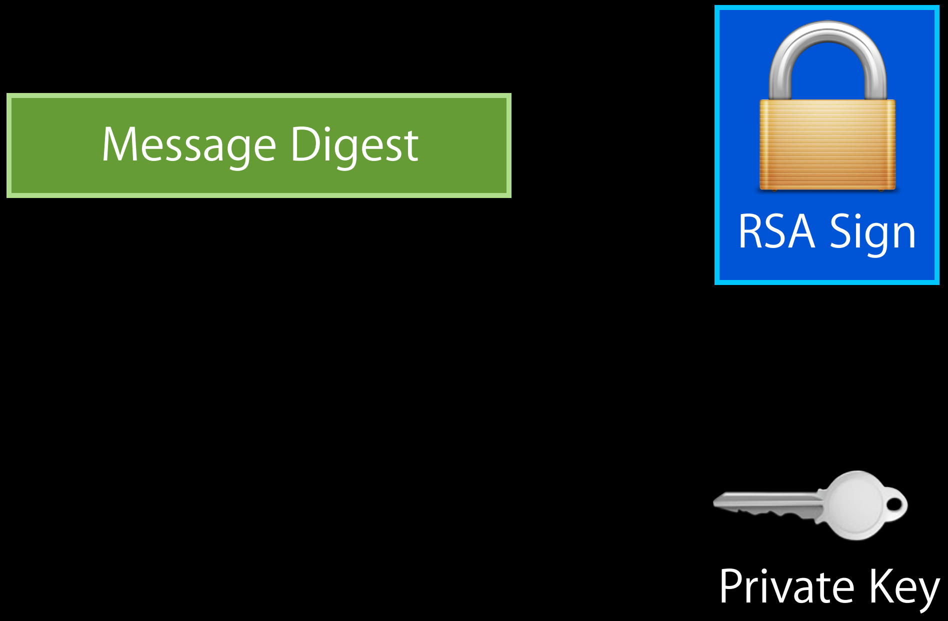


Public Key

Private Key

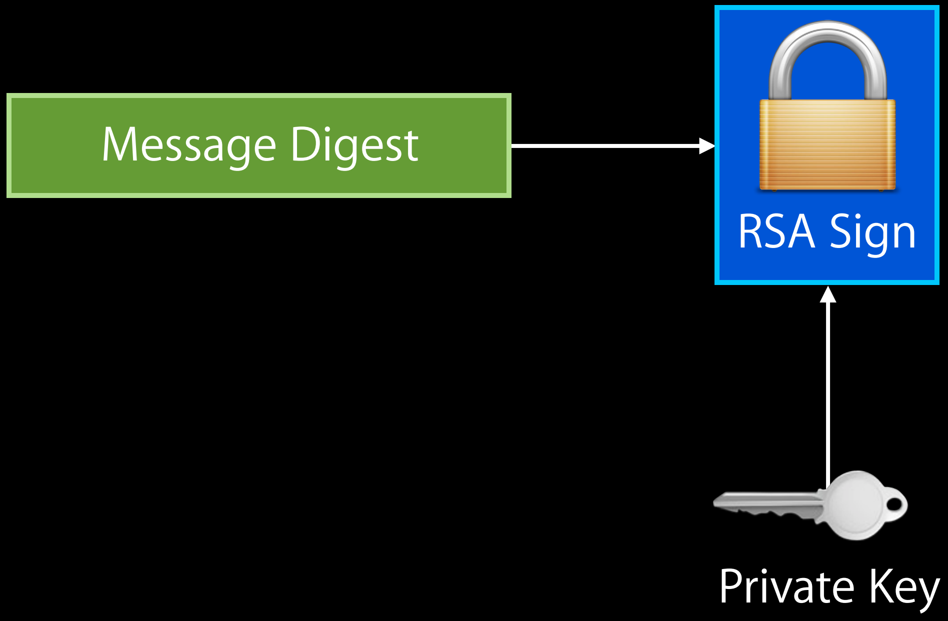
Cryptography

Signing a message digest



Cryptography

Signing a message digest



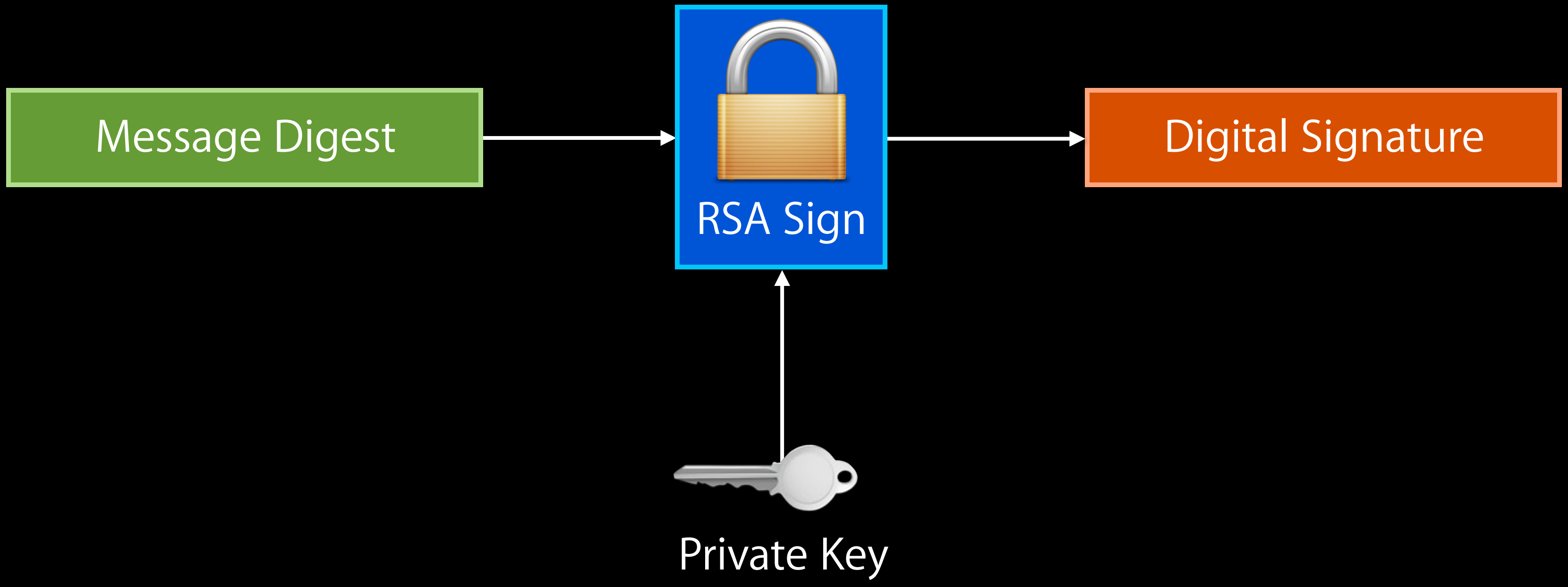
Message Digest

RSA Sign

Private Key

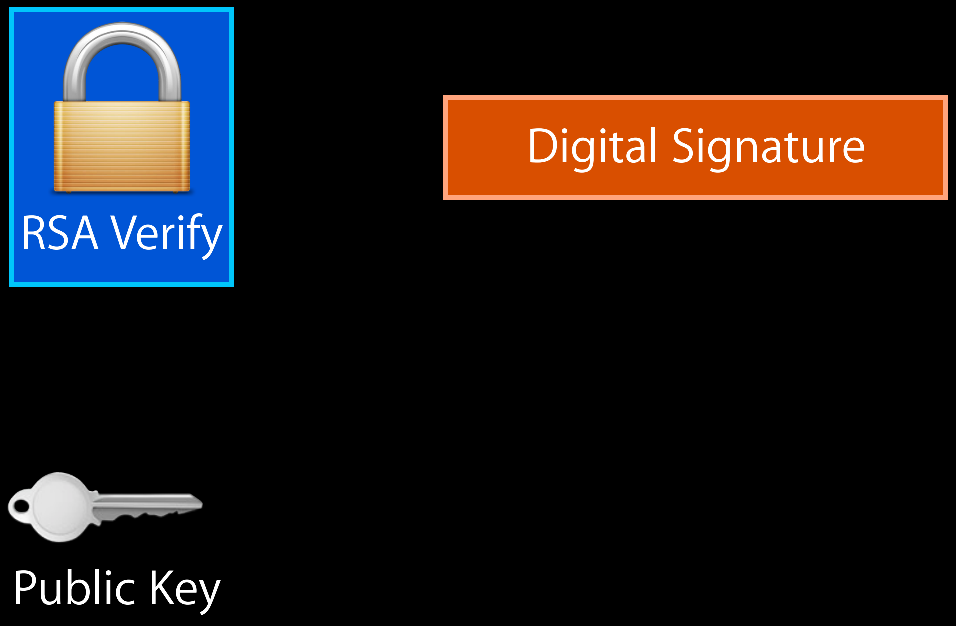
Cryptography

Signing a message digest



Cryptography

Verifying a digital signature



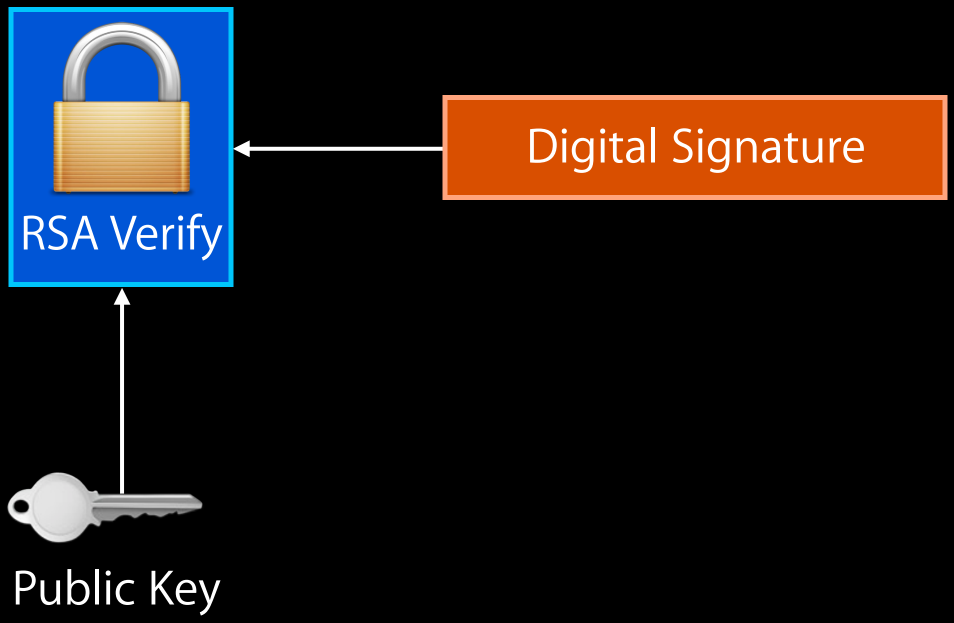
RSA Verify

Digital Signature

Public Key

Cryptography

Verifying a digital signature



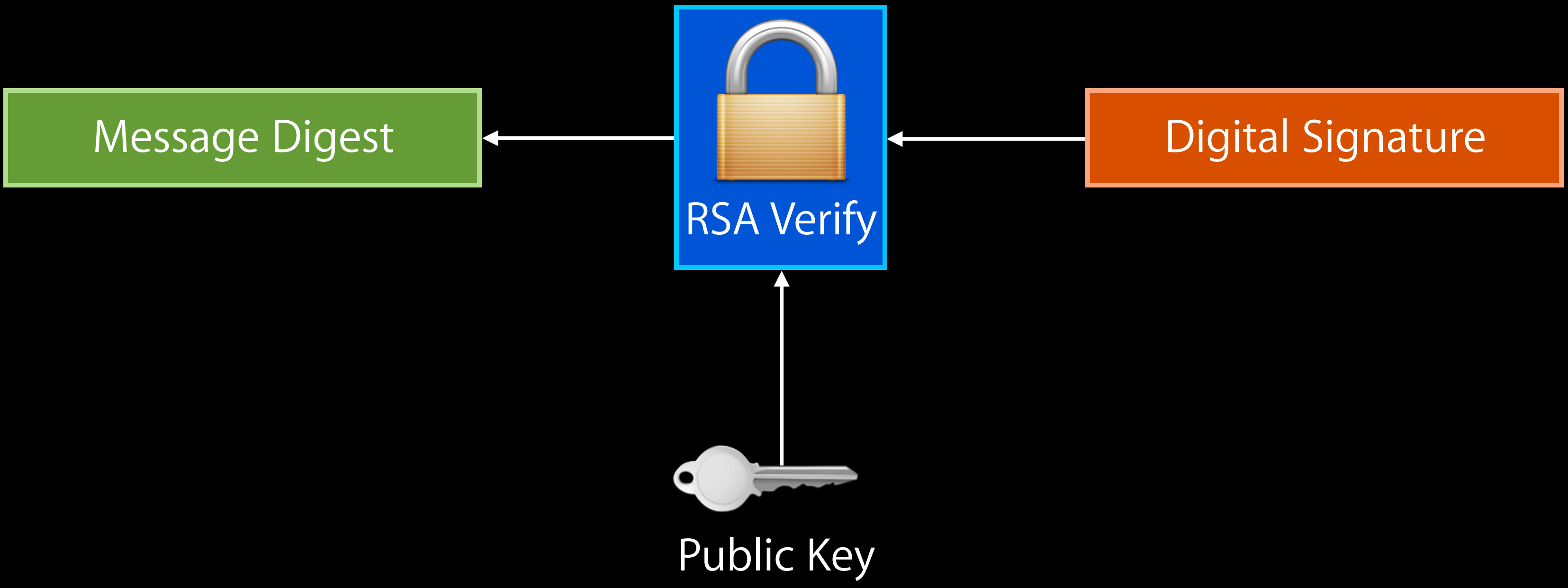
RSA Verify

Digital Signature

Public Key

Cryptography

Verifying a digital signature

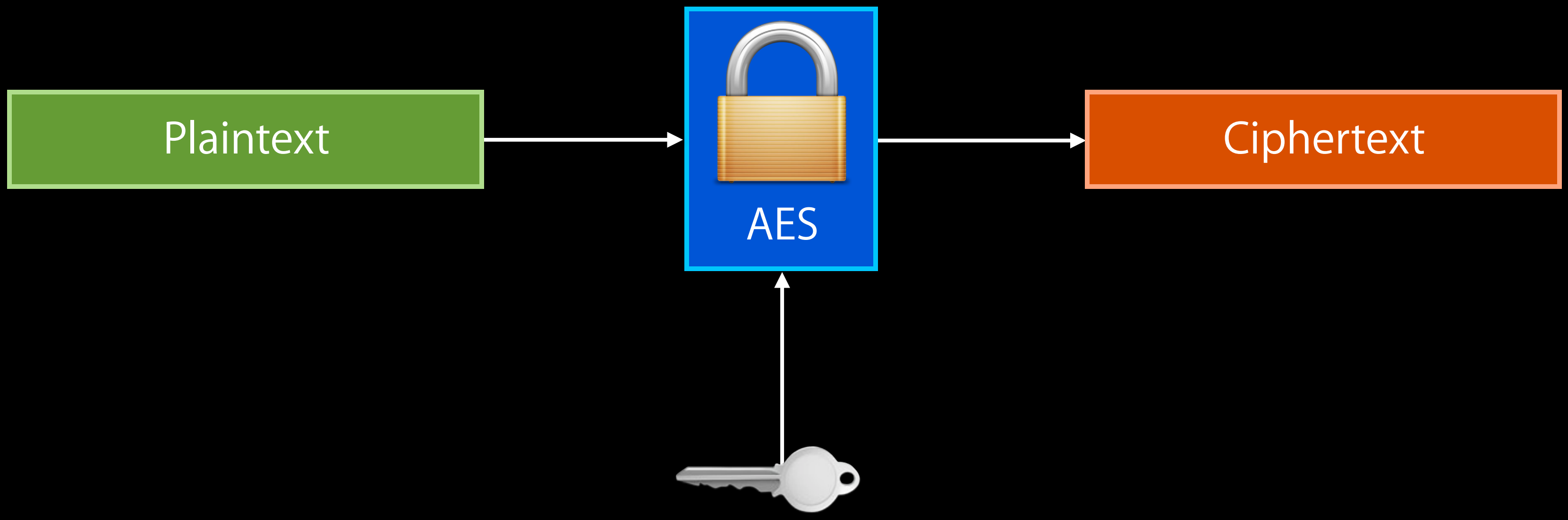


Cryptography

The devil is in the details

Cryptography

The devil is in the details



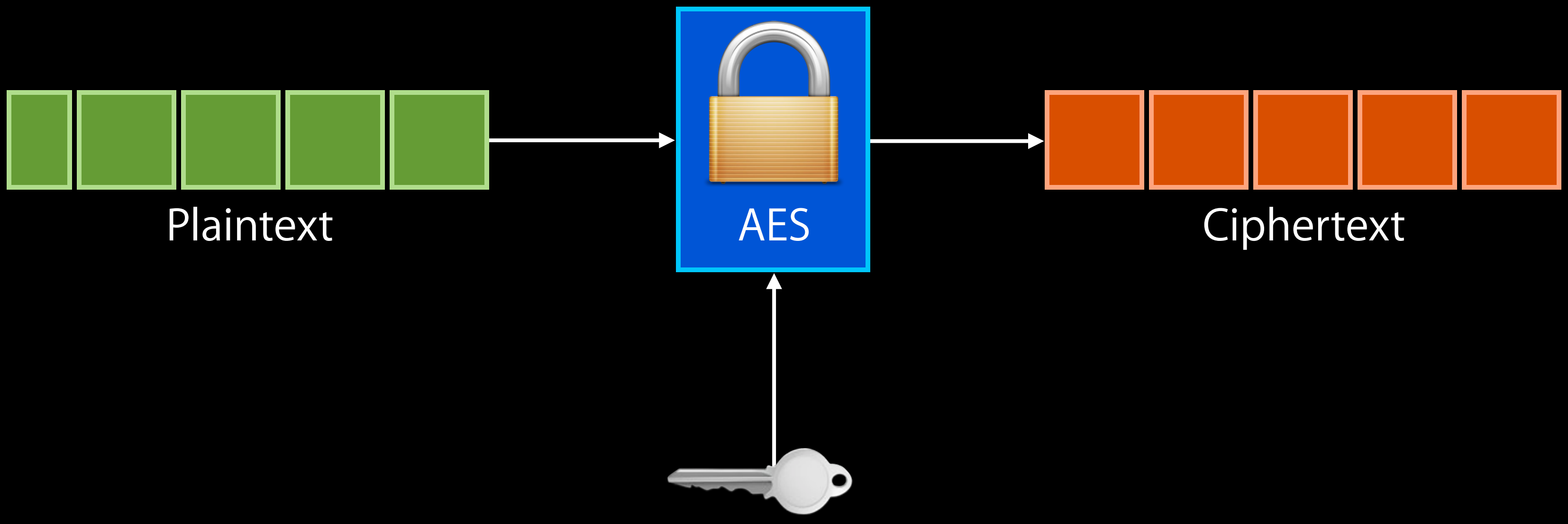
Plaintext

AES

Ciphertext

Cryptography

The devil is in the details



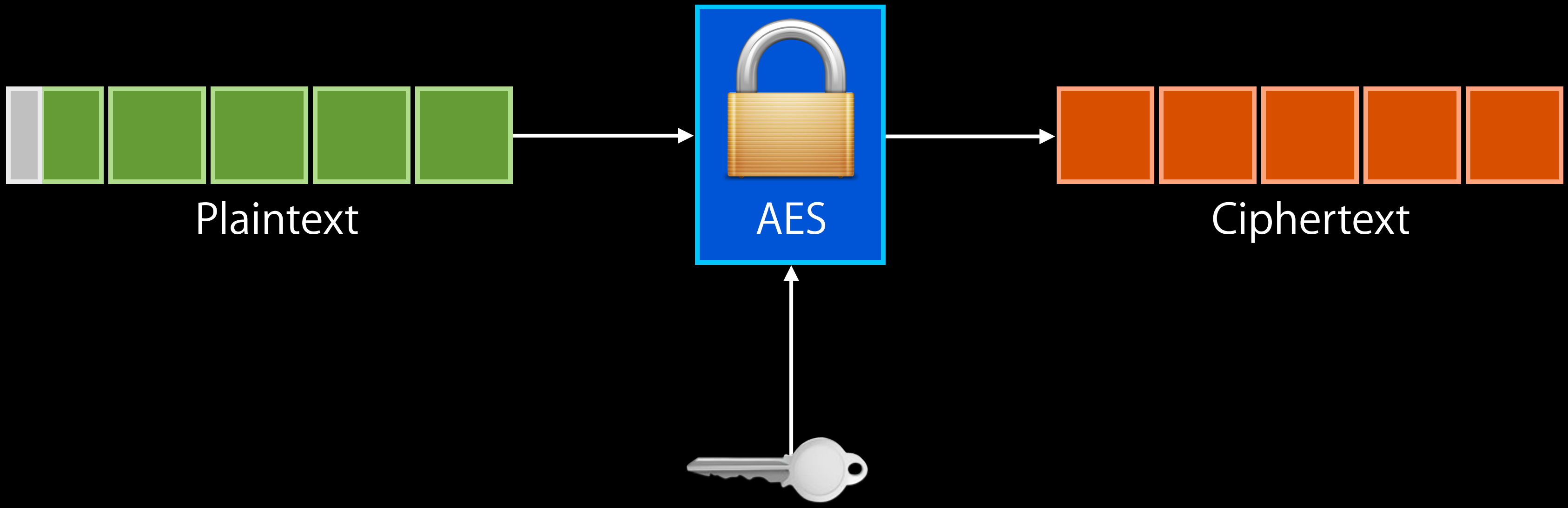
Plaintext

AES

Ciphertext

Cryptography

The devil is in the details



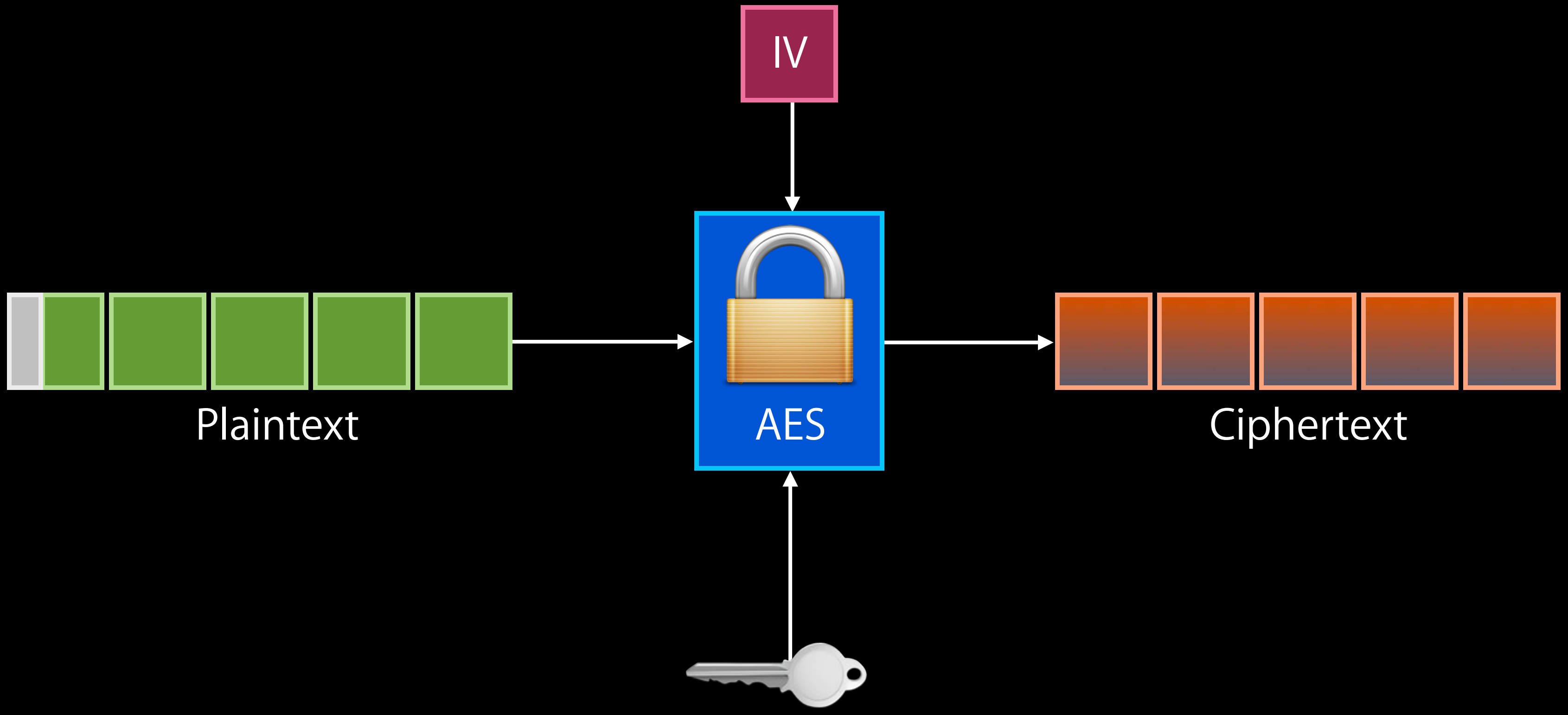
Plaintext

AES

Ciphertext

Cryptography

The devil is in the details



IV

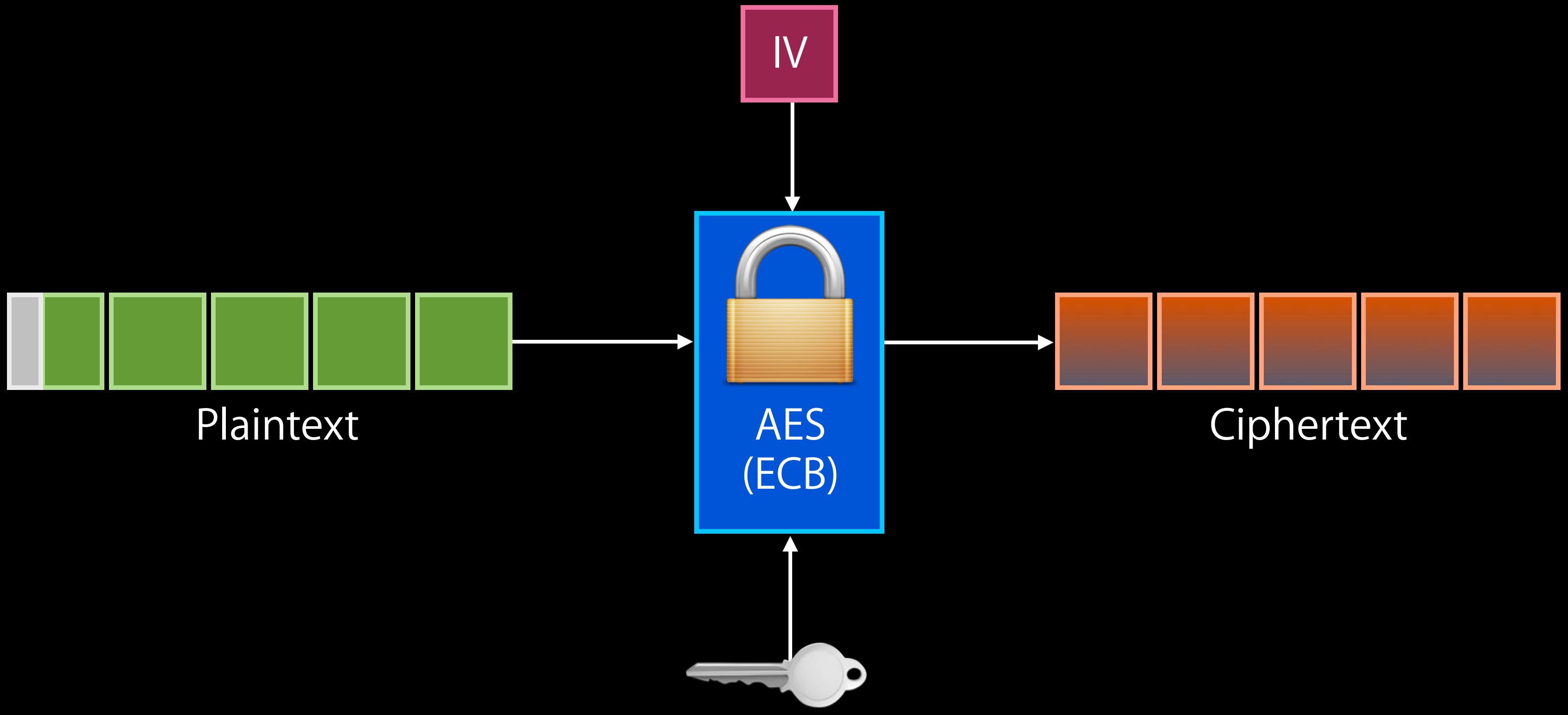
AES

Plaintext

Ciphertext

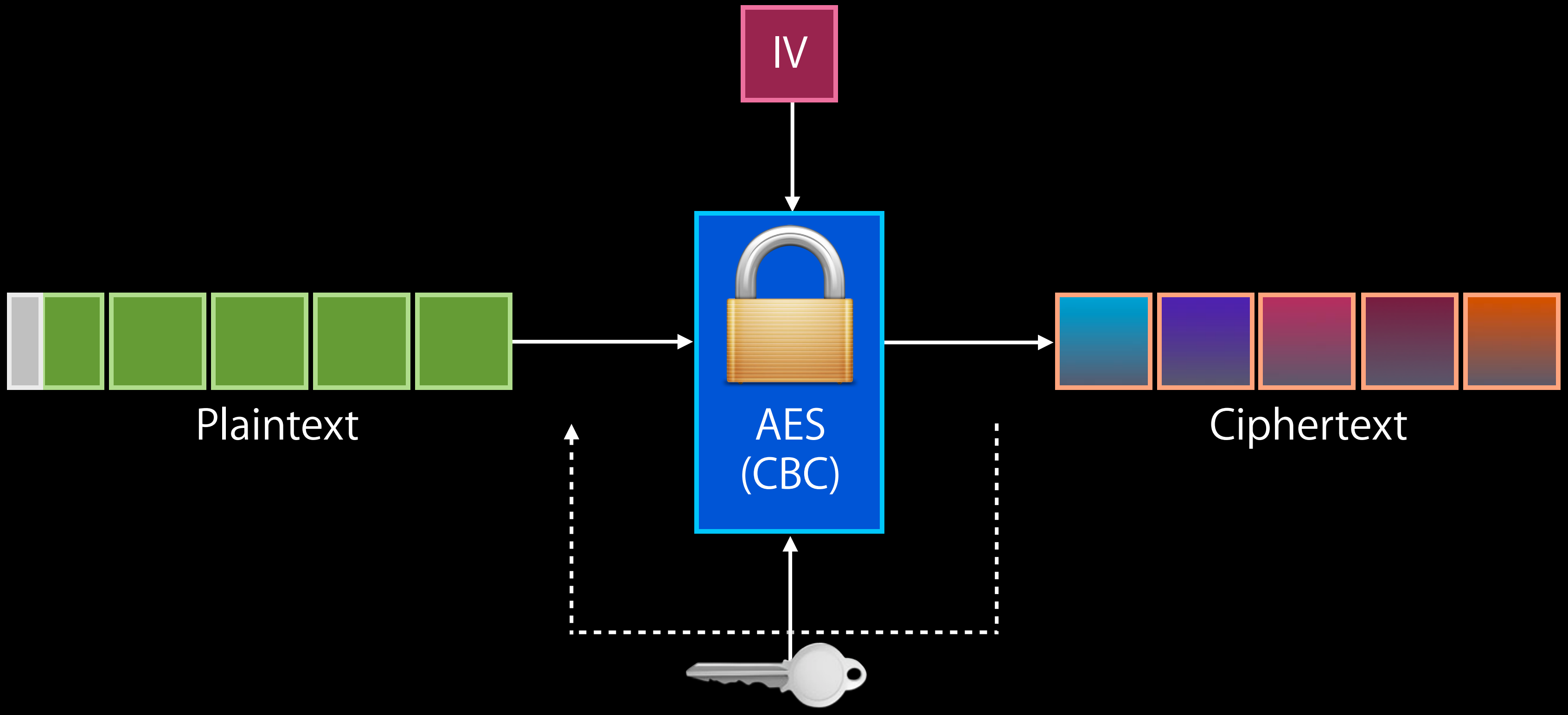
Cryptography

The devil is in the details



Cryptography

The devil is in the details



Cryptography

The devil is in the details

Cryptography

The devil is in the details

Cryptography

The devil is in the details

Cryptography

The devil is in the details

Cryptography

The devil is in the details

- Avoid using crypto primitives

Cryptography

The devil is in the details

- Avoid using crypto primitives
- Use higher level services

Cryptography

The devil is in the details

- Avoid using crypto primitives
- Use higher level services
  - Cryptographic Message Syntax

Cryptography

The devil is in the details

- Avoid using crypto primitives
- Use higher level services
    - Cryptographic Message Syntax
        - S/MIME

Cryptography

The devil is in the details

- Avoid using crypto primitives
- Use higher level services
