Problem

Constrained environments using OSCORE in network environments such as NB-IoT, 6TiSCH, and LoRaWAN need a ‘lightweight’ authenticated key exchange (LAKE) that enables forward security. 'Lightweight' refers to:

* resource consumption, measured by bytes on the wire, wall-clock time to complete, or power consumption.
* the amount of new code required on end systems which already have an OSCORE stack.

Goals

This working group is intended to be a narrowly focused activity intended to produce only at most one LAKE and close.

The working group will collaborate and coordinate with other IETF WGs such as ACE, CORE, 6TISCH, and LPWAN to understand and validate the requirements and solution. The WG will also evaluate prior work from the TLS WG and derivatives thereof, and draft-selander-ace-cose-ecdhe.

Program of Work

The deliverables of this WG are:

1. Design requirements of the LAKE in constrained environments (this draft will not be published as an RFC but will be used to driving WG consensus on the deliverable (2)

2. Standardize a lightweight authenticated key exchange (LAKE) for suitable for use in a documented class of constrained environments.