



TLS 1.3

Nick Sullivan
@grittygrease

Filippo Valsorda
@FiloSottile



1994 – SSLv2

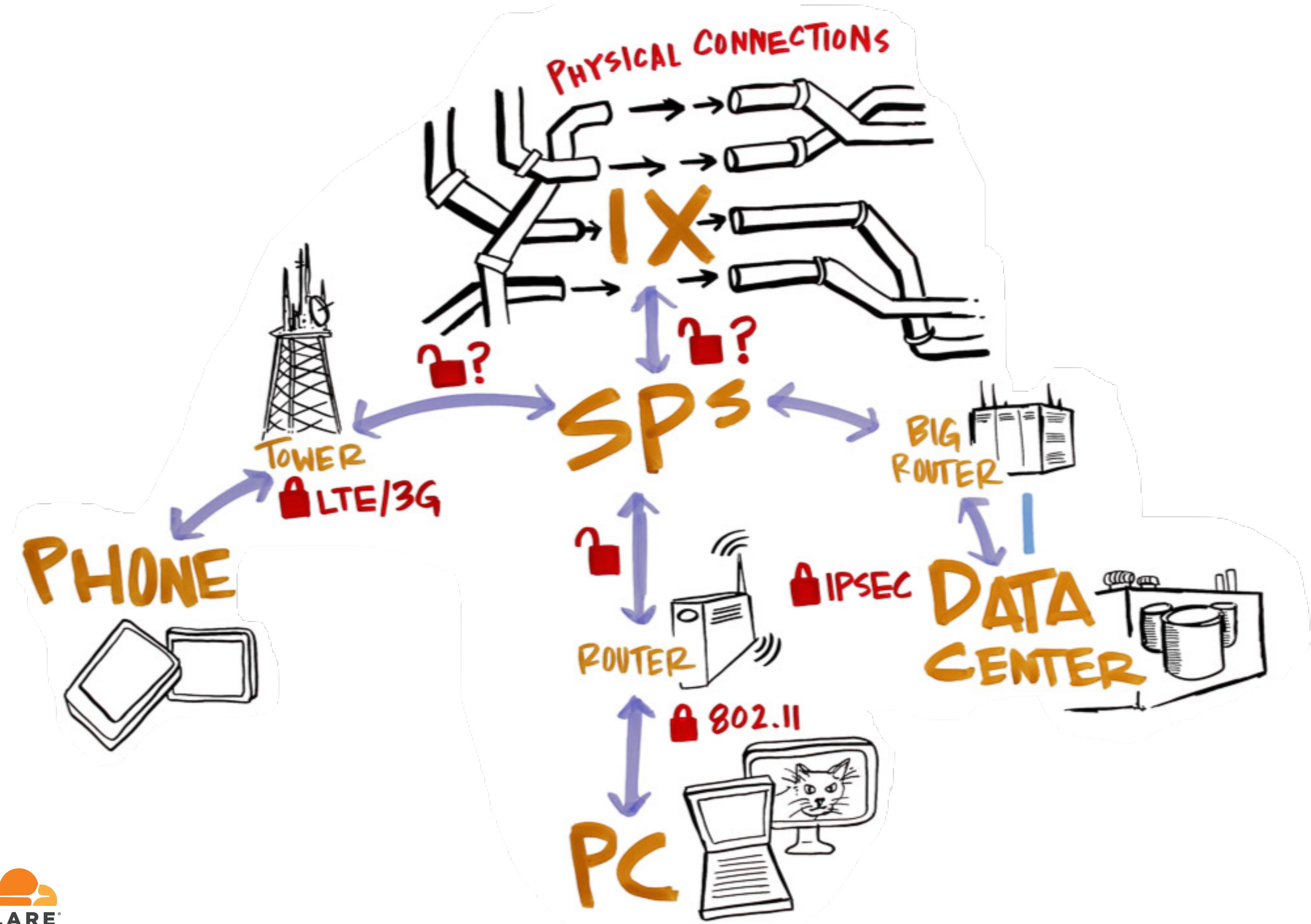
1995 – SSLv3

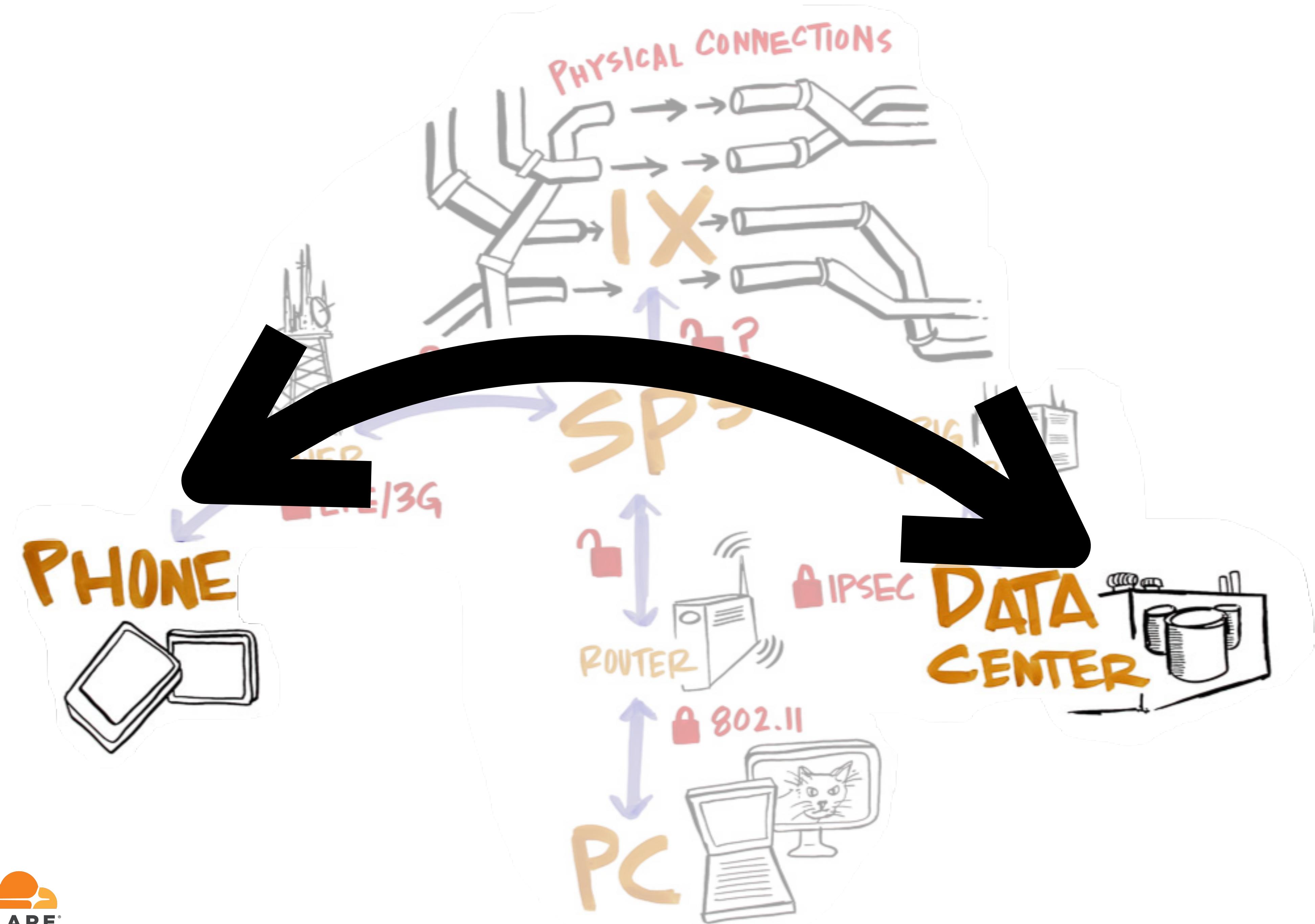
1999 – TLS 1.0

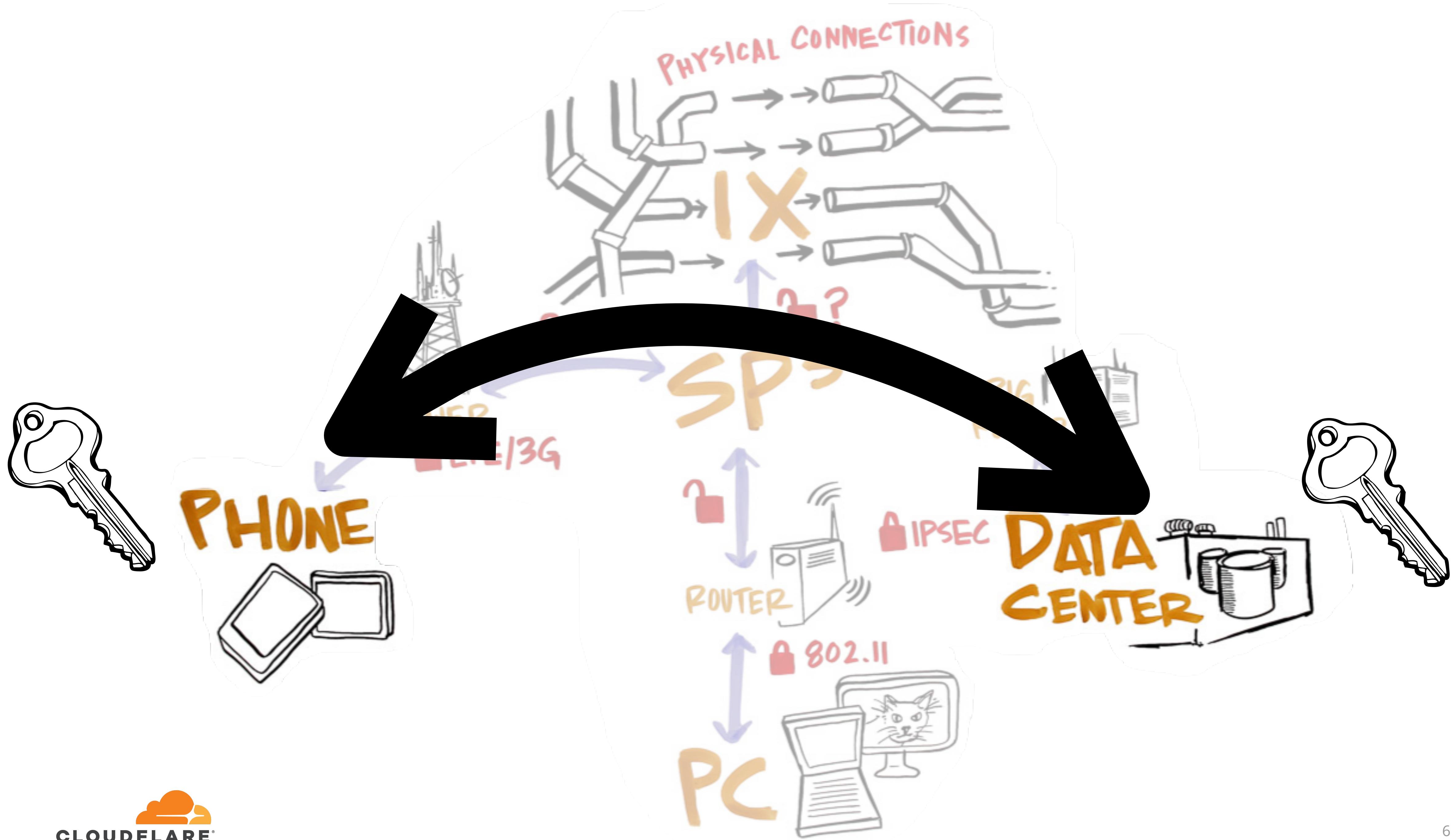
2006 – TLS 1.1

2008 – TLS 1.2

...



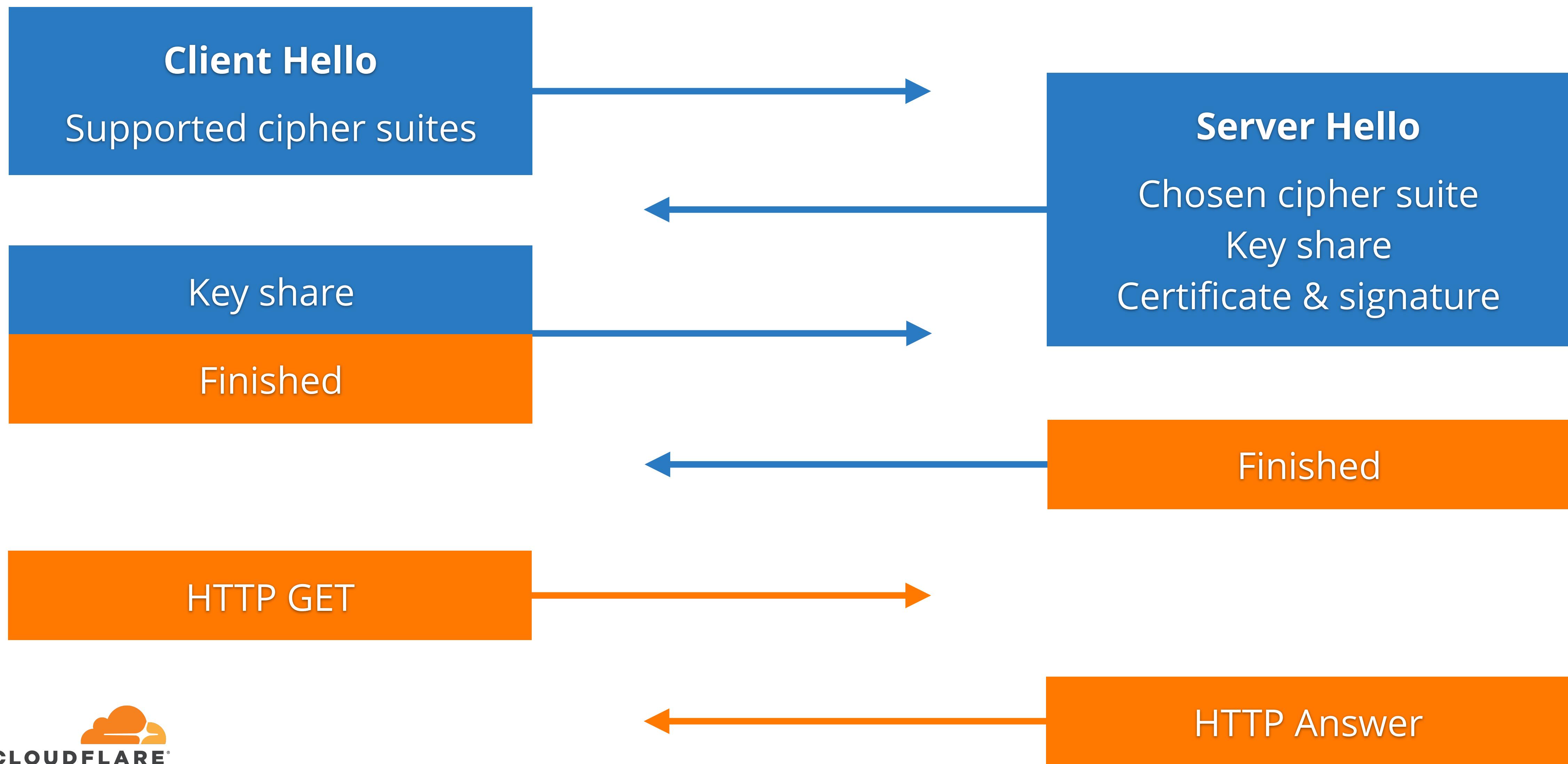




TLS 1.2 ECDHE

Client

Server



TLS 1.2 ECDHE

Time	Source	Destin	Protocol	Length	Info
1051.721834	10.1...	104...	TLSv1.2	251	Client Hello
1051.747907	104...	10...	TLSv1.2	1404	Server Hello
1051.747993	104...	10...	TLSv1.2	811	Certificate Certificate Status, Server Key Exchange, Server Hello Done
1051.749915	10.1...	104...	TLSv1.2	170	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
1051.774692	104...	10...	TLSv1.2	302	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1051.774846	104...	10...	TLSv1.2	113	Application Data
1052.104322	10.1...	104...	TLSv1.2	97	Application Data
1052.104447	10.1...	104...	TLSv1.2	100	Application Data
1052.104574	10.1...	104...	TLSv1.2	86	Application Data
1052.104984	10.1...	104...	TLSv1.2	82	Application Data
1052.105458	10.1...	104...	TLSv1.2	540	Application Data
1052.128825	104...	10...	TLSv1.2	82	Application Data
1052.132494	104...	10...	TLSv1.2	449	Application Data
1052.132561	104...	10...	TLSv1.2	82	Application Data

