Your Apps and Evolving Network Security Standards

Session 701

Bailey Basile, Secure Transports Engineer
Chris Wood, Secure Transports Engineer

BEAST

FREAK

CRIME

POODLE

LogJam

Lucky13

Mis-issuance

BREACH

DROWN

3HS

BEAST

FREAK

CRIME

POODLE

Sweet32

SLOTH

LogJam

FLAME

SHAttered

Lucky13

NOMORE

Factoring

BREACH

DROWN

Mis-issuance

3HS

Best practices

Best practices

App Transport Security update

Best practices

App Transport Security update

Transport Layer Security

Best Practices

Best Practices

Best Practices

No “set and forget”

Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Update libraries

Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Update libraries

OS removes insecure options

Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Update libraries

OS removes insecure options

ATS enforces best practices

Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Update libraries

OS removes insecure options

ATS enforces best practices

Worth the maintenance cost

Best Practices

BEAST	FREAK	CRIME	POODLE
Sweet32	SLOTH	NOMORE	FLAME
SHAttered	Lucky13	LogJam	Factoring
BREACH	DROWN	Mis-issuance	3HS

Best Practices

Encryption

BEAST FREAK CRIME POODLE

Sweet32 SLOTH NOMORE FLAME

SHAttered Lucky13 LogJam Factoring

BREACH DROWN Mis-issuance 3HS

Best Practices

Encryption

Cryptographic hashes

BEAST	FREAK	CRIME	POODLE
Sweet32	SLOTH	NOMORE	FLAME
SHAttered	Lucky13	LogJam	Factoring
BREACH	DROWN	Mis-issuance	3HS

Best Practices

Encryption

Cryptographic hashes

Public keys

BEAST FREAK CRIME POODLE

Sweet32 SLOTH NOMORE FLAME

SHAttered Lucky13 LogJam Factoring

BREACH DROWN Mis-issuance 3HS

Best Practices

Encryption

Cryptographic hashes

Public keys

Protocols

BEAST	FREAK	CRIME	POODLE
Sweet32	SLOTH	NOMORE	FLAME
SHAttered	Lucky13	LogJam	Factoring
BREACH	DROWN	Mis-issuance	3HS

Best Practices

Encryption

Cryptographic hashes

Public keys

Protocols

Revocation

BEAST FREAK CRIME POODLE

Sweet32 SLOTH NOMORE FLAME

SHAttered Lucky13 LogJam Factoring

BREACH DROWN Mis-issuance 3HS

Best Practices

Encryption

Cryptographic hashes

Public keys

Protocols

Revocation

BEAST FREAK CRIME POODLE

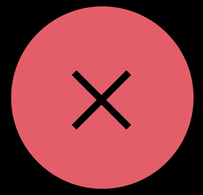
Sweet32 SLOTH NOMORE FLAME

SHAttered Lucky13 LogJam Factoring

BREACH DROWN Mis-issuance 3HS

Encryption

Encryption

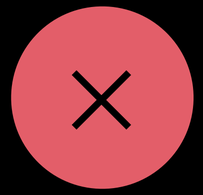


RC4

3DES-CBC

AES-CBC

Encryption



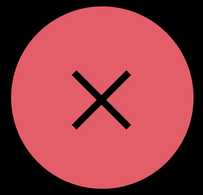
RC4

3DES-CBC

AES-CBC

Future removal: RC4 and 3DES

Encryption



RC4

3DES-CBC

AES-CBC

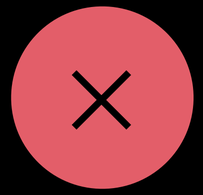
AES-GCM

ChaCha20/Poly1305

Future removal: RC4 and 3DES

Cryptographic Hashes

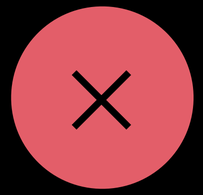
Cryptographic Hashes



MD5

SHA-1

Cryptographic Hashes

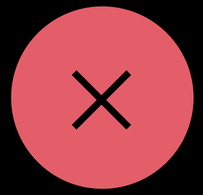


MD5

SHA-1

New removal: SHA-1 signed certificates for TLS

Cryptographic Hashes



MD5

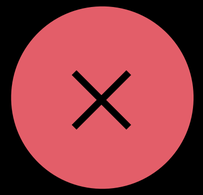
SHA-1

SHA-2 Family

New removal: SHA-1 signed certificates for TLS

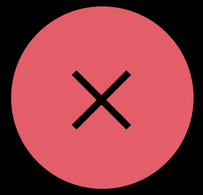
Public Keys

Public Keys



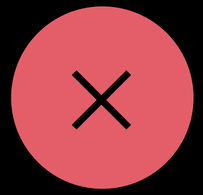
<1024-bit RSA

Public Keys



<2048-bit RSA

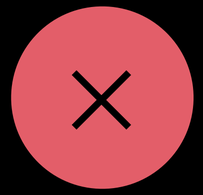
Public Keys



<2048-bit RSA

New removal: <2048-bit RSA for TLS

Public Keys



<2048-bit RSA

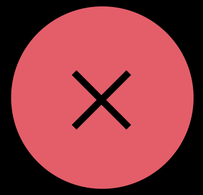
≥ 2048-bit RSA

Elliptic Curves

New removal: <2048-bit RSA for TLS

Protocols

Protocols



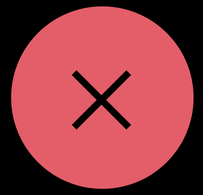
http://

SSLv3

TLS 1.0

TLS 1.1

Protocols



http://

SSLv3

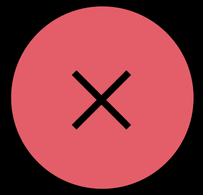
TLS 1.0

TLS 1.1

https://

TLS 1.2

Protocols



http://

SSLv3

TLS 1.0

TLS 1.1

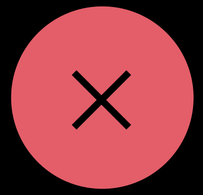
https://

TLS 1.2

New addition: TLS 1.3 (draft)

