draft-ietf-tokbind-protocol-01

Andrei Popov, Microsoft Corp.

Changes Since IETF92

- Replaced ALPN-based negotiation with TLS extension-based negotiation (draft-popov-tokbind-negotiation-00).
- Added a Security Considerations sub-section discussing Token Binding key sharing between applications.
- Minor edits, nits, etc.

Open Issue: Token Binding Key Parameters

- draft-ietf-tokbind-protocol-01 uses TLS-style SignatureAndHashAlgorithm structure:

```
enum {
   sha256(4), (255)
} HashAlgorithm;
enum {
   rsa(1), ecdsap256(3), (255)
} SignatureAlgorithm;
struct {
   HashAlgorithm hash;
   SignatureAlgorithm signature;
} SignatureAndHashAlgorithm;
```

- draft-popov-tokbind-negotiation-00 defines 1-byte key parameter IDs:

```
enum {
   rsa2048_pkcs1.5_sha256(0), rsa2048_pss_sha256(1), ecdsap256_sha256(2), (255)
} TokenBindingKeyParameters;
```

- Should we use the same 1-byte IDs in both drafts?

Open Issue: Token Binding Extensions

- Token Binding Protocol messages in the current I-D allow optional extensions:

```
struct {
    ExtensionType extension_type;
    opaque extension_data<0..2^16-1>;
} Extension;
struct {
    TokenBindingID tokenbindingid;
    opaque signature<0..2^16-1>;// Signature over hashed ("token binding", tls_unique)
    Extension extensions<0..2^16-1>;
} TokenBinding;
```

- No initial extension types are specified, and there has been a suggestion to remove the “extensions” field.
- A likely future use of extensions is attestation (cryptographic proof that the Token Binding key is hardware-bound).
- Should we keep the “extensions” field in the TokenBinding message?

Links And Contact Information

- TLS Extension for Token Binding Negotiation: https://tools.ietf.org/html/draft-popov-tokbind-negotiation-00
- The Token Binding Protocol Version 1.0: https://tools.ietf.org/html/draft-ietf-tokbind-protocol-01
- Token Binding over HTTP: https://tools.ietf.org/html/draft-ietf-tokbind-https-01
- GitHub: https://github.com/TokenBinding/Internet-Drafts

- Dirk Balfanz balfanz@google.com
- Andrei Popov andreipo@microsoft.com

The Token Binding Protocol Message Format

```
struct {
    ExtensionType extension_type;
    opaque extension_data<0..2^16-1>;
} Extension;
struct {
    TokenBindingID tokenbindingid;
    opaque signature<0..2^16-1>;// Signature over hashed ("token binding", tls_unique)
    Extension extensions<0..2^16-1>;
} TokenBinding;
struct {
    TokenBinding tokenbindings<0..2^16-1>;
} TokenBindingMessage;
```

Token Binding ID Format

```
enum {
  provided_token_binding(0), referred_token_binding(1), (255)
} TokenBindingType;
struct {
  TokenBindingType tokenbinding_type;
  SignatureAndHashAlgorithm algorithm;
  select (algorithm.signature) {
    case rsa: RSAPublicKey rsapubkey;
    case ecdsa: ECDSAParams ecdsaparams;
  }
} TokenBindingID;
```

- Provided_token_binding is used to establish a Token Binding when connecting to a server.
- Referred_token_binding is used when requesting tokens to be presented to a different server.