TLS 1.0, 1.1 and 1.2 are not that different

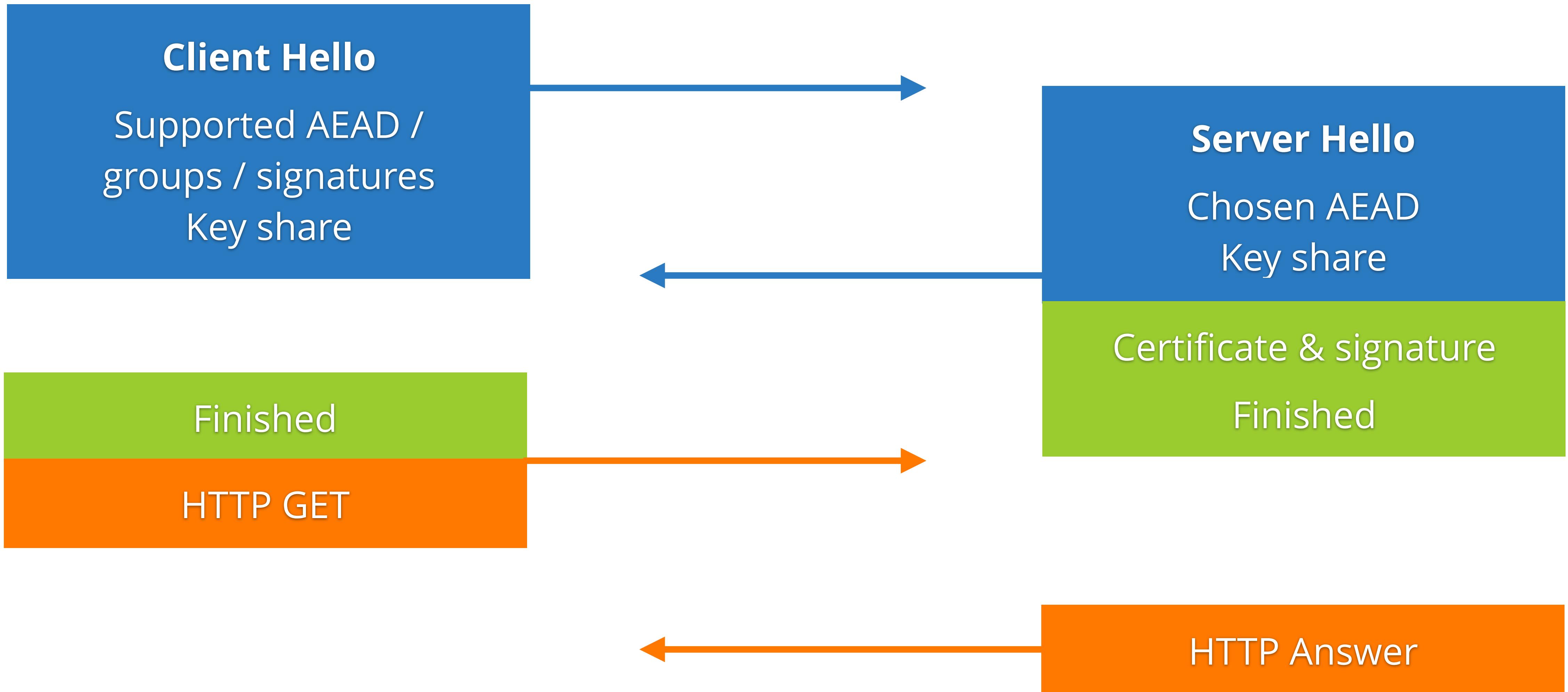
TLS 1.3 is a BIG jump

RTT - - ;

TLS 1.3

Client

Server



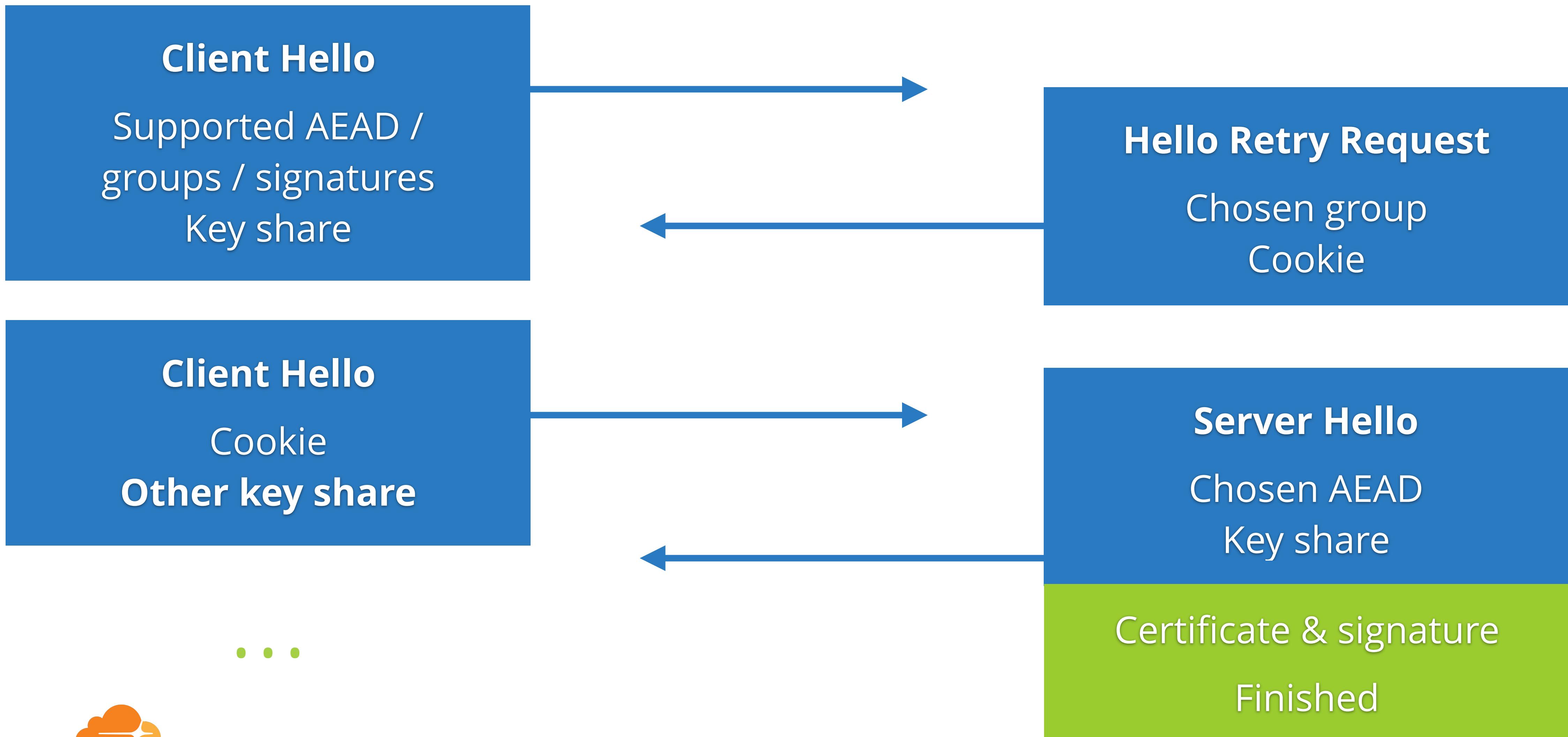
TLS 1.3

Time	Source	Destin	Protocol	Length	Info
3.819792	10.1...	104...	TLSv1.3	561	Client Hello
3.848558	104...	10...	TLSv1.3	1404	Server Hello, Application Data
3.849548	104...	10...	TLSv1.3	580	Application DataApplication Data, Application Data
3.849608	104...	10...	TLSv1.3	93	Application Data
3.851004	10.1...	104...	TLSv1.3	102	Application Data
3.875635	104...	10...	TLSv1.3	221	Application Data

Client

Hello Retry Request

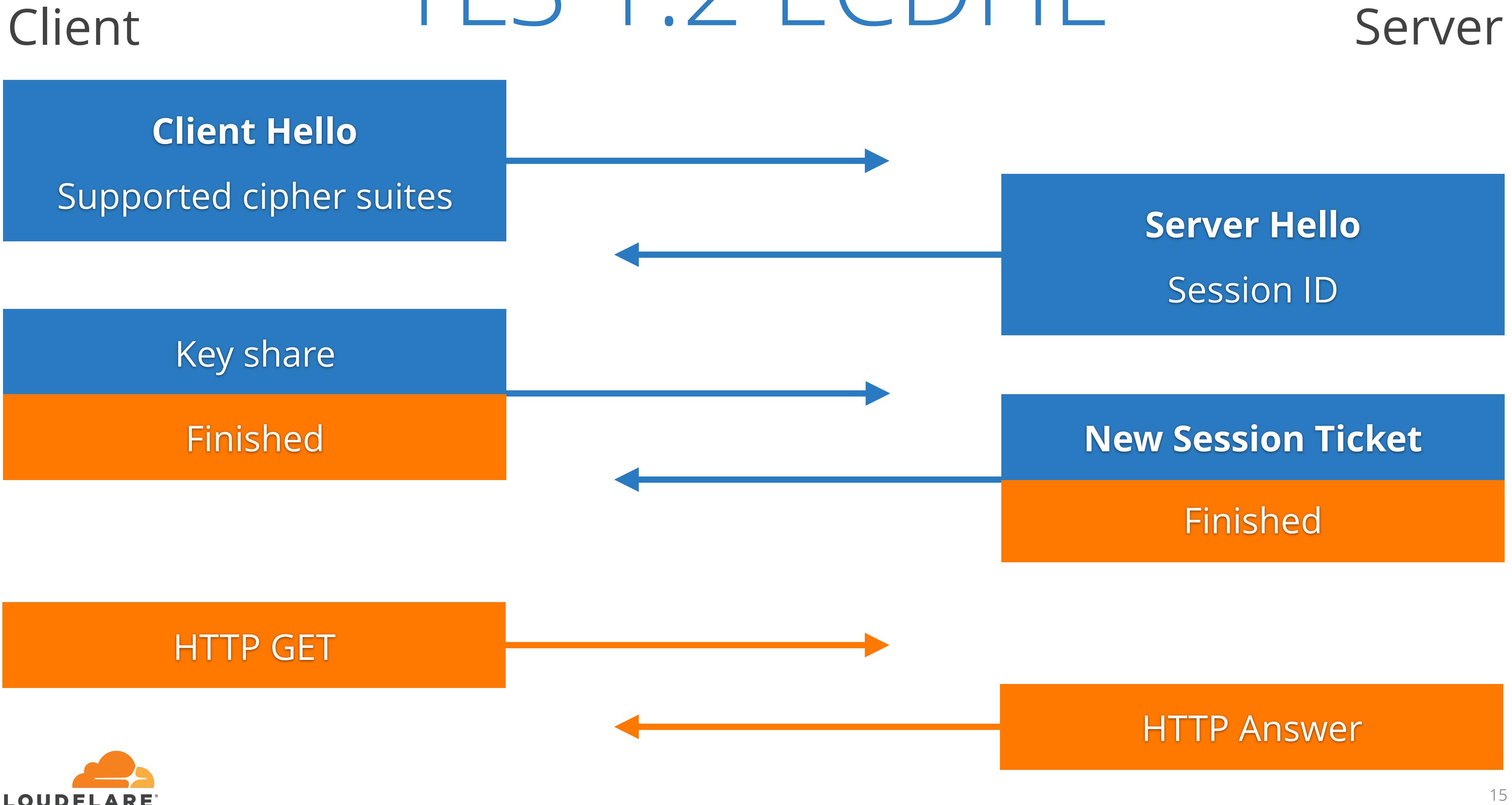
Server



Resumption

“Hey, I know you!”

