Importing External PSKs for TLS

`draft-ietf-tls-external-psk-importer`

David Benjamin, **Christopher A. Wood**

IETF 106 - TLS WG - Singapore

Changes since -00

1. Replace `ImportedIdentity` (label, hash) tuple with (target protocol, target KDF) tuple.
    - Introduce an IANA registry for KDFs, parttially managed under Specification Required rules.
2. Added opaque `ImportedIdentity.context` field for application-specific key derivation context.
    - Appendix specifies how to use `ImportedIdentity.context` for Selfie mitigation.
3. Expanded security considerations to clarify key importer goals (KDF input independence) and authentication guarantees.
    - Formal analysis underway, to be completed before document publication.

Selfie Attack Clarification [#22]

Overview: Attempted clarification of Selfie-style mitigations.

Proposal: Simplify PR with added clarification that node roles (identities) are unique in `ImportedIdentity.context`.

Binder Label Change [#10]

Overview: Use a new PSK binder label for imported keys.

Problem: A vanilla (non-imported) PSK with a value and identity can match an imported PSK without. It seems important that both peers agree on whether or not a key was imported.

Proposal: Merge the PR.

- More domain separation is better, even though we haven't shown it's necessary.

Status

Implementations:

- BoringSSL and mint implementations in progress.

Next steps:

- Start WGLC once complete and continue formal analysis in parallel.