    - Cryptographic Message Syntax
        - S/MIME
    - SecKey

Cryptography

The devil is in the details

- Avoid using crypto primitives
- Use higher level services
  - Cryptographic Message Syntax
    - S/MIME
  - SecKey
  - SecTransform

Cryptography

SecTransform

Cryptography

SecTransform

- Data driven CF interface to GCD

Cryptography

SecTransform

- Data driven CF interface to GCD
    - Only on OS X

Cryptography

SecTransform

- Data driven CF interface to GCD
  - Only on OS X
- Cryptography

Cryptography

SecTransform

- Data driven CF interface to GCD
  - Only on OS X
- Cryptography
- Data encoding

Cryptography

SecTransform

- Data driven CF interface to GCD
  - Only on OS X
- Cryptography
- Data encoding
- Simpler code!

SecTransform

Base 64 encoding

```
CFDataRef dataToEncode;
CFErrorRef error = NULL;

SecTransformRef encodingRef = SecEncodeTransformCreate(
                                     kSecBase64Encoding,&error);

SecTransformSetAttribute(encodingRef,
                         kSecTransformInputAttributeName,
                          dataToEncode, &error);

CFDataRef resultData = SecTransformExecute(encodingRef, &error);
```

SecTransform

Base 64 encoding

```
CFDataRef dataToEncode;
CFErrorRef error = NULL;

SecTransformRef encodingRef = SecEncodeTransformCreate(
                                     kSecBase64Encoding,&error);

SecTransformSetAttribute(encodingRef,
                         kSecTransformInputAttributeName,
                          dataToEncode, &error);

CFDataRef resultData = SecTransformExecute(encodingRef, &error);
```

SecTransform

Base 64 encoding

```
CFDataRef dataToEncode;
CFErrorRef error = NULL;

SecTransformRef encodingRef = SecEncodeTransformCreate(
                                     kSecBase64Encoding,&error);

SecTransformSetAttribute(encodingRef,
                         kSecTransformInputAttributeName,
                          dataToEncode, &error);

CFDataRef resultData = SecTransformExecute(encodingRef, &error);
```

SecTransform

Base 64 encoding

```
CFDataRef dataToEncode;
CFErrorRef error = NULL;