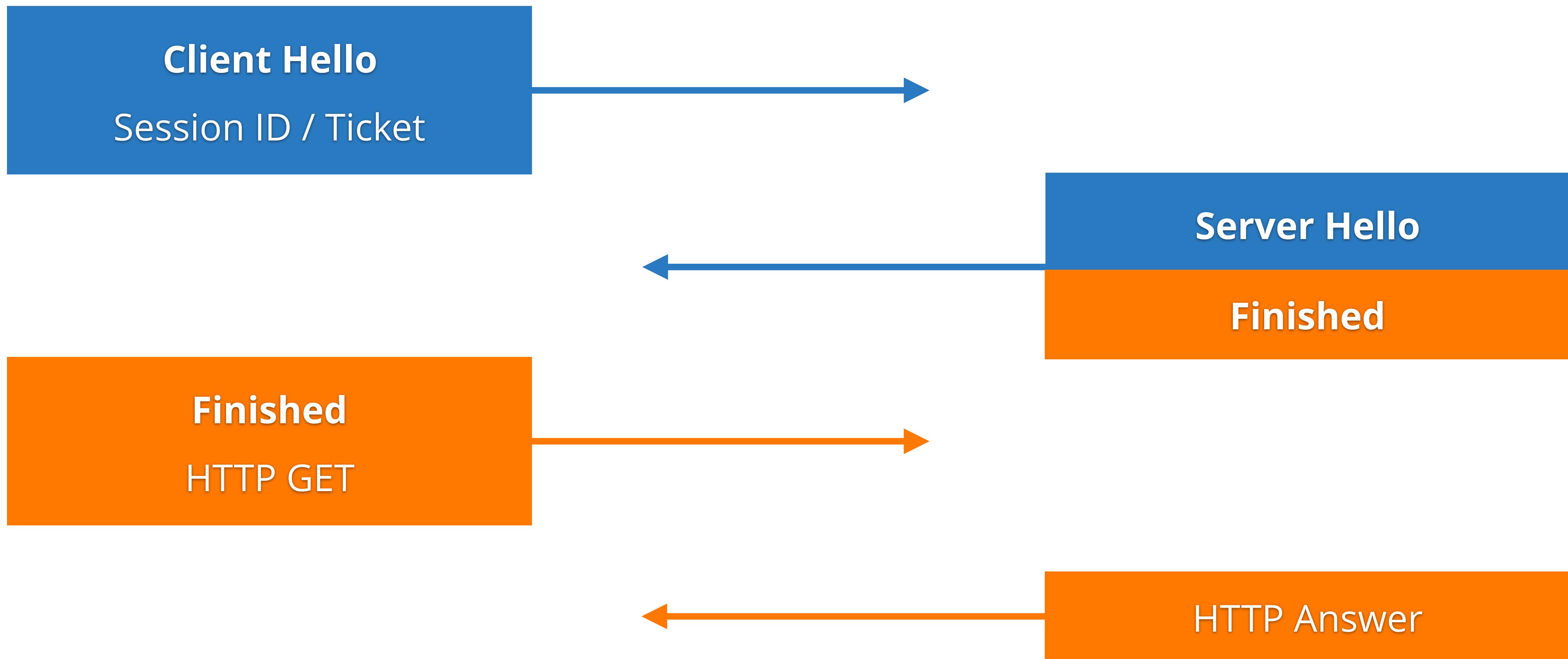
TLS 1.2 ECDHE



TLS 1.2 Resumption

Client

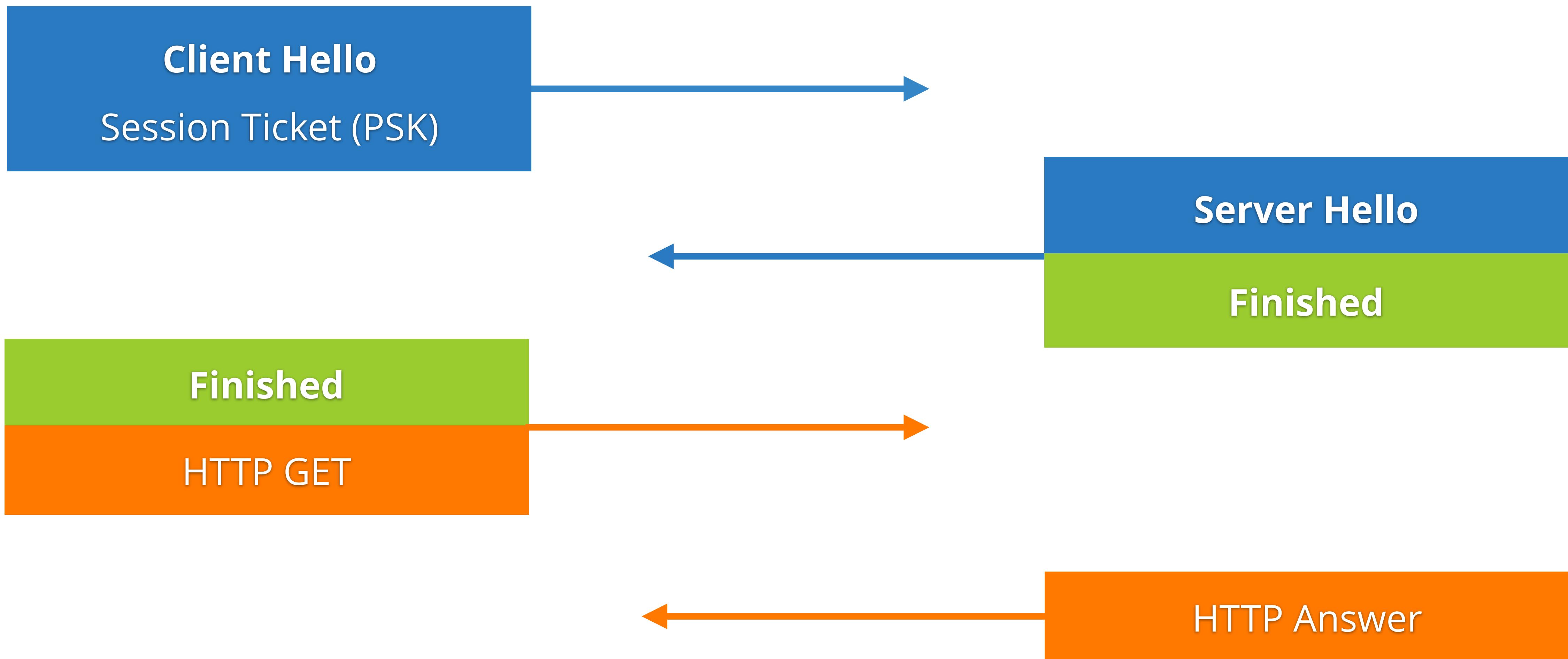
Server



TLS 1.3 Resumption

Client

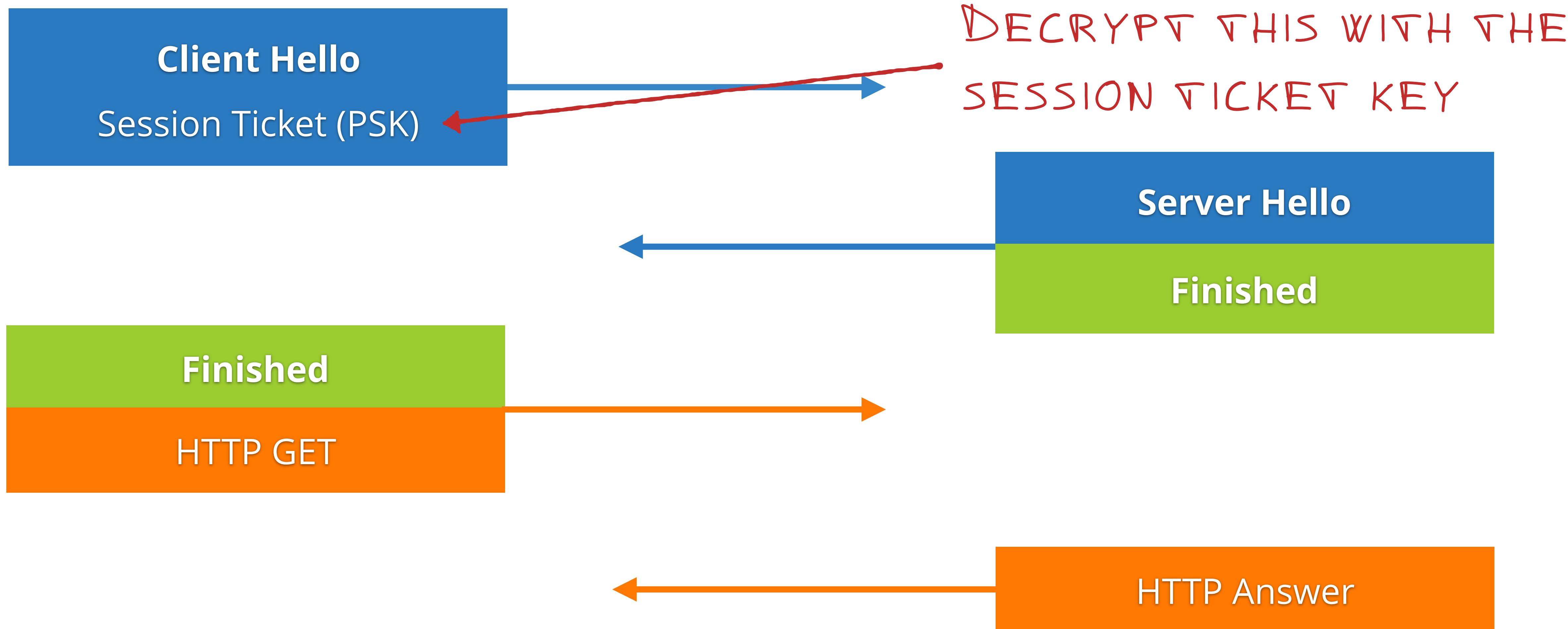
Server



Forward Secrecy

Client

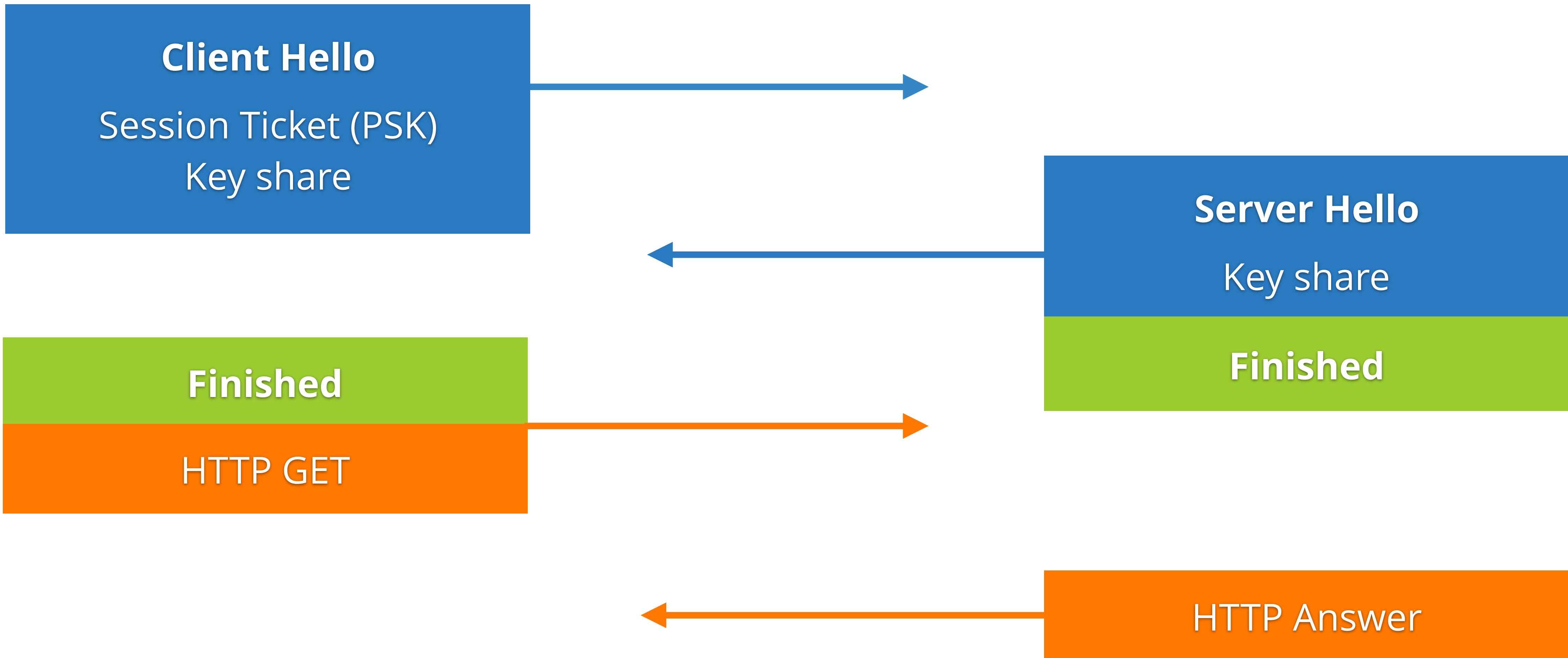
Server



PSK-ECDHE

Client

Server

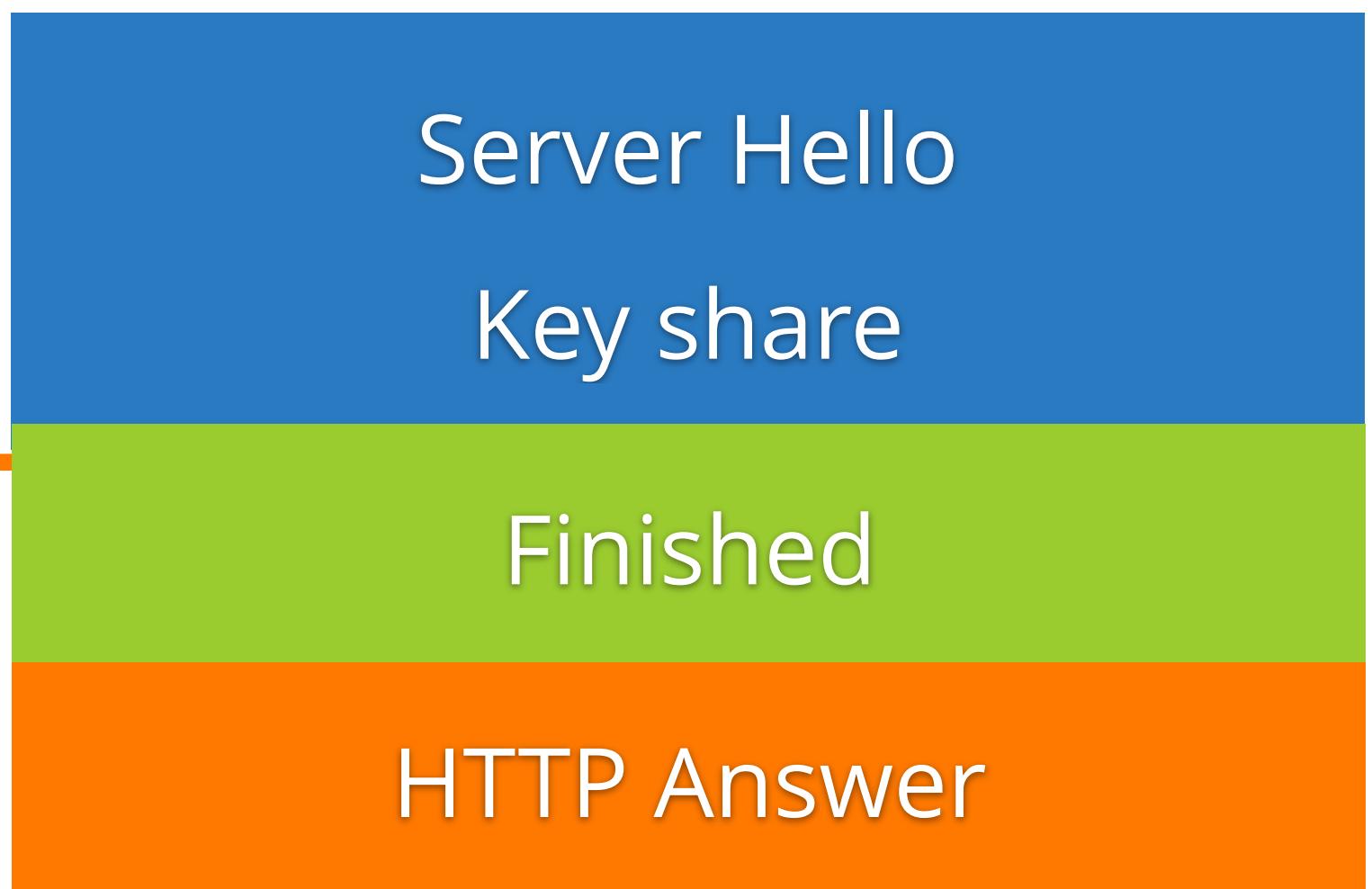
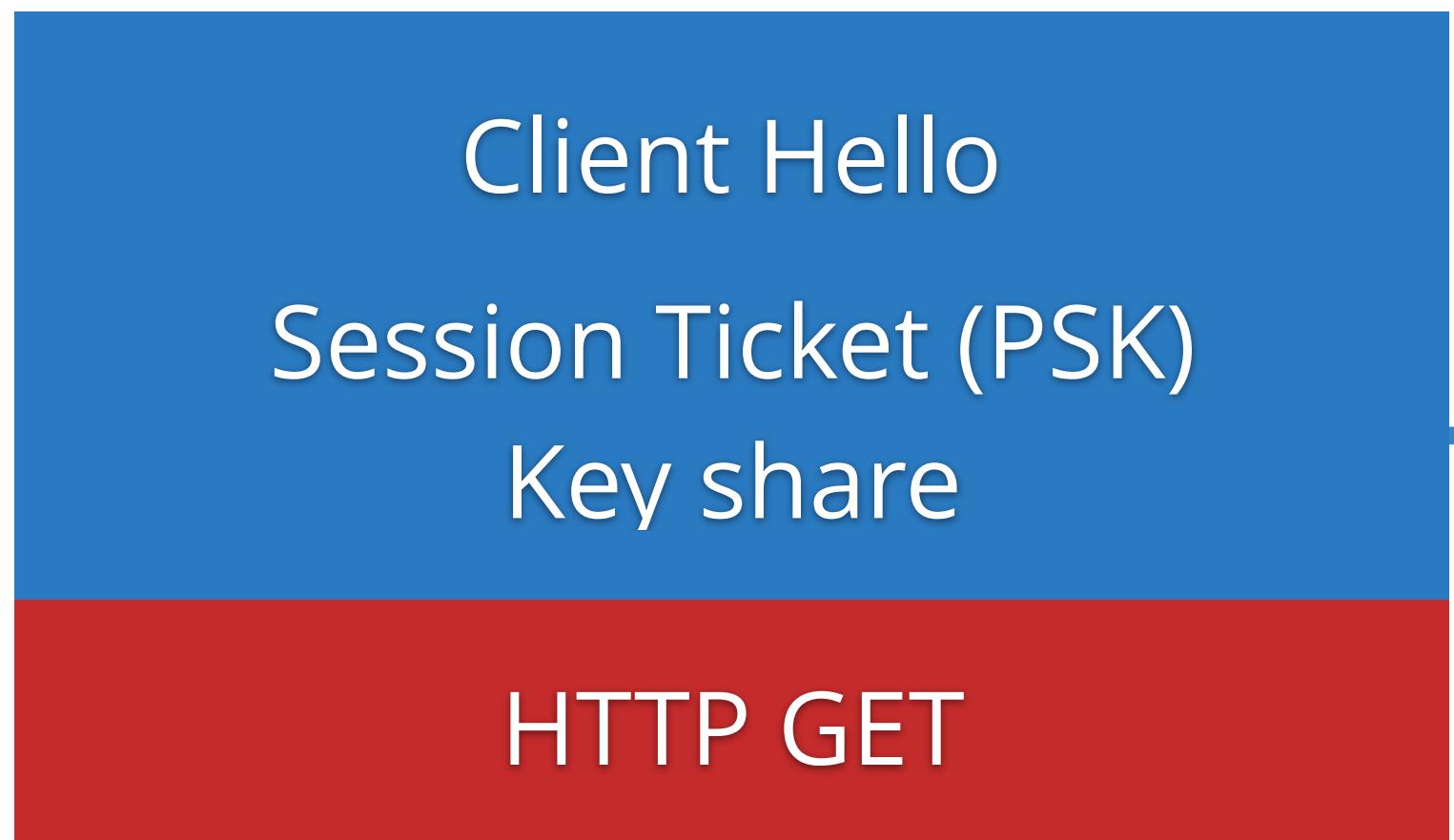


O-RTT!

0-RTT

Client

Server



0-RTT!

But...

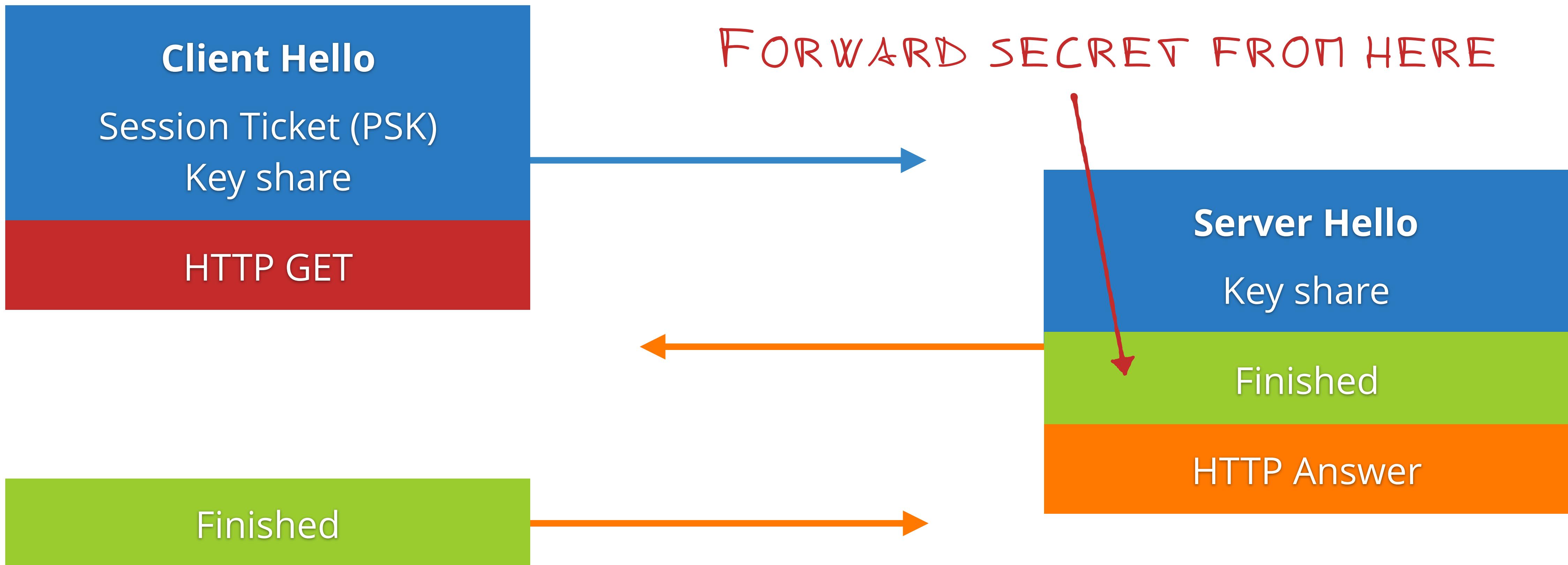
0-RTT

No PSK-ECDHE

0-RTT w/ ECDHE

Client

Server



TLS 1.2 is forward secret:

- Relatively to the certificate: **always** (using ECDHE)
- Relatively to the ticket key: **never**

