Token Binding & OAuth: Status & Next Steps

Securing what were previously bearer tokens

Dr. Michael B. Jones
Identity Standards Architect at Microsoft

Brian Campbell
Distinguished Engineer at Ping Identity

July 13, 2017

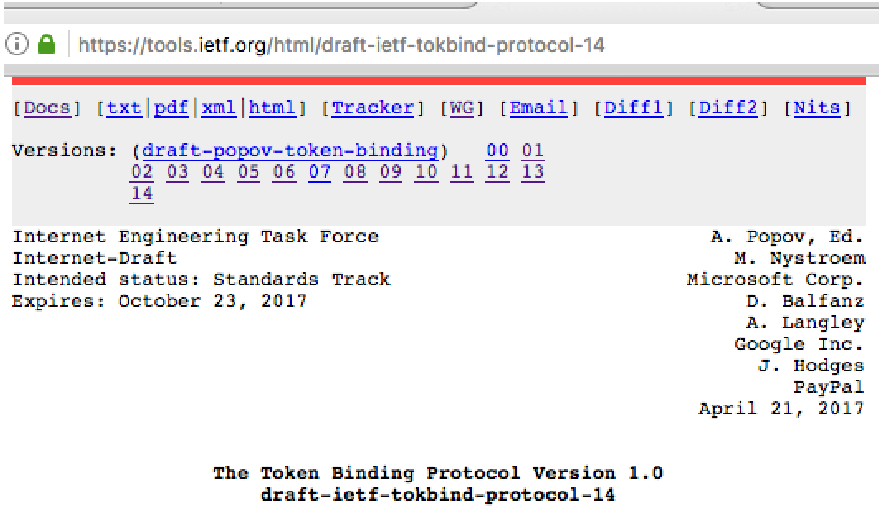
The Problem With Bearer Tokens

One truth and a lie

Token Binding Solution

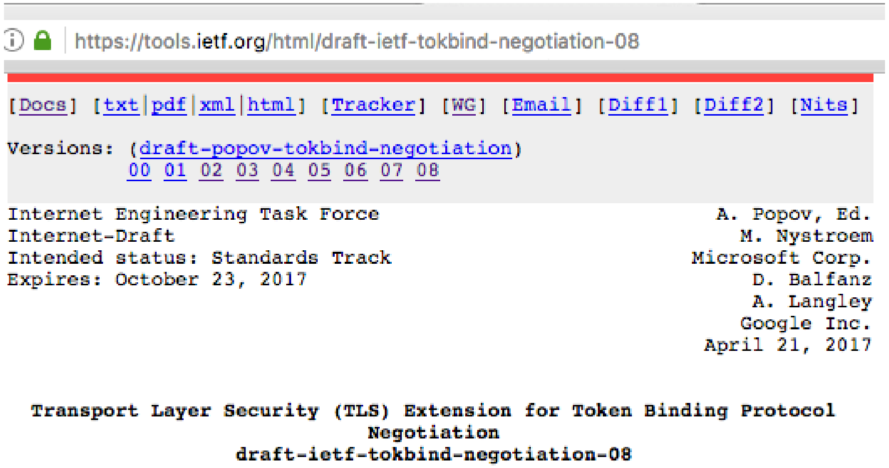
- Token Binding enables data structures to be cryptographically bound to a particular TLS channel
  - *Making them no longer bearer tokens*
  - Prevents them from being used in unintended ways
- Data structures that can be Token Bound include:
  - Browser cookies, ID Tokens, access tokens, refresh tokens, authorization codes
- Presentation will discuss:
  - Token Binding mechanisms
  - Kinds of threats they mitigate
  - Current deployment status