SecTransformRef encodingRef = SecEncodeTransformCreate(
                                     kSecBase64Encoding,&error);

SecTransformSetAttribute(encodingRef,
                         kSecTransformInputAttributeName,
                          dataToEncode, &error);

CFDataRef resultData = SecTransformExecute(encodingRef, &error);
```

SecTransform

Base 64 encoding

```
CFDataRef dataToEncode;
CFErrorRef error = NULL;

SecTransformRef encodingRef = SecEncodeTransformCreate(
                                     kSecBase64Encoding,&error);

SecTransformSetAttribute(encodingRef,
                         kSecTransformInputAttributeName,
                          dataToEncode, &error);

CFDataRef resultData = SecTransformExecute(encodingRef, &error);
```

SecTransform

Base 64 encoding

```
CFDataRef dataToEncode;
CFErrorRef error = NULL;

SecTransformRef encodingRef = SecEncodeTransformCreate(
                                     kSecBase64Encoding,&error);

SecTransformSetAttribute(encodingRef,
                         kSecTransformInputAttributeName,
                          dataToEncode, &error);

CFDataRef resultData = SecTransformExecute(encodingRef, &error);
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

SecTransform

Encrypt and then base 64 encode

```
SecKeyRef key;
CFDataRef dataToEncryptAndEncode;
SecTransformRef encryptionRef = SecEncryptTransformCreate(keyRef, &error);
SecTransformRef encodingRef = SecEncodeTransformCreate(kSecBase64Encoding,
                                                       &error);
SecGroupTransformRef group = SecTransformCreateGroupTransform();

SecTransformConnectTransforms(
                   encryptionRef, kSecTransformOutputAttributeName,
                   encodingRef, kSecTransformInputAttributeName, group,
                    &error);

SecTransformSetAttribute(encryptionRef, kSecTransformInputAttributeName,
                   dataToEncryptAndEncode,  &error);

SecTransformExecuteAsync(group, ^(data, error, isFinal){} );
```

Keychain

Keychain

- Protects the user’s secrets

Keychain