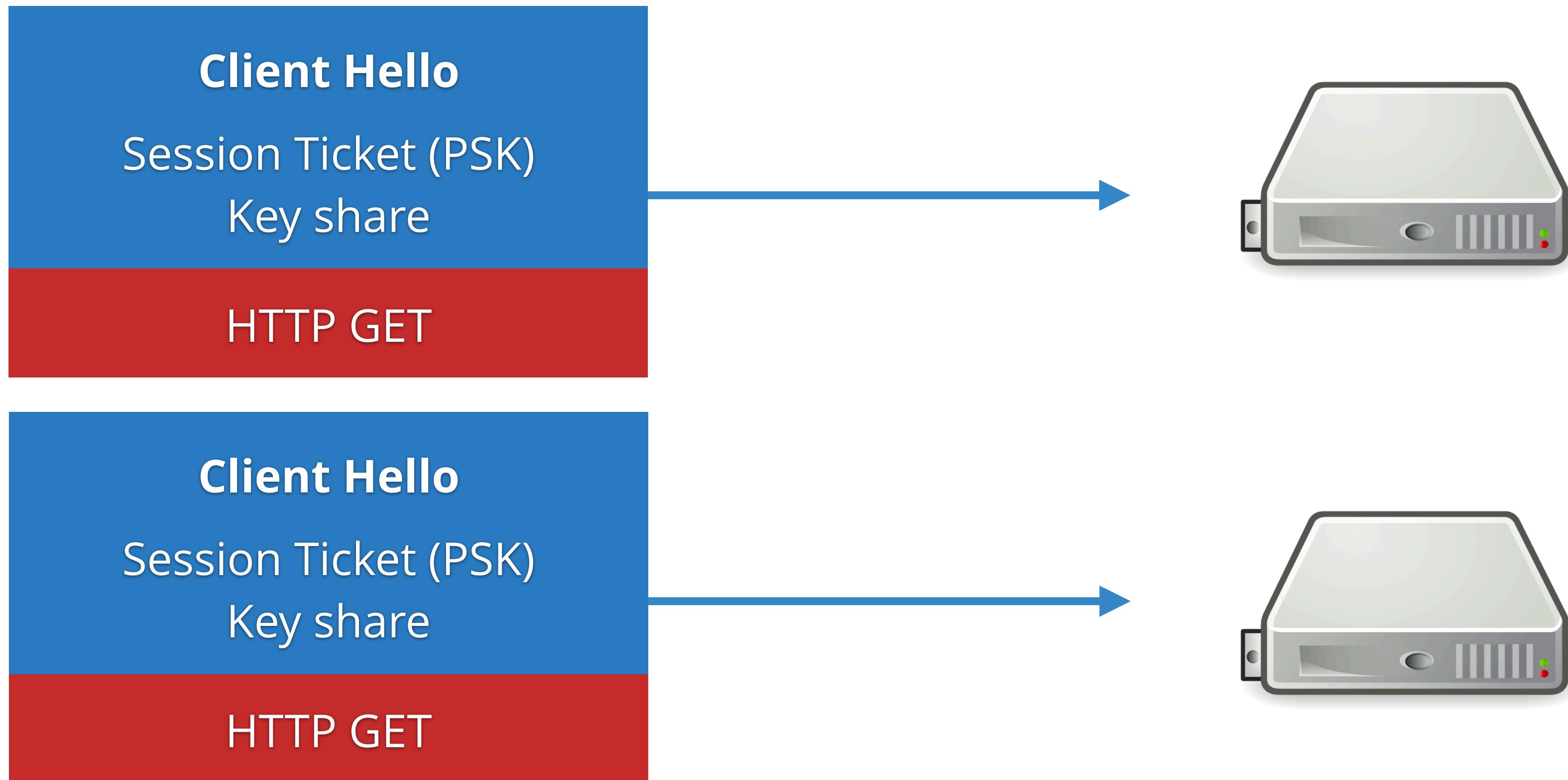
TLS 1.3 is forward secret:

- Relatively to the certificate: **always**
- Relatively to the ticket key: **except 0-RTT early data** (w/ PSK-ECDHE)

0-RTT

Replays

0-RTT replay

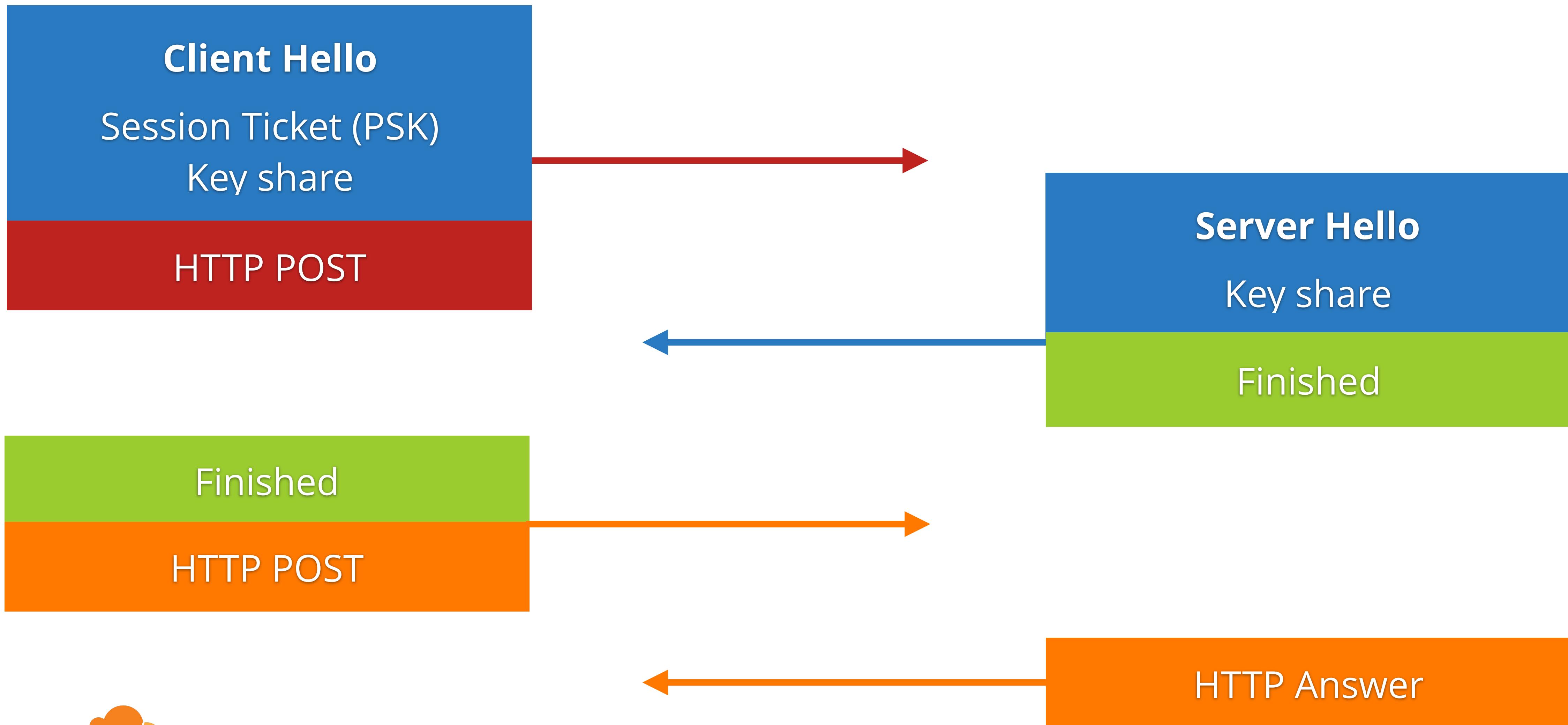


obfuscated_ticket_age

- The client sends the age in milliseconds of the ticket
- The server checks it matches its view, with some leeway
- Obfuscated with a ticket_age_add value sent as part of the New Session Ticket message

```
struct {  
    opaque identity<1..2^16-1>;  
    uint32 obfuscated_ticket_age;  
} PskIdentity;
```

0-RTT confirmation



max_early_data_size

- The server must either *accept* or *reject* the early data, entirely, without knowing how much there will be
- If it accepts it and can't process it, it must **buffer** it
- Once the Finished comes, all early data is confirmed
- max_early_data_size limits the buffer size
- Devised with Drew Springall

It's the application's responsibility

Protocols MUST NOT use 0-RTT data without a profile that defines its use.

It's the API's responsibility

- Default to 1-RTT
- Allow the server to reject / wait for the Finished
- Let the client to decide what to send in the early data

HTTP and 0-RTT

- Utopia: **GET** is idempotent!
- Reality: nope.

GET /send_money.php?to=filippo&amount=1000

HTTP and 0-RTT

- Utopia: **GET** is idempotent!
- Reality: nope.



HTTP and 0-RTT

Thai Duong, Thiago Valverde, Quan Nguyen

Google Security Team

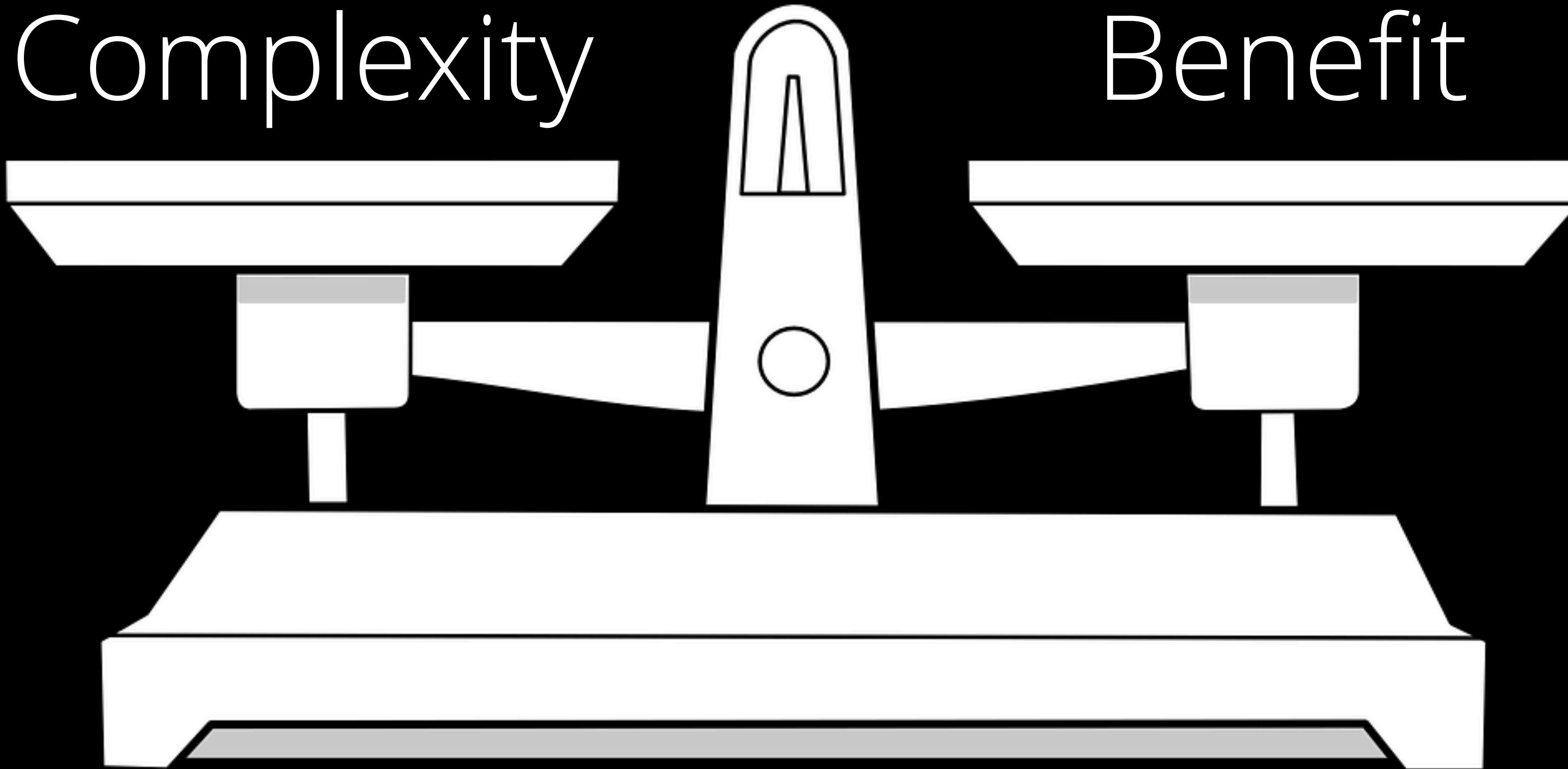
{thaidn, valverde, quannguyen}@google.com

Never, never, never, never give up.

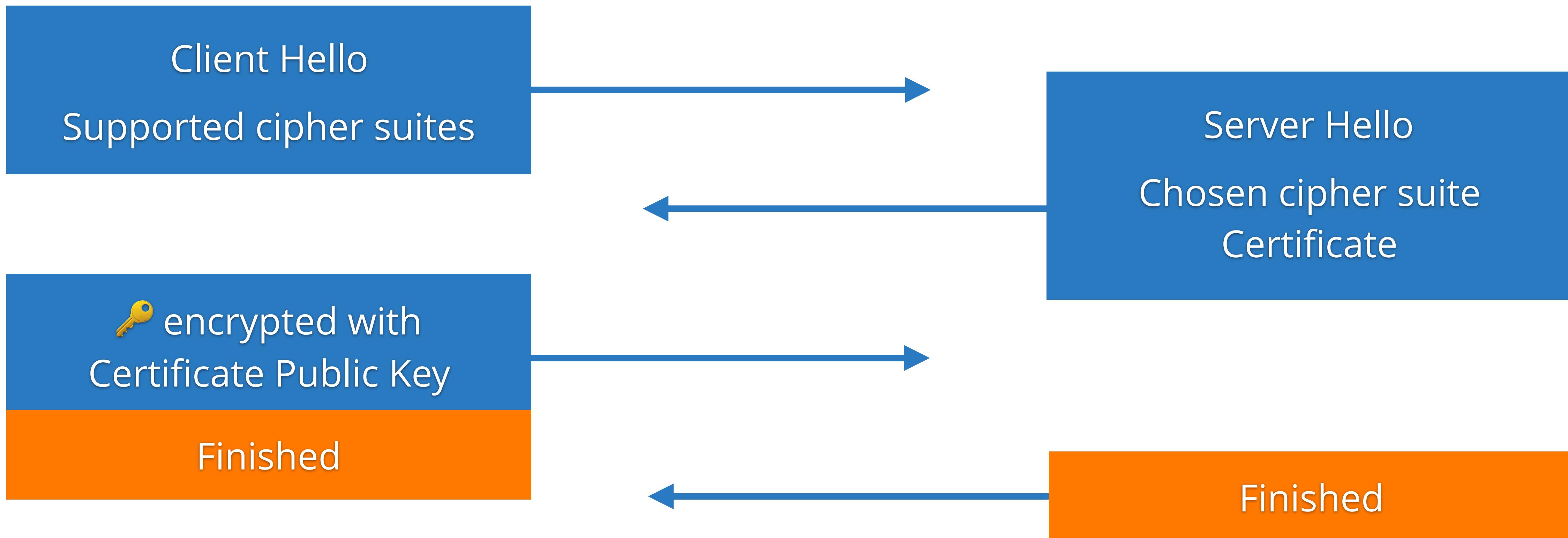
Winston Churchill

Complexity

Benefit



TLS 1.2 Static RSA mode



No Forward Secrecy

To: IETF TLS 1.3 Working Group Members

My name is Andrew Kennedy and I work at BITS, the technology policy division of the Financial Services Roundtable (<http://www.fsroundtable.org/bits>). My organization represents approximately 100 of the top 150 US-based financial services companies including banks, insurance, consumer finance, and asset management firms.

[...]

Deprecation of the RSA key exchange in TLS 1.3 will cause significant problems for financial institutions, almost all of whom are running TLS internally and have significant, security-critical investments in out-of-band TLS decryption.

[...]

Out-of-band TLS decryption?

Yes, please!



Hi Andrew,

My view concerning your request: no.

Rationale: We're trying to build a more secure internet.

Meta-level comment:

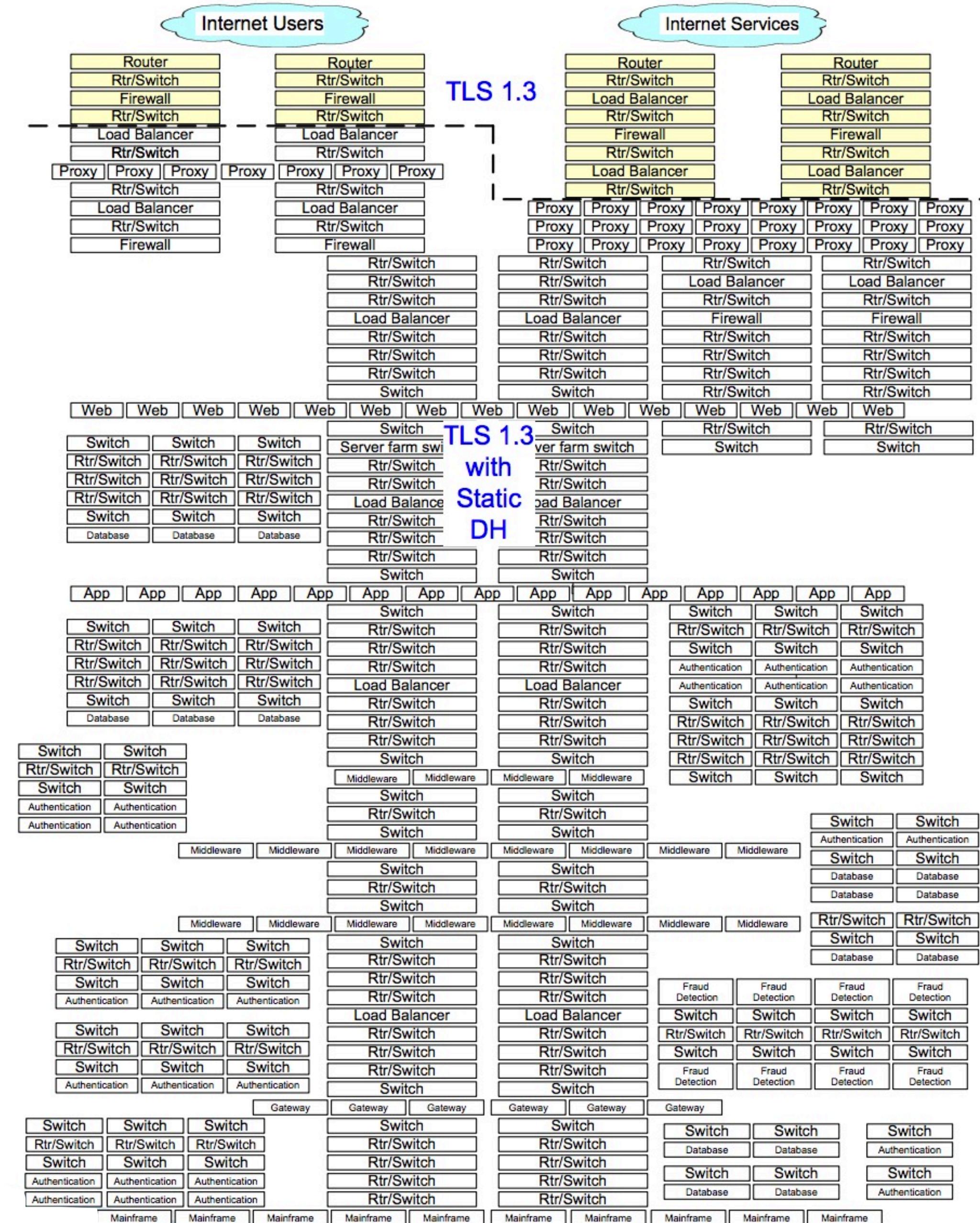
You're a bit late to the party. We're metaphorically speaking at the stage of emptying the ash trays and hunting for the not quite empty beer cans.

