Functionalities

	Functionalities				
Id	HRR	TKT	1RTT	PHA	0RTT
1	no	no	no	no	no
2	no	yes	no	no	no
3	no	yes	yes	no	no
4	no	yes	yes	yes	no
5	no	yes	yes	yes	yes
6	yes	no	no	no	no
7	yes	yes	no	no	no
8	yes	yes	yes	no	no
9	yes	yes	yes	yes	no
10	yes	yes	yes	yes	yes

Behaviors

Id	PSK-DHE	CC	Grease	DHE
1	no	no	no	choice
2	choice	no	no	choice
3	choice	choice	no	choice
4	choice	choice	choice	choice

Agents

Id	TLS Clients	ECH Clients	TLS Server	ECH Server
1	yes	no	yes	no
2	no	yes	no	yes
3	no	yes	yes	yes
4	yes	yes	yes	yes

Safety of Keys, Cipher suites and groups

	Compromised Keys Allowed				Cipher Suites and group	
Id	HPKE Priv	External PSK	Ticket PSK	Signing Key	Multiple	Weak Crypto
1	yes	yes	yes	no	no	no
2	yes	yes	yes	yes	no	no
3	yes	yes	yes	yes	yes	no

Summary Verification

Status	Description	Reachability		Equivalence		Total	
Verified	In green	358	60 %	208	69 %	566	63 %
Stoped (OOM)	In yellow	38	6 %	20	7 %	58	7 %
Ignored (previous OOM)	In yellow (-500GB)	192	32 %	67	22 %	259	29 %
Remaining to Verify	In red	4	1 %	5	2 %	9	1 %
Total		592	100 %	300	100 %	892	100 %

Number of of possible scenarios per query	480

Security properties (Reachability)

	Details
Key Secrecy (SEC), Key Uniqueness (UNIQ)	Includes secrecy of client_write_key and server_write_key for Application Data record. Also includes synchronisation of exporter_master_key and resumption master key
Authentication (CAUTH, SAUTH, AGR)	Injective agreement ClientFinished => PreServerFinished and ServerFinished => ClientFinished
ECH Downgrade Resilience (DOWN)	If ClientFinished, ServerFinished, Sever Run ECH with some config and client offered to do ECH with that same config then both Client and Server accepted ECH
0RTT Secrecy (SEC0), 0RTT Authenticity	Secrecy of the msg + injective agreement ServerReceived0 ==> ClientReceived0.
	The injectivity is guaranteed by modeling the Single-Use ticket (8.1 RFC TLS)
Key_sequentiality	Properties on how PSK can be compromised. Three important events: ServerNewTicket (indicates the new psk on the server side), Client_PSKChoosen (the psk choosen on the client side) and UnsafePSK (Indicates a new psk on the client side that may be know by the attacker)
	Intuitively, if ServerNewTicket(psk) && attacker(psk) then the client must have been played by the attacker using either noPSK or a compromised PSK or a psk generated by a previous server with whom the attacker also played the client (sequentiallity of compromised key typically)

	Details
	If UnsafePsk(psk) && attacker(psk) then the server must have been played by the attacker and it either compromised the long term key of the server or used and knows an old compromised psk or an unsafe psk or a psk generated by an honest server without whom the attacker played the role of the client.
Post-Handshake Authentication (PHA CAUTH)	Injective agreement ClientFinishedPH => ServerRequestPH and ServerFinishedPH => ClientFinishedPH
1RTT Forward Secrecy (FS), 1RTT Stream Integrity (INT)	Secrecy of what the client sends and receives + secrecy of what the server sends + Injective agreement ClientReceives => ServerSends and ServerReceives => ClientSends

Security properties (Equivalence)

	Details
Server Identity Privacy (SIP)	Assumption of uncompromised ECH config + the attacker is not allowed to compromised the PSK obtained from the handshake with BackendA/BackendB
Client Extension Privacy (C-EXT)	Assumption of uncompromised ECH config
Server Extension Privacy (S-EXT)	Assumption of safe PSK or honest DH share by the client (otherwise it's directly visible by the attacker that can impersonate the client)
Key Indistinguishability (IND)	The PSK that are assimilated as a random on one side and the real value on the other side are one that were not already deducible by the attacker before compromising it.
TLS Client Identity Privacy and Unlinkability (TLS-CIP, TLS-UNL)	Assumption of unique usage of PSK + uncompromised PSK (for the sessions where we have clientA vs clientB)
ECH Client Identity Privacy and Unlinkability (ECH-CIP, ECH-UNL)	Assumption of no grease (otherwise it's like TLS client) and uncompromised ECH config => No assumption for PSK.