- Protects the user's secrets
- Enforces access control

Keychain

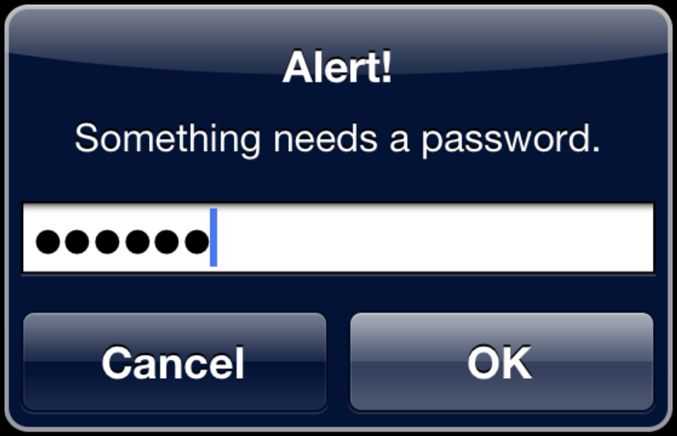
- Protects the user’s secrets
- Enforces access control
- Cryptographically secure

Keychain

- Protects the user's secrets
- Enforces access control
- Cryptographically secure
- OS X supports multiple keychains

Using the Keychain

SecItem API



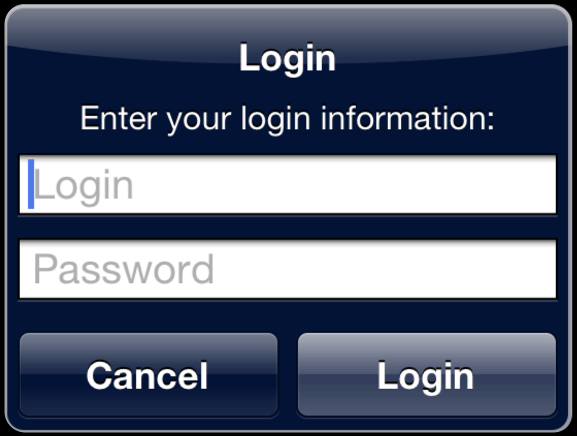
Alert!

Something needs a password.

`UIAlertViewStyleSecureTextInput`

Using the Keychain

SecItem API



Login

Enter your login information:

`UIAlertViewStyleLoginAndPasswordInput`

Storing the Password

```
// Create a dictionary.
NSMutableDictionary *attrs = [NSMutableDictionary dictionary];

// Set the attributes.
[attrs setObject:kSecClassGenericPassword forKey:kSecClass];
[attrs setObject:@”MyAccount” forKey:kSecAttrAccount];
[attrs setObject:password forKey:kSecValueData];


// Store it in the keychain.
OSStatus error = SecItemAdd((CFDictionaryRef)attrs, NULL);
```

Storing the Password

```
// Create a dictionary.
NSMutableDictionary *attrs = [NSMutableDictionary dictionary];
```

```
// Set the attributes.
[attrs setObject:kSecClassGenericPassword forKey:kSecClass];
[attrs setObject:@”MyAccount” forKey:kSecAttrAccount];
[attrs setObject:password forKey:kSecValueData];


// Store it in the keychain.
OSStatus error = SecItemAdd((CFDictionaryRef)attrs, NULL);
```

Storing the Password

```
// Create a dictionary.
NSMutableDictionary *attrs = [NSMutableDictionary dictionary];
```

```
// Set the attributes.
[attrs setObject:kSecClassGenericPassword forKey:kSecClass];
[attrs setObject:@”MyAccount” forKey:kSecAttrAccount];
[attrs setObject:password forKey:kSecValueData];
```

```
// Store it in the keychain.
OSStatus error = SecItemAdd((CFDictionaryRef)attrs, NULL);
```

Storing the Password

```
// Create a dictionary.
NSMutableDictionary *attrs = [NSMutableDictionary dictionary];

// Set the attributes.
[attrs setObject:kSecClassGenericPassword forKey:kSecClass];
[attrs setObject:@”MyAccount” forKey:kSecAttrAccount];
[attrs setObject:password forKey:kSecValueData];
```

