SPAKE 2

Watson Ladd

Cloudflare

July 13, 2020

SPAKE 2

- draft-irtf-cfrg-spake2-11

SPAKE 2

- draft-irtf-cfrg-spake2-11
- Defines a PAKE with no (mandatory) hash to curve requirements

SPAKE 2

- draft-irtf-cfrg-spake2-11
- Defines a PAKE with no (mandatory) hash to curve requirements
- Preexisting work item from before PAKE bakeoff

SPAKE 2

- draft-irtf-cfrg-spake2-11
- Defines a PAKE with no (mandatory) hash to curve requirements
- Preexisting work item from before PAKE bakeoff
- Supports work in kitten WG as well as deployed usages

SPAKE 2

- draft-irtf-cfrg-spake2-11
- Defines a PAKE with no (mandatory) hash to curve requirements
- Preexisting work item from before PAKE bakeoff
- Supports work in kitten WG as well as deployed usages
- Recent revision to clarify position vis. a vis. competition

SPAKE 2

- draft-irtf-cfrg-spake2-11
- Defines a PAKE with no (mandatory) hash to curve requirements
- Preexisting work item from before PAKE bakeoff
- Supports work in kitten WG as well as deployed usages
- Recent revision to clarify position vis. a vis. competition

Way forward

- Recently regained a sheaphard

Way forward

- Recently regained a sheaphard
- I think RGLC would be appropriate, issues that arise can be dealt with then

Way forward

- Recently regained a sheaphard
- I think RGLC would be appropriate, issues that arise can be dealt with then
- Significant review as part of the PAKE competition has taken place

Way forward

- Recently regained a sheaphard
- I think RGLC would be appropriate, issues that arise can be dealt with then
- Significant review as part of the PAKE competition has taken place
- but I can't claim to have addressed it all

Way forward

- Recently regained a sheaphard
- I think RGLC would be appropriate, issues that arise can be dealt with then
- Significant review as part of the PAKE competition has taken place
- but I can't claim to have addressed it all

Questions?