Key Secrecy (SEC), Key Uniqueness (UNIQ) - Time

6	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	0h 0min	0h 1min	0h 4min	0h 12min	0h 6min	0h 18min
	3	0h 1min	0h 1min	0h 15min	0h 55min	0h 18min	1h 10min
3	2	0h 0min	0h 1min	0h 5min	0h 13min	0h 7min	0h 20min
	3	0h 1min	0h 2min	0h 16min	0h 57min	0h 20min	1h 12min
4	2	0h 1min	0h 2min	0h 8min	0h 22min	0h 12min	0h 35min
	3	0h 1min	0h 3min	0h 29min	-1h 0min	0h 38min	-48h 0min
5	2	0h 1min	0h 2min	0h 8min	0h 22min	0h 12min	0h 36min
	3	0h 1min	0h 3min	0h 30min	-48h 0min	0h 38min	-48h 0min
7	2	0h 1min	0h 3min	0h 27min	1h 8min	0h 32min	1h 23min
	3	0h 2min	0h 5min	1h 13min	-1h 44min	1h 19min	-48h 0min
8	2	0h 1min	0h 3min	0h 32min	1h 19min	0h 36min	1h 44min
	3	0h 2min	0h 5min	1h 21min	-48h 0min	1h 34min	-48h 0min
9	2	0h 2min	0h 6min	0h 55min	2h 17min	1h 4min	2h 48min
	3	0h 4min	0h 10min	-1h 51min	-48h 0min	-48h 0min	-48h 0min
10	2	0h 2min	0h 6min	0h 54min	-1h 54min	1h 5min	-1h 32min
	3	0h 3min	0h 10min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
Data		96	78	18	13		

SEC, UNIQ - Memory

6	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	0,7GB	1,6GB	4,3GB	13GB	6,5GB	20GB
	3	1,2GB	3,2GB	20GB	70GB	23GB	92GB
3	2	0,8GB	1,9GB	4,9GB	15GB	6,5GB	23GB
	3	1,2GB	3,7GB	20GB	70GB	26GB	92GB
4	2	1,4GB	4,3GB	9,9GB	35GB	15GB	61GB
	3	2,8GB	7,5GB	46GB	-122GB	61GB	-500GB
5	2	1,4GB	4,3GB	9,9GB	35GB	15GB	61GB
	3	2,5GB	7,5GB	46GB	-500GB	61GB	-500GB
7	2	1,4GB	4,3GB	15GB	40GB	17GB	61GB
	3	2,8GB	8,6GB	53GB	-122GB	70GB	-500GB
8	2	1,6GB	4,3GB	15GB	46GB	20GB	61GB
	3	3,2GB	9,9GB	61GB	-500GB	70GB	-500GB
9	2	3,2GB	11GB	30GB	106GB	46GB	162GB
	3	7,5GB	23GB	-122GB	-500GB	-500GB	-500GB
10	2	3,2GB	11GB	30GB	-106,2GB	46GB	-92,4GB
	3	7,5GB	23GB	-500GB	-500GB	-500GB	-500GB

Authentication (CAUTH, SAUTH, AGR) - Time

7	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	0h 1min	0h 2min	0h 9min	0h 21min	0h 12min	0h 33min
	3	0h 1min	0h 3min	0h 28min	-1h 12min	0h 35min	-48h 0min
3	2	0h 1min	0h 2min	0h 10min	0h 25min	0h 14min	0h 39min
	3	0h 1min	0h 3min	0h 33min	-48h 0min	0h 42min	-48h 0min
4	2	0h 1min	0h 3min	0h 17min	0h 42min	0h 24min	1h 9min
	3	0h 2min	0h 5min	0h 58min	-48h 0min	-0h 53min	-48h 0min
5	2	0h 1min	0h 3min	0h 17min	0h 43min	0h 24min	-0h 44min
	3	0h 2min	0h 5min	1h 0min	-48h 0min	-48h 0min	-48h 0min
7	2	0h 2min	0h 5min	1h 0min	2h 20min	1h 8min	2h 51min
	3	0h 3min	0h 9min	-2h 24min	-48h 0min	-48h 0min	-48h 0min
8	2	0h 3min	0h 6min	1h 13min	3h 0min	1h 21min	3h 26min
	3	0h 4min	0h 10min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
9	2	0h 4min	0h 11min	1h 59min	-1h 51min	-1h 33min	-1h 27min
	3	0h 7min	0h 18min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
10	2	0h 4min	0h 11min	2h 1min	-48h 0min	2h 19min	-48h 0min
	3	0h 7min	0h 18min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
Data		96	64	32	25		