```
// Store it in the keychain.
OSStatus error = SecItemAdd((CFDictionaryRef)attrs, NULL);
```

Storing the Password

```
// Create a dictionary.
NSMutableDictionary *attrs = [NSMutableDictionary dictionary];

// Set the attributes.
[attrs setObject:kSecClassGenericPassword forKey:kSecClass];
[attrs setObject:@”MyAccount” forKey:kSecAttrAccount];
[attrs setObject:password forKey:kSecValueData];


// Store it in the keychain.
OSStatus error = SecItemAdd((CFDictionaryRef)attrs, NULL);
```

Retrieving the Password

```
// Create a query.
NSMutableDictionary *query = [NSMutableDictionary dictionary];

// Set the attributes.
[query setObject:kSecClassGenericPassword forKey:kSecClass];
[query setObject:@”MyAccount” forKey:kSecAttrAccount];
[query setObject:kCFBooleanTrue forKey:kSecReturnData];

// Retrieve it from the keychain.
OSStatus error = SecItemCopyMatching((CFDictionaryRef)query, (CFTypeRef
*)&password);
```

Retrieving the Password

```
// Create a query.
NSMutableDictionary *query = [NSMutableDictionary dictionary];

// Set the attributes.
[query setObject:kSecClassGenericPassword forKey:kSecClass];
[query setObject:@”MyAccount” forKey:kSecAttrAccount];
[query setObject:kCFBooleanTrue forKey:kSecReturnData];

// Retrieve it from the keychain.
OSStatus error = SecItemCopyMatching((CFDictionaryRef)query, (CFTypeRef
*)&password);
```

Retrieving the Password

```
// Create a query.
NSMutableDictionary *query = [NSMutableDictionary dictionary];

// Set the attributes.
[query setObject:kSecClassGenericPassword forKey:kSecClass];
[query setObject:@”MyAccount” forKey:kSecAttrAccount];
[query setObject:kCFBooleanTrue forKey:kSecReturnData];

// Retrieve it from the keychain.
OSStatus error = SecItemCopyMatching((CFDictionaryRef)query, (CFTypeRef
*)&password);
```

Retrieving the Password

```
// Create a query.
NSMutableDictionary *query = [NSMutableDictionary dictionary];

// Set the attributes.
[query setObject:kSecClassGenericPassword forKey:kSecClass];
[query setObject:@”MyAccount” forKey:kSecAttrAccount];
[query setObject:kCFBooleanTrue forKey:kSecReturnData];

// Retrieve it from the keychain.
OSStatus error = SecItemCopyMatching((CFDictionaryRef)query, (CFTypeRef
*)&password);
```

Retrieving the Password

```
// Create a query.
NSMutableDictionary *query = [NSMutableDictionary dictionary];

// Set the attributes.
[query setObject:kSecClassGenericPassword forKey:kSecClass];
[query setObject:@”MyAccount” forKey:kSecAttrAccount];
[query setObject:kCFBooleanTrue forKey:kSecReturnData];

// Retrieve it from the keychain.
OSStatus error = SecItemCopyMatching((CFDictionaryRef)query, (CFTypeRef
*)&password);
```

Retrieving the Password

```
// Create a query.
NSMutableDictionary *query = [NSMutableDictionary dictionary];

// Set the attributes.
[query setObject:kSecClassGenericPassword forKey:kSecClass];
[query setObject:@”MyAccount” forKey:kSecAttrAccount];
[query setObject:kCFBooleanTrue forKey:kSecReturnData];