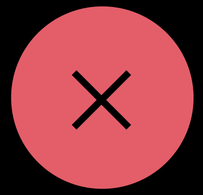
Revocation

Revocation



No checking

Revocation

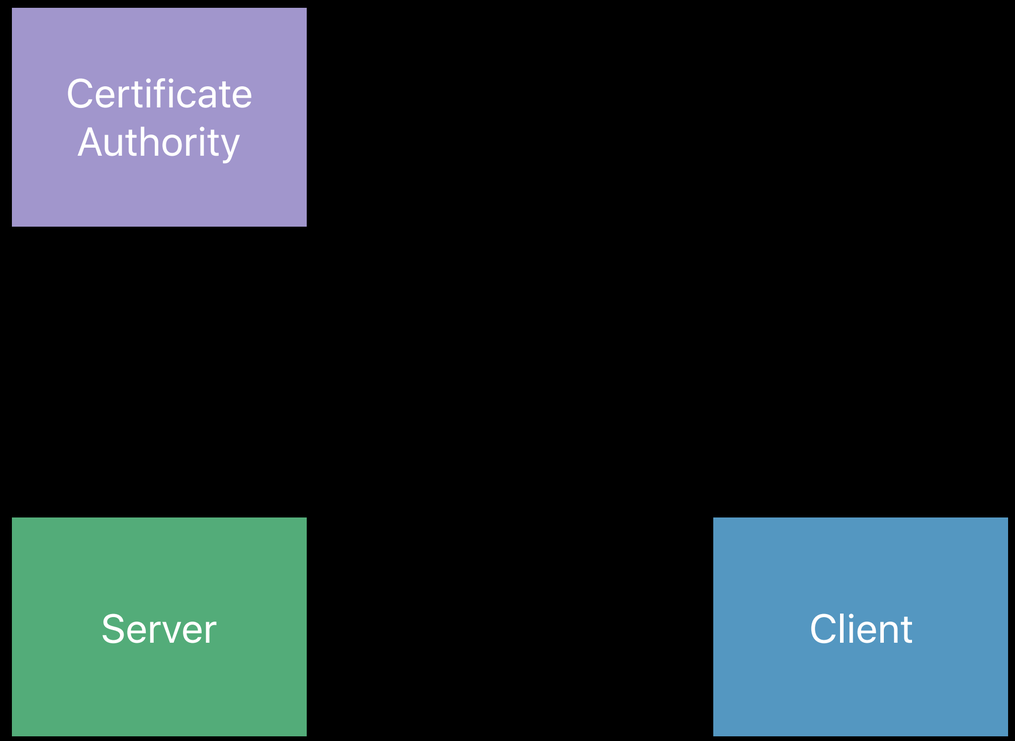


No checking

OCSP Stapling

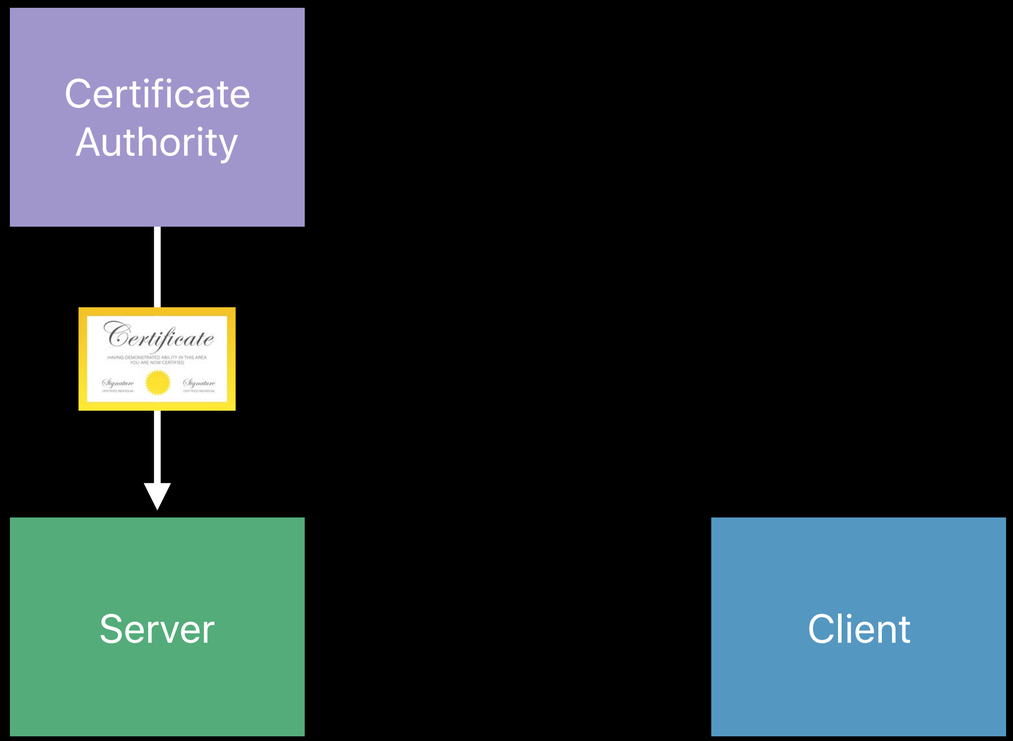
Revocation

Online Certificate Status Protocol



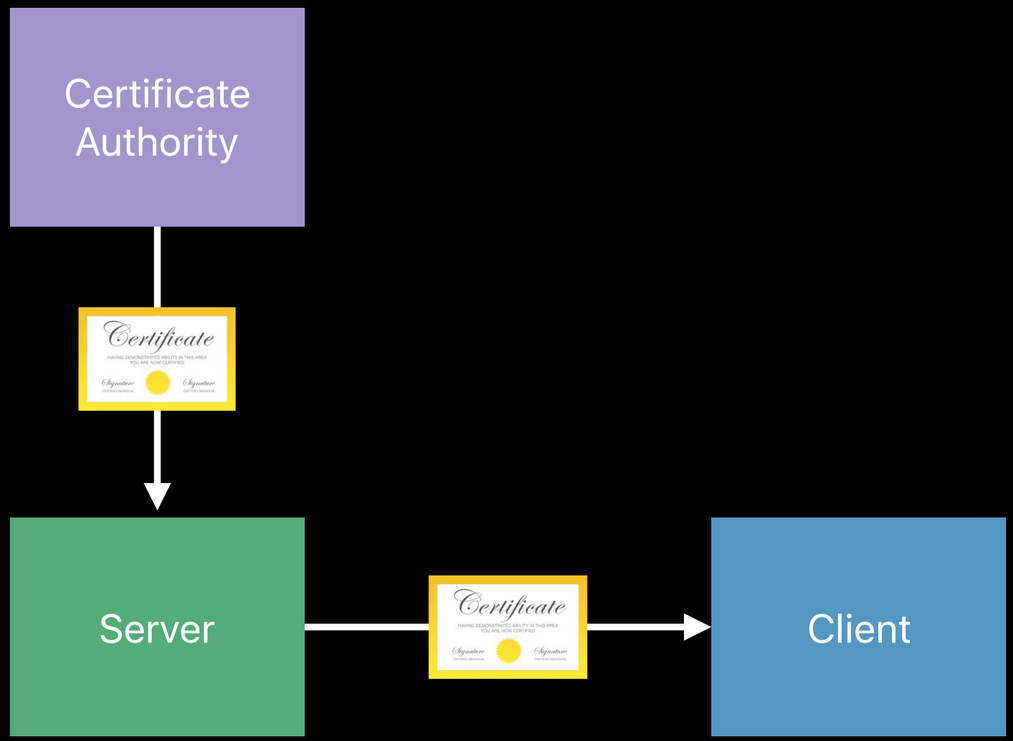
Revocation

Online Certificate Status Protocol



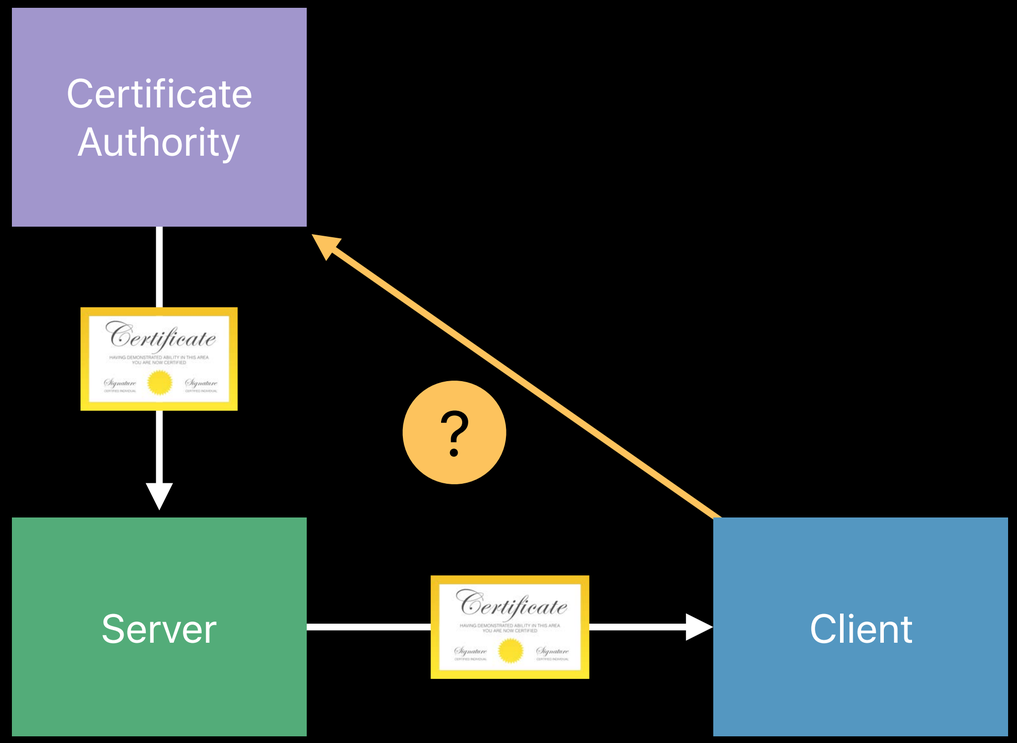
Revocation

Online Certificate Status Protocol



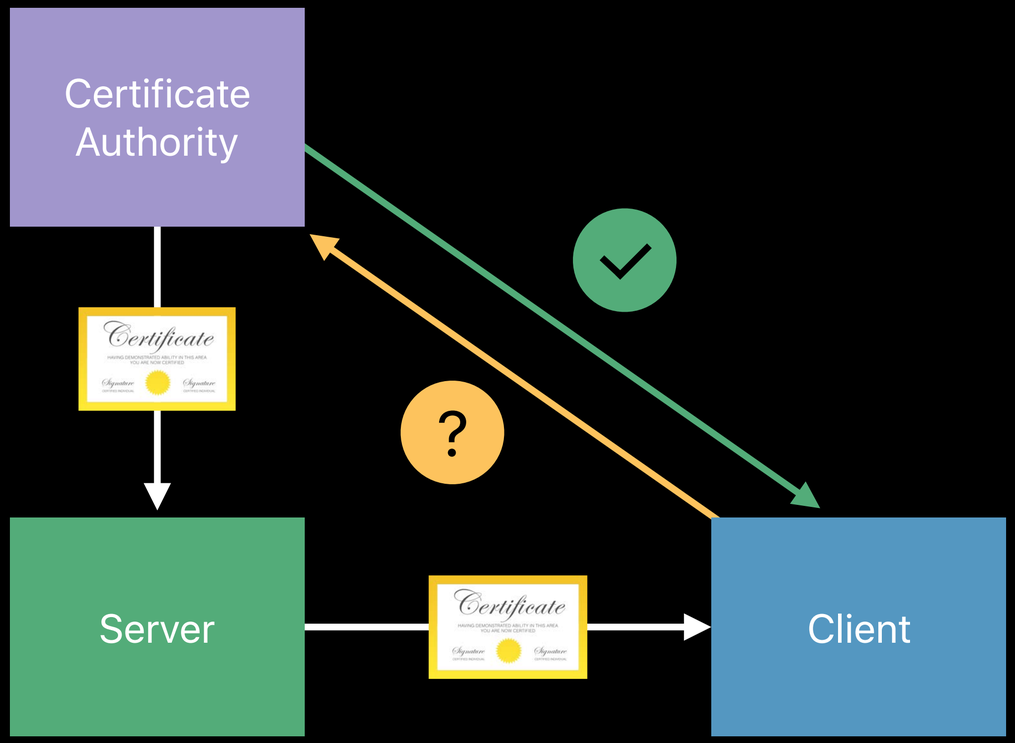
Revocation

Online Certificate Status Protocol



Revocation

Online Certificate Status Protocol



Revocation

Online Certificate Status Protocol

Revocation

Online Certificate Status Protocol

Additional network connection

Revocation

Online Certificate Status Protocol