IETF Token Binding Specifications



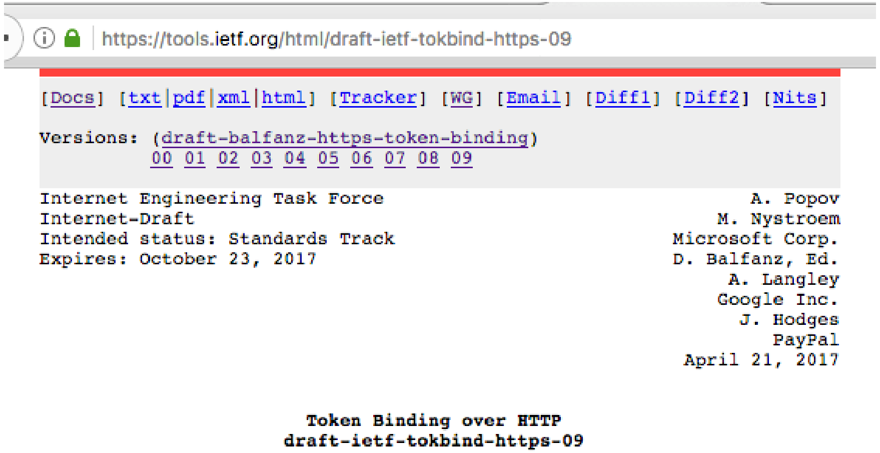
https://tools.ietf.org/html/draft-ietf-tokbind-protocol-14

```
[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-popov-token-binding)    00 01
           02 03 04 05 06 07 08 09 10 11 12 13
           14

Internet Engineering Task Force                           A. Popov, Ed.
Internet-Draft                                             M. Nystroem
Intended status: Standards Track                        Microsoft Corp.
Expires: October 23, 2017                                   D. Balfanz
                                                            A. Langley
                                                           Google Inc.
                                                             J. Hodges
                                                                PayPal
                                                        April 21, 2017


                 The Token Binding Protocol Version 1.0
                     draft-ietf-tokbind-protocol-14
```



https://tools.ietf.org/html/draft-ietf-tokbind-negotiation-08

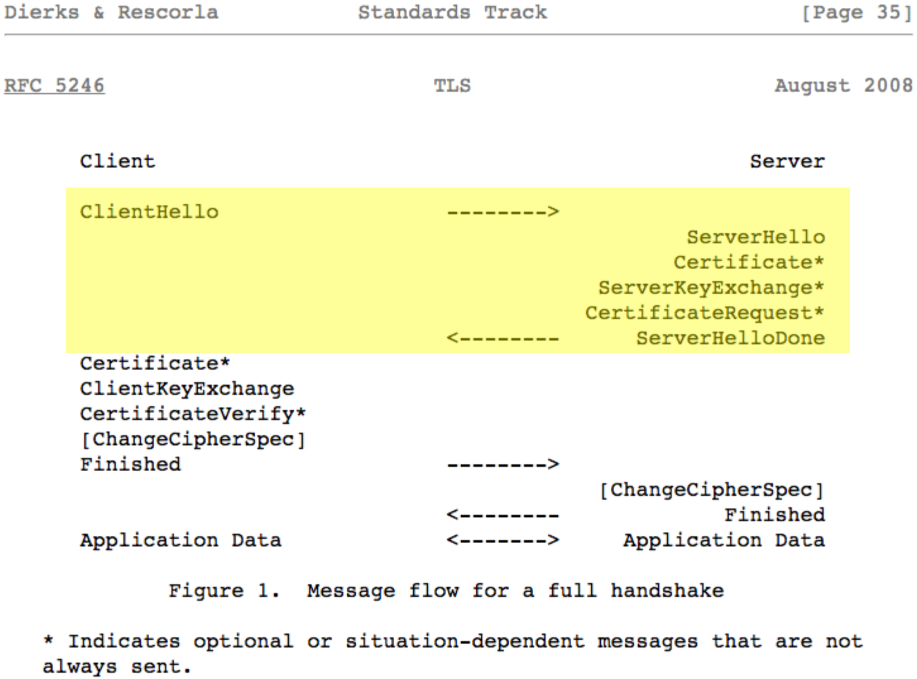
```
[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-popov-tokbind-negotiation)
           00 01 02 03 04 05 06 07 08

Internet Engineering Task Force                           A. Popov, Ed.
Internet-Draft                                             M. Nystroem
Intended status: Standards Track                        Microsoft Corp.
Expires: October 23, 2017                                   D. Balfanz
                                                            A. Langley
                                                           Google Inc.
                                                        April 21, 2017


  Transport Layer Security (TLS) Extension for Token Binding Protocol
                              Negotiation
                   draft-ietf-tokbind-negotiation-08
```