More exactly, we are at draft 15 and RSA key transport disappeared from the spec about a dozen drafts ago. I know the banking industry is usually a bit slow off the mark, but this takes the biscuit.

Cheers,

Kenny

Proposed Data Center Visibility Solution



[\[Docs\]](#) [\[txt|pdf\]](#) [\[Tracker\]](#) [\[Email\]](#) [\[Nits\]](#)

Versions: [00](#)

Network Working Group

Internet-Draft

Intended status: Informational

Expires: May 1, 2017

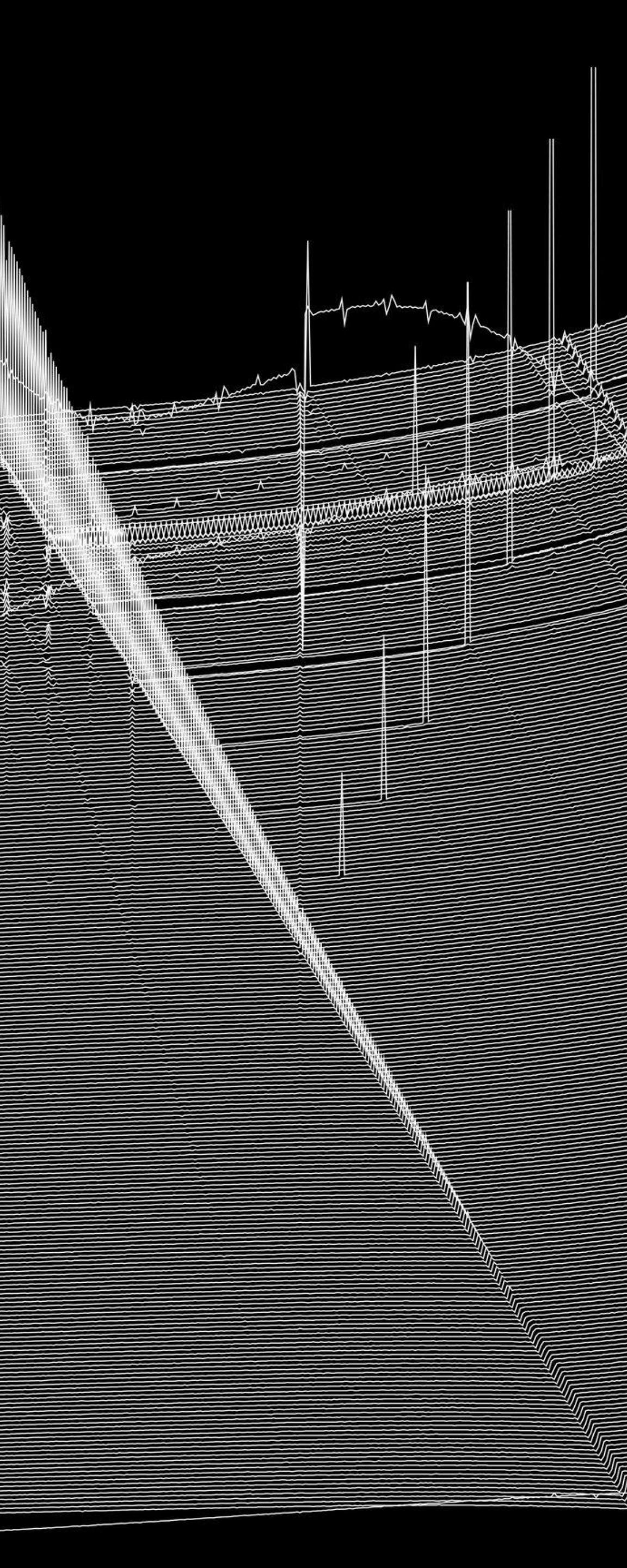
M. Green

Cryptography Engineering LLC

October 31, 2016

Data Center use of Static Diffie-Hellman in TLS 1.3
[<draft-green-tls-static-dh-in-tls13-00>](#)

RC4



3DES



MD5 & SHA1

SLOTH 2016

AES-CBC

Vaudenay 2002

Boneh/Brumley 2003

BEAST 2011

Lucky13 2013

POODLE 2014

Lucky Microseconds 2015

RSA-PKCS1-1.5

Bleichenbacher 1998 (!!)

Jager 2015

DROWN 2016

Compression

CRIME 2012

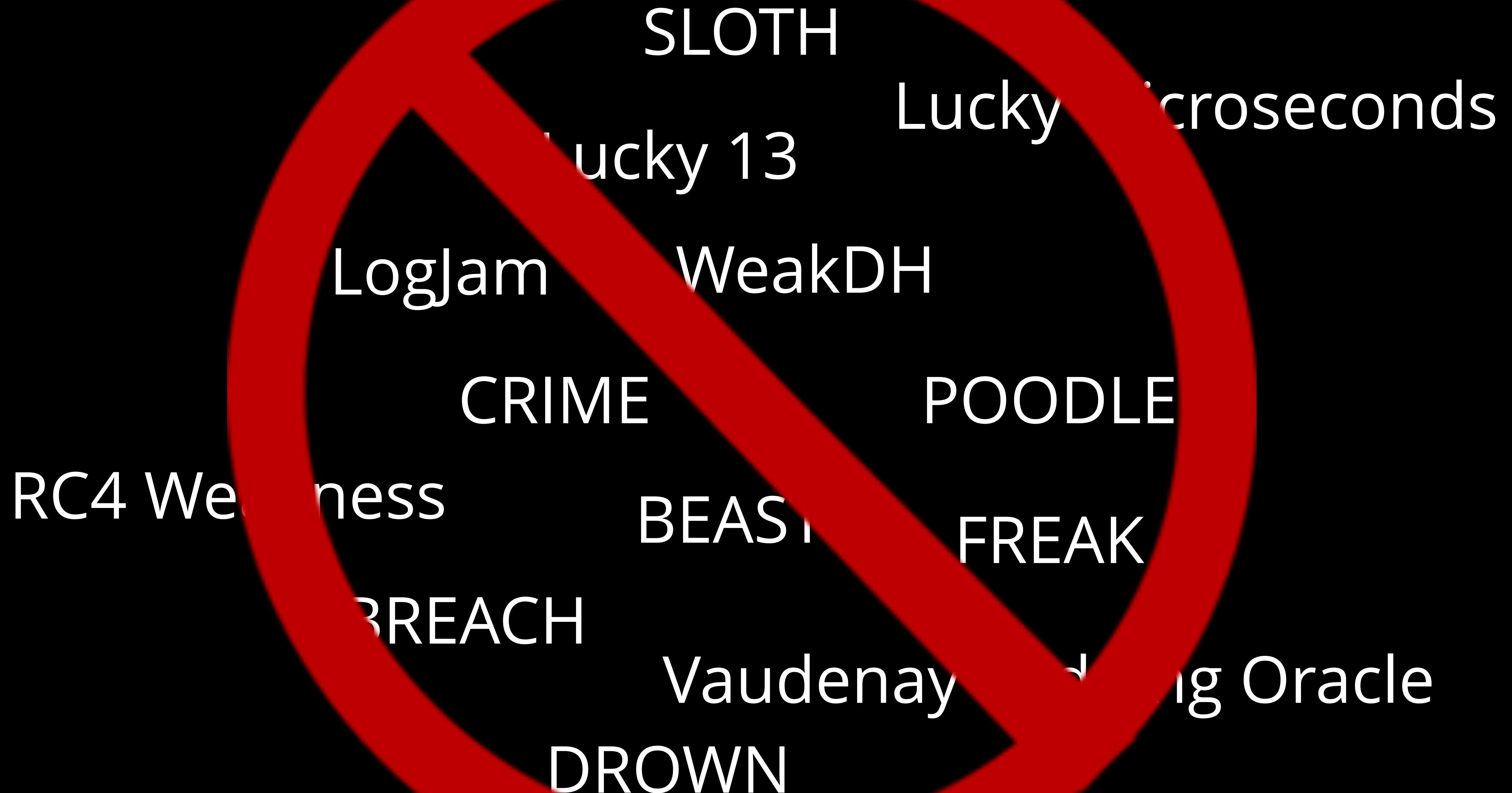
Renegotiation

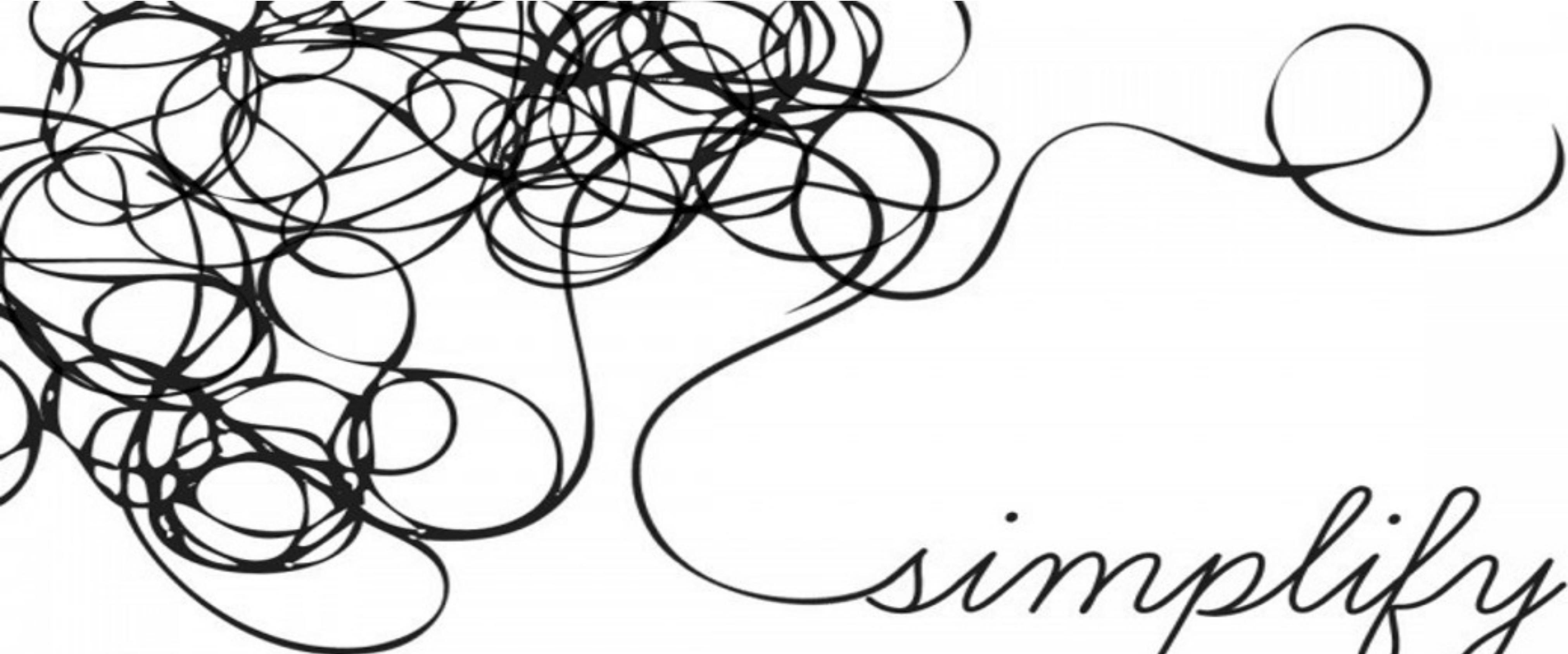
Marsh Ray Attack 2009

Renegotiation DoS 2011

Triple Handshake 2014

Replaced with lightweight key update





simplify
& Fortify

Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS

Hanno Böck*

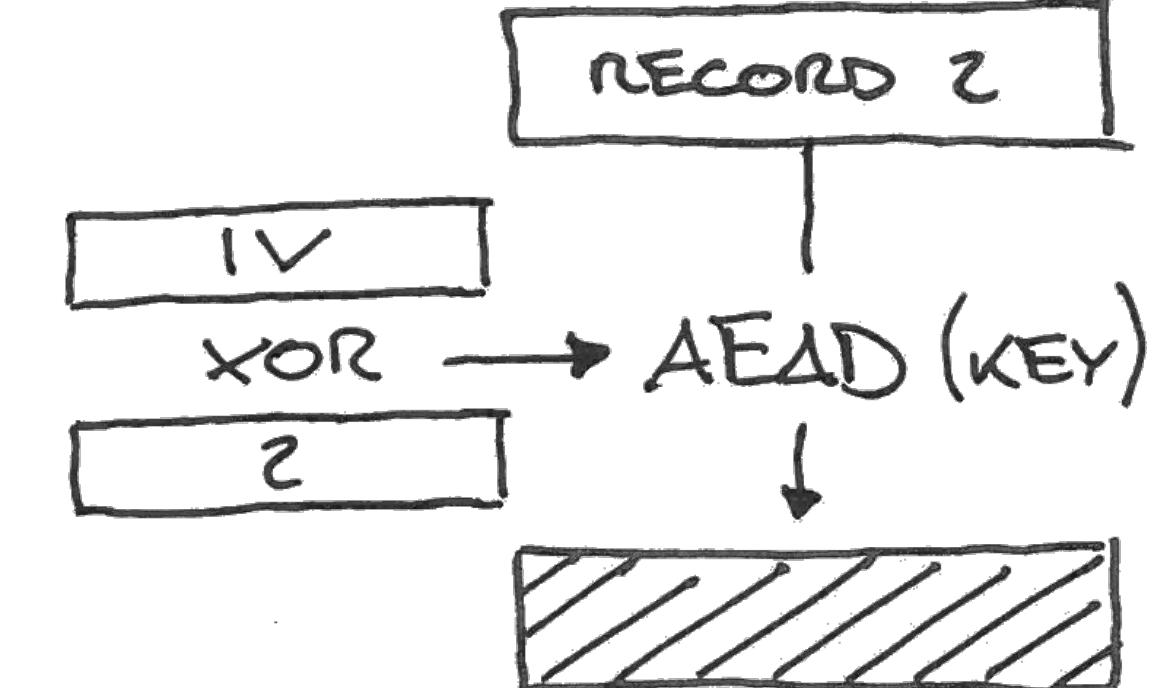
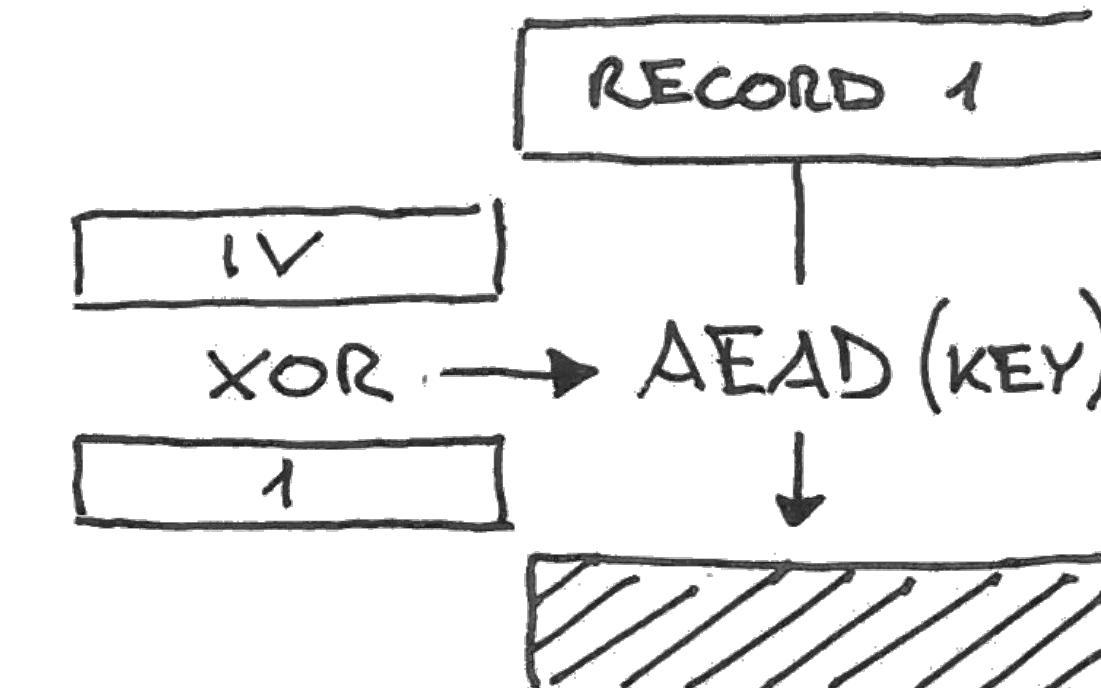
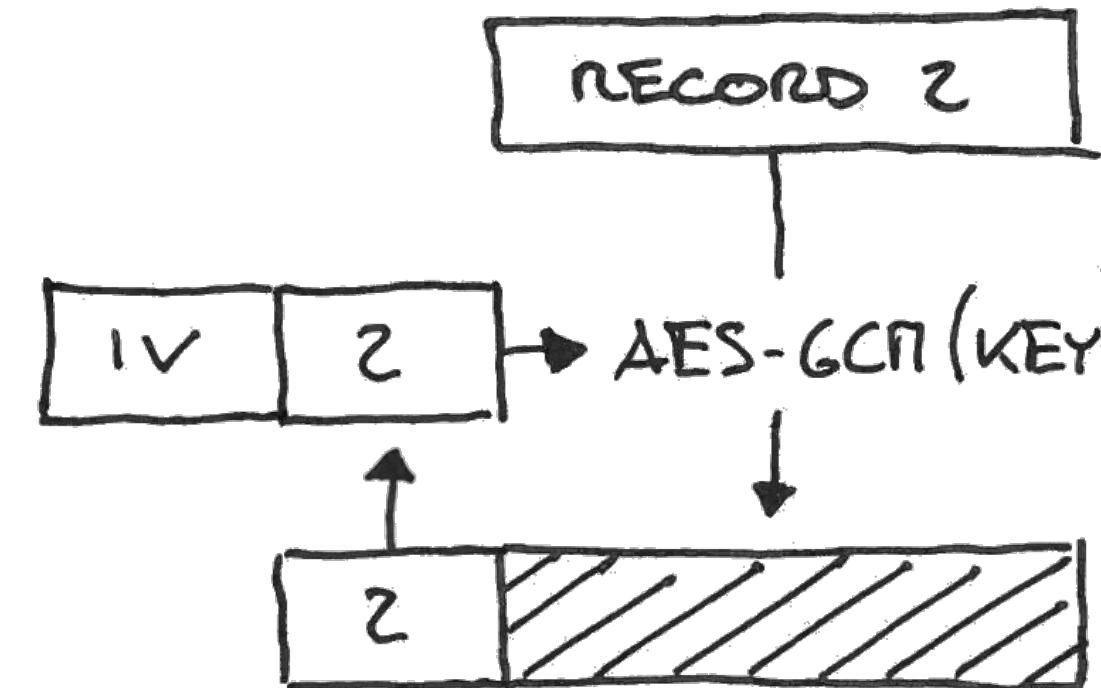
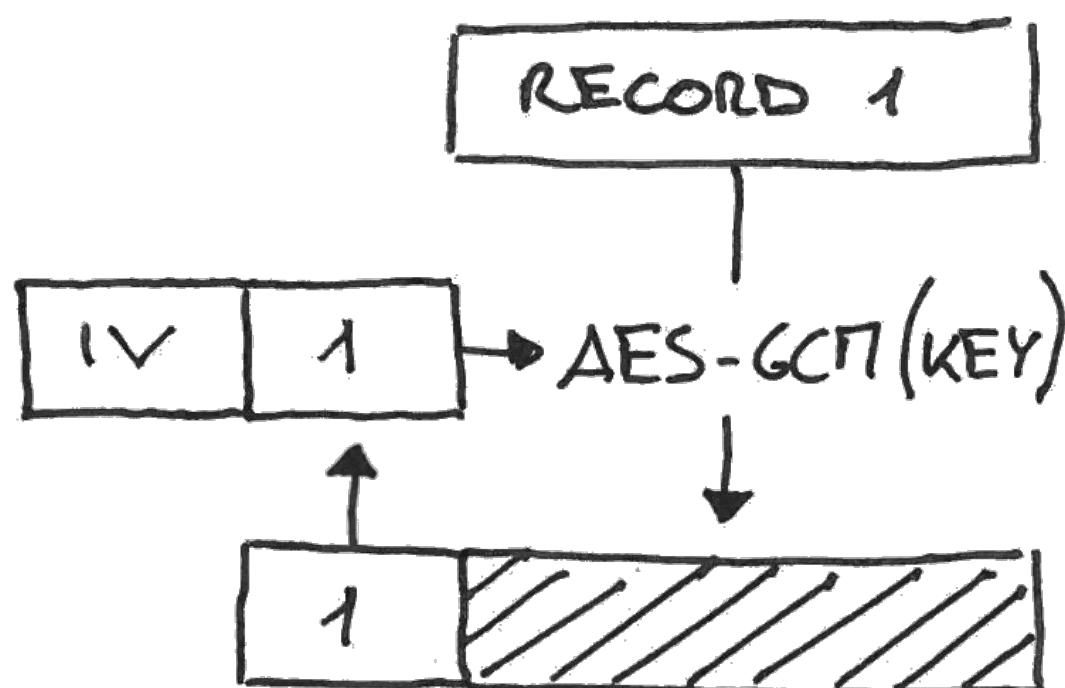
Aaron Zauner[#]