Additional network connection

Compromises user privacy

Revocation

Online Certificate Status Protocol

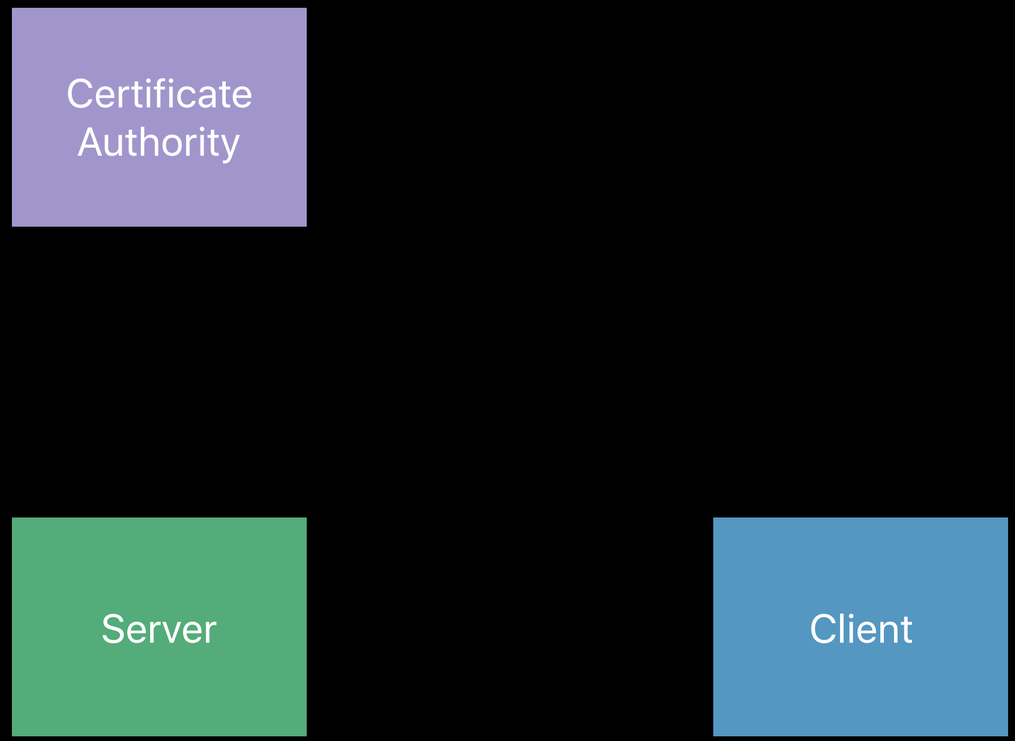
Additional network connection

Compromises user privacy

Requires app opt-in

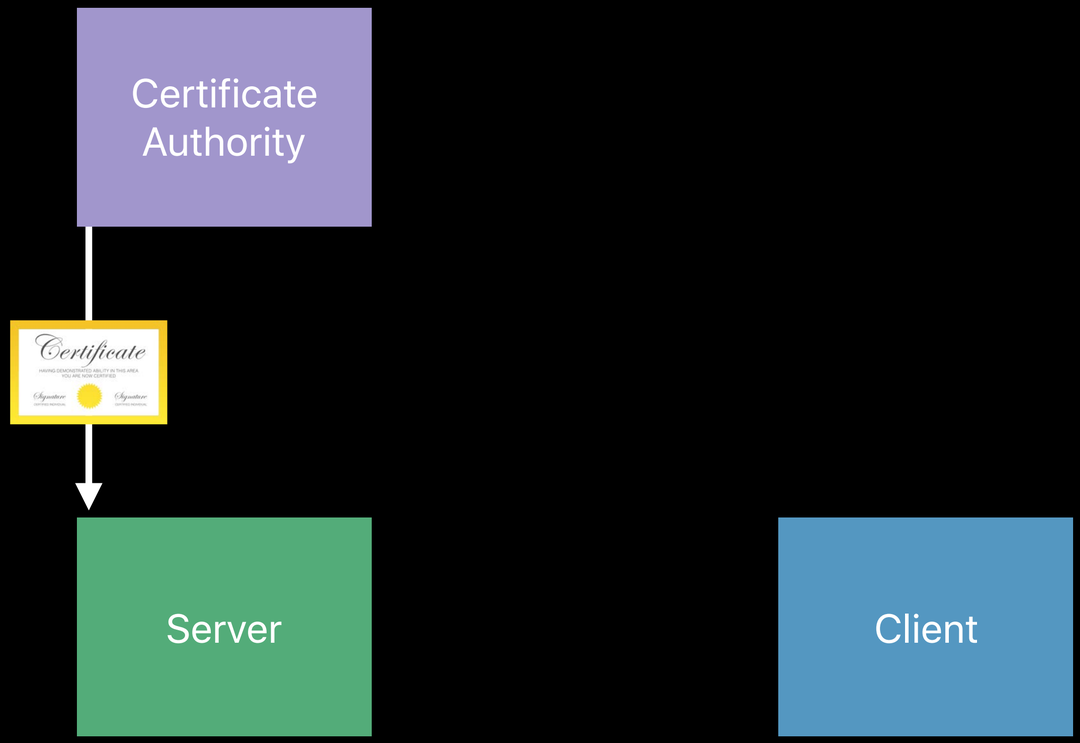
Revocation

OCSP Stapling



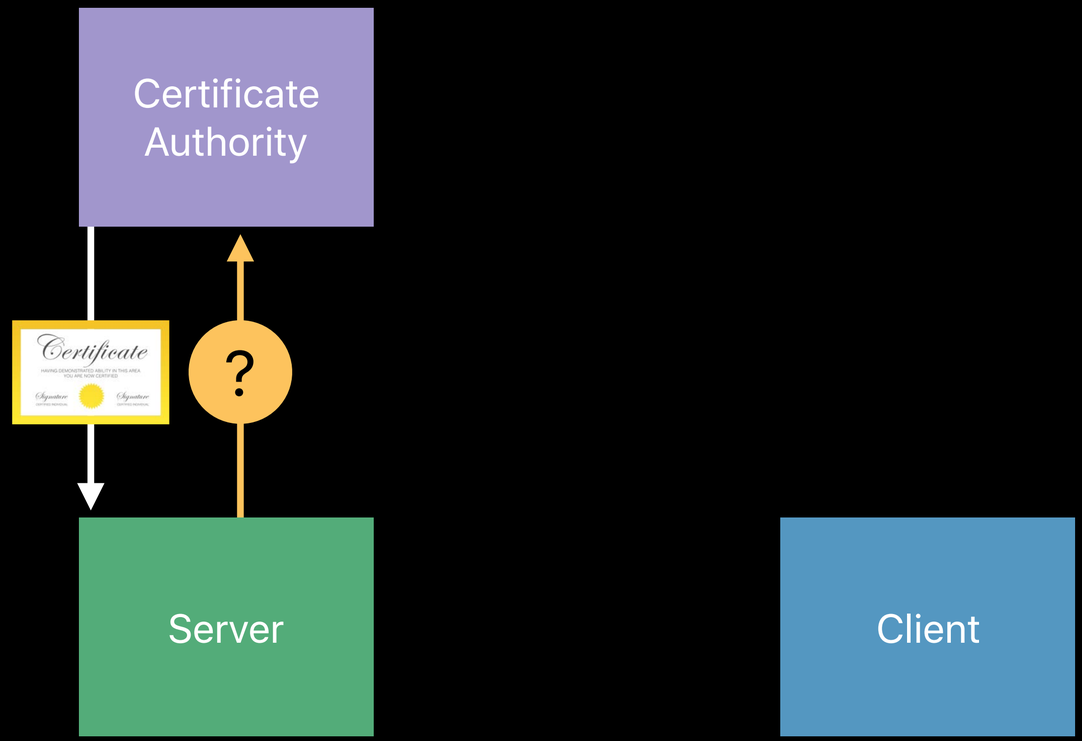
Revocation

OCSP Stapling



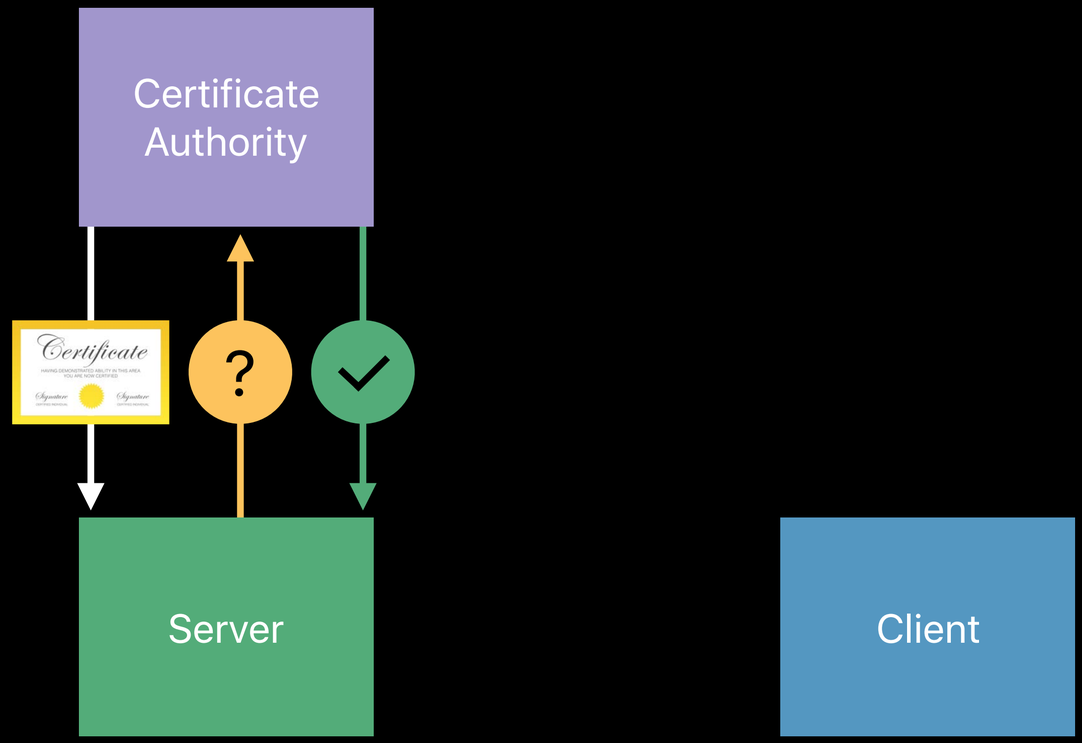
Revocation

OCSP Stapling



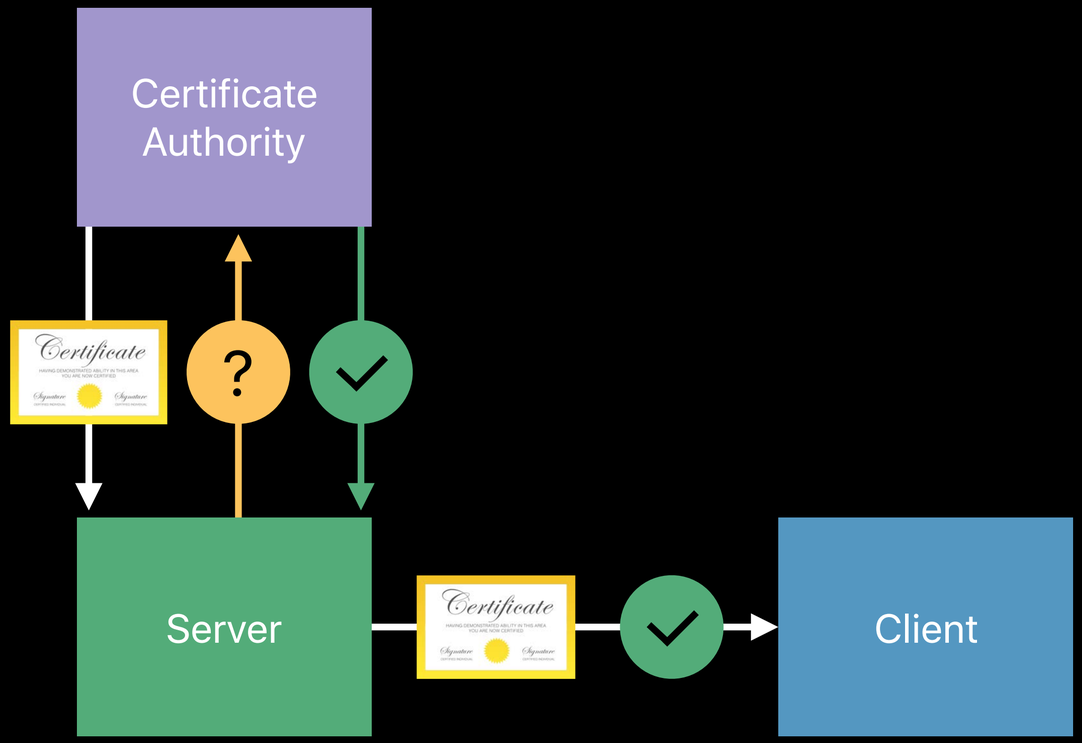
Revocation

OCSP Stapling



Revocation

OCSP Stapling



Revocation

OCSP Stapling

Revocation

OCSP Stapling

Slow adoption

Revocation

OCSP Stapling

Slow adoption

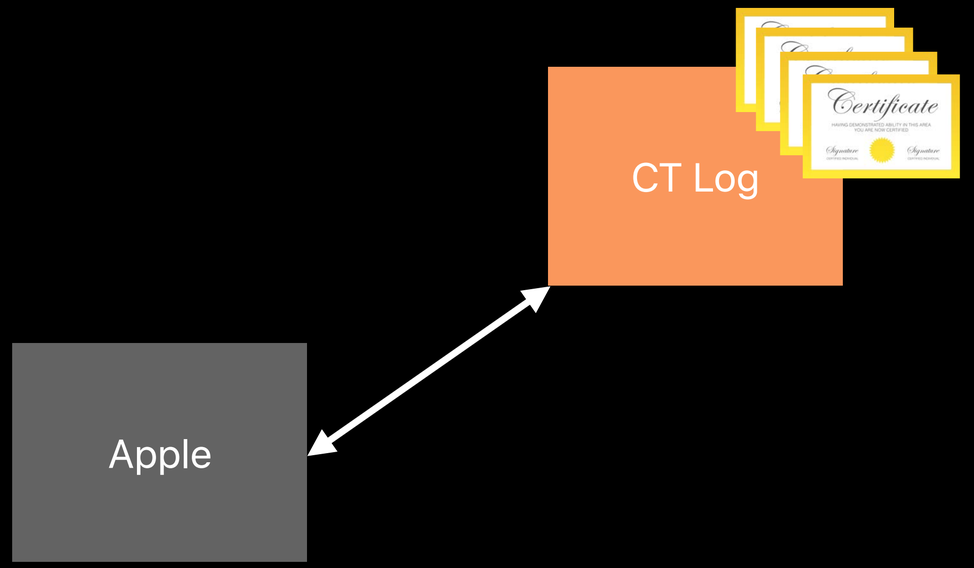
Does not protect against malicious servers