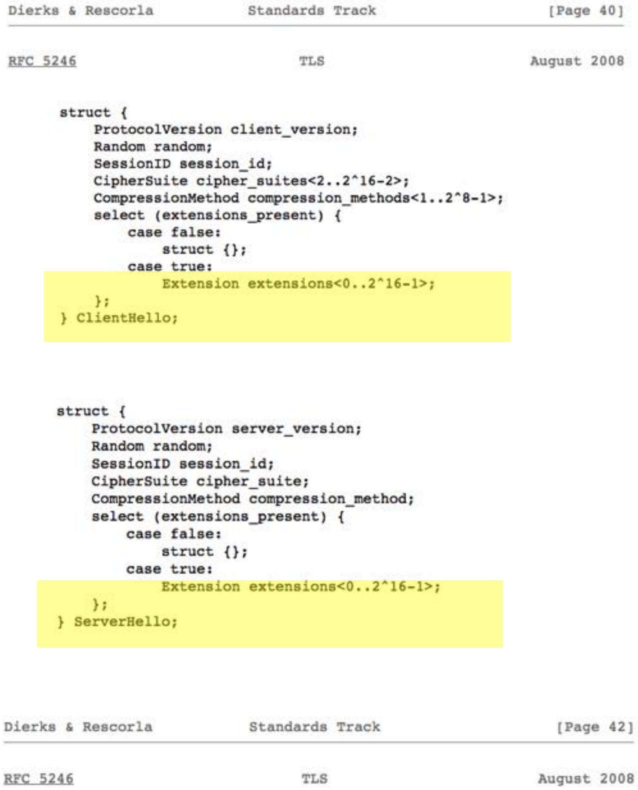
https://tools.ietf.org/html/draft-ietf-tokbind-https-09

```
[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-balfanz-https-token-binding)
           00 01 02 03 04 05 06 07 08 09

Internet Engineering Task Force                                A. Popov
Internet-Draft                                              M. Nystroem
Intended status: Standards Track                        Microsoft Corp.
Expires: October 23, 2017                              D. Balfanz, Ed.
                                                            A. Langley
                                                           Google Inc.
                                                             J. Hodges
                                                                PayPal
                                                        April 21, 2017


                        Token Binding over HTTP
                      draft-ietf-tokbind-https-09
```

Hello! Do you like my extension?