Sean Devlin[§]

Juraj Somorovsky[¶]

Philipp Jovanovic^{||}

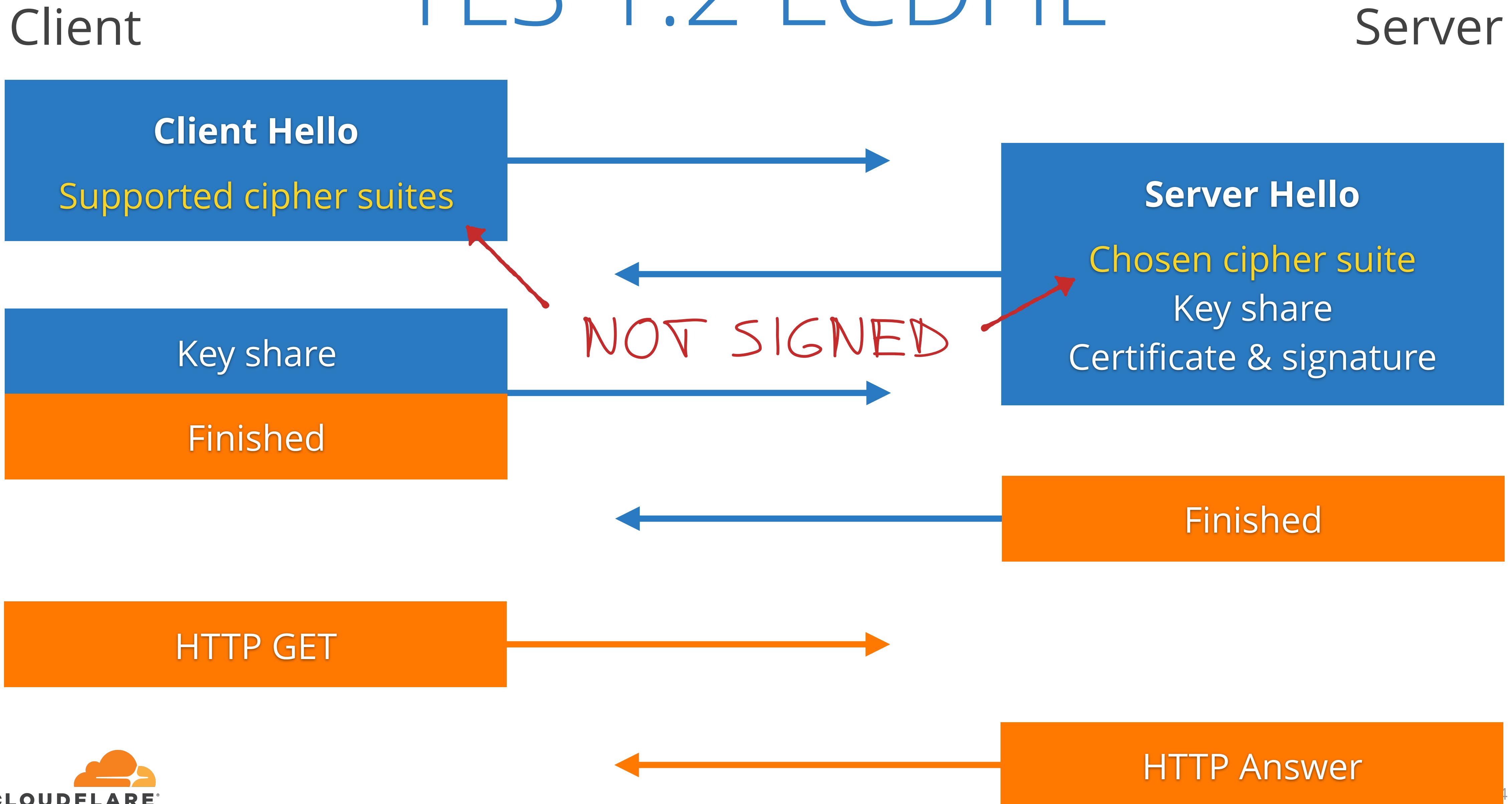
May 17, 2016



TLS 1.2 Certificate Authentication

- Cipher negotiation protected by Finished Message (MAC)
- MAC algorithm determined by cipher negotiation
- FREAK, LogJam, CurveSwap: choose weak parameters

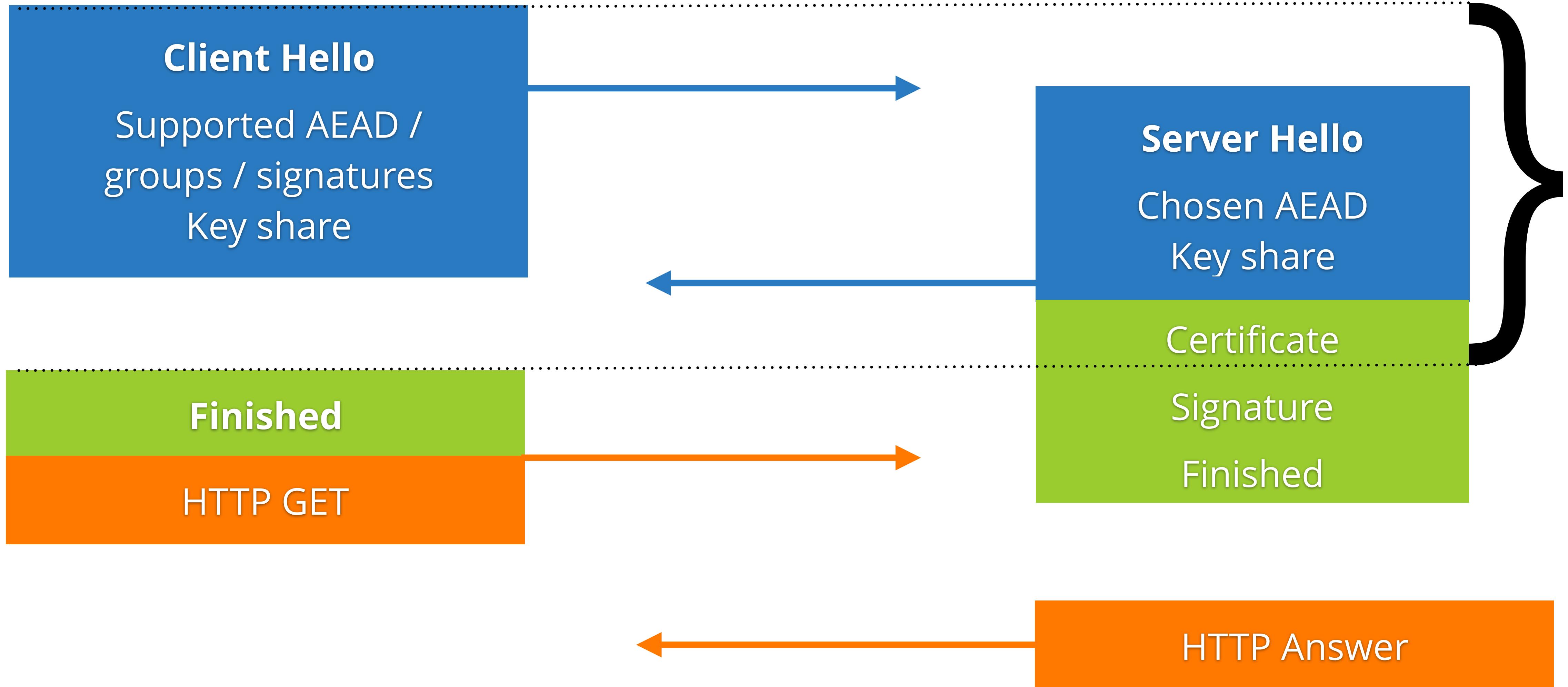
TLS 1.2 ECDHE



TLS 1.3

Client

Server



Fewer, better choices

- Key Exchange, Cipher, Authentication negotiated separately
- No arbitrary DH groups
- No arbitrary curves

AMERICAN DISH

			w. French Fried or Plain	w. Roast pork or Chicken Fried Rice	w. Beef or Shrimp Fried Rice
炸 雞 翼	A1.	Fried Chicken Wings(4).....	5.15.....	5.95.....	6.25.....7.35
辣 雞 翼	A2.	Buffalo Wings.....	5.35.....	6.25.....	6.75.....7.55
炸 雞 串	A4.	Chicken Teriyak(4).....	4.95.....	5.95.....	6.35.....6.75
炸 小 蝦	A5.	Fried Baby Shrimp(12).....	4.25.....	5.25.....	5.35.....5.55
炸 雞 塊	A6.	Fried Chicken Nugget(12).....	3.95.....	4.95.....	5.15.....5.75
薯 條	A7.	French Fries.....(S) 1.75 (L) 2.95			

APPETIZERS

叉 蝦 菜 牛 炸 雞 肉 雲 烤 骨 排 寶	燒 卷 卷 卷 卷 卷 卷	1. Roast Pork Egg Roll(Each).....1.20
		2. Shrimp Egg Roll(Each).....1.35
		3. Vegetable Spring Roll(3).....2.50
		4. Beef Egg Roll(2).....2.50
		5. Fried Pork Wonton(10).....2.75
		6. B-B-Q Spare Ribs.....(S)6.95 (L)13.25
		7. Boneless Spare Rib.....(S)5.25 (L)9.95
		8. Pu Pu Platter.....10.95
		2.Egg roll,2 shrimp roast,2 teriyaki beef, 4 cheese wonton,2 ribs & 2 chicken wing
		9. Steamed or Fried Dumpling(10).....4.50
		10. Teriyaki Beef(4).....4.50
		11. Shrimp Toast(4).....2.95
		12. Fried Cheese Wonton(8).....4.25
		13. Fried Donuts(10).....2.75

SOUP

	(w. Fried Noodles)	Pt.	Qt.
雲 吞 汤	Wonton Soup.....	1.75	3.25
蛋 花 汤	Egg Drop Soup.....	1.50	2.85
鷄 湯 面 / 飯	Chicken Rice/Noodle Soup.....	1.75	3.25
雲 吞 蛋 汤	Wonton Egg Drop Mixed.....	1.95	3.50
酸 辣 湯	Hot & Sour Soup.....	2.15	4.15
菜 樓 湯	Vegetable Soup w. Bean Curd.....	1.75	3.25
本 樓 湯	House Special Soup.....	2.25	

CHOP SUEY

	(w. White Rice & Fried Noodle) (Celery, onion, Napa and Bean Sprouts)	Pt.	Qt.
鷄 雜 碎	23. Chicken Chop Suey.....	4.35	6.95
叉 燒 雜 碎	24. Roast Pork Chop Suey.....	4.35	6.95
牛 肉 雜 碎	25. Beef Chop Suey.....	4.95	7.95
蝦 雜 碎	26. Shrimp Chop Suey.....	4.95	7.95
素 菜 雜 碎	27. Vegetable Chop Suey.....	3.75	6.55
本 樓 雜 碎	28. House Special Chop Suey.....	8.35	

FRIED RICE

	Pt.	Qt.
叉 燒 炒 飯	29. Roast Pork Fried Rice.....	3.25
鷄 炒 飯	30. Chicken Fried Rice.....	3.25
牛 肉 炒 飯	31. Beef Fried Rice.....	3.95
蝦 炒 飯	32. Shrimp Fried Rice.....	3.95
素 菜 炒 飯	33. Vegetable Fried Rice.....	3.25
本 樓 炒 飯	34. House Special Fried Rice....	4.25
淨 炒 飯	35. Plain Fried Rice.....	1.50

LO MEIN

	(Chinese soft Noodles)	Pt.	Qt.
素 菜 捞 面	36. Vegetable Lo Mein.....	3.05	5.95
淨 捞 面	37. Plain Lo Mein.....	3.05	5.50
叉 燒 捞 面	38. Roast Pork Lo Mein.....	3.35	6.50
鷄 捞 面	39. Chicken Lo Mein.....	3.35	6.50
蝦 捞 面	40. Shrimp Lo Mein.....	3.95	7.25
牛 肉 捞 面	41. Beef Lo Mein.....	3.95	7.25
本 樓 捞 面	42. House Special Lo Mein.....	4.50	7.55

FREE2 Egg Rolls
w. Order of \$20 or More
only for dinner**FREE**3 Egg Rolls or Soda(2L)
w. Order of \$30 or More
only for dinner**FREE**4 Egg Rolls or Soda (2L)
w. Order of \$40 or More
only for dinner**FREE**General's Chicken
w. Order of \$55 or More
only for dinner

AMERICAN DISH

	w. French Fried or Plain Fried Rice	w. Roast pork or Chicken Fried Rice	w. Beef or Shrimp Fried Rice
炸 雞 翼	A1. Fried Chicken Wings(4).....	5.15.....	5.95.....6.25.....7.35
辣 雞 翼	A2. Buffalo Wings.....	5.35.....	6.25.....6.75.....7.55
炸 雞 串	A4. Chicken Teriyak(4).....	4.95.....	5.95.....6.35.....6.75
炸 小 蝦	A5. Fried Baby Shrimp(12).....	4.25.....	5.25.....5.35.....5.55
炸 雞 塊	A6. Fried Chicken Nugget(12).....	3.95.....	4.95.....5.15.....5.75
薯 條	A7. French Fries.....(S) 1.75 (L) 2.95		

SEAFOOD

	(w. White Rice or Fried Rice)	Pt.	Qt.
什 蝦 菜	78. Shrimp w. Mixed Veggies.....	6.25	10.25
糊 蝦	79. Shrimp w. Lobster Sauce.....	6.25	10.25
豆 蝦	81. Shrimp w. Black Bean Sauce.....	6.25	10.25
腰 蝦	82. Shrimp w. Cashew Nuts.....	6.25	10.25
芥 蝦	83. Shrimp w. Broccoli.....	6.25	10.25
咖 蝦	84. Curry Shrimp w. Onion.....(Order)	10.25	
四 川 蝦	85. Szechuan Shrimp.....(Order)	10.25	
宮 保 蝦	86. Kung Po Shrimp.....(Order)	10.25	
魚 湖 南	87. Shrimp w. Garlic Sauce...(Order)	10.25	
香 南	88. Hunan Shrimp.....(Order)	10.25	

VEGETABLE

	(w. white Rice or Fried Rice)	Pt.	Qt.
什 菜	106. Mixed Vegetables.....		5.95
香 菜	107. Mixed Vegetables w. Garlic Sauce	5.95	
芥 蘭	108. Sauteed Broccoli.....		5.95
香 蘭	109. Broccoli w. Garlic Sauce.....		5.95
魚 葵	110. Bean Curd w. Garlic Sauce.....		7.15
芝 葵	111. Sesame Bean Curd.....		7.15
麻 葵	112. Bean Curd Szechuan Style.....		7.15

EGG FOO YOUNG

	(w. White Rice or Fried Rice)	Pt.
叉 燒 菜	43. Roast Pork Egg Foo Young.....	6.75
鷄 菜	44. Chicken Egg Foo Young.....	6.75
蝦 菜	45. Shrimp Egg Foo Young.....	7.75
牛 肉 菜	46. Beef Egg Foo Young.....	7.75
菜 菜	47. Vegetable Egg Foo Young.....	6.35

SWEET & SOUR

	(w. White Rice or Fried Rice)	Pt.
甜 酸 雞	48. Sweet & Sour Chicken.....	7.95
甜 酸 肉	49. Sweet & Sour Pork.....	7.95
甜 酸 蝦	50. Sweet & Sour Shrimp.....	9.75

PORK

	(w. White Rice or Fried Rice)	Pt.	Qt.