CAUTH, SAUTH, AGR - Memory

7	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	1,2GB	3,7GB	8,6GB	30GB	13GB	46GB
	3	2,5GB	7,5GB	40GB	-140,8GB	53GB	-500GB
3	2	1,4GB	4,3GB	9,9GB	35GB	15GB	53GB
	3	2,8GB	8,6GB	46GB	-500GB	61GB	-500GB
4	2	2,8GB	8,6GB	23GB	80GB	30GB	122GB
	3	5,7GB	17GB	106GB	-500GB	-97,8GB	-500GB
5	2	2,8GB	8,6GB	20GB	80GB	30GB	-92,4GB
	3	5,7GB	17GB	106GB	-500GB	-500GB	-500GB
7	2	2,8GB	8,6GB	30GB	92GB	40GB	141GB
	3	6,5GB	20GB	-122GB	-500GB	-500GB	-500GB
8	2	3,2GB	9,9GB	35GB	106GB	46GB	162GB
	3	7,5GB	23GB	-500GB	-500GB	-500GB	-500GB
9	2	6,5GB	23GB	70GB	-122GB	-92,4GB	-110,7GB
	3	15GB	46GB	-500GB	-500GB	-500GB	-500GB
10	2	6,5GB	23GB	70GB	-500GB	92GB	-500GB
	3	15GB	46GB	-500GB	-500GB	-500GB	-500GB

0RTT Secrecy and Authenticity (SEC0) - Time

8	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
5	2	0h 1min	0h 2min	0h 6min	0h 16min	0h 9min	0h 27min
	3	0h 1min	0h 3min	0h 23min	1h 21min	0h 29min	-1h 34min
10	2	0h 2min	0h 5min	0h 50min	1h 55min	0h 55min	-2h 4min
	3	0h 3min	0h 9min	-1h 52min	-1h 45min	-1h 38min	-1h 25min
Data		24	18	6	0		

SEC0 - Memory

8	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
5	2	1,4GB	4,3GB	9,9GB	30GB	15GB	53GB
	3	2,8GB	8,6GB	46GB	162GB	61GB	-213,5GB
10	2	3,7GB	11GB	30GB	92GB	40GB	-140,8GB
	3	7,5GB	23GB	-122GB	-140,8GB	-122GB	-109,4GB

1RTT Forward Secrecy and Stream Integrity (FS, INT) - Time

9	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
3	2	0h 1min	0h 4min	0h 25min	1h 42min	0h 44min	3h 40min
	3	0h 2min	0h 6min	1h 37min	-1h 5min	2h 23min	-48h 0min
4	2	0h 27min	1h 1min	-11h 13min	-2h 11min	-48h 0min	-48h 0min
	3	0h 35min	1h 18min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
5	2	0h 26min	1h 0min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
	3	0h 37min	1h 14min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
8	2	0h 4min	0h 16min	-16h 26min	-33h 58min	-48h 0min	-48h 0min
	3	0h 6min	0h 23min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
9	2	6h 30min	-1h 33min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
	3	8h 2min	-48h 0min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
10	2	6h 19min	-48h 0min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
	3	8h 2min	-48h 0min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
Data		72	26	46	40		

FS, INT - Memory

9	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
3	2	1,2GB	3,2GB	9,9GB	30GB	13GB	46GB
	3	2,1GB	6,5GB	40GB	-106,2GB	46GB	-500GB
4	2	17GB	70GB	-116,9GB	-138,5GB	-500GB	-500GB
	3	20GB	80GB	-500GB	-500GB	-500GB	-500GB
5	2	17GB	70GB	-500GB	-500GB	-500GB	-500GB
	3	21GB	80GB	-500GB	-500GB	-500GB	-500GB
8	2	2,8GB	8,6GB	-106,2GB	-106,2GB	-500GB	-500GB
	3	5,7GB	20GB	-500GB	-500GB	-500GB	-500GB
9	2	61GB	-80,4GB	-500GB	-500GB	-500GB	-500GB
	3	106GB	-500GB	-500GB	-500GB	-500GB	-500GB
10	2	61GB	-500GB	-500GB	-500GB	-500GB	-500GB
	3	106GB	-500GB	-500GB	-500GB	-500GB	-500GB