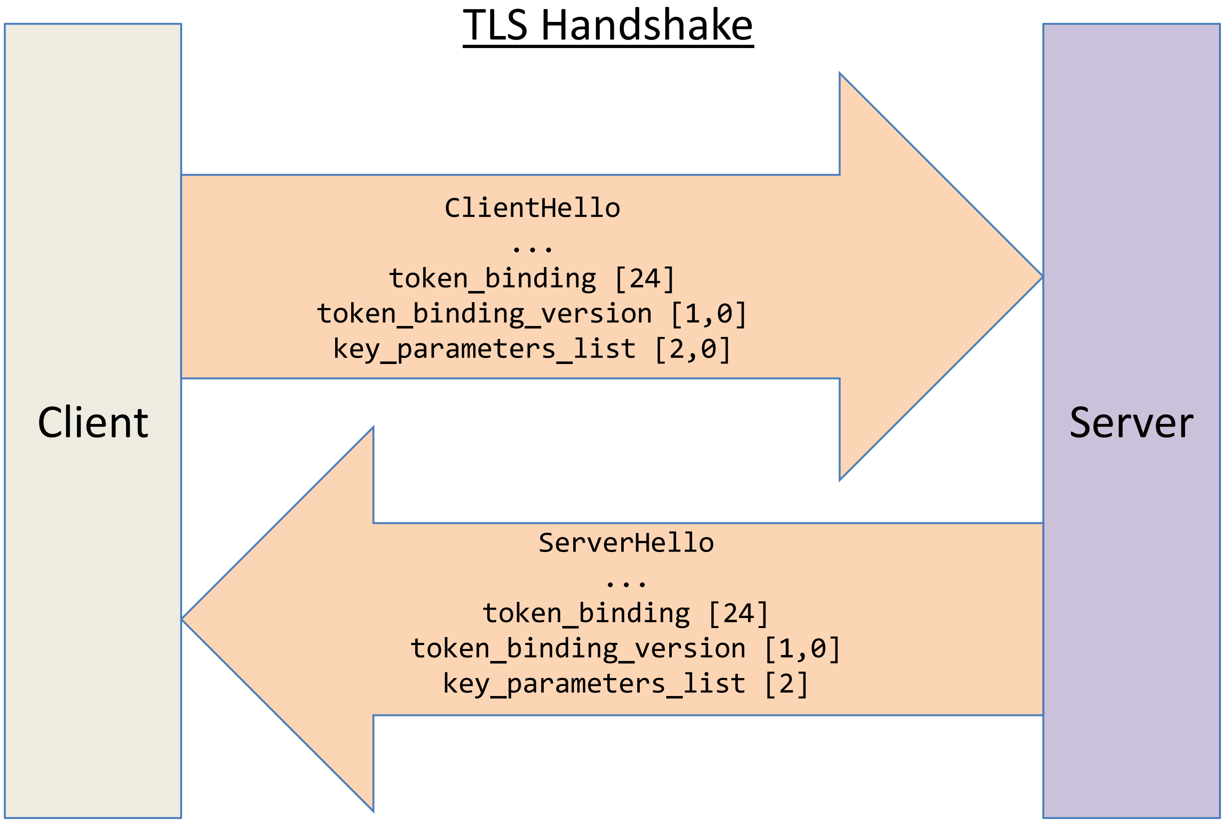


```
Dierks & Rescorla            Standards Track                   [Page 35]

RFC 5246                          TLS                        August 2008

      Client                                               Server

      ClientHello                  -------->
                                                      ServerHello
                                                     Certificate*
                                               ServerKeyExchange*
                                              CertificateRequest*
                                   <--------      ServerHelloDone
      Certificate*
      ClientKeyExchange
      CertificateVerify*
      [ChangeCipherSpec]
      Finished                     -------->
                                               [ChangeCipherSpec]
                                   <--------             Finished
      Application Data             <------->     Application Data

             Figure 1.  Message flow for a full handshake

   * Indicates optional or situation-dependent messages that are not
   always sent.
```



```
Dierks & Rescorla            Standards Track                   [Page 40]

RFC 5246                          TLS                        August 2008

      struct {
          ProtocolVersion client_version;
          Random random;
          SessionID session_id;
          CipherSuite cipher_suites<2..2^16-2>;
          CompressionMethod compression_methods<1..2^8-1>;
          select (extensions_present) {
              case false:
                  struct {};
              case true:
                  Extension extensions<0..2^16-1>;
          };
      } ClientHello;


      struct {
          ProtocolVersion server_version;
          Random random;
          SessionID session_id;
          CipherSuite cipher_suite;
          CompressionMethod compression_method;
          select (extensions_present) {
              case false:
                  struct {};
              case true:
                  Extension extensions<0..2^16-1>;
          };
      } ServerHello;


Dierks & Rescorla            Standards Track                   [Page 42]

RFC 5246                          TLS                        August 2008
```

Do you support Token Binding?



