Problem Statement

- HTTPS application deployments often have TLS ‘terminated’ by a reverse proxy (TTRP) sitting in front of the actual application
- For applications in such deployments to take advantage of token binding, some information needs to be communicated from the TLS layer to the application
  - (in the general case anyway)
- In the absence of a standard means of doing this, different implementations will do it differently
  - Terrible for interoperability
  - A boon to unneeded complexity
  - Improved opportunity to get things wrong
  - i.e. client certificate authentication
'consensus to work on the problem’ in Seoul

- draft-campbell-tokbind-tls-term-00
- New HTTP header: "Token-Binding-Context" sent from TTRP to backend application
  - base64url-encoded byte sequence, which is the concatenation of the following from the TLS connection between the client and reverse proxy
    - Token Binding Protocol Version
    - Token Binding Key parameters
    - EKM
  - Sufficient for backend application to validate the Sec-Token-Binding header
- Trust between the TTRP and backend application
- TTRP sanitizes header
Example

Token-Binding-Context: AA0CkEPAbQvkTEvnJGtTtryOfEQ_SEjXg0XT64JHpBEyrFo

TB Key Parameters: ecdsap256

Version: draft -13
Running Code

It works!

DATE_LOCAL = Thursday, 23-Mar-2017 19:53:50 UTC
Token-Binding-ID-Provided = AgBBQD4s2LqkOvOQkCIZUYoa6R9UenBZFWY-ZcX-FqmNWY0LbbgmQ_xfMGNlk3ITfWrusIBy21vnhRUqxTSKhKW8
Token-Binding-ID-Referred = (none)
Token-Binding-Context = AA0CgsV6oHwrX9Vc3pCSSUZq7xAsv1F1Pu_IPnnB8PlGm8

(Apache with mod_token_binding brought to you by Hans Zandbelt)
Rough Consensus

- Once more: is this the right approach?
  - Current: backend application validates the Token Binding Message using the context from TTRP
    - Keeps the TTRP lite
    - Reconciling and updating supported key parameters difficult with lots of apps
  - Alternative: TTRP validates the Token Binding Message and passes Token Binding ID(s)
    - Simpler for apps
    - Supported key parameters isolated to TTRP
    - Does not keep the TTRP lite

- Both…
  - Really?
Current Approach: Issues/Questions

- Explain the rational of keeping the TTRP lightweight
- Is Token Binding Protocol Version needed or useful?
- EKM lengths
- Recently on the mailing list
  - Sec- for Token-Binding-Context?
  - MAC the header?
Next...

- Call for Adoption by the WG?
- Do some work
- Discuss at IETF 99 in Prague