// Retrieve it from the keychain.
OSStatus error = SecItemCopyMatching((CFDictionaryRef)query, (CFTypeRef
*)&password);
```

Secure Transport

Secure Transport

- Protects data over the network

Secure Transport

- Protects data over the network
- Negotiates secure channel via TLS/SSL

Secure Transport

- Protects data over the network
- Negotiates secure channel via TLS/SSL
- Mountain Lion and iOS 5 support TLS 1.2

Secure Transport

- Protects data over the network
- Negotiates secure channel via TLS/SSL
- Mountain Lion and iOS 5 support TLS 1.2
- Supported via CFNetwork, NSURL*

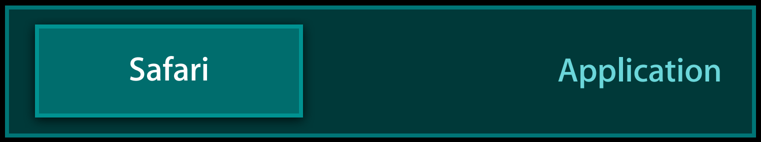
Secure Transport

- Protects data over the network
- Negotiates secure channel via TLS/SSL
- Mountain Lion and iOS 5 support TLS 1.2
- Supported via CFNetwork, NSURL*

TLS 1.2 Interoperability
http://developer.apple.com/library/ios/#technotes/tn2287/_index.html

Secure Transport

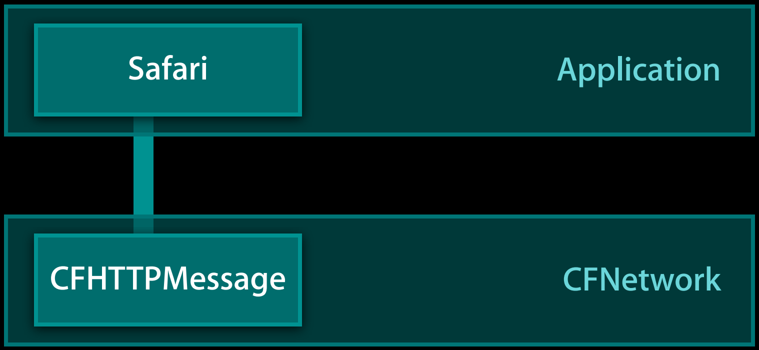
Secure Transport



Safari

Application

Secure Transport



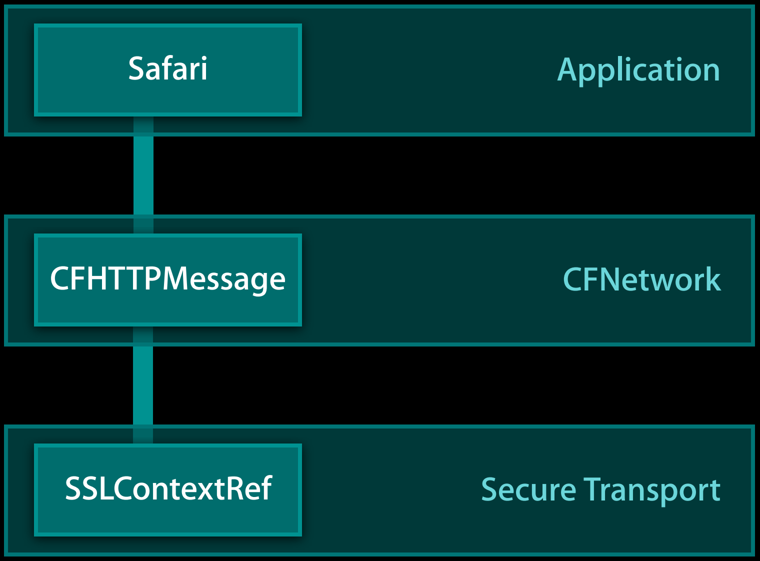
Safari

Application

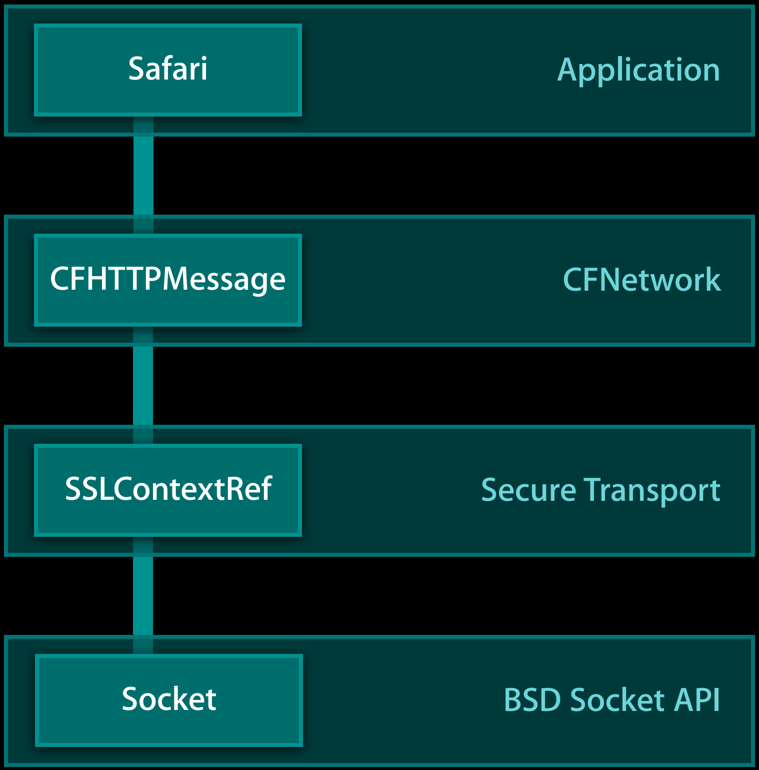
CFHTTPMessage

CFNetwork

Secure Transport



Secure Transport



Safari

Application

CFHTTPMessage

CFNetwork

SSLContextRef

Secure Transport

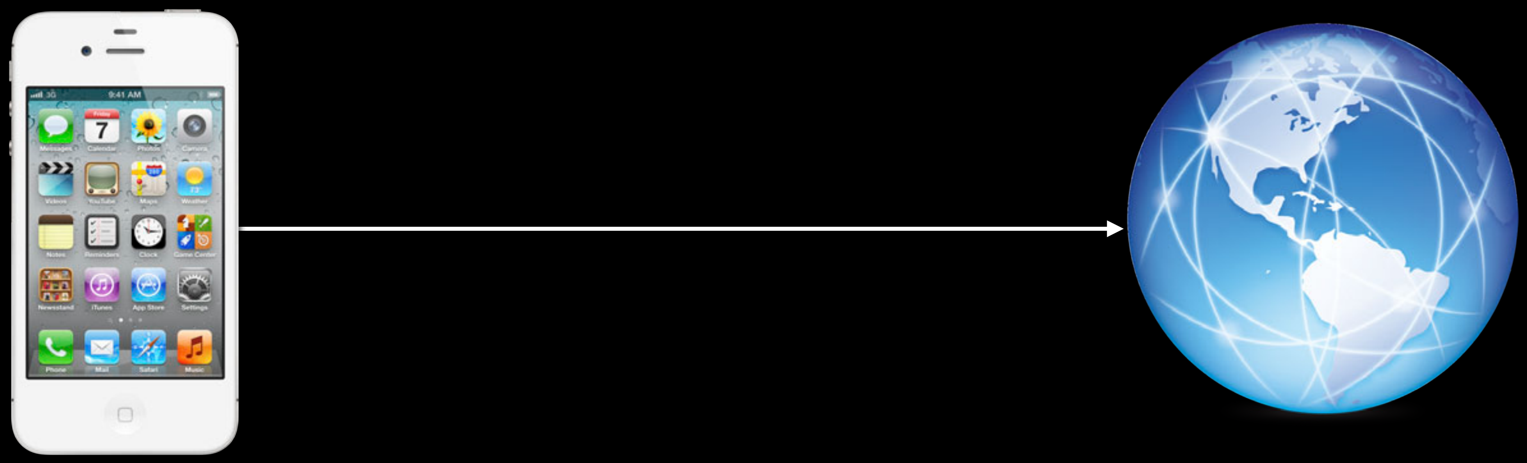
Socket

BSD Socket API

Secure Transport

Secure Transport

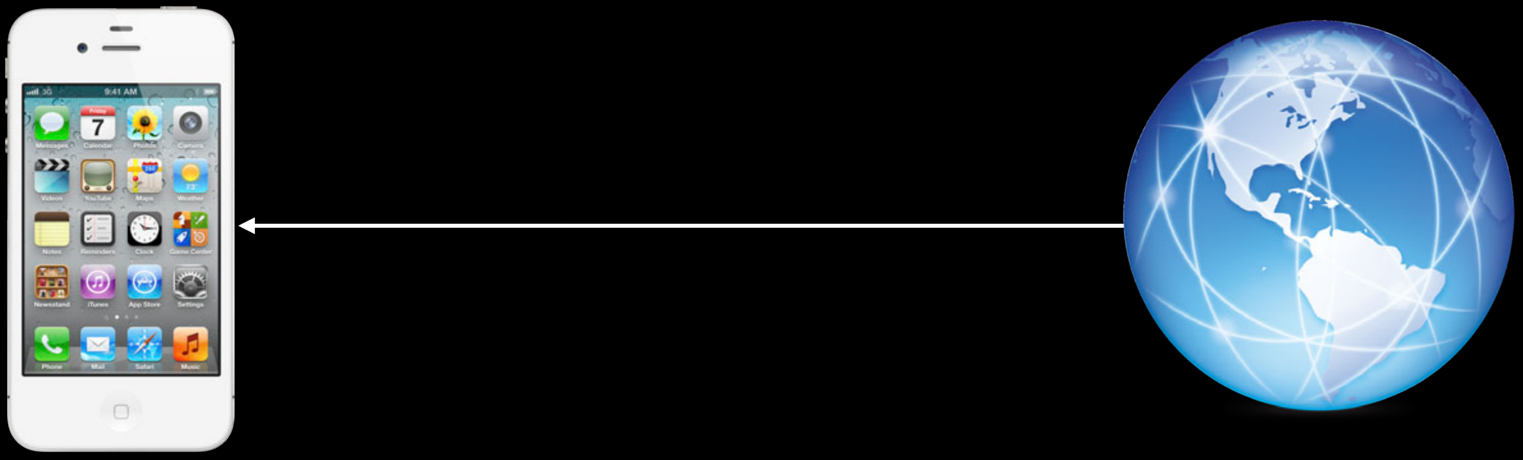
Secure Transport



“Hello!”

Supported Versions
Cipher Suites
Compression Methods

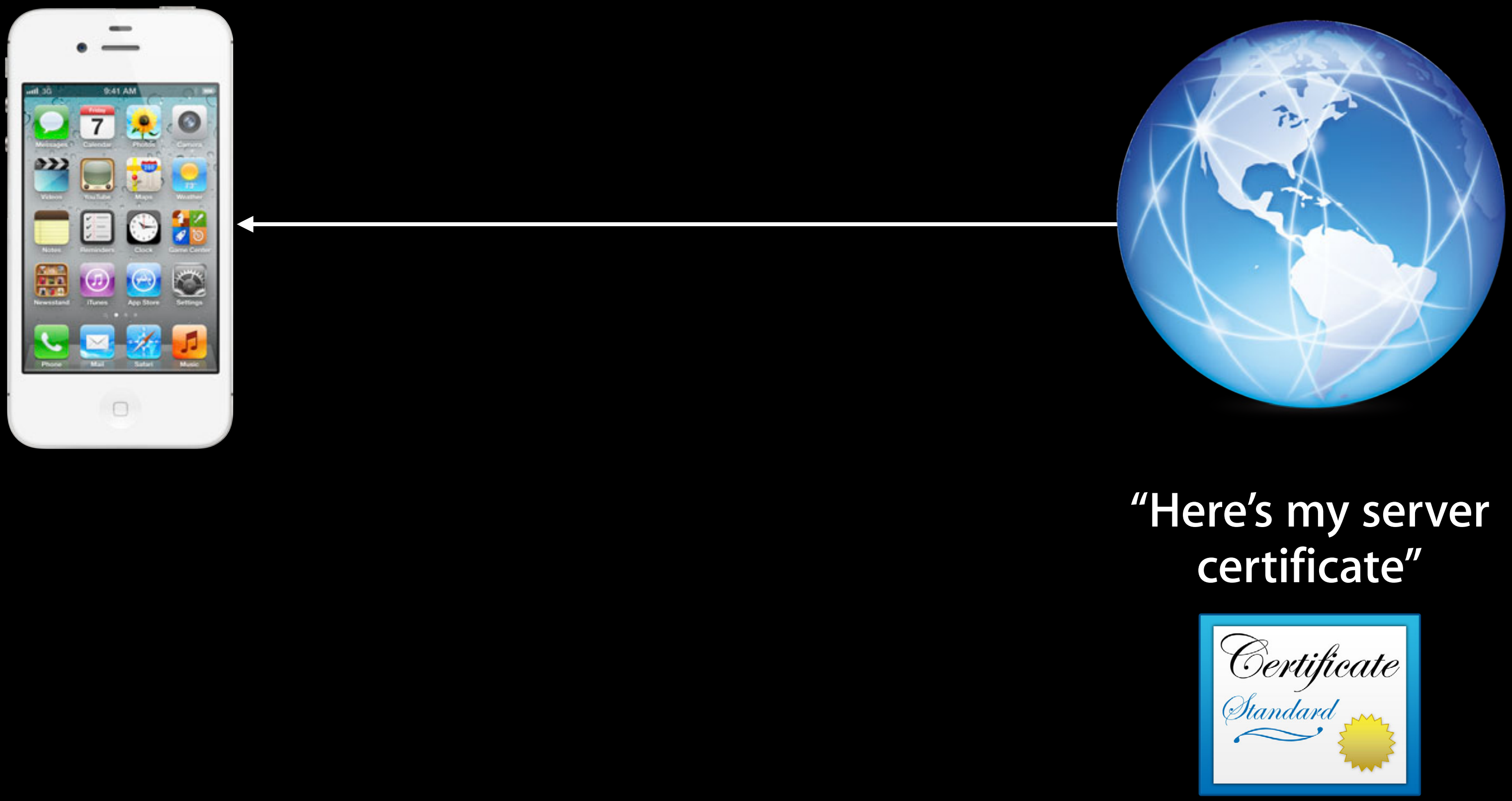
Secure Transport



“Hello!”

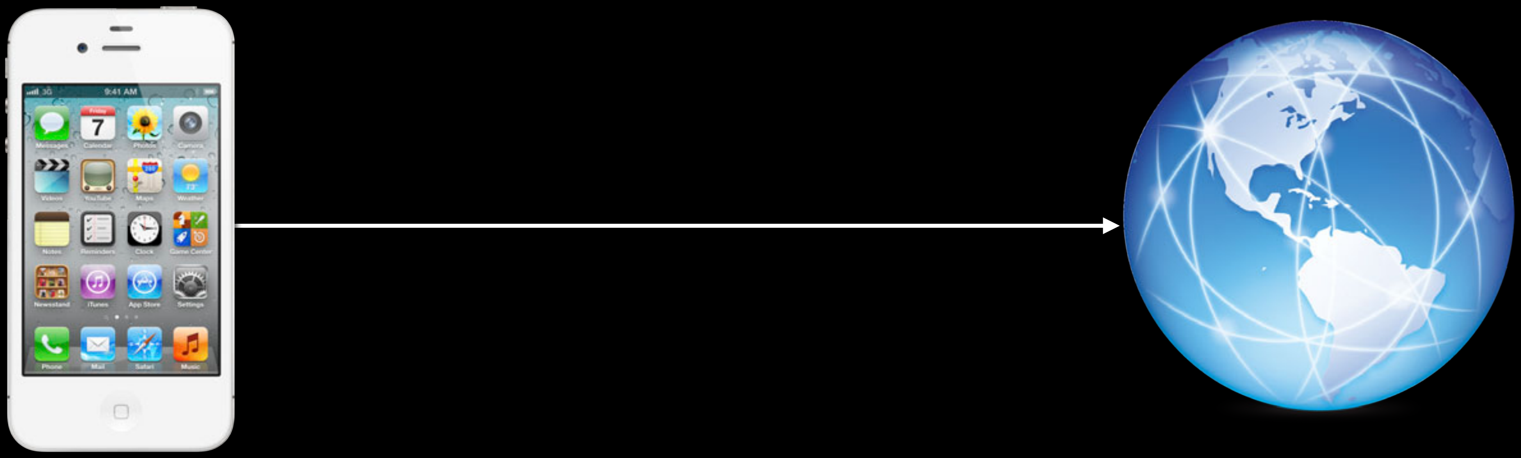
Chosen Versions
Chosen Cipher
Chosen Compression

Secure Transport



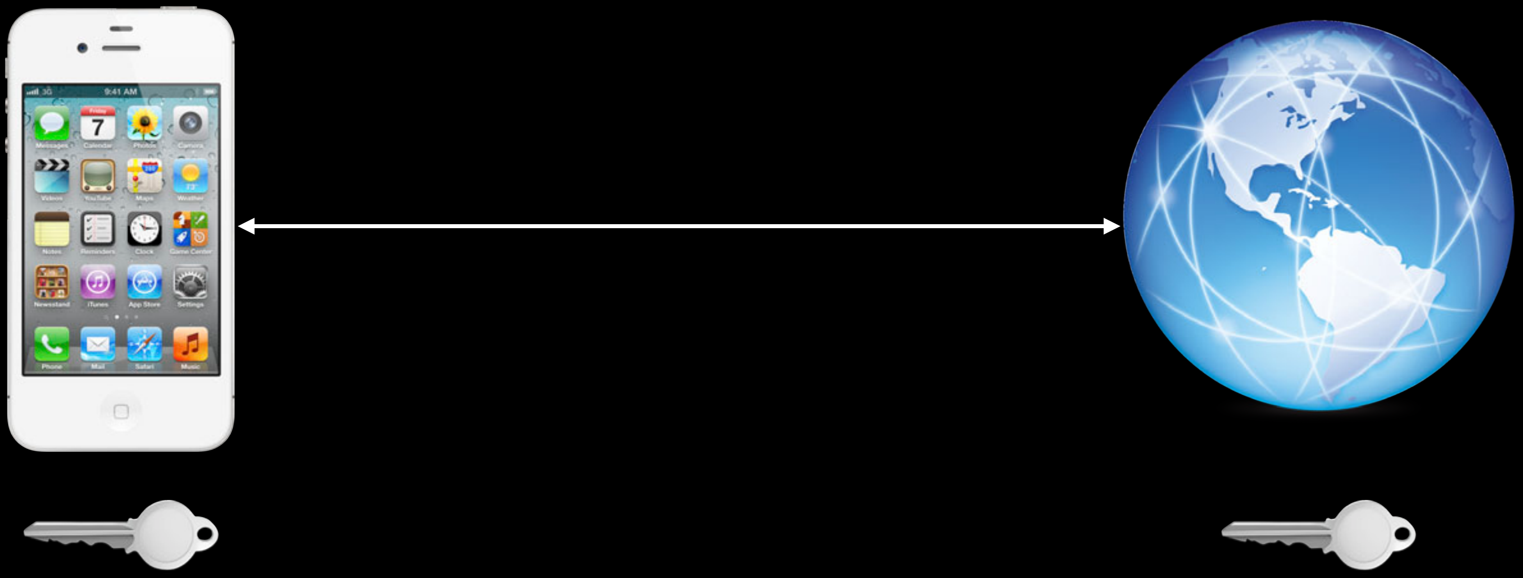
“Here’s my server certificate”

Secure Transport



“Here’s my client certificate”

Secure Transport



Trust Evaluation

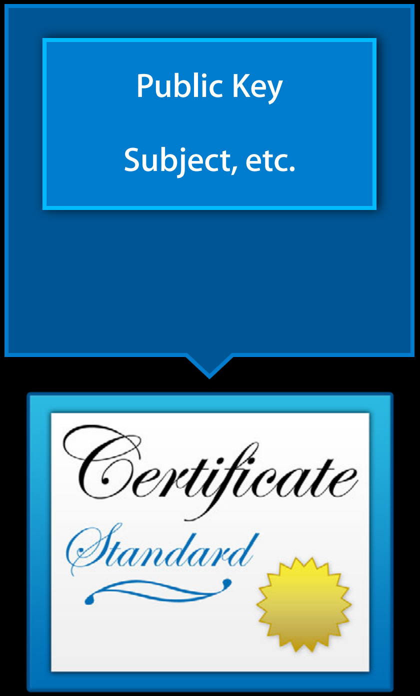
What are certificates?

Trust Evaluation

What are certificates?

Trust Evaluation

What are certificates?

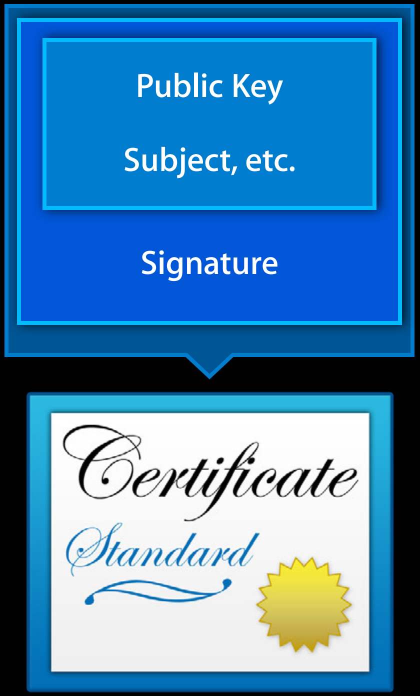


Public Key

Subject, etc.

Trust Evaluation

What are certificates?



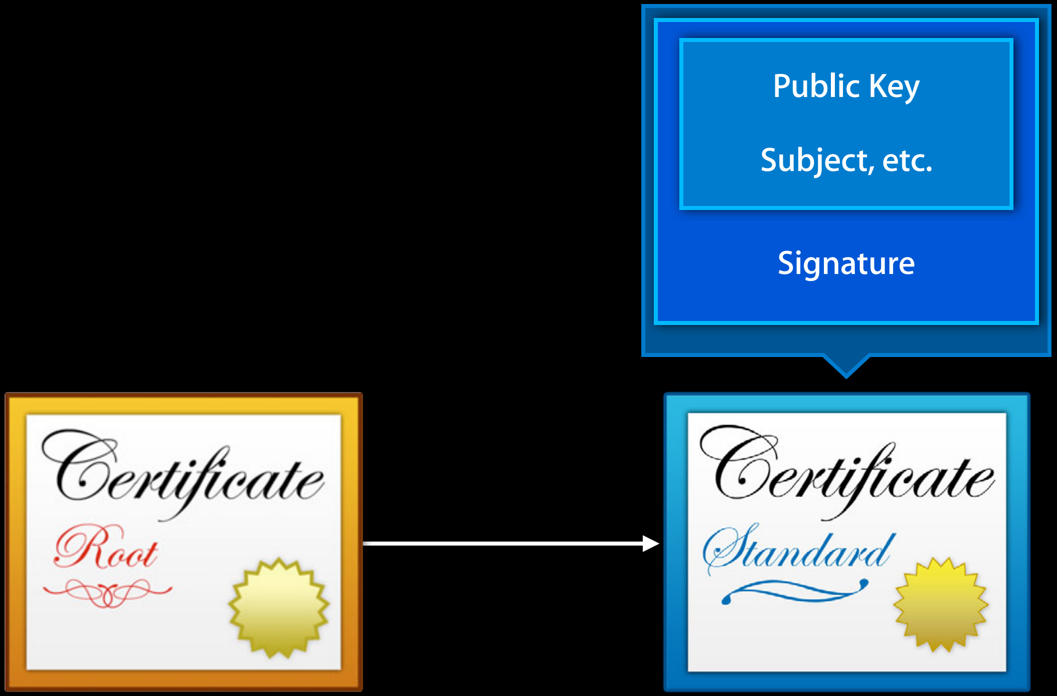
Public Key

Subject, etc.

Signature

Trust Evaluation

What are certificates?



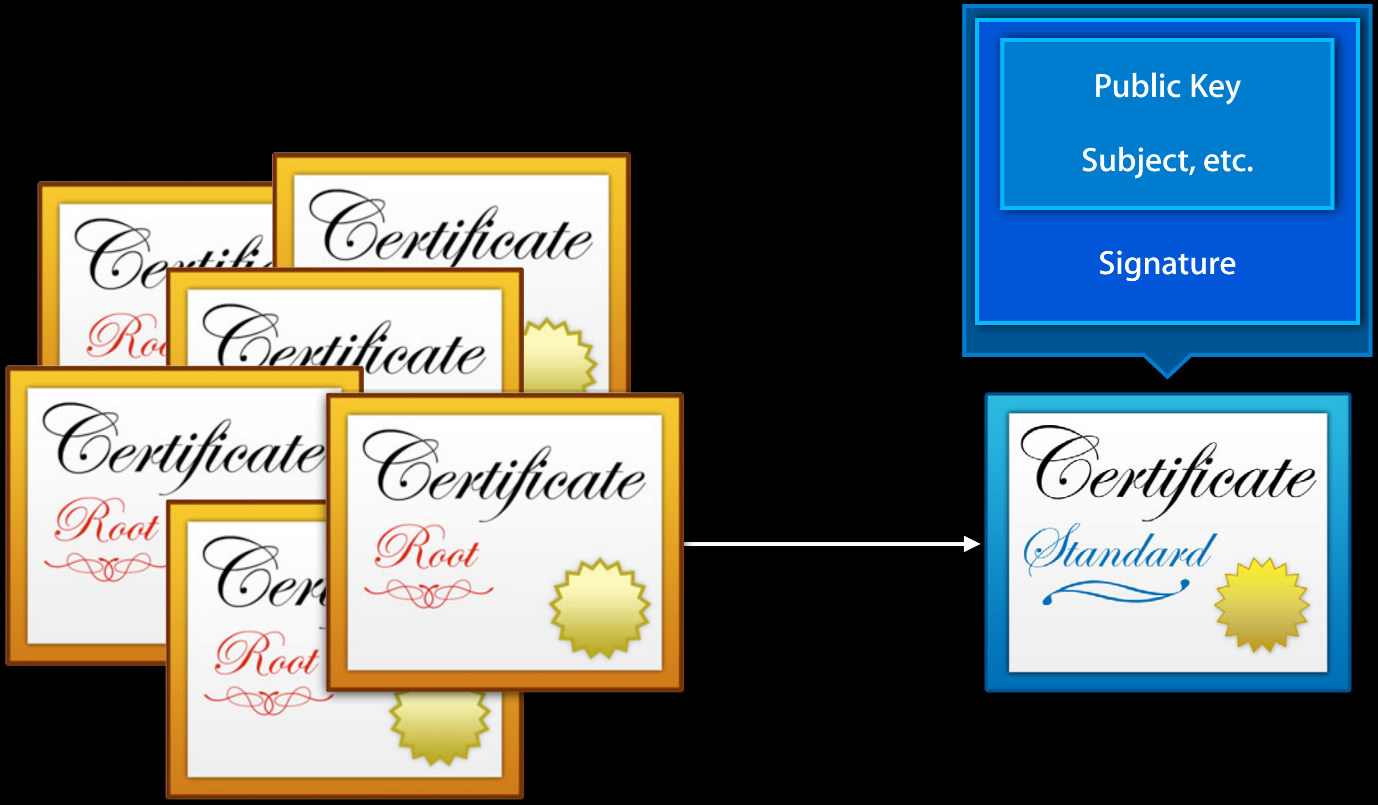
Public Key

Subject, etc.

Signature

Trust Evaluation

What are certificates?