Post-Handshake Authentication (PHA CAUTH) - Time

10	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
4	2	0h 4min	0h 17min	1h 52min	-5h 21min	2h 36min	-3h 55min
	3	0h 7min	0h 26min	-6h 55min	-48h 0min	-48h 0min	-48h 0min
5	2	0h 5min	0h 18min	1h 55min	-48h 0min	2h 39min	-48h 0min
	3	0h 7min	0h 27min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
9	2	0h 14min	0h 51min	-10h 19min	-48h 0min	-48h 0min	-48h 0min
	3	0h 22min	1h 26min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
10	2	0h 14min	0h 54min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
	3	0h 22min	1h 28min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
Data		48	20	28	24		

PHA CAUTH - Memory

10	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
4	2	4,9GB	17GB	40GB	-161,7GB	61GB	-208,7GB
	3	9,9GB	35GB	-80,4GB	-500GB	-500GB	-500GB
5	2	4,9GB	17GB	40GB	-500GB	61GB	-500GB
	3	9,9GB	35GB	-500GB	-500GB	-500GB	-500GB
9	2	11GB	46GB	-122GB	-500GB	-500GB	-500GB
	3	26GB	92GB	-500GB	-500GB	-500GB	-500GB
10	2	11GB	46GB	-500GB	-500GB	-500GB	-500GB
	3	26GB	92GB	-500GB	-500GB	-500GB	-500GB

ECH Downgrade Resilience (DOWN) - Time

11	A	2		4	
	B	2	3	2	3
F	S				
2	2	0h 27min	1h 25min	0h 34min	1h 54min
	3	-27h 10min	-48h 0min	-48h 0min	-48h 0min
3	2	0h 34min	1h 46min	0h 44min	2h 21min
	3	-48h 0min	-48h 0min	-48h 0min	-48h 0min
4	2	0h 51min	2h 39min	1h 7min	-2h 42min
	3	-48h 0min	-48h 0min	-48h 0min	-48h 0min
5	2	0h 51min	2h 43min	1h 7min	-48h 0min
	3	-48h 0min	-48h 0min	-48h 0min	-48h 0min
7	2	24h 20min	-23h 11min	24h 55min	-48h 0min
	3	-48h 0min	-48h 0min	-48h 0min	-48h 0min
8	2	32h 16min	-48h 0min	34h 16min	-48h 0min
	3	-48h 0min	-48h 0min	-48h 0min	-48h 0min
9	2	0h 0min	-48h 0min	0h 0min	-48h 0min
	3	-48h 0min	-48h 0min	-48h 0min	-48h 0min
10	2	0h 0min	-48h 0min	0h 0min	-48h 0min
	3	-48h 0min	-48h 0min	-48h 0min	-48h 0min
Data		64	18	42	39

DOWN - Memory

11	A	2		4	
	B	2	3	2	3
F	S				
2	2	8,6GB	26GB	13GB	46GB
	3	-92,4GB	-500GB	-500GB	-500GB
3	2	9,9GB	30GB	15GB	53GB
	3	-500GB	-500GB	-500GB	-500GB
4	2	20GB	70GB	30GB	-106,2GB
	3	-500GB	-500GB	-500GB	-500GB
5	2	20GB	70GB	30GB	-500GB
	3	-500GB	-500GB	-500GB	-500GB
7	2	46GB	-80,4GB	53GB	-500GB
	3	-500GB	-500GB	-500GB	-500GB
8	2	53GB	-500GB	61GB	-500GB
	3	-500GB	-500GB	-500GB	-500GB
9	2	0GB	-500GB	0GB	-500GB
	3	-500GB	-500GB	-500GB	-500GB
10	2	0GB	-500GB	0GB	-500GB
	3	-500GB	-500GB	-500GB	-500GB