TLS Handshake

```
ClientHello
...
token_binding [24]
token_binding_version [1,0]
key_parameters_list [2,0]
```

```
ServerHello
...
token_binding [24]
token_binding_version [1,0]
key_parameters_list [2]
```

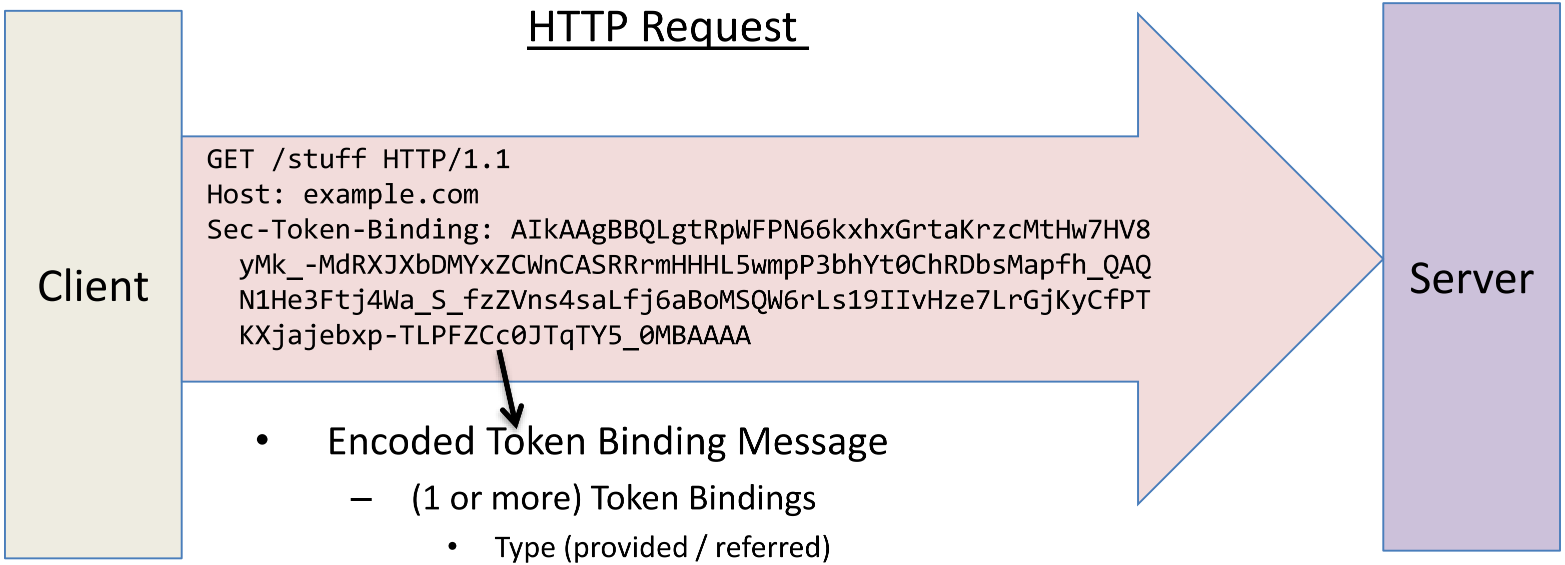
Key Parameters:

(0) rsa2048_pkcs1.5
(1) rsa2048_pss
(2) ecdsap256

Also need extenstions:

Extended Master Secret
Renegotiation Indication

Token Binding over HTTPS



```
GET /stuff HTTP/1.1
Host: example.com
Sec-Token-Binding: AIkAAgBBQLgtRpWFPN66kxhxGrtaKrzcMtHw7HV8
  yMk_-MdRXJXbDMYxZCWnCASRRrmHHHL5wmpP3bhYt0ChRDbsMapfh_QAQ
  N1He3Ftj4Wa_S_fzZVns4saLfj6aBoMSQW6rLs19IIvHze7LrGjKyCfPT
  KXjajebxp-TLPFZCc0JTqTY5_0MBAAAA
```

- Encoded Token Binding Message
  - (1 or more) Token Bindings
    - Type (provided / referred)
    - Token Binding ID (key type and public key)
    - Signature over type, key type, and EKM (TLS **E**xported **K**eying **M**aterial)
    - Extensions
- Proves possession of the private key on the TLS connection
- Keys are long-lived and span TLS connections

