Apple Private Relay Questions

Technical Details

1. What protocols (particularly IETF protocols) will be used and how? For example, is MASQUE going to be used?

2. How exactly is ODoH used within private relay?

3. ODoH isn't finished in the IETF, how will Apple deal with version differences? Or will Apple wait until ODoH is finished before deploying?

4. Is OHTTP used within Private Relay? Will it be?

5. What is the hostname of the iCloud Private Relay proxy server?

6. Are other Apple services associated with the hostname? If so, which ones?

7. Will a single client device use a single Private Relay tunnel per network? Or can it use multiple tunnels, even through a single network? If so, when are these set up and torn down?
8. Which applications other than Safari use Private Relay?

Ingress Proxies:

9. Which company or companies provide the hosting for ingress proxies?

Egress Proxies:

10. Will Apple work with different Egress proxy providers in different territories? For example, is it likely that there will be a different provider in Europe compared to the US? Will there be multiple providers in some/all territories?

11. Which companies Apple will work with as egress proxies? How were these companies chosen? Will the list be expanded over time?

12. What are the transparency and privacy policy requirements that Apple has placed on the egress proxy operators? How will these be audited?

13. Does Apple guarantee that there will be no collusion between the Ingress and Egress proxies?

14. Will Apple ever operate Egress proxies?

User Experience

15. Is the user experience of accessing a network where the iCloud Private Relay proxy server hostname is blocked different if the user is connected to a cellular data connection, WI-FI, or an Ethernet network?

16. If the IP addresses associated with the iCloud Private Relay proxy server are blocked, are other Apple services impacted?

17. Some service providers provide device-agnostic opt-in security and parental control services using DNS and/or DPI. Is Apple taking any steps to prevent service providers from blocking access to the iCloud Private Relay proxy server for opt-in subscribers on their networks.

18. Could network operators opt out of Private Relay for individual connections, for example to respect customer requirements for parental controls? What user dialogue will Apple present to explain the impact of using Private Relay on parental controls, malware filtering etc?

19. In the release version of iOS15, will Apple private relay be turned on by default?

20. What happens in the event that the Private Relay service is not working correctly? What will the user experience be?

21. Would a user (e.g. an enterprise) be able to run their own ingress proxy or are they limited to using Apple?

22. For Apple users, will Enterprise MDM solutions have the ability to control Apple Private relay behaviour on devices they manage? EG either via 3rd party MDM which will rely on Apple APIs or Apple Business Manager?

23. If the user (or corporate MDM) has specified a DoH server in iOS via a profile (using the functionality added in 14.x), will that DoH server still be used if Apple Private relay is available?

24. If you have an existing DNS provider installed (eg Nextdns) and you then turn on Apple Private relay which service gets precedence for your Safari DNS queries?

25. What changes will users without iCloud+ experience? For example, will they also use ODoH?

26. What are Apple's plans for further rollout beyond iCloud+ users? Is there a plan to make this new functionality free for Apple users in the long term?

27. Many websites require an increased level of authentication if the client is connecting from:
    a. An address that is not your usual ISP, or
    b. An address shared by thousands of others and has previously seen some malicious activity.

    Are you measuring the extent to which Private Relay drives this website response?

Network

28. QUIC encapsulation adds transmission overhead. This is probably not a problem on the downlink (mast to device), but could impact uplink (device to mast) as that is typically scaled for significantly less capacity than the downlink, and the additional encapsulation may exacerbate performance issues under weaker signal conditions with multiple retransmission attempts etc.

29. QUIC sits atop UDP, which is typically treated as a special case at operator firewalls/CGNATs (e.g. UE-initiated UDP is granted a temporary pinhole in the firewall which closes after a timeout). TCP connections have a stateful mapping at the CGNAT to match outbound to inbound connections, and on average there are 6 TCP connections per Web domain. If these TCP connections are now encapsulated in QUIC/UDP, there is likely to be an impact in scaling and configuration at the firewall/CGNAT.

30. QUIC involves padding for privacy reasons, however mobile networks typically have standard MTUs of about 1500 bytes and maximum segment sizes to avoid fragmentation. If there is a QUIC encapsulation that exceeds the MTU then there could be fragmentation causing configuration problems and a poor user experience. [This may warrant further collaboration between Apple and mobile operators to determine optimal setting(s)].

31. Mobile has historically performed poorly with ‘classic’ TCP algorithms, which wrongly infer packet loss for packets where an ACK has not been received by the sender, but which are undergoing radio-layer retransmission. This disconnect between volatile radio conditions and e2e congestion control results in the inefficient ‘sawtooth’ pattern of sender rate over time. Recent CC-algorithms such as BBRv2 attempt to rather monitor jitter (variance in latency) for finer tuning, so I’d be interested to hear what CC algorithms Apple has in mind for the QUIC encapsulation.

    NB It may be that the above four points are applicable to QUIC rather than being Apple-specific, albeit they still highlight potential challenges, especially on mobile networks.

32. Propagation latency is typically the biggest contributor to e2e latency (notwithstanding poor signal conditions). If the Ingress proxy and Egress proxy are geographically remote to each other this would increase propagation latency significantly on a round trip, so I’d be interested to hear the strategy for ‘good matchmaking’ between ingress and egress.

Geolocation

33. For geolocation purposes, is the intent that the Ingress and Egress proxies will always be in the same country as the user? Are there any circumstances when this will not be true?

34. Noting the potential disruption for serving content efficiently, is there a maximum distance from the user to the Egress proxy?

35. For DNS traffic, how will resolver selection be made? Will resolvers implement any national legislative or regulatory requirements in the country where the user is located? Will malicious content be blocked? CSAM? How will network-based parental control settings be preserved?

36. How will geo-filtering requirements for copyright protection purposes be respected?

Impact Assessments

37. What impact assessments have Apple undertaken on network operations and network performance including DNS and SNI based content filtering, zero rating of traffic, cybersecurity, content caching and peering routes? If none, are these planned and will the results be published?

38. More generally, has Apple done an impact assessment on how this will affect the existing Internet architecture, including security, safety, etc.? If not, is this planned and will the results be published?

39. What other engagement took place concerning the deployment of the service? Have ISPs been consulted on this and, if not, is there a plan to engage with them and the wider stakeholder community ahead of rollout to identify any other potential concerns or unintended consequences?

Geographic Deployment

40. How has the decision been reached to not roll the new functionality out in certain countries and was there any consultation with governments?

41. Is it correct the Private Relay will not operate in China, Belarus, Colombia, Egypt, Kazakhstan, Saudi Arabia, South Africa, Turkmenistan, Uganda and the Philippines?

42. Were countries excluded due to possible conflict with domestic surveillance or anti-encryption laws?

Compliance

43. What support will there be for investigations by law enforcement agencies?

44. Will Private Relay be GDPR compliant? Is Apple acting as a data controller for Private Relay, with the Egress proxy providers acting as data processors?