<tbl_r cells="4" ix="3" maxcspan="1" max

ENTREE

BABY COS SALAD

WITH MARINATED CHICKEN STRIPS, TOASTED
BREAD AND CLASSIC CAESAR DRESSING

SHREDDED DUCK SALAD

WITH SHIITAKE MUSHROOMS, SPRING
ONION AND BEAN THREAD NOODLES

MAINS

SIRLOIN OF BEEF

WITH ROASTED POTATOES, TOMATO,
ONION, ROSEMARY AND GARLIC COMPOTE

GRILLED CHICKEN BREAST

WITH CARAMELISED ONION, MASH
POTATOES, TOMATOES, PEAS AND JUS

DESSERT

STICKY DATE PUDDING

WITH BUTTERSCOTCH SAUCE, VANILLA
ICECREAM AND SWEET PASTRY

CHOCOLATE MACADAMIA BROWNIE

WITH CHOCOLATE GARNISH AND
COCONUT ICE CREAM

- ▼ Cipher Suites (19 suites)
 - Cipher Suite: Unknown (0xdada)
 - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 - Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
- ▼ Extension: signature_algorithms (len=20)
 - Type: signature_algorithms (13)
 - Length: 20
 - Signature Hash Algorithms Length: 18
 - Signature Hash Algorithms (9 algorithms)
- ▼ Extension: elliptic_curves (len=10)
 - Type: elliptic_curves (10)
 - Length: 10
 - Elliptic Curves Length: 8
 - ▼ Elliptic curves (4 curves)
 - Elliptic curve: Unknown (0x9a9a)
 - Elliptic curve: ecdh_x25519 (0x001d)
 - Elliptic curve: secp256r1 (0x0017)
 - Elliptic curve: secp384r1 (0x0018)

Safer Resumption

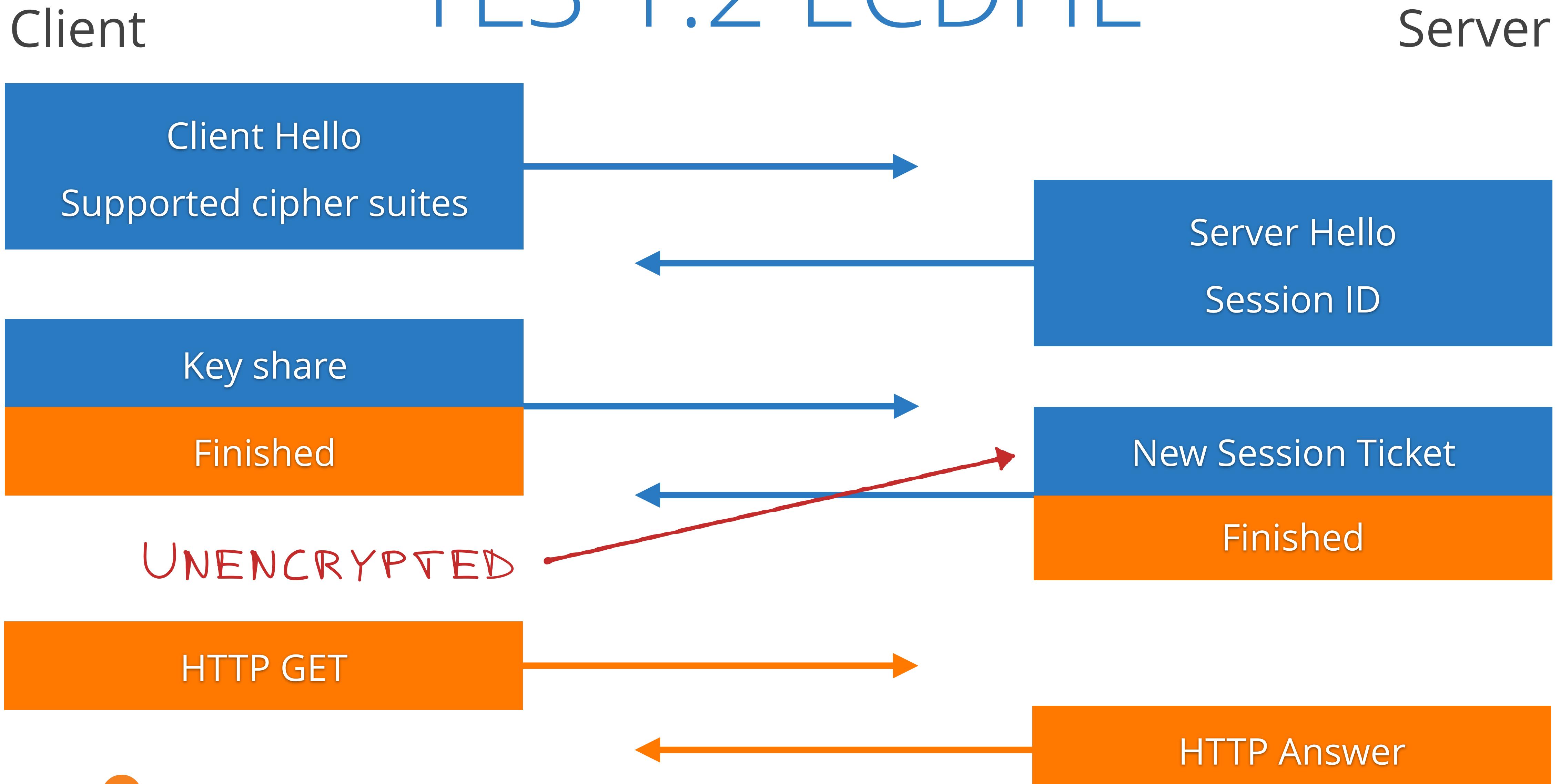
TLS 1.2 tickets

- **Current** session keys encrypted with session ticket key
- Session ticket key compromise a risk for all connections

TLS 1.3 tickets

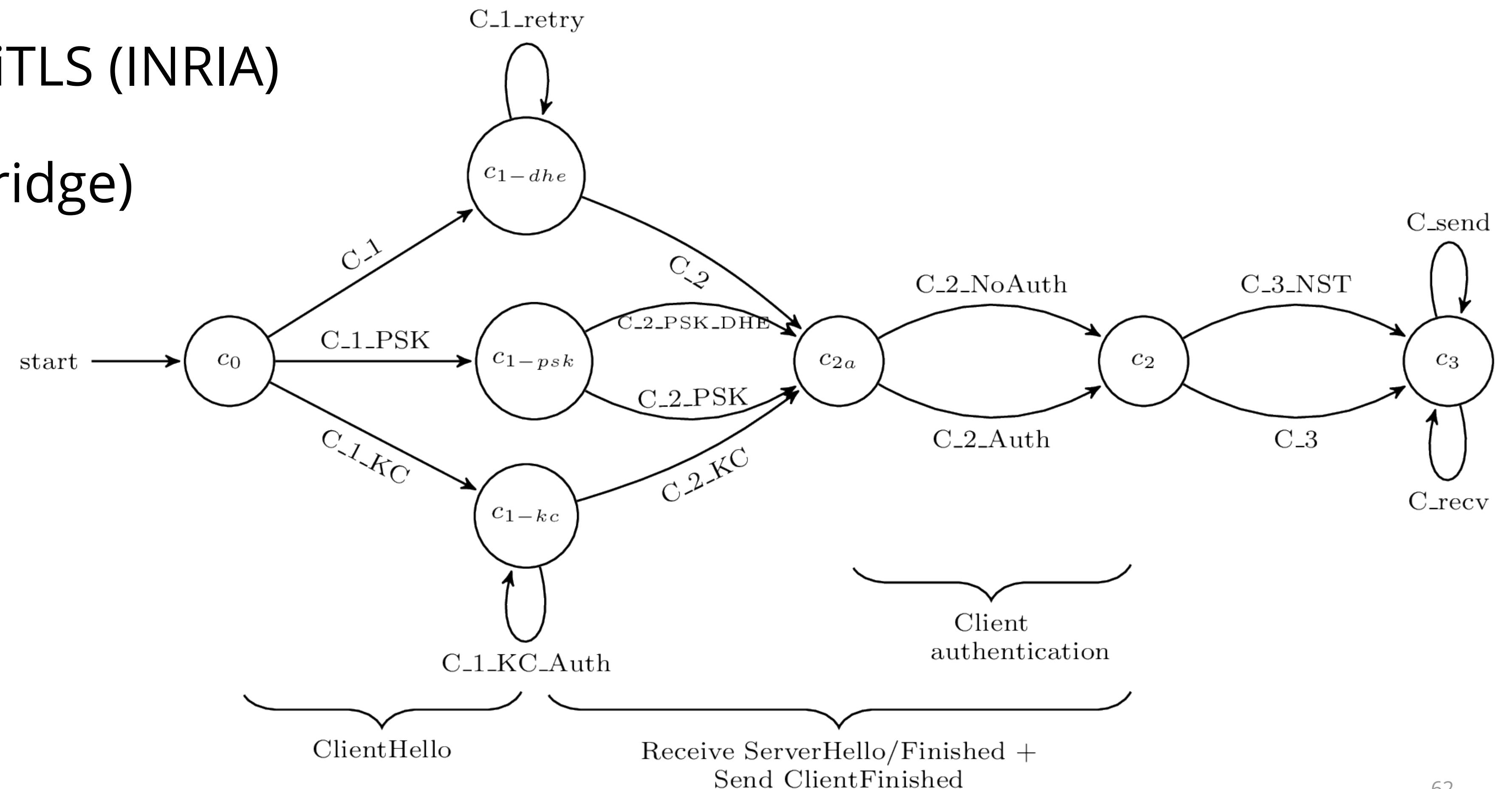
- **Next** session keys encrypted with session ticket key
- Session ticket key compromise only risk for resumed connections

TLS 1.2 ECDHE



Formal Verification

- Tamarin (Oxford, Royal Holloway)
- ProScript-TLS, miTLS (INRIA)
- nqsbt-TLS (Cambridge)



Standards

The IETF way



Nick Sullivan 
@grittygrease

TLS 1.3 Wish List - it's a short list.
[ietf.org/proceedings/87/](https://www.ietf.org/proceedings/87/) ...

5:26 PM - 4 Sep 2013

Timeline

- First Draft: April 17, 2014
 - 3Shake, POODLE, FREAK, LogJam, DROWN, Lucky Microseconds, SLOTH, more...
- Draft 18: October 26, 2016
- Final draft: **February, 2017** (we hope)
- TLS 1.2: **79 pages**
- TLS 1.3: **81 pages** (minus references and appendices)

Github + Mailing List

tlswg / tls13-spec

Code Issues 9 Pull requests 7 Projects 0 Wiki Pulse Graphs

1,459 commits 4 branches 19 releases 49 contributors

Transport Layer Security working group of the IETF Discussion Archive - Date Index

[Prev Page] [Next Page] [Thread Index] [IETF Main Archive Directory]