Key sequentiality - Time

12	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	0h 0min	0h 1min	0h 6min	0h 18min	0h 9min	0h 29min
	3	0h 1min	0h 2min	0h 23min	1h 20min	0h 29min	1h 44min
3	2	0h 1min	0h 1min	0h 7min	0h 19min	0h 10min	0h 31min
	3	0h 1min	0h 2min	0h 26min	-0h 58min	0h 32min	-48h 0min
4	2	0h 1min	0h 2min	0h 10min	0h 29min	0h 15min	0h 52min
	3	0h 1min	0h 4min	0h 37min	-48h 0min	0h 48min	-48h 0min
5	2	0h 1min	0h 2min	0h 10min	0h 29min	0h 14min	0h 46min
	3	0h 1min	0h 4min	0h 36min	-48h 0min	0h 47min	-48h 0min
7	2	0h 2min	0h 4min	1h 31min	5h 0min	1h 36min	5h 23min
	3	0h 2min	0h 7min	3h 4min	-1h 32min	3h 23min	-48h 0min
8	2	0h 2min	0h 4min	1h 39min	5h 26min	1h 46min	5h 50min
	3	0h 3min	0h 7min	3h 22min	-48h 0min	3h 35min	-48h 0min
9	2	0h 3min	0h 7min	2h 1min	-1h 25min	2h 11min	-48h 0min
	3	0h 4min	0h 12min	-2h 9min	-48h 0min	-48h 0min	-48h 0min
10	2	0h 2min	0h 7min	2h 5min	-48h 0min	2h 12min	-48h 0min
	3	0h 4min	0h 12min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
Data		96	74	22	18		

Key sequentiality - Memory

12	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	0,9GB	2,5GB	6,5GB	20GB	8,6GB	30GB
	3	1,6GB	4,9GB	26GB	92GB	35GB	122GB
3	2	1,1GB	2,5GB	6,5GB	20GB	9,9GB	35GB
	3	1,9GB	4,9GB	30GB	-106,2GB	35GB	-500GB
4	2	1,6GB	4,9GB	13GB	40GB	17GB	70GB
	3	3,2GB	8,6GB	61GB	-500GB	70GB	-500GB
5	2	1,6GB	4,9GB	13GB	40GB	17GB	70GB
	3	3,2GB	8,6GB	61GB	-500GB	70GB	-500GB
7	2	2,1GB	6,5GB	23GB	61GB	30GB	92GB
	3	4,3GB	13GB	80GB	-138,6GB	106GB	-500GB
8	2	2,1GB	6,5GB	23GB	70GB	30GB	92GB
	3	4,3GB	13GB	92GB	-500GB	106GB	-500GB
9	2	3,7GB	13GB	40GB	-80,4GB	53GB	-500GB
	3	8,6GB	26GB	-158,6GB	-500GB	-500GB	-500GB
10	2	3,7GB	13GB	40GB	-500GB	53GB	-500GB
	3	8,6GB	26GB	-500GB	-500GB	-500GB	-500GB

Lemma - Time

5	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	0h 3min	0h 4min	0h 22min	0h 42min	0h 30min	1h 10min
	3	0h 3min	0h 6min	0h 55min	2h 35min	1h 8min	3h 33min
3	2	0h 2min	0h 4min	0h 23min	0h 41min	0h 29min	1h 10min
	3	0h 3min	0h 6min	0h 55min	2h 34min	1h 10min	3h 38min
4	2	0h 3min	0h 5min	0h 26min	0h 48min	0h 34min	1h 24min
	3	0h 4min	0h 8min	1h 10min	-1h 15min	1h 27min	-48h 0min
5	2	0h 3min	0h 5min	0h 25min	0h 49min	0h 37min	1h 26min
	3	0h 4min	0h 8min	1h 8min	-48h 0min	1h 28min	-48h 0min

Lemma - Memory

5	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
2	2	1,3GB	2,2GB	7,5GB	15GB	11GB	23GB
	3	2,1GB	3,8GB	24GB	64GB	30GB	80GB
3	2	1,3GB	1,9GB	6,8GB	14GB	9,9GB	21GB
	3	2,1GB	3,9GB	23GB	64GB	30GB	80GB
4	2	1,4GB	4,3GB	8,6GB	26GB	13GB	53GB
	3	2,5GB	7,5GB	40GB	-140,8GB	53GB	-500GB
5	2	1,4GB	4,3GB	8,6GB	26GB	13GB	53GB
	3	2,5GB	7,5GB	40GB	-500GB	53GB	-500GB

