Request for data collection review for new features of TLS 1.3

1) What questions will you answer with this data?

This data will give us information about how often the Post Handshake Authentication feature and the 0-RTT feature of TLS 1.3 is used.

2) Why does Mozilla need to answer these questions? Are there benefits for users? Do we need this information to address product or business requirements?

This will give us an indication of the adoption rates of new TLS 1.3 features. This data is of benefit to the Cryptography Engineering team as it would like to understand real-world usage of the new TLS 1.3 protocol. Additionally,
I am writing my bachelor thesis about TLS and the adoption of TLS 1.3 in cooperation with Mozilla. This effort is part of the SecEng University Relationship Framework (SURF) initiative at Mozilla.

3) What alternative methods did you consider to answer these questions? Why were they not sufficient?

I looked at all the available telemetry probes Mozilla collects and could not find any probe that answered this question. Since my thesis tries to answer this question with real world data from Firefox I need to collect that data in Firefox directly.

4) Can current instrumentation answer these questions?

Currently we do not have probes that look at the new features of TLS 1.3.

5) List all proposed measurements and indicate the category of data collection for each measurement, using the [Firefox data collection categories](https://wiki.mozilla.org/Firefox/Data_Collection) found on the Mozilla wiki.

Measurement Description	Data Collection Category	Tracking Bug #
Tracking how often the PHA feature of TLS 1.3 is used	Category 1 “Technical data”	Bug 1649472
Tracking how often the 0-RTT feature of TLS 1.3 is used	Category 1 “Technical data”	Bug 1654309

6) Please provide a link to the documentation for this data collection which describes the ultimate data set in a public, complete, and accurate way.

This collection is documented in its definition file Histograms.json and in the Probe Dictionary at https://probes.telemetry.mozilla.org.

The data collection will consist of following probes:

- TLS_1_3_CLIENT_AUTH_USES_PHA
  - A boolean, emitted on each new TLS connection where a client certificate was used, True if that connection used PHA, False otherwise.
- TLS_1_3_USES_0RTT
  - A boolean, emitted on each TLS resumption, True if the resumption used 0RTT and False otherwise.

7) How long will this data be collected?

This is scoped to a time-limited experiment/project until date 03-31-2021.

8) What populations will you measure?

* Which release channels?

All release channels will be measured.

* Which countries?

All countries will be measured.

* Which locales?

All locales will be measured.

9) If this data collection is default on, what is the opt-out mechanism for users?

This data collection can be opt-out through the standard opt-out mechanism.

10) Please provide a general description of how you will analyze this data.

This data will give me information about how many users use these features and how many do not. I will then look at the percentage of connections that use these features to make a statement on the state of the adoption of these features.

11) Where do you intend to share the results of your analysis?

The results will be shared via Mozilla's telemetry portal in my bachelor thesis.

12) Is there a third-party tool (i.e. not Telemetry) that you are proposing to use for this data collection?

No