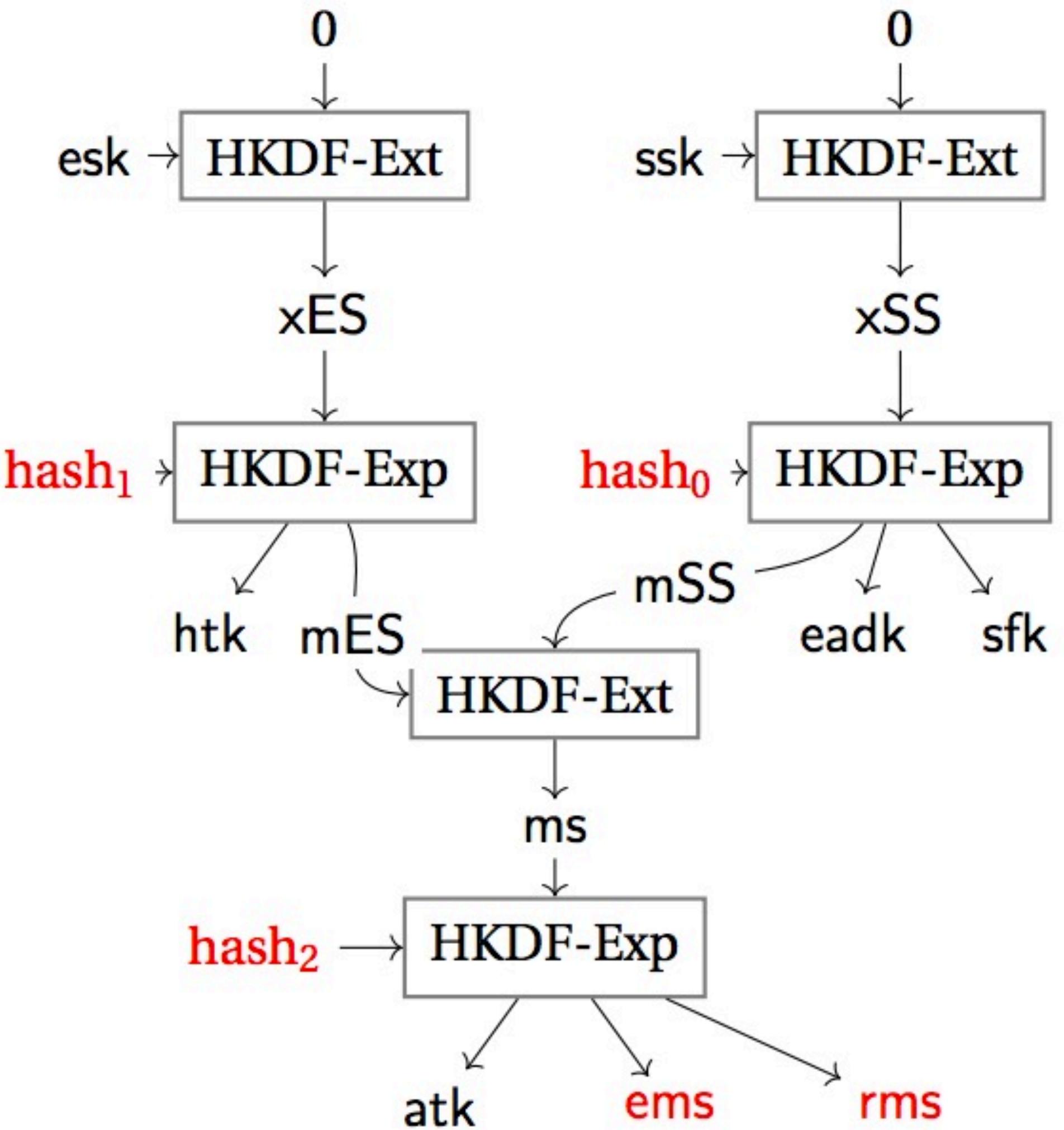
- Dec 22 2016

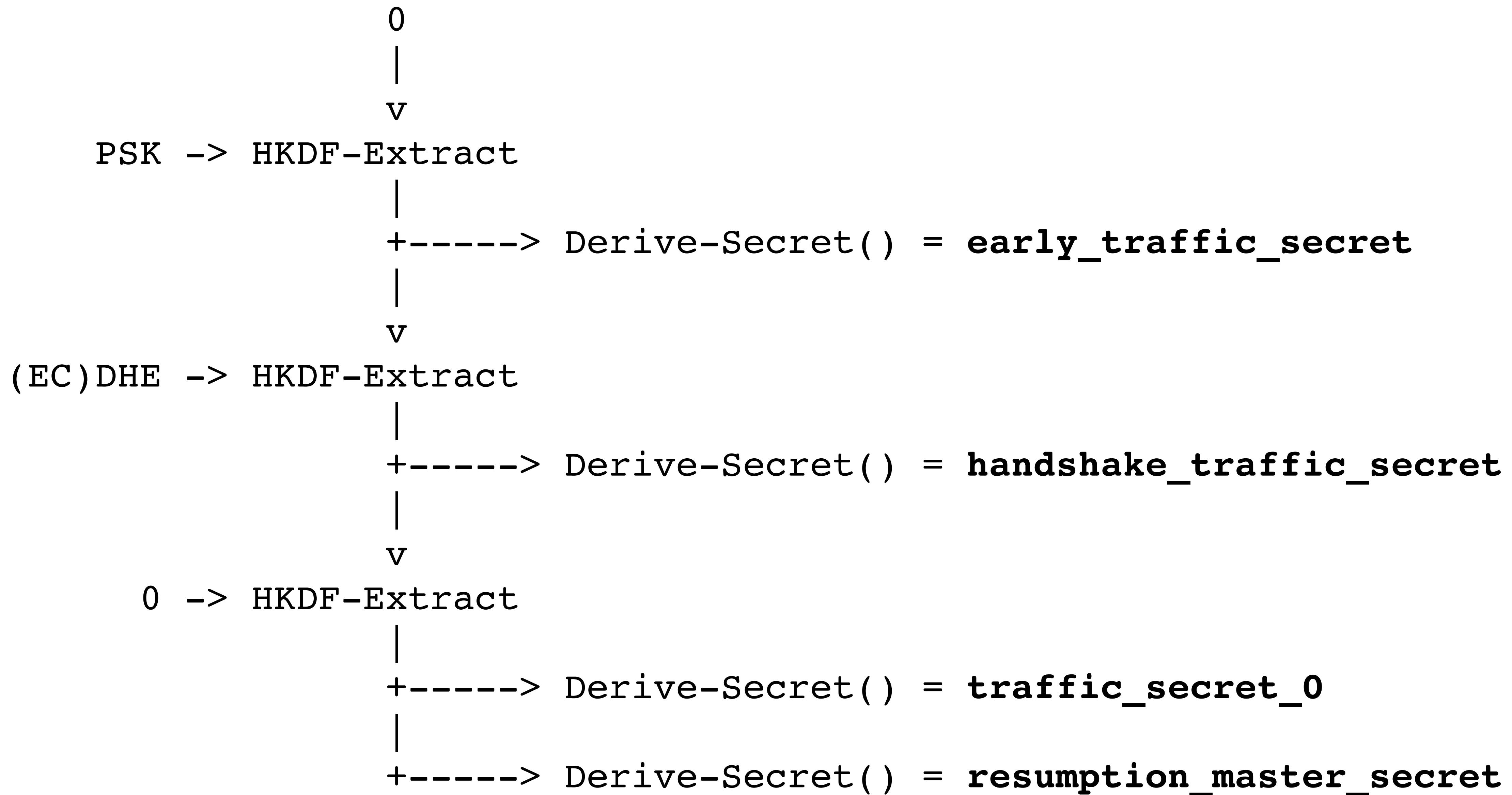
- [Re: \[TLS\] Using both External PSK and \(EC\)DH in TLS 1.3, Eric Rescorla](#)
- [Re: \[TLS\] Using both External PSK and \(EC\)DH in TLS 1.3, Russ Housley](#)
- [Re: \[TLS\] Using both External PSK and \(EC\)DH in TLS 1.3, Joseph Salowey](#)
- [Re: \[TLS\] Using both External PSK and \(EC\)DH in TLS 1.3, David Benjamin](#)
- [\[TLS\] Using both External PSK and \(EC\)DH in TLS 1.3, Russ Housley](#)

Key Schedule

- Inspired by QUIC crypto
- Semi-static DH key shared out of band
- Tree-based key schedule

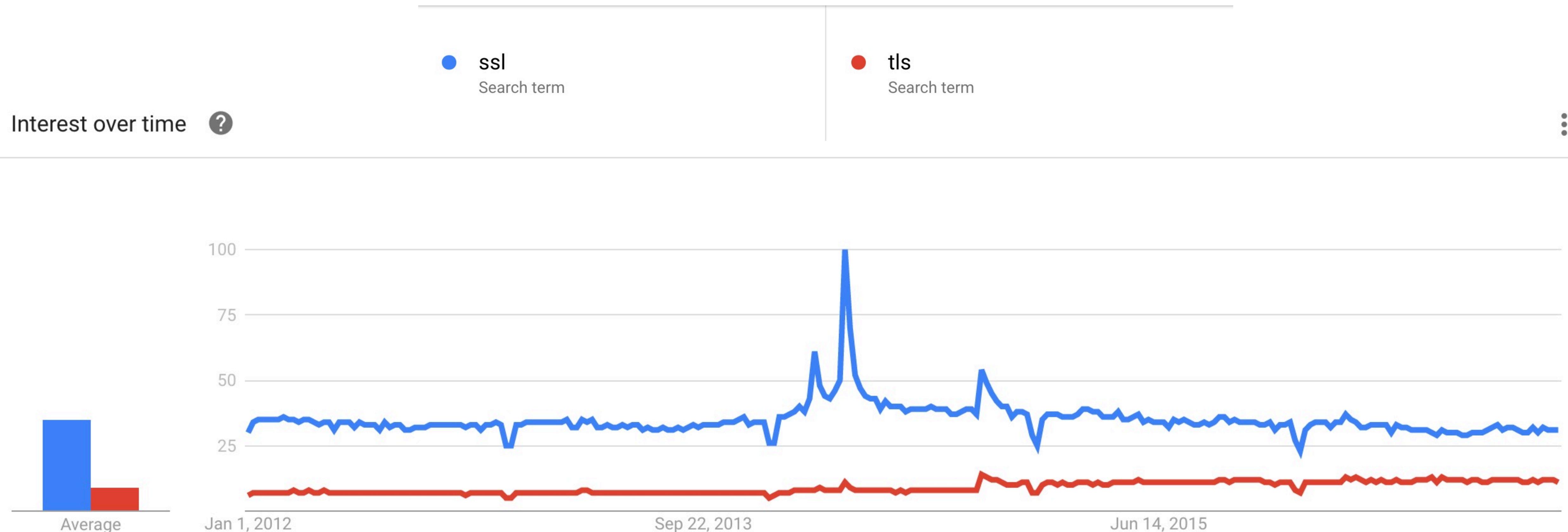
OPTLS in TLS 1.3 draft-09





What's in a name?

Is it TLS 1.3, TLS 2, TLS 2.0, TLS 4, TLS 7, TLS 2017?





Whitney Merrill @wbm312 · Aug 31

What should the next version of TLS (after TLS 1.2) be called? ietf.org/mail-archive/w...

39% TLS 1.3

28% TLS 2.0

13% TLS/2

20% TLS 3

1,105 votes • Final results

← 50 22 14 ...



Nick Sullivan @grittygrease · Nov 29

What should the next version of TLS be called? (it's currently called TLS 1.3)

34% TLS 1.3

27% TLS 2

15% TLS 4

24% TLS 7

545 votes • Final results

← 39 12 4 ...



Ryan Hurst @rmhrisk · Aug 31

What should the new version of TLS be called? #ssl #bikeshedding
#standardsbycomitee

21% TLS/42

27% TLS/Bacon

52% Mmmm Bacon

322 votes • Final results

← 9

16

8

...

Version Intolerance

- Wire versions
 - SSL 3.0: 3.0
 - TLS 1.0: 3.1
 - TLS 1.1: 3.2
 - TLS 1.2: 3.3
 - TLS 1.3: 3.4 ???
- Servers are intolerant of 3.4
 - >2% of servers fail connection
 - Solution: “3.3” in ClientHello, real versions in extension
 - GREASE by David Benjamin

Version Intolerance

```
▼ Extension: supported_versions (len=11)
  Type: supported_versions (43)
  Length: 11
  Supported Versions length: 10
  Supported Versions: Unknown (0x8a8a)
  Supported Versions: TLS 1.3 (draft 18) (0x7f12)
  Supported Versions: TLS 1.2 (0x0303)
  Supported Versions: TLS 1.1 (0x0302)
  Supported Versions: TLS 1.0 (0x0301)
```

Implementation

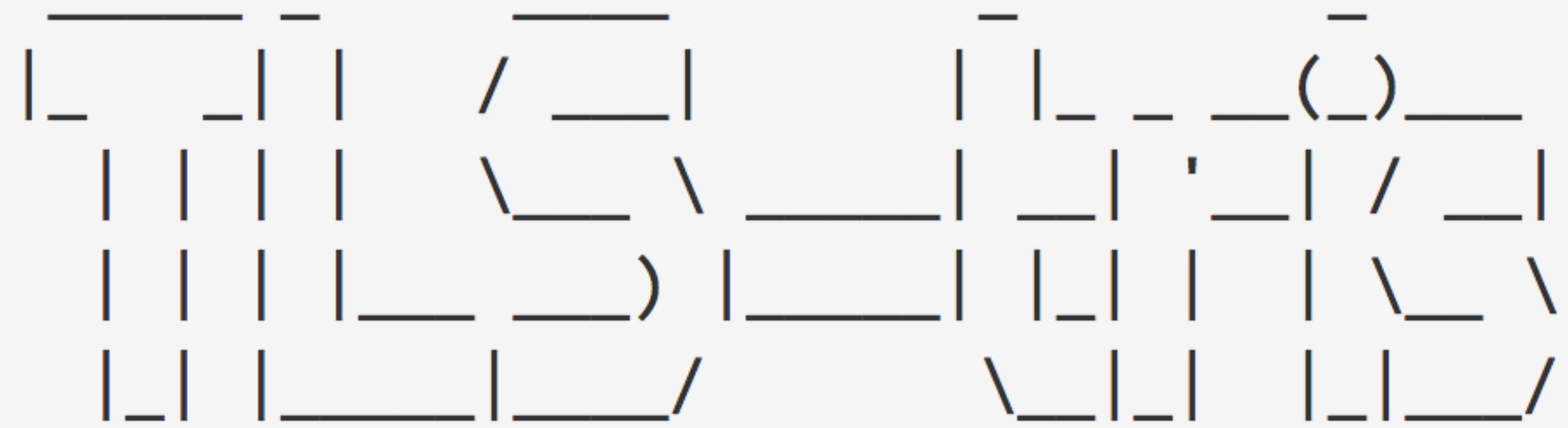
Getting our hands dirty

IETF 95 Hackathon - April 2016

- NSS (C): Martin Thomson and Eric Rescorla
- Mint (Go): Richard Barnes and Nick Sullivan

Result:

Firefox was able to load [https://tls13.cloudflare.com!](https://tls13.cloudflare.com)



crypto/tls, now with 100% more 1.3.

- Based on Go crypto/tls
- Server only
- Audited

DO NOT USE THIS FOR THE SAKE OF EVERYTHING THAT'S GOOD AND JUST.

build passing

▶ [dev.tls] crypto/tls: implement TLS 1.3 cipher suites

[dev.tls] crypto/tls: implement TLS 1.3 messages

[dev.tls] crypto/tls: implement TLS 1.3 record layer

<https://go-review.googlesource.com/q/branch:+dev.tls>

Deploying is hard

- First deployed Tris: draft 13
- Supported multiple drafts at a time (“hybrids”)
- Browsers sometimes... diverged

Build Jobs

✓ # 206.1		</> Go: 1.7	MODE=interop CLIENT=boring	5 min 26 sec
✓ # 206.2		</> Go: 1.7	MODE=interop CLIENT=bogo	4 min 9 sec
✓ # 206.3		</> Go: 1.7	MODE=interop CLIENT=tstclnt	6 min 49 sec
✓ # 206.4		</> Go: 1.7	MODE=interop CLIENT=picotls ZRTT=1	3 min 28 sec
✓ # 206.5		</> Go: 1.7	MODE=interop CLIENT=mint	2 min 57 sec
✓ # 206.6		</> Go: 1.7	MODE=gotest	3 min 3 sec

Allowed Failures

✗ # 206.7		</> Go: 1.7	MODE=interop CLIENT=tstclnt ZRTT=1	6 min 21 sec
✓ # 206.8		</> Go: 1.7	MODE=interop CLIENT=boring REVISION=	5 min 17 sec
✗ # 206.9		</> Go: 1.7	MODE=interop CLIENT=tstclnt REVISION=	6 min 56 sec

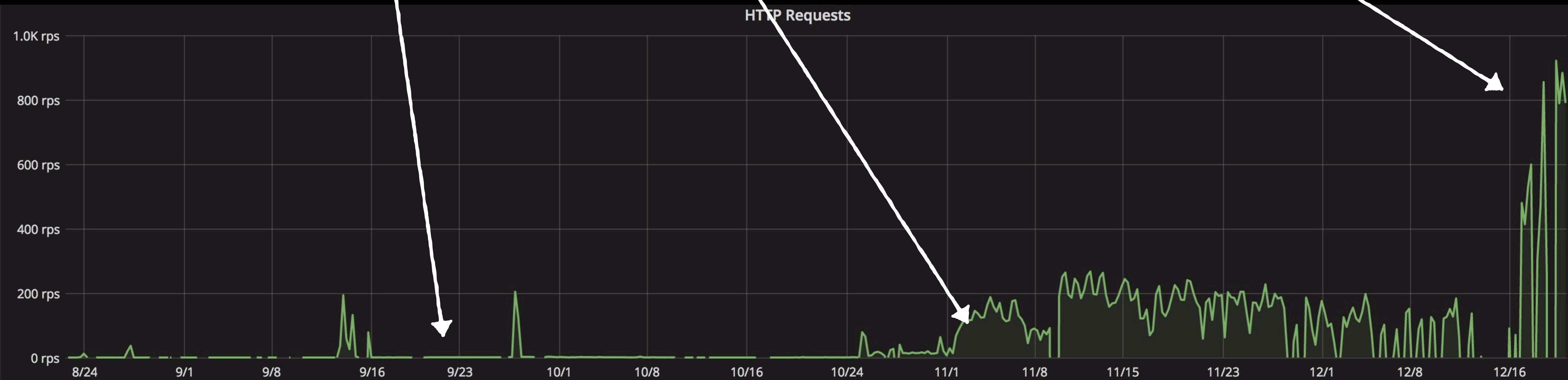
You may already be using it

- Firefox Nightly
- Chrome Beta (50%) / Canary

■ Secure Connection

The connection to this site is encrypted and authenticated using a strong protocol (TLS 1.3), a strong key exchange (X25519), and a strong cipher (AES_128_GCM).

FIREFOX NIGHTLY CHROME FIELD TEST
CLOUDFLARE LAUNCH





<https://tlswg.github.io/tls13-spec/>

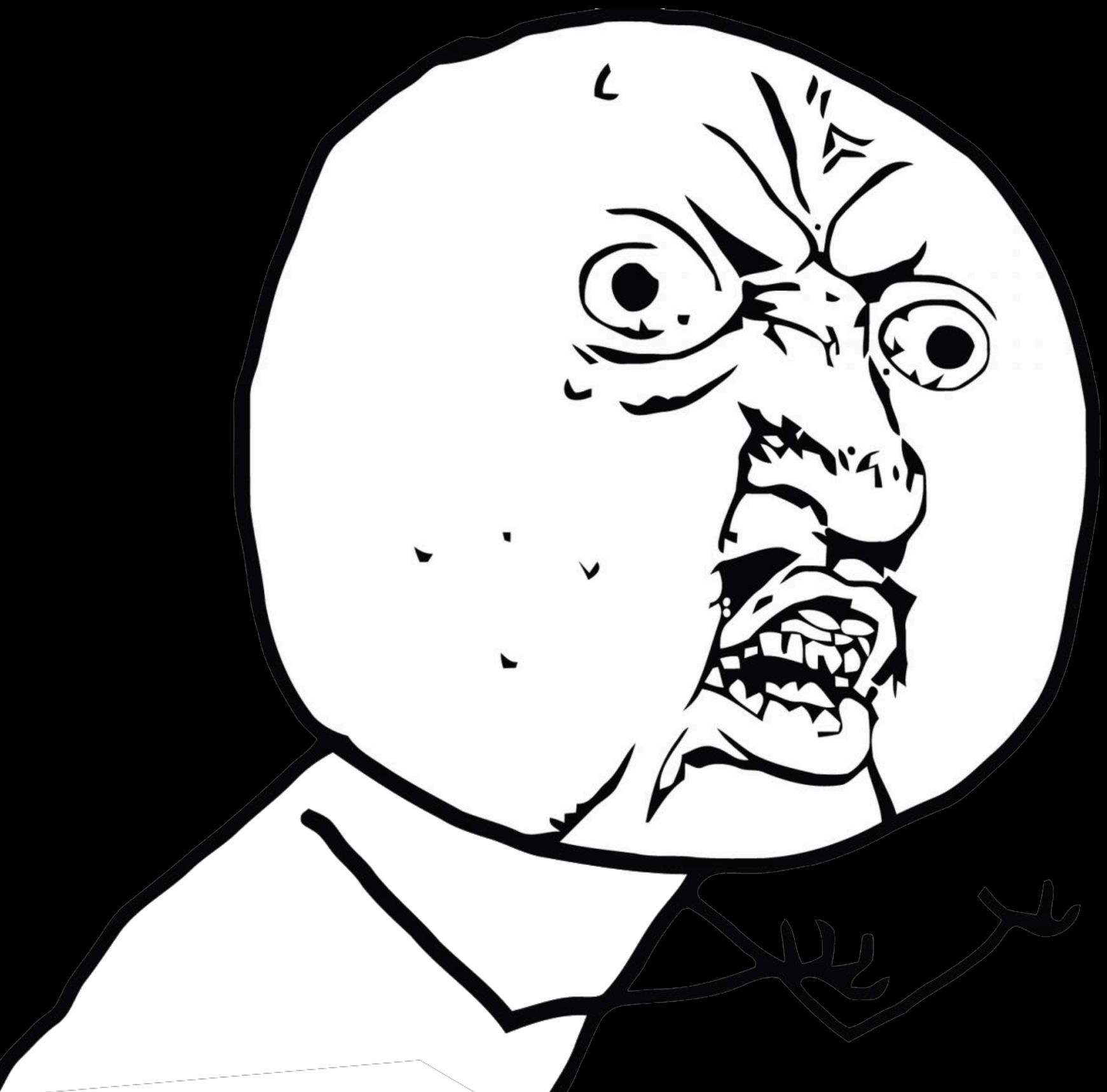
<https://github.com/cloudflare/tls-tris>

<https://blog.cloudflare.com/tag/tls-1-3/>

Nick Sullivan
@grittygrease

Filippo Valsorda
@FiloSottile

Y U NO ENCRYPT SNI!?



TLS 1.3 can't encrypt SNI