Browser cookies low hanging fruit

`secure`

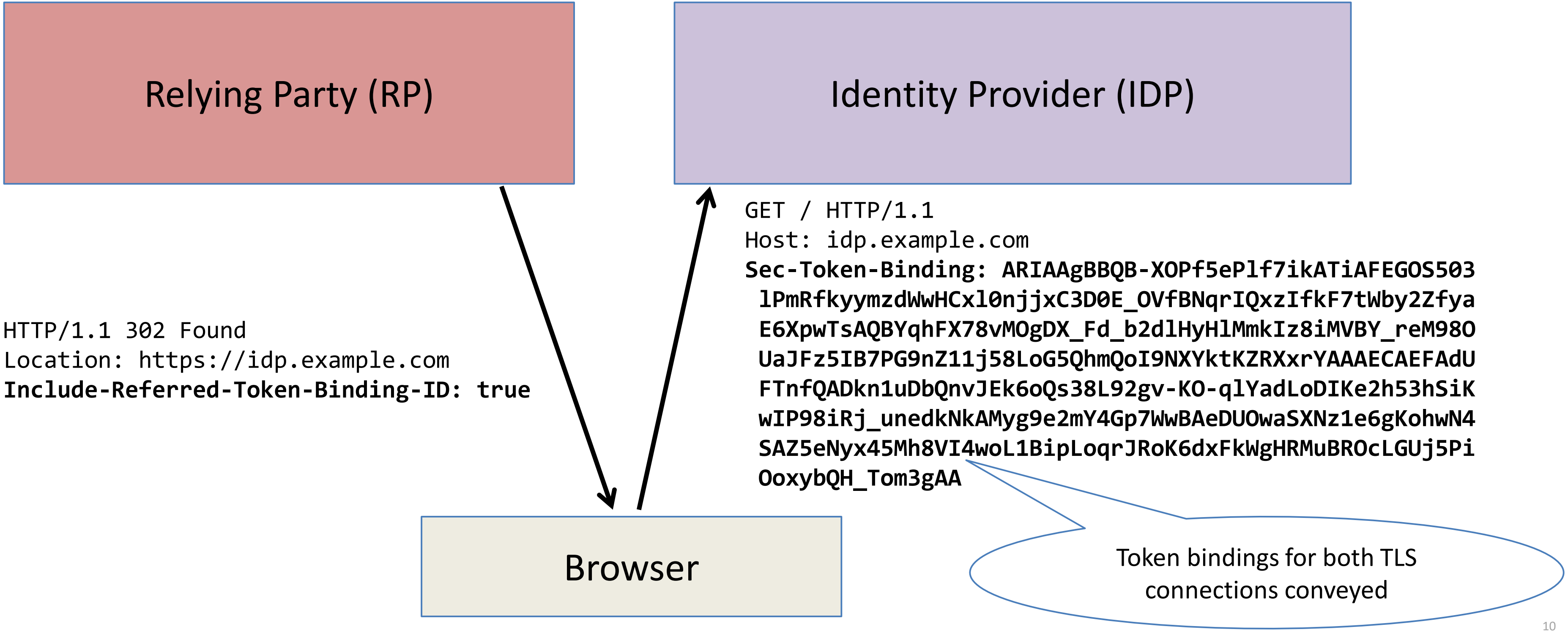
`HttpOnly`

Binding Cookies

- Server associates Token Binding ID with cookie & checks on subsequent use
- Augments existing authentication and session mechanisms
- Transparent to users
- Deployment can be phased in

What about federation?

There’s an HTTP response header for that! Tells the browser that it should reveal the Token Binding ID used between itself and the RP (referred) in addition to the one used between itself and the IDP (provided).