5	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
7	2	0h 9min	0h 15min	-3h 49min	-48h 0min	-4h 7min	-48h 0min
	3	0h 12min	0h 21min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
8	2	0h 8min	0h 14min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
	3	0h 12min	0h 21min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
9	2	0h 10min	0h 17min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
	3	0h 14min	0h 27min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
10	2	0h 10min	0h 18min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
	3	0h 14min	0h 27min	-48h 0min	-48h 0min	-48h 0min	-48h 0min
Data		96	60	36	33		

5	A	1		2		4	
	B	2	3	2	3	2	3
F	S						
7	2	3,2GB	5,2GB	-251,8GB	-500GB	-214,3GB	-500GB
	3	5,9GB	11GB	-500GB	-500GB	-500GB	-500GB
8	2	3,2GB	4,9GB	-500GB	-500GB	-500GB	-500GB
	3	5,9GB	11GB	-500GB	-500GB	-500GB	-500GB
9	2	3,4GB	9,9GB	-500GB	-500GB	-500GB	-500GB
	3	6,5GB	23GB	-500GB	-500GB	-500GB	-500GB
10	2	3,2GB	9,9GB	-500GB	-500GB	-500GB	-500GB
	3	6,5GB	23GB	-500GB	-500GB	-500GB	-500GB

Key Indistinguishability (IND) - Time

13	A	1			2			4		
	B	1	2	3	1	2	3	1	2	3
F	S									
2	1	0h 1min	0h 10min	0h 23min	0h 7min	5h 42min	9h 30min	0h 11min	8h 51min	21h 16min
	2	0h 2min	0h 21min	1h 24min	0h 23min	14h 53min	-11h 6min	0h 31min	20h 33min	-48h 0min
7	1	0h 1min	0h 30min	1h 18min	5h 27min	-33h 3min	-33h 16min	3h 45min	-48h 0min	-48h 0min
	2	0h 3min	1h 10min	4h 49min	19h 11min	-48h 0min	-48h 0min	12h 47min	-48h 0min	-48h 0min
Data		36	26	10	7					

IND - Memory

13	A	1			2			4		
	B	1	2	3	1	2	3	1	2	3
F	S									
2	1	0,6GB	2,6GB	4,5GB	2,6GB	22GB	45GB	4GB	35GB	79GB
	2	0,8GB	4,2GB	15GB	5,2GB	39GB	-122GB	7GB	69GB	-500GB
7	1	0,8GB	5,3GB	12GB	19GB	-92,4GB	-80,4GB	15GB	-500GB	-500GB
	2	1,3GB	10GB	34GB	52GB	-500GB	-500GB	37GB	-500GB	-500GB

Server Identity Privacy (SIP) - Time

14	A	2			4		
	B	1	2	3	1	2	3
F	S						
1	1	0h 1min	0h 53min	2h 8min	0h 2min	2h 9min	4h 54min
	2	0h 3min	1h 49min	8h 27min	0h 4min	3h 54min	20h 7min
2	1	0h 20min	24h 27min	-41h 57min	0h 35min	-8h 27min	-48h 0min
	2	0h 57min	-9h 42min	-48h 0min	1h 26min	-7h 24min	-48h 0min
6	1	0h 22min	-48h 0min	-48h 0min	0h 20min	-48h 0min	-48h 0min
	2	1h 13min	-48h 1min	-48h 0min	1h 3min	-48h 0min	-48h 0min
7	1	8h 46min	-48h 0min	-48h 0min	6h 40min	-48h 0min	-48h 0min
	2	0h 0min	-48h 0min	-48h 0min	20h 48min	-48h 0min	-48h 0min
Data		48	24	23	17		

SIP - Memory

14	A	2			4		
	B	1	2	3	1	2	3
F	S						
1	1	1,4GB	9,9GB	17GB	1,6GB	15GB	30GB
	2	2,2GB	17GB	46GB	2,5GB	26GB	70GB
2	1	3,2GB	46GB	-92,4GB	4,9GB	-133,9GB	-500GB
	2	7,5GB	-92,4GB	-500GB	11GB	-106,2GB	-500GB
6	1	4,9GB	-70GB	-500GB	4,9GB	-500GB	-500GB
	2	11GB	-80,4GB	-500GB	11GB	-500GB	-500GB
7	1	23GB	-500GB	-500GB	20GB	-500GB	-500GB
	2	0GB	-500GB	-500GB	53GB	-500GB	-500GB