Revocation

Enhancement

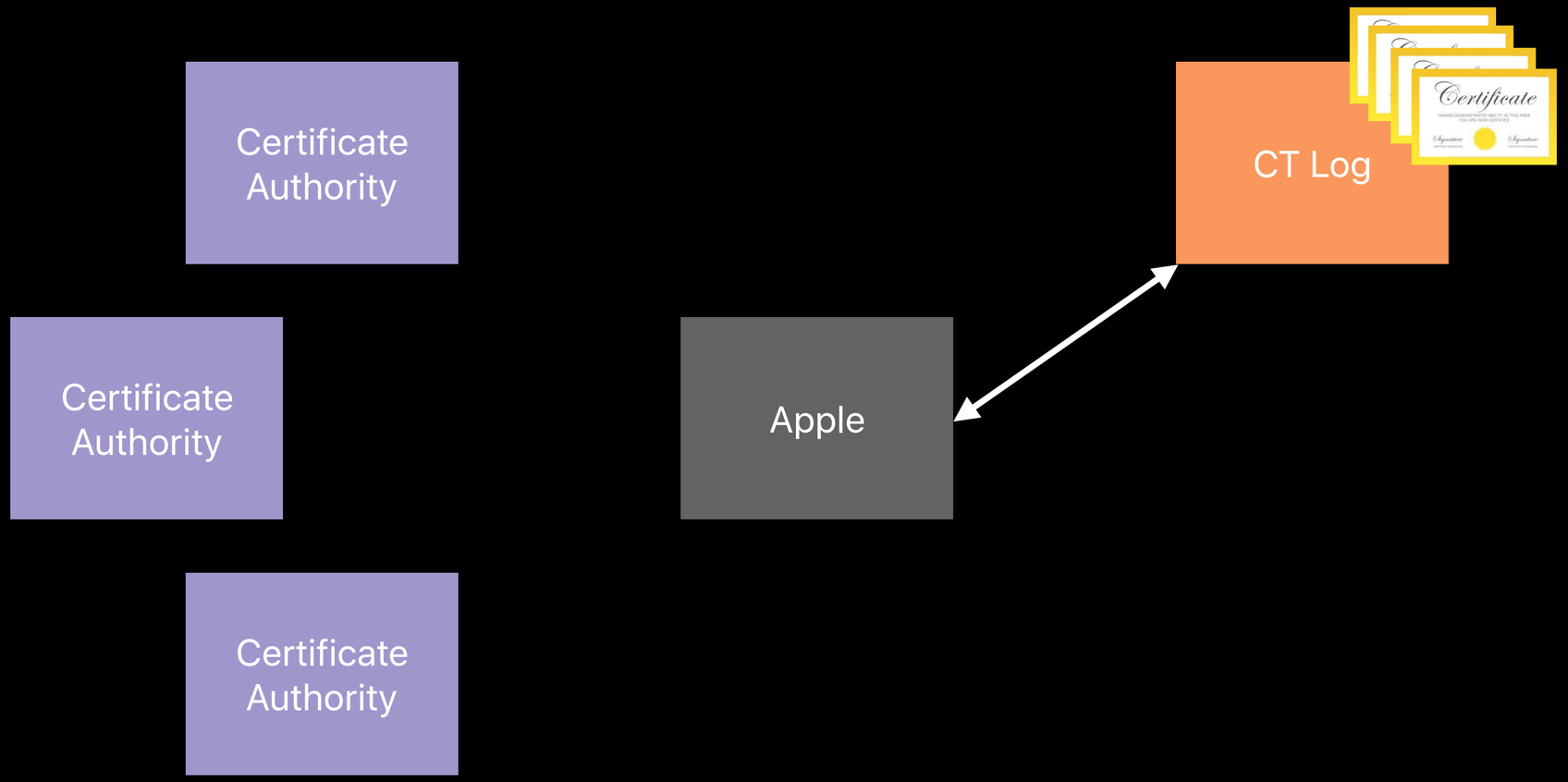
Revocation

Enhancement



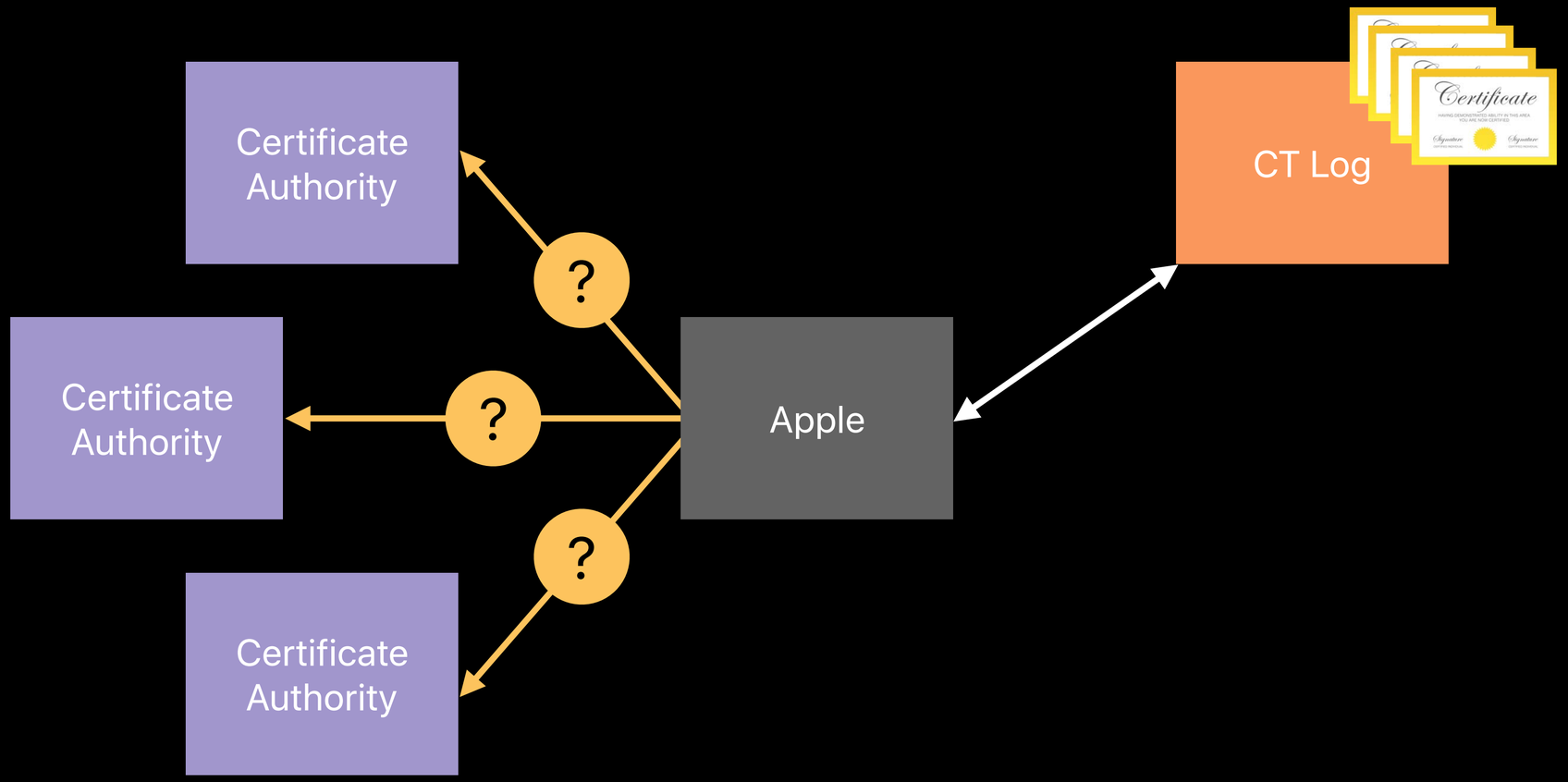
Revocation

Enhancement



Revocation

Enhancement



Revocation

Enhancement

Certificate Authority

Certificate Authority

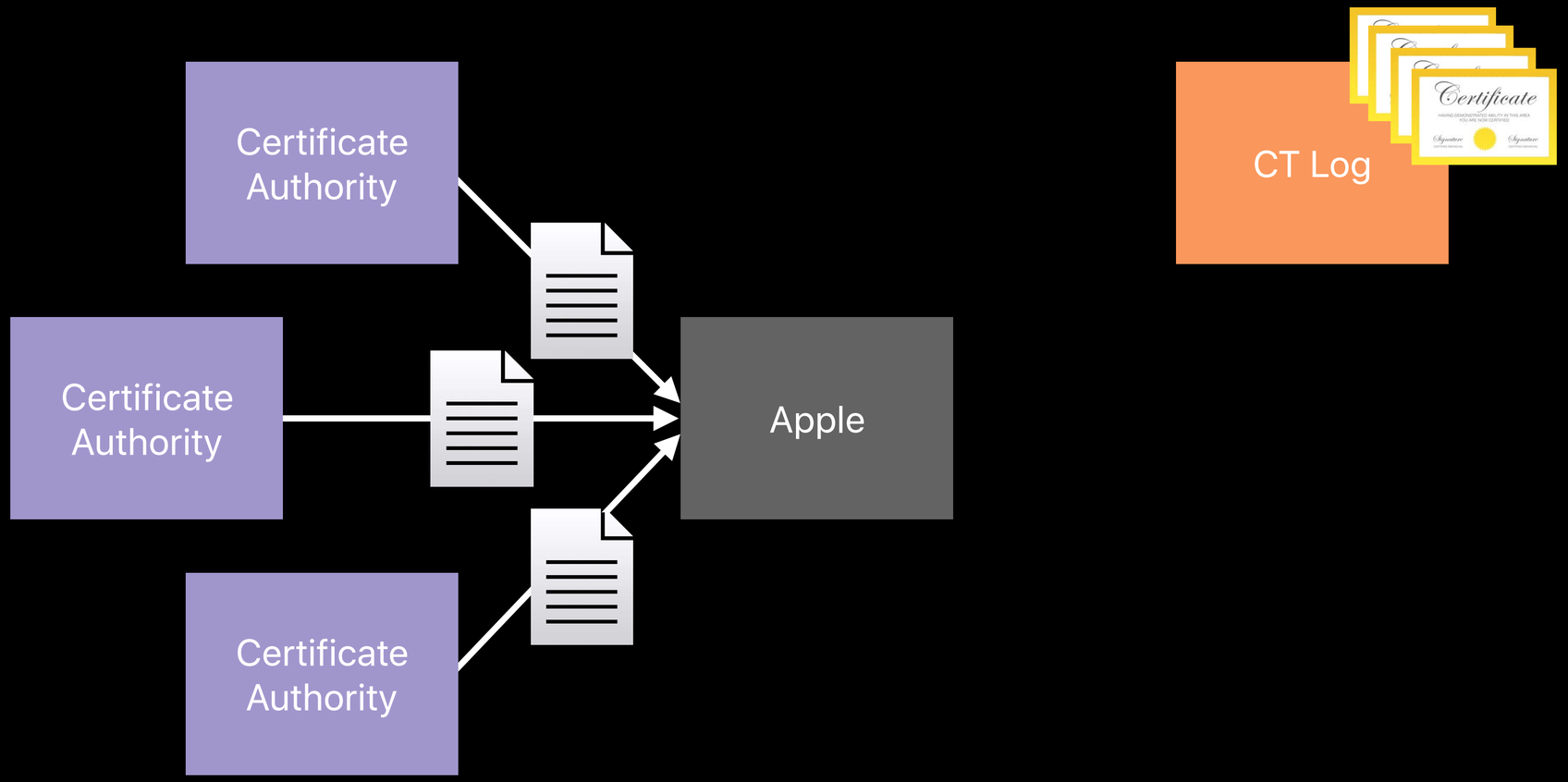
Certificate Authority

Apple

CT Log

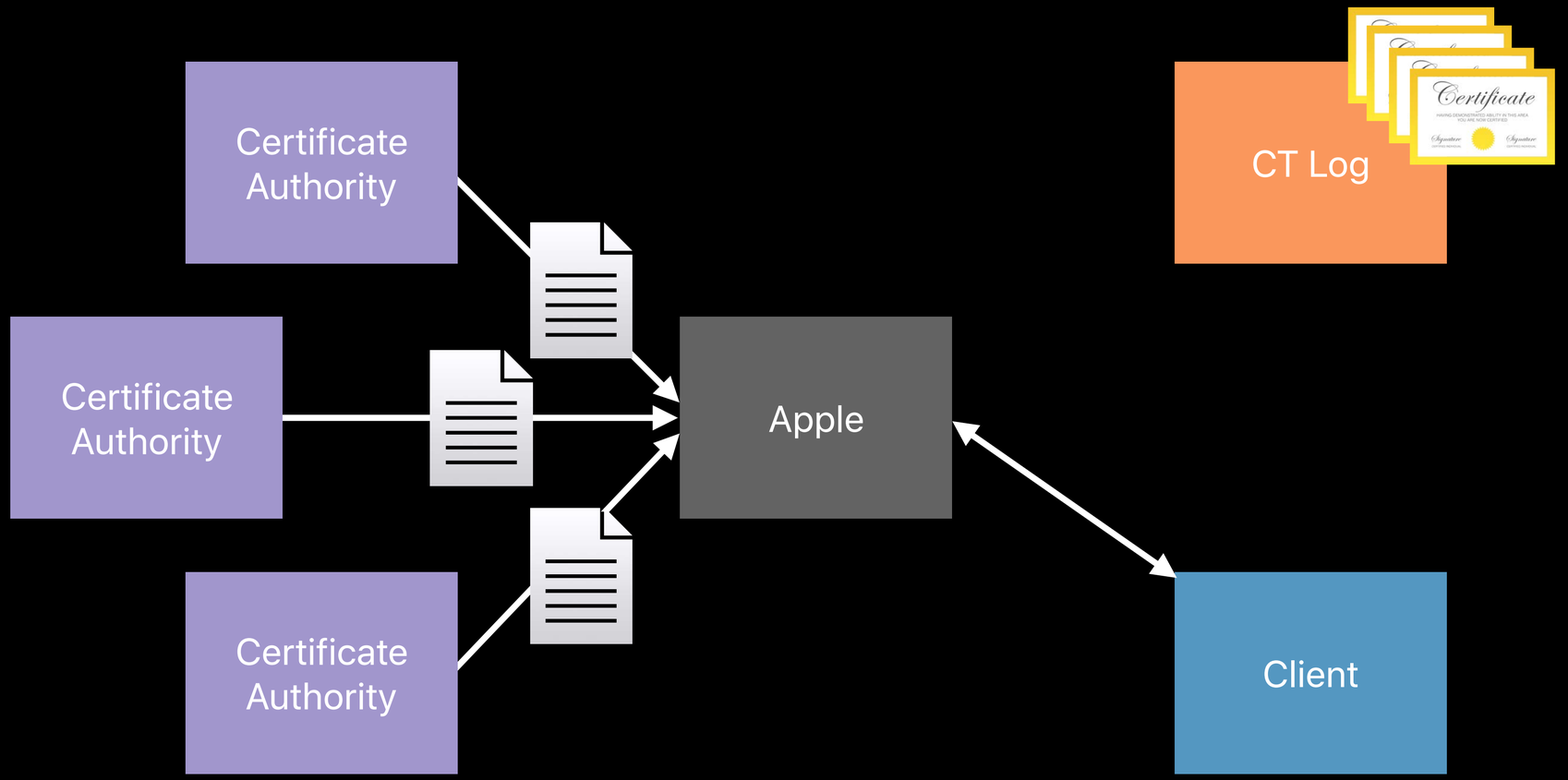
Revocation

Enhancement



Revocation

Enhancement



Revocation

Improvements

Revocation

Improvements

Reduced privacy compromise

Revocation

Improvements

Reduced privacy compromise

Automatic updating

Revocation

Improvements

Reduced privacy compromise

Automatic updating

Faster connections

Evolving Standards

Evolving Standards

Encryption	RC4, CBC modes	AES-GCM ChaCha20/Poly1305

Evolving Standards

Encryption	RC4, CBC modes	AES-GCM ChaCha20/Poly1305
Hashes	MD5, SHA-1	SHA-2 family

Evolving Standards

	✗	✓
Encryption	RC4, CBC modes	AES-GCM ChaCha20/Poly1305
Hashes	MD5, SHA-1	SHA-2 family
Public Keys	<2048-bit RSA	≥ 2048-bit RSA Elliptic curves

Evolving Standards

	✗	✓
Encryption	RC4, CBC modes	AES-GCM ChaCha20/Poly1305
Hashes	MD5, SHA-1	SHA-2 family
Public Keys	<2048-bit RSA	≥ 2048-bit RSA Elliptic curves
Protocols	http://, SSLv3, TLS 1.0, TLS 1.1	https://, TLS 1.2+

Evolving Standards

	✗	✓
Encryption	RC4, CBC modes	AES-GCM ChaCha20/Poly1305
Hashes	MD5, SHA-1	SHA-2 family
Public Keys	<2048-bit RSA	≥ 2048-bit RSA Elliptic curves
Protocols	http://, SSLv3, TLS 1.0, TLS 1.1	https://, TLS 1.2+
Revocation	No checking	Certificate Transparency OCSP Stapling