Trust Evaluation

Trust Evaluation

- X.509 certificates

Trust Evaluation

- X.509 certificates
- Root Anchors

Trust Evaluation

- X.509 certificates
- Root Anchors
- Certificate chain

Trust Evaluation

- X.509 certificates
- Root Anchors
- Certificate chain
- Revocation

Trust Evaluation

- X.509 certificates
- Root Anchors
- Certificate chain
- Revocation
  - CRL

Trust Evaluation

- X.509 certificates
- Root Anchors
- Certificate chain
- Revocation
  - CRL
  - OCSP

Chain of Trust

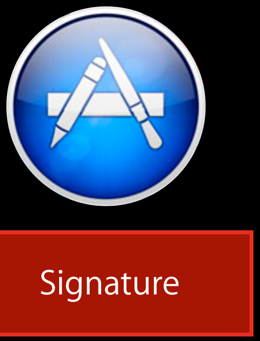
Evaluating a signature

Chain of Trust

Evaluating a signature

Chain of Trust

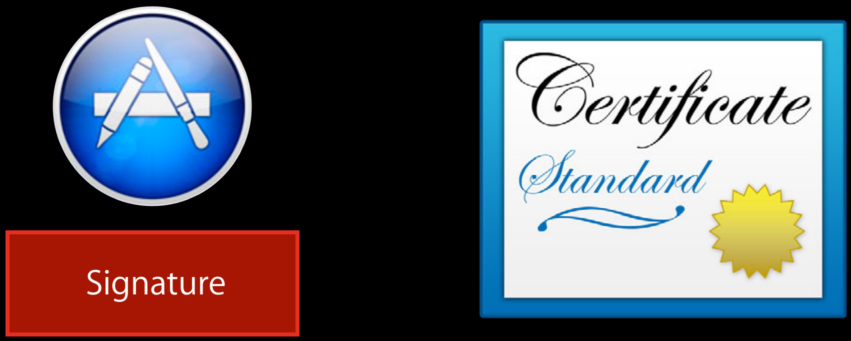
Evaluating a signature



Signature

Chain of Trust

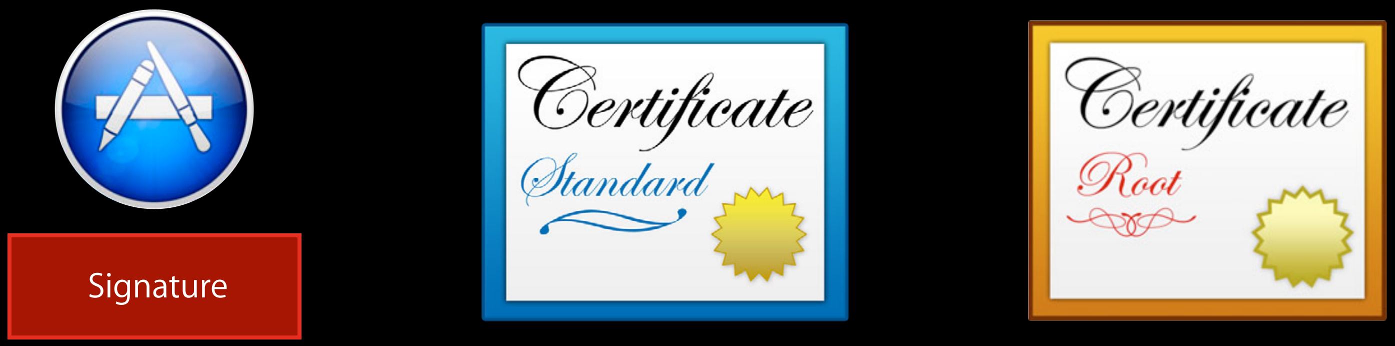
Evaluating a signature



Signature

Chain of Trust

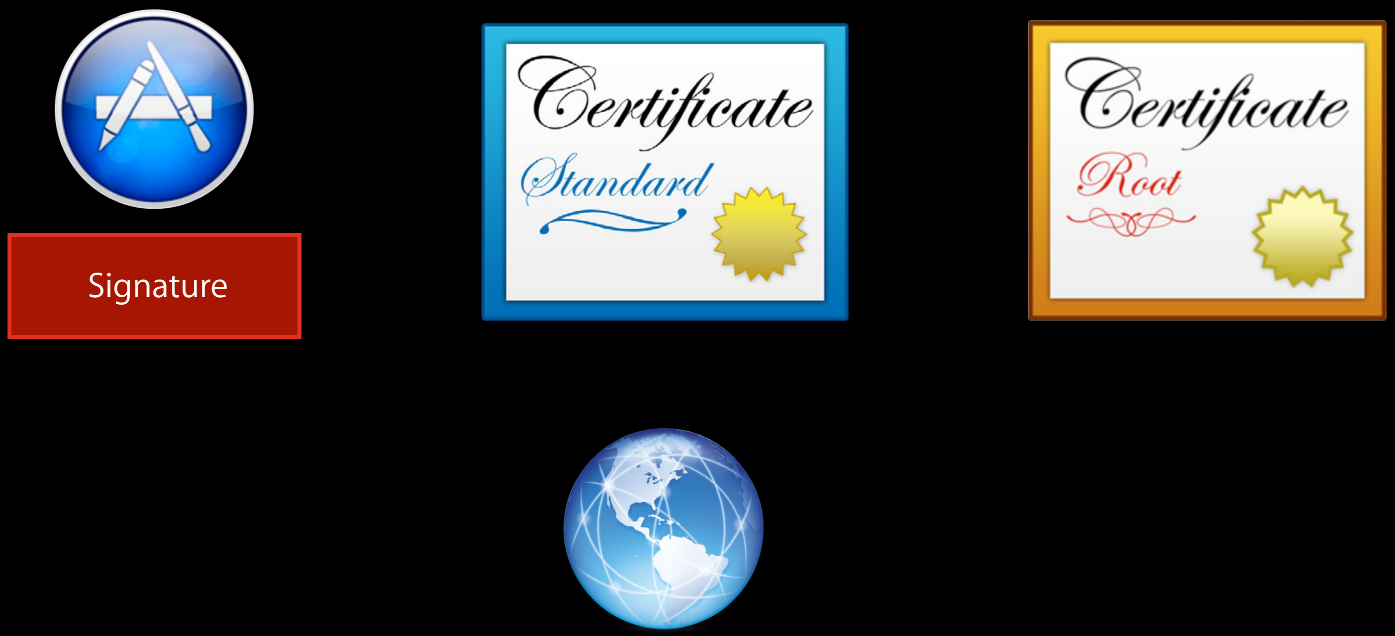
Evaluating a signature



Signature

Chain of Trust

Evaluating a signature



Signature

Trust Evaluation

SecTrust API

Certificate, Key, and Trust Services Reference
http://developer.apple.com/library/mac/#documentation/security/Reference/certifkeytrustservices

Related Sessions

Protecting the User’s Data	Pacific Heights Friday 11:30AM

Labs

Security Lab	Core OS Lab B Tuesday 3:15PM
Security Lab	Core OS Lab B Thursday 9:00AM

Cross Platform

Cross Platform

- Shared source base

Cross Platform

- Shared source base
  - CommonCrypto

Cross Platform

- Shared source base
  - CommonCrypto
  - Secure Transport

Cross Platform

- Shared source base
  - CommonCrypto
  - Secure Transport
- iOS Security.framework is a subset

Cross Platform

- Shared source base
  - CommonCrypto
  - Secure Transport
- iOS Security.framework is a subset
  - Single keychain

Cross Platform

- Shared source base
  - CommonCrypto
  - Secure Transport
- iOS Security.framework is a subset
  - Single keychain
  - SecItem API Only

Cross Platform

- Shared source base
  - CommonCrypto
  - Secure Transport
- iOS Security.framework is a subset
  - Single keychain
  - SecItem API Only
- Data Protection API

Data Protection

Data Protection

- Protects data on a compromised device

Data Protection

- Protects data on a compromised device
- Encrypts files and keychain items with unique keys

Data Protection

- Protects data on a compromised device
- Encrypts files and keychain items with unique keys