TLS Client Identity Privacy and Unlinkability (TLS-CIP, TLS-UNL) - Time

15	A	1			4		
	B	1	2	3	1	2	3
F	S						
1	1	0h 0min	0h 1min	0h 3min	0h 1min	1h 47min	4h 35min
	2	0h 0min	0h 2min	0h 8min	0h 3min	3h 27min	16h 10min
2	1	0h 2min	1h 2min	2h 31min	0h 25min	-5h 24min	-48h 0min
	2	0h 4min	2h 15min	9h 2min	1h 8min	-48h 0min	-48h 0min
6	1	0h 1min	0h 4min	0h 9min	0h 14min	-48h 1min	-48h 0min
	2	0h 1min	0h 7min	0h 31min	0h 40min	-48h 0min	-48h 0min
7	1	0h 4min	3h 26min	8h 20min	4h 16min	-48h 0min	-48h 0min
	2	0h 8min	7h 52min	-4h 15min	15h 6min	-48h 0min	-48h 0min
Data		48	35	13	10		

TLS-CIP, TLS-UNL - Memory

15	A	1			4		
	B	1	2	3	1	2	3
F	S						
1	1	0,6GB	1,2GB	1,9GB	1,4GB	13GB	23GB
	2	0,7GB	1,7GB	3,7GB	2,1GB	23GB	61GB
2	1	0,7GB	9,1GB	20GB	4,3GB	-106,2GB	-500GB
	2	1,1GB	15GB	61GB	10GB	-500GB	-500GB
6	1	0,7GB	2,5GB	4,3GB	3,7GB	-80,4GB	-500GB
	2	0,8GB	3,7GB	9,9GB	8,6GB	-500GB	-500GB
7	1	1GB	30GB	70GB	17GB	-500GB	-500GB
	2	1,9GB	46GB	-213,5GB	46GB	-500GB	-500GB

Special cases TLS-CIP, TLS-UNL

PHA-CC-S2-A1	0h 16min	15GB
PHA-B3-S2-A1	0h 0min	
HRR-PHA-B3-S2-A1	0h 0min	

ECH Client Identity Privacy and Unlinkability (ECH-CIP, ECH-UNL) -

16	A	2			4		
54	B	1	2	3	1	2	3
F	S						
1	1	0h 1min	0h 44min	2h 51min	0h 2min	2h 50min	6h 34min
	2	0h 2min	2h 8min	9h 38min	0h 3min	4h 38min	21h 42min
2	1	0h 18min	35h 22min	0h 0min	0h 32min	0h 0min	0h 0min
	2	0h 52min	-10h 14min	-48h 0min	1h 22min	-48h 0min	-48h 0min
6	1	0h 22min	-48h 1min	-48h 0min	0h 20min	-48h 0min	-48h 0min
	2	1h 3min	-48h 1min	-48h 0min	0h 57min	-48h 0min	-48h 0min
7	1	8h 35min	-48h 0min	-48h 0min	6h 39min	-48h 0min	-48h 0min
	2	0h 0min	-48h 0min	-48h 0min	21h 11min	-48h 0min	-48h 0min
Data		48	24	20	17		

ECH-CIP, ECH-UNL - Memory

16	A	2			4		
	B	1	2	3	1	2	3
F	S						
1	1	1,4GB	8,6GB	20GB	1,6GB	17GB	35GB
	2	2,1GB	17GB	53GB	2,5GB	26GB	80GB
2	1	3,2GB	53GB	0GB	4,9GB	0GB	0GB
	2	7,8GB	-92,4GB	-500GB	11GB	-500GB	-500GB
6	1	4,9GB	-70GB	-500GB	4,9GB	-500GB	-500GB
	2	11GB	-92,4GB	-500GB	11GB	-500GB	-500GB
7	1	23GB	-500GB	-500GB	20GB	-500GB	-500GB
	2	0GB	-500GB	-500GB	53GB	-500GB	-500GB

Special cases ECH-CIP, ECH-UNL

PHA-A2-S2-B1	0h 57min	46GB
PHA-CC-A2-S2-B1	3h 27min	141GB
HRR-CC-A2-S2	4h 34min	214GB
HRR-PHA-CC-A2-S2	-17h 42min	-245GB