TLS Trust Removals

Trust Removals

Trust Removals

SHA-1 signed certificates for TLS

Trust Removals

SHA-1 signed certificates for TLS

Certificates using <2048-bit RSA for TLS

Trust Removals

Trust Removals

Does not affect

Trust Removals

Does not affect

- Root certificates

Trust Removals

Does not affect

- Root certificates
- Enterprise-distributed certificates

Trust Removals

Does not affect

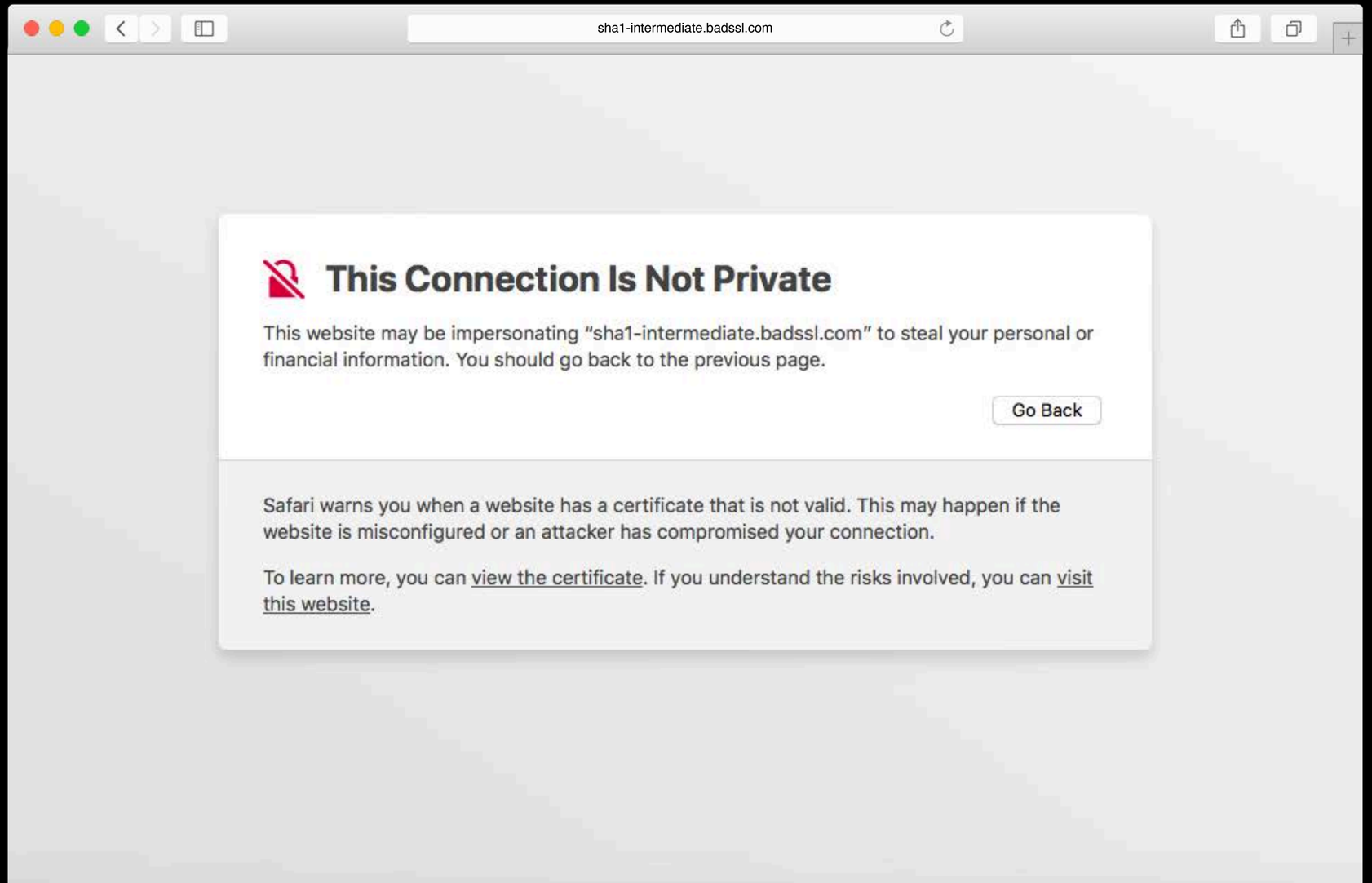
- Root certificates
- Enterprise-distributed certificates
- User-installed certificates

Trust Removals

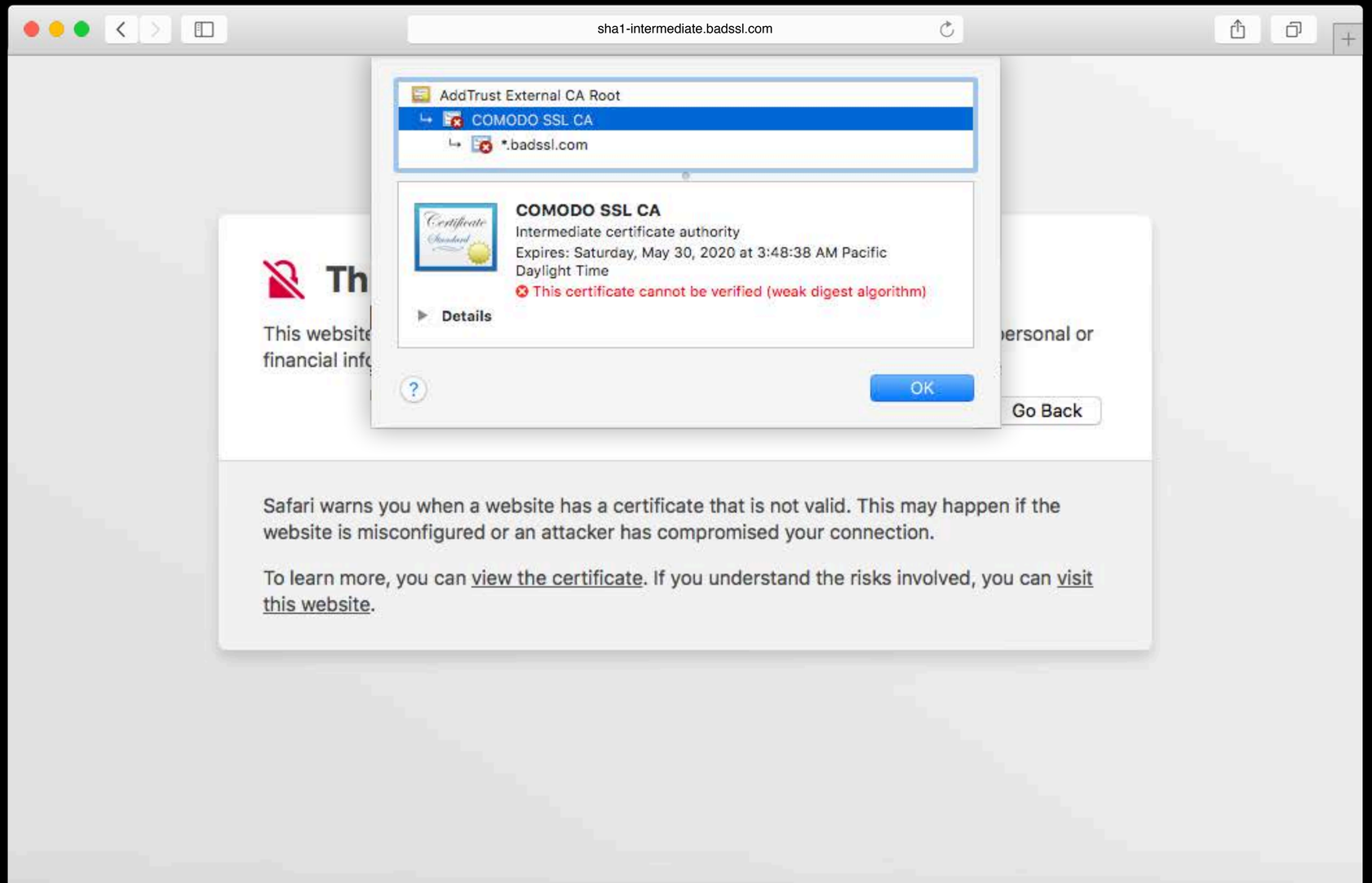
Does not affect

- Root certificates
- Enterprise-distributed certificates
- User-installed certificates
- Client certificates

Trust Removals



Trust Removals



Trust Removals

Trust Removals

InvalidCertChain (-9807) SSL errors with URLSession

Trust Removals

InvalidCertChain (-9807) SSL errors with URLSession

Servers to upgrade to new certificates

Trust Removals

InvalidCertChain (-9807) SSL errors with URLSession

Servers to upgrade to new certificates

- https://support.apple.com/kb/HT204132

What to Do Now?

What to Do Now?

Check your implementations, libraries, and servers

What to Do Now?

Check your implementations, libraries, and servers

Server Developers

What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys

What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers

What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling

What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling
- Check that your certificates are in CT logs

What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling
- Check that your certificates are in CT logs

App Developers

What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling
- Check that your certificates are in CT logs

App Developers

- Avoid ATS exceptions

App Transport Security Update

Chris Wood, Secure Transports Engineer

App Transport Security

Current standards

App Transport Security

Current standards

From HTTP to HTTPS

- TLS 1.2
- Strong cryptography—AES and SHA-2
- Forward Secrecy—ECDHE

App Transport Security

Current standards

From HTTP to HTTPS

- TLS 1.2
- Strong cryptography—AES and SHA-2
- Forward Secrecy—ECDHE

Exceptions—per-domain, narrow

Exception Updates

Exception Updates

Expansion beyond WebKit

- AVFoundation loads
- WebView requests
- Local network connections

Exception Updates

Expansion beyond WebKit

- AVFoundation loads
- WebView requests
- Local network connections

Certificate Transparency requirement

ATS-Compliant Services

Practice what you preach

APNs

FaceTime

Game Center

Apple Services

iCloud Services (Mail, CloudKit)