- Keys are protected with the passcode

Data Protection

- Protects data on a compromised device
- Encrypts files and keychain items with unique keys
- Keys are protected with the passcode
- Provides different classes of protection

Data Protection

- Protects data on a compromised device
- Encrypts files and keychain items with unique keys
- Keys are protected with the passcode
- Provides different classes of protection
  - Always available

Data Protection

- Protects data on a compromised device
- Encrypts files and keychain items with unique keys
- Keys are protected with the passcode
- Provides different classes of protection
    - Always available
    - After first unlock

Data Protection

- Protects data on a compromised device
- Encrypts files and keychain items with unique keys
- Keys are protected with the passcode
- Provides different classes of protection
    - Always available
    - After first unlock
    - Only when unlocked

Unsupported

Unsupported

- DRM

Unsupported

- DRM
- Jailbreak detection

Summary

Summary

- Crypto

Summary

- Crypto
- Keychain

Summary

- Crypto
- Keychain
- Secure Transport

Summary

- Crypto
- Keychain
- Secure Transport
- Trust Evaluation

Summary

- Crypto
- Keychain
- Secure Transport
- Trust Evaluation
- Data Protection

Useful References

Security Introduction
http://developer.apple.com/library/mac/#referencelibrary/GettingStarted/GS_Security

Security Overview
http://developer.apple.com/library/mac/#documentation/Security/Conceptual/Security_Overview

Secure Coding Guide
http://developer.apple.com/library/mac/#documentation/Security/Conceptual/SecureCodingGuide

iOS Security
http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf

More Information

Paul Danbold

Core OS Evangelist
danbold@apple.com

Documentation

OS X Dev Center
http://developer.apple.com/devcenter/mac

iOS Dev Center
http://developer.apple.com/devcenter/ios

Apple Developer Forums

http://devforums.apple.com

Related Sessions

The OS X App Sandbox	Nob Hill Tuesday 10:15AM
Gatekeeper and Developer ID	Nob Hill Tuesday 11:30AM
Privacy Support in iOS and OS X	Pacific Heights Thursday 3:15PM
The OS X App Sandbox	Nob Hill Friday 10:15AM
Protecting the User’s Data	Pacific Heights Friday 11:30AM

Labs

Security Lab	Core OS Lab B Tuesday 3:15PM
Security Lab	Core OS Lab B Thursday 9:00AM

Q&A

WWDC2012