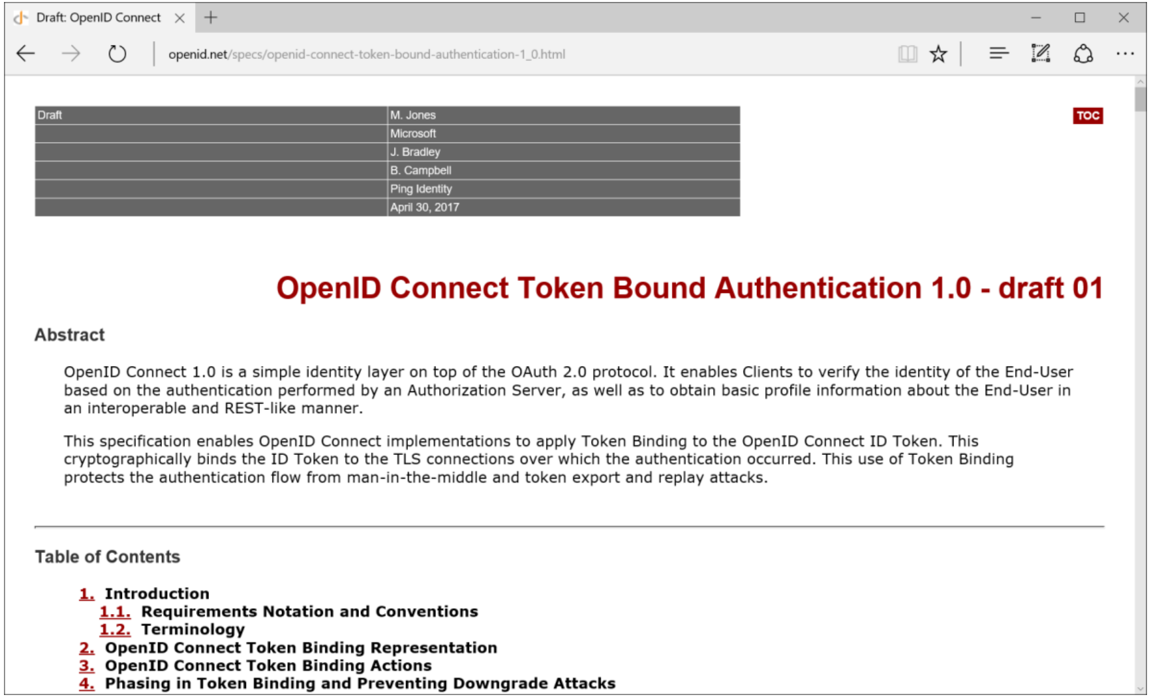


```
HTTP/1.1 302 Found
Location: https://idp.example.com
Include-Referred-Token-Binding-ID: true
```

```
GET / HTTP/1.1
Host: idp.example.com
Sec-Token-Binding: ARIAAgBBQB-XOPf5ePlf7ikATiAFEGOS503
 lPmRfkyymzdWwHCxl0njjxC3D0E_OVfBNqrIQxzIfkF7tWby2Zfya
 E6XpwTsAQBYqhFX78vMOgDX_Fd_b2dlHyHlMmkIz8iMVBY_reM98O
 UaJFz5IB7PG9nZ11j58LoG5QhmQoI9NXYktKZRXxrYAAAECAEFAdU
 FTnfQADkn1uDbQnvJEk6oQs38L92gv-KO-qlYadLoDIKe2h53hSiK
 wIP98iRj_unedkNkAMyg9e2mY4Gp7WwBAeDUOwaSXNz1e6gKohwN4
 SAZ5eNyx45Mh8VI4woL1BipLoqrJRoK6dxFkWgHRMuBROcLGUj5Pi
 OoxybQH_Tom3gAA
```

Token bindings for both TLS connections conveyed

Token Binding for OpenID Connect


Draft: OpenID Connect
openid.net/specs/openid-connect-token-bound-authentication-1_0.html
TOC

Draft	M. Jones
	Microsoft
	J. Bradley
	B. Campbell
	Ping Identity
	April 30, 2017