iWork

Spotlight

iAd

iTunes

Software Update

ATS on the Rise

ATS on the Rise

ATS adoption is increasing

ATS on the Rise

ATS adoption is increasing

Still more work to be done

ATS on the Rise

ATS adoption is increasing

Still more work to be done

Minimize or reduce exceptions

Transport Layer Security

SSL and TLS Lineage

A long road

SSL and TLS Lineage

A long road

TLS 1.0

1999

SSL and TLS Lineage

A long road

TLS 1.0 — 1999

TLS 1.1 — 2006

SSL and TLS Lineage

A long road

TLS 1.0 — 1999

TLS 1.1 — 2006

TLS 1.2 — 2008

SSL and TLS Lineage

A long road

TLS 1.0 — 1999

TLS 1.1 — 2006

TLS 1.2 — 2008

TLS 1.3 (draft) — 2017

TLS 1.3

Best practice by design

TLS 1.3

Best practice by design

Strong cryptography and Forward Secrecy by default

- Legacy options, ciphers, and key exchange algorithms removed

TLS 1.3

Best practice by design

Strong cryptography and Forward Secrecy by default

- Legacy options, ciphers, and key exchange algorithms removed

Overall simpler specification

TLS 1.3

Best practice by design

Strong cryptography and Forward Secrecy by default

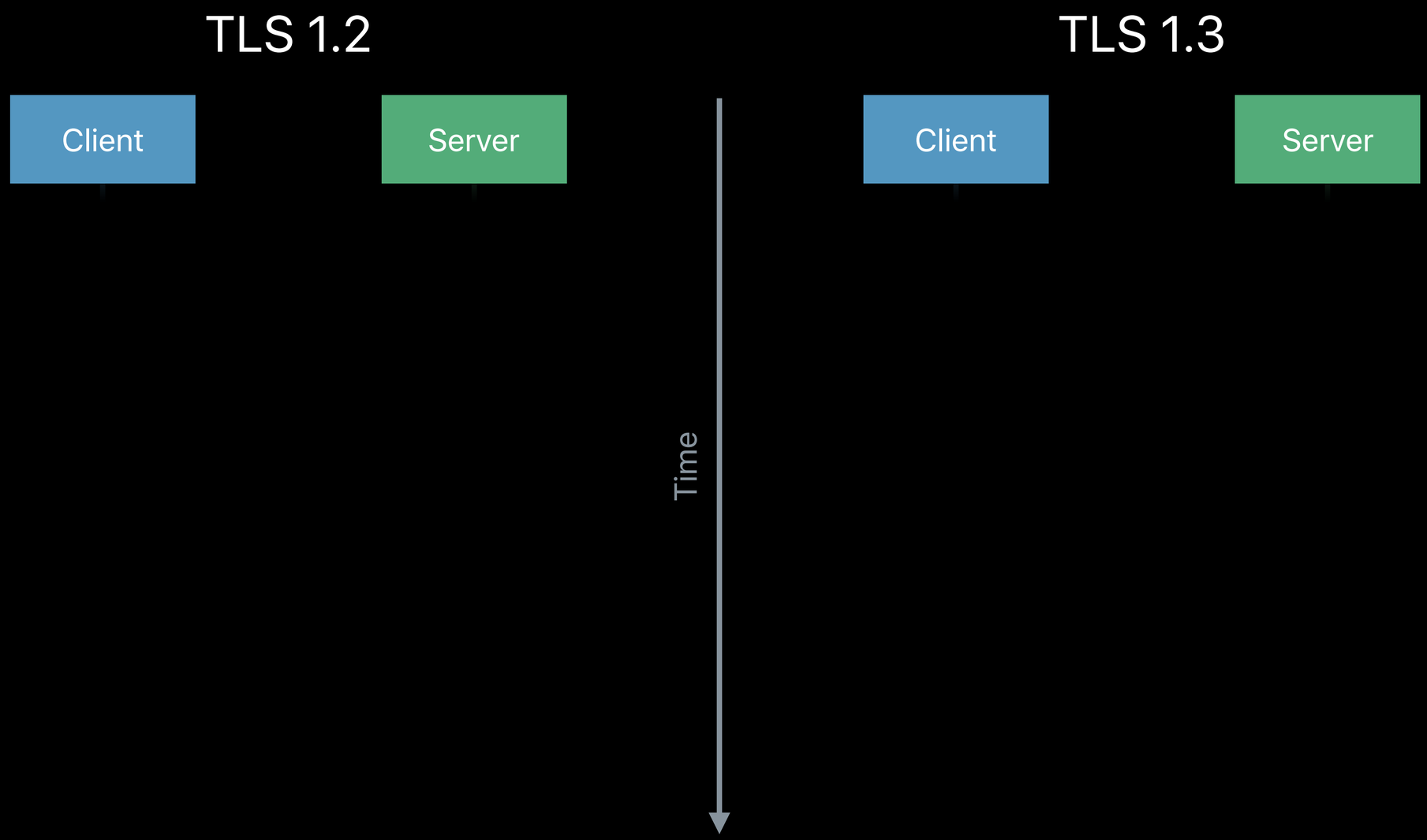
- Legacy options, ciphers, and key exchange algorithms removed