Client Extension Privacy (C-EXT) - Time

18	A	2			4		
	B	1	2	3	1	2	3
F	S						
1	1	0h 1min	0h 4min	0h 7min	0h 1min	0h 9min	0h 19min
	2	0h 1min	0h 9min	0h 25min	0h 2min	0h 22min	1h 18min
2	1	0h 2min	0h 50min	1h 59min	0h 5min	1h 45min	4h 9min
	2	0h 23min	5h 55min	-13h 32min	0h 28min	9h 13min	-48h 0min
6	1	0h 2min	0h 36min	1h 5min	0h 3min	1h 14min	2h 35min
	2	0h 6min	1h 39min	5h 14min	0h 8min	3h 31min	13h 1min
7	1	0h 13min	-8h 15min	-48h 0min	0h 22min	-48h 0min	-48h 0min
	2	2h 37min	-48h 0min	-48h 0min	3h 9min	-48h 0min	-48h 0min
Data		48	38	10	8		

C-EXT - Memory

18	A	2			4		
	B	1	2	3	1	2	3
F	S						
1	1	0,9GB	2,8GB	4,3GB	1,1GB	4,3GB	7,5GB
	2	1,2GB	4,3GB	9,9GB	1,6GB	7,4GB	17GB
2	1	1,7GB	11GB	29GB	2,6GB	22GB	52GB
	2	6,2GB	42GB	-92,4GB	6,7GB	51GB	-500GB
6	1	1,6GB	9,9GB	17GB	1,9GB	15GB	26GB
	2	3,2GB	20GB	46GB	3,7GB	30GB	70GB
7	1	4,2GB	-112,6GB	-500GB	6,4GB	-500GB	-500GB
	2	30GB	-500GB	-500GB	33GB	-500GB	-500GB

Server Extension Privacy (S-EXT) - Time

17	A	1			2			4		
	B	1	2	3	1	2	3	1	2	3
F	S									
1	1	0h 0min	0h 1min	0h 1min	0h 1min	0h 6min	0h 14min	0h 1min	0h 14min	0h 34min
	2	0h 0min	0h 1min	0h 3min	0h 1min	0h 11min	0h 38min	0h 2min	0h 26min	1h 40min
2	1	0h 1min	0h 7min	0h 16min	0h 3min	1h 2min	2h 34min	0h 5min	2h 19min	6h 15min
	2	0h 2min	0h 27min	1h 21min	0h 19min	5h 48min	-1h 37min	0h 25min	10h 39min	-48h 0min
6	1	0h 0min	0h 1min	0h 3min	0h 2min	1h 10min	3h 22min	0h 3min	2h 46min	8h 19min
	2	0h 1min	0h 3min	0h 7min	0h 6min	3h 19min	15h 5min	0h 9min	7h 14min	-20h 42min
7	1	0h 1min	0h 22min	0h 49min	0h 15min	-11h 52min	-48h 0min	0h 24min	-48h 0min	-48h 0min
	2	0h 4min	1h 25min	4h 6min	2h 24min	-48h 0min	-48h 0min	2h 55min	-48h 0min	-48h 0min
Data		72	61	11	8					

S-EXT - Memory

17	A	1			2			4		
	B	1	2	3	1	2	3	1	2	3
F	S									
1	1	0,6GB	0,9GB	1,2GB	0,9GB	3,2GB	6,5GB	1,1GB	5,7GB	11GB
	2	0,6GB	1,2GB	2,1GB	1,4GB	5GB	13GB	1,6GB	8,6GB	23GB
2	1	0,6GB	2,4GB	4,5GB	1,9GB	14GB	35GB	3GB	26GB	69GB
	2	0,9GB	4,6GB	15GB	5,2GB	39GB	-87,2GB	7,4GB	65GB	-500GB
6	1	0,6GB	1,4GB	2,1GB	1,9GB	13GB	26GB	2,1GB	23GB	46GB
	2	0,7GB	2,1GB	4,3GB	3,2GB	26GB	70GB	4,3GB	40GB	-70GB
7	1	0,8GB	5,2GB	10GB	4,5GB	-98GB	-500GB	7,3GB	-500GB	-500GB
	2	1,5GB	10GB	38GB	26GB	-500GB	-500GB	29GB	-500GB	-500GB