

HTTPS Token Binding with TLS Terminating Reverse Proxies (TTRP)

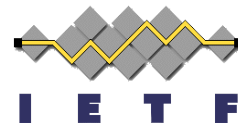


Brian Campbell

IETF 101

London

March 2018



draft-ietf-tokbind-ttrp

<https://tools.ietf.org/html/draft-ietf-tokbind-ttrp-03>

Problem Statement



- HTTPS application deployments often have TLS ‘terminated’ by a reverse proxy in front of the actual application
 - products, open source, services
- 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 (or not do it at all)

Solution Overview

draft-ietf-tokbind-ttrp-03



- Define HTTP headers that enable a TTRP and backend server to function together as a single logical server side deployment of HTTPS Token Binding
- TTRP validates the TokenBindingMessage from the `Sec-Token-Binding` header and removes it from dispatched request
- `Sec-Provided-Token-Binding-ID` header with base64url encoded provided TokenBindingID added to dispatched request
- `Sec-Referred-Token-Binding-ID` header with encoded referred TokenBindingID added to dispatched request (if applicable)
- [new] `Sec-Other-Token-Binding-ID` header with additional Token Bindings type and ID added to dispatched request (if applicable)
- Trust between the TTRP and backend server
- TTRP required to sanitize headers

Different view of the Overview



Old fashioned Token
Binding over HTTPS

(Negotiates)
Validates Token Binding message
Sanitize headers

Passes encoded provided
token binding ID as new
header (referred and others too,
if applicable)

Binds/verifies
using token
binding ID(s)

Client

```
GET /stuff HTTP/1.1
Host: example.com
Sec-Token-Binding: AIkAAgBBQKzyIrmcY_Yct
HVoSHBut69vrGfFdy1_YKTZfFJv6BjrZsKD9b9F
RzSBxDs1twTqnAS71M1RBumuihhI9xqxXKkAQEt
xe4jeUJU0Wezx1QXWVSBFeHxFMdXRBiH_LK0SAu
SMOJ0XEw1Q8DE248qkOiRKzw3KdSNYukYEP
m021bQi3YAAAA
```

Reverse
Proxy
aka
TTRP

```
GET /stuff HTTP/1.1
Host: ...
Sec-Provided-Token-Binding-ID: AgBB
QKzyIrmcY_YcTHVoSHBut69vrGfFdy1_YK
TZfFJv6BjrZsKD9b9FRzSBxDs1twTqnAS7
1M1RBumuihhI9xqxXKk
```

Origin
Server

Changes since Singapore

- Drafts -02 & -03
- Use RFC 8174 boilerplate
- Add to acknowledgements
- Update references
- Minor editorial / formatting updates
- Reword the Abstract somewhat for (hopefully) improved readability
- Reformat the "HTTP Header Fields and Processing Rules" section to make header names more prominent and move the encoding definitions earlier
- Add a new header to allow for additional token binding types (other than provided and referred) to be conveyed
 - Comma-separated list
 - Concatenation of base16 encoded Token Binding Type, a period ("."), and the base64url encoded Token Binding ID



Next Steps

- Consensus on Sec-Other-Token-Binding-ID?
- WGLC?