Overall simpler specification

Improved network efficiency

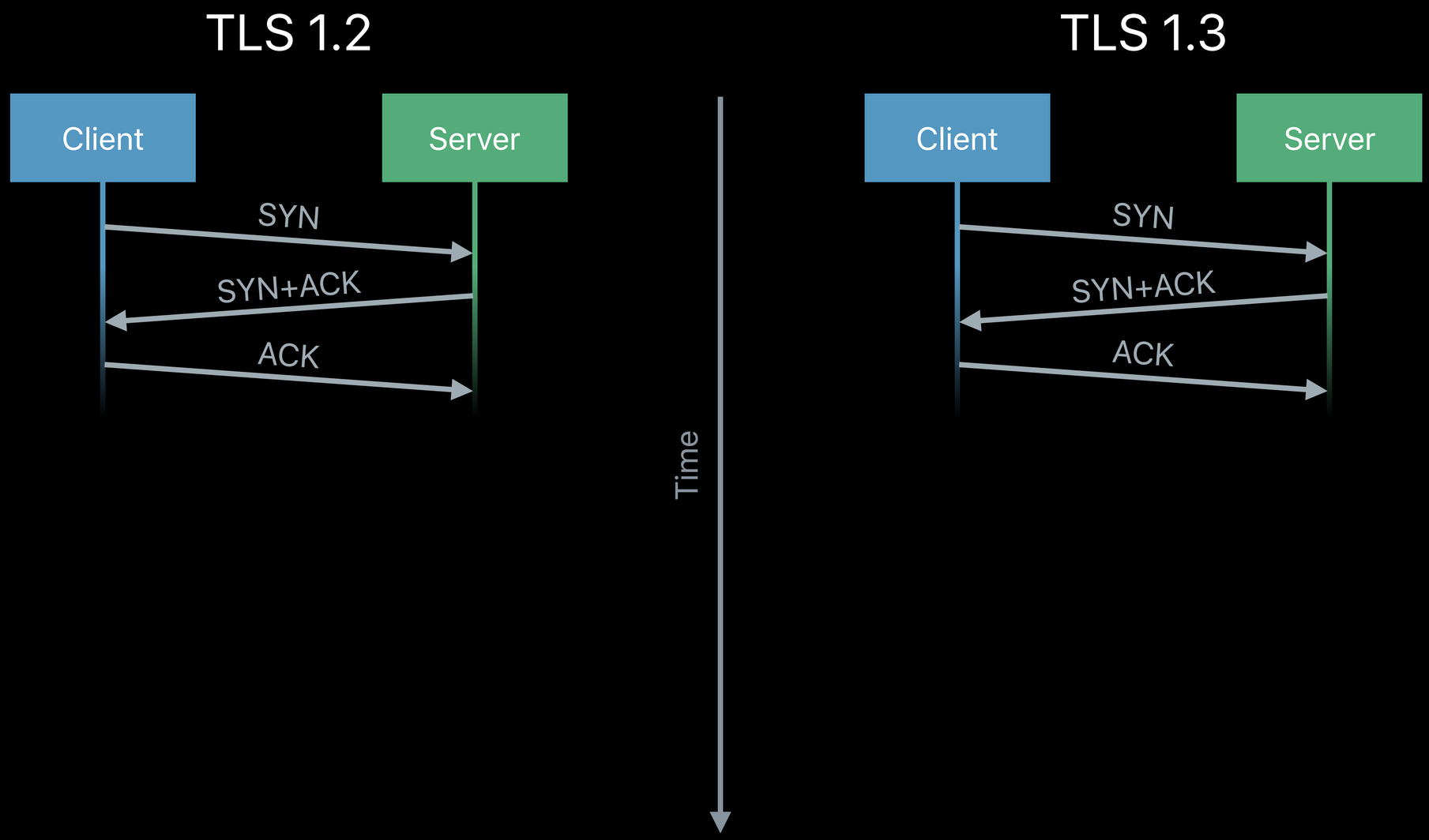
TLS 1.3 Overview

Improved efficiency



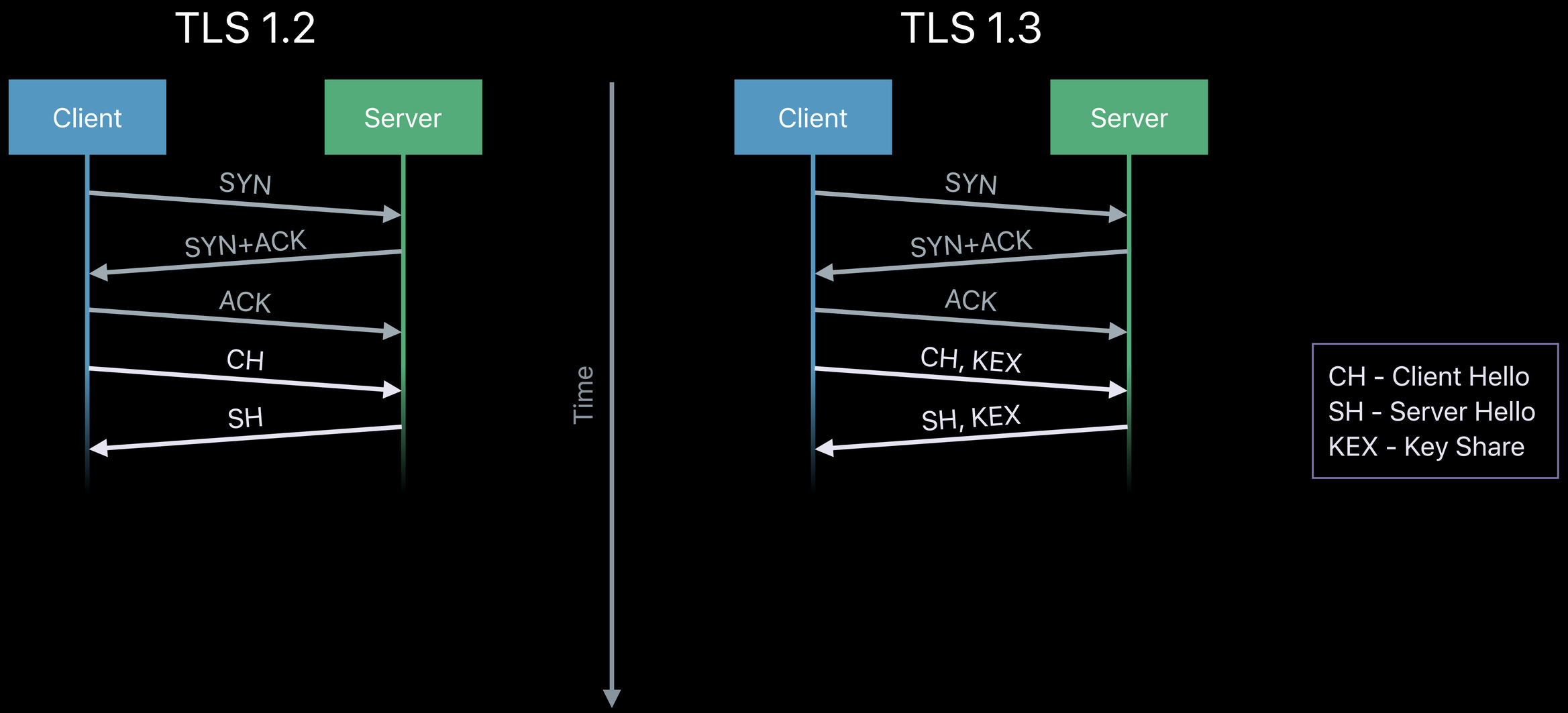
TLS 1.3 Overview

Improved efficiency



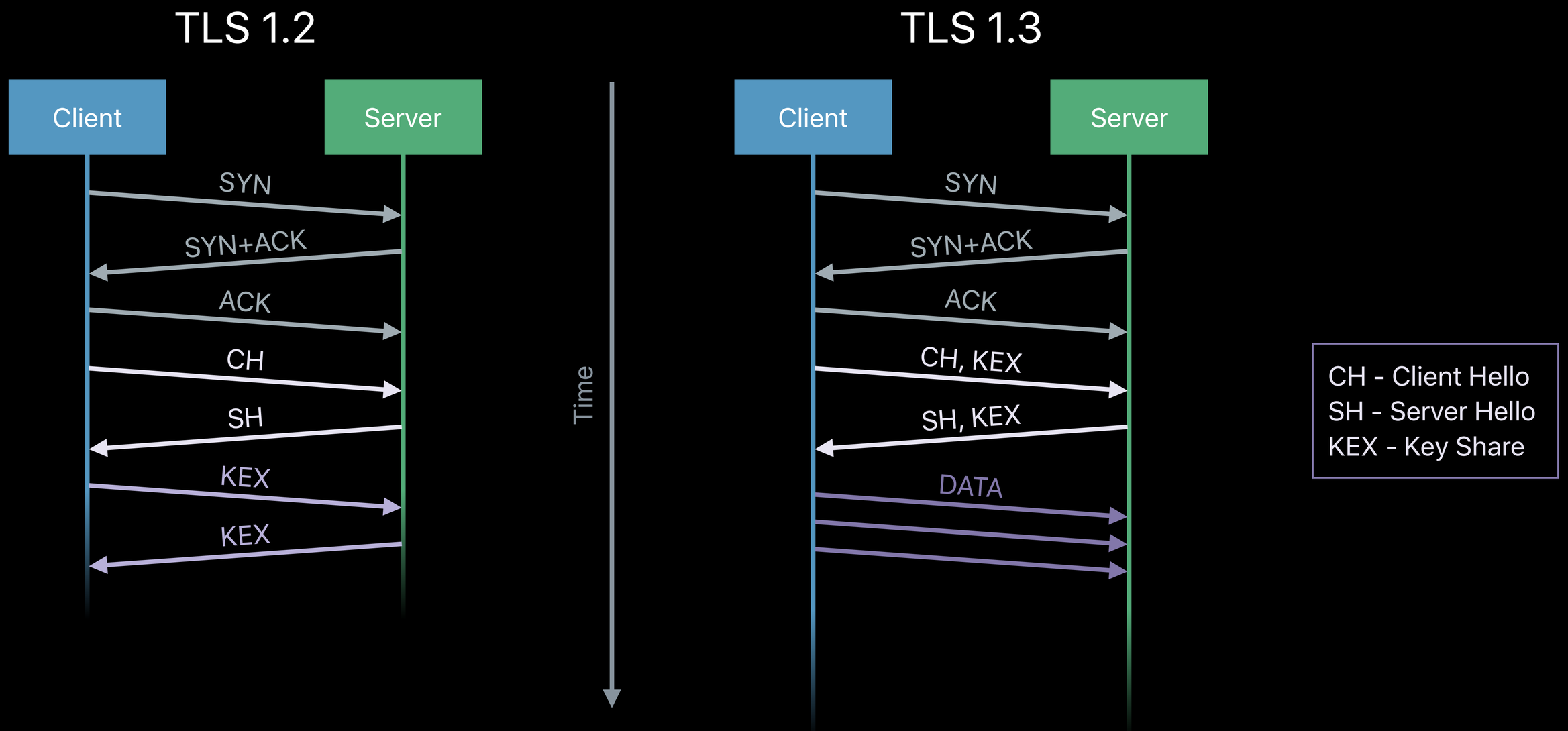
TLS 1.3 Overview

Improved efficiency



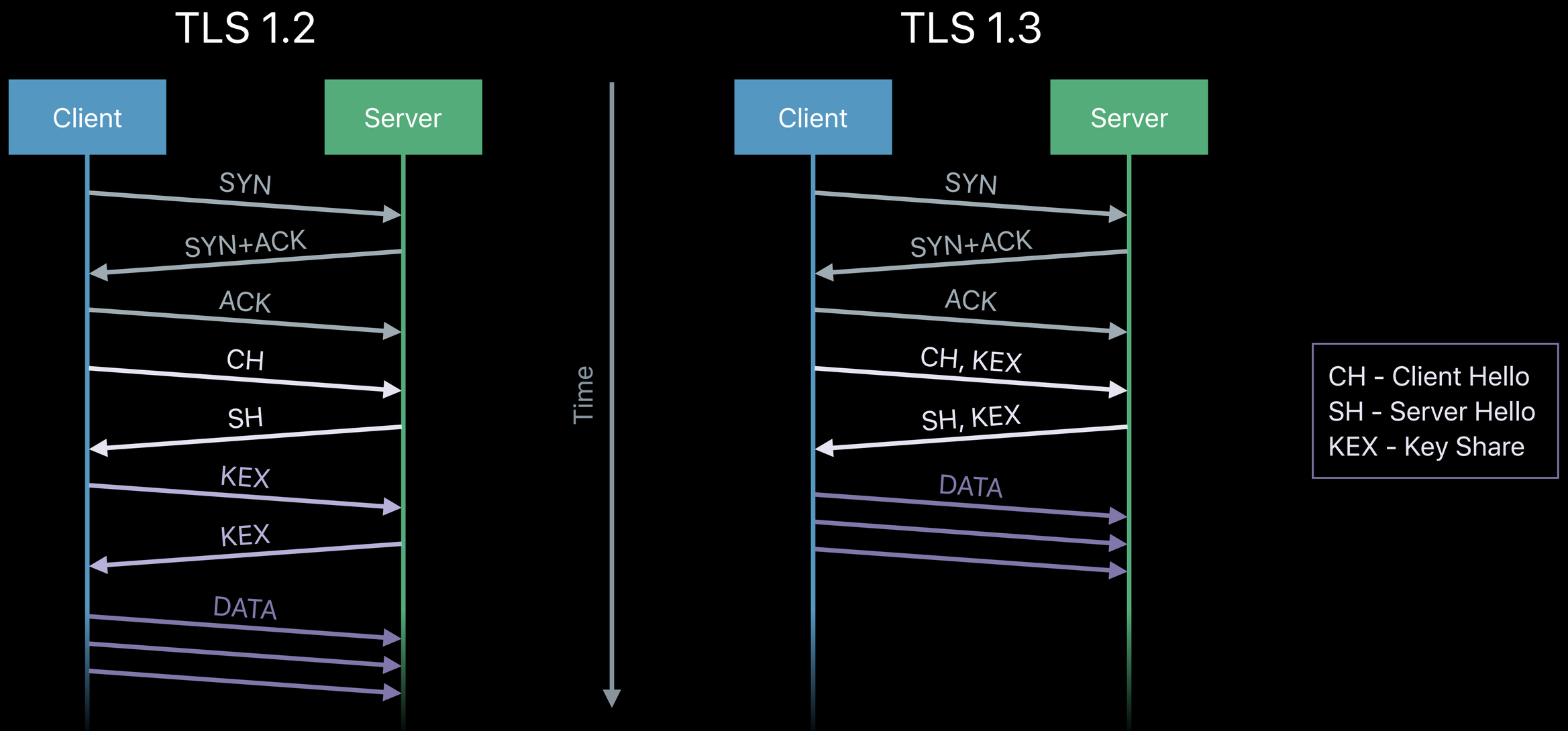
TLS 1.3 Overview

Improved efficiency



TLS 1.3 Overview

Improved efficiency



How to Enable TLS 1.3 Beta?

How to Enable TLS 1.3 Beta?

It is not on by default

How to Enable TLS 1.3 Beta?

It is not on by default

You can install a profile on iOS
https://developer.apple.com/go/?id=tls13-mobile-profile

How to Enable TLS 1.3 Beta?

It is not on by default

You can install a profile on iOS
https://developer.apple.com/go/?id=tls13-mobile-profile

You can enable system-wide TLS 1.3 on macOS

```
defaults write /Library/Preferences/com.apple.networkd tcp_connect_enable_tls13 1
```

TLS 1.3 Outlook

TLS 1.3 Outlook

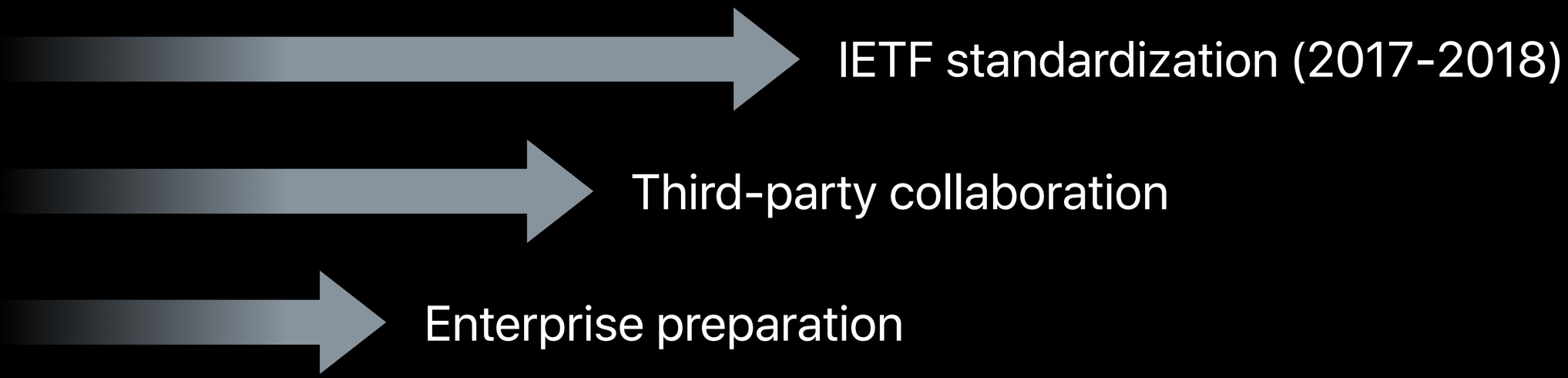
IETF standardization (2017-2018)

TLS 1.3 Outlook

IETF standardization (2017-2018)

Third-party collaboration

TLS 1.3 Outlook



Takeaways

Takeaways

Implement best practices

Takeaways

Implement best practices

Avoid new and future algorithm removals

Takeaways

Implement best practices

Avoid new and future algorithm removals

Continue upgrading to modern TLS configurations

Takeaways

Implement best practices

Avoid new and future algorithm removals

Continue upgrading to modern TLS configurations

- Minimize or remove App Transport Security exceptions

Takeaways

Implement best practices

Avoid new and future algorithm removals

Continue upgrading to modern TLS configurations

- Minimize or remove App Transport Security exceptions
- Try out TLS 1.3

More Information

https://developer.apple.com/wwdc17/701

Related Sessions

Privacy and Your Apps	Executive Ballroom	Tuesday 11:20AM
Advances in Networking, Part 1	Executive Ballroom	Wednesday 3:10PM
Advances in Networking, Part 2	Executive Ballroom	Wednesday 4:10PM

Labs

Security & Privacy	Technology Lab D	Tue 1:50PM-3:50PM
Security & Privacy	Technology Lab J	Wed 1:00PM-3:30PM
Networking Lab	Technology Lab D	Thu 9:00AM-11:00AM
Networking Lab	Technology Lab J	Fri 1:50PM-3:50PM


WWDC17