OpenID Connect Token Bound Authentication 1.0 - draft 01

Abstract

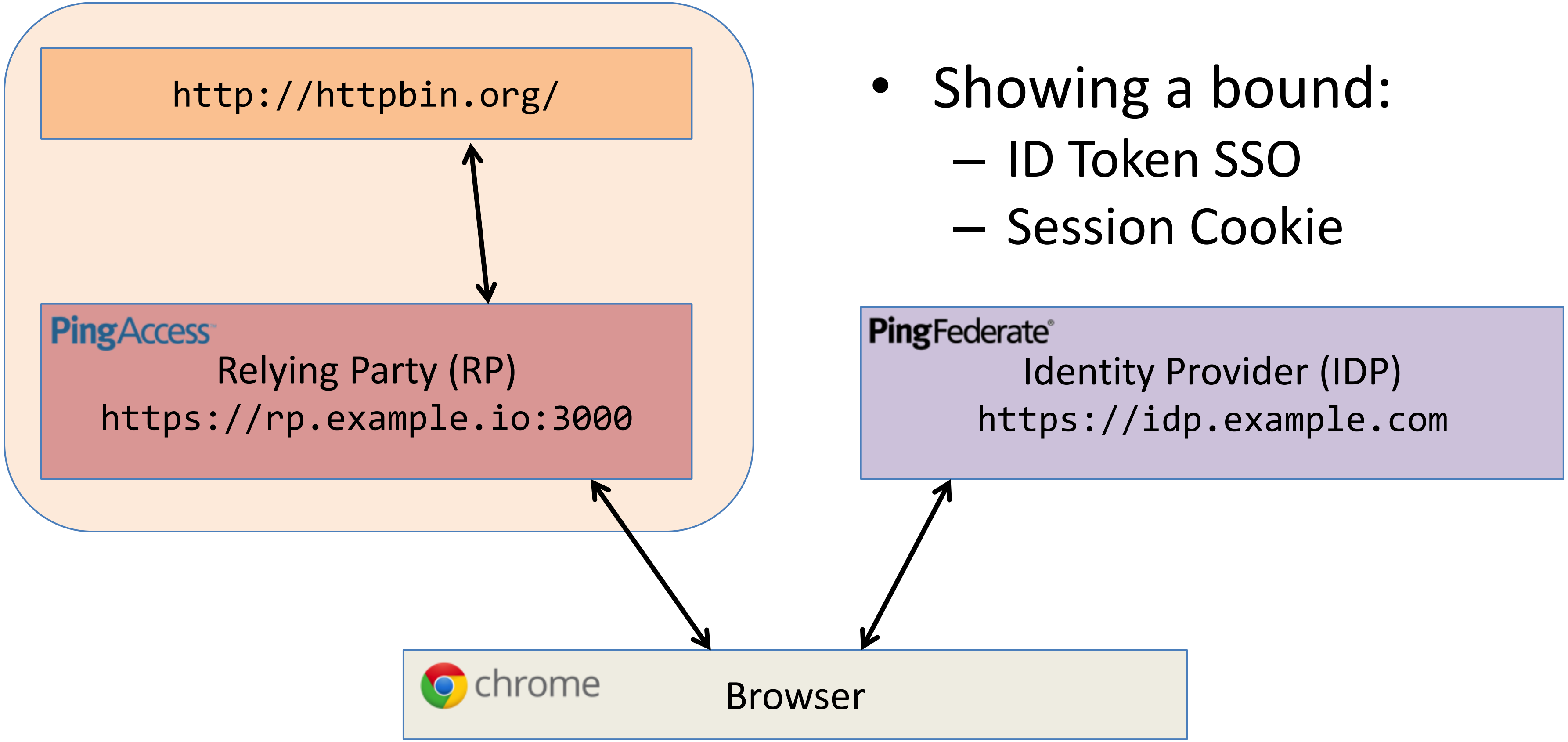
OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

This specification enables OpenID Connect implementations to apply Token Binding to the OpenID Connect ID Token. This cryptographically binds the ID Token to the TLS connections over which the authentication occurred. This use of Token Binding protects the authentication flow from man-in-the-middle and token export and replay attacks.

Table of Contents

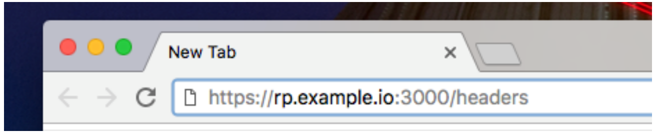
- Utilizes the `Include-Referred-Token-Binding-ID` header
- Binds the ID Token to the Token Binding ID the browser uses between itself and the Relying Party
- Uses token binding hash “`tbh`” member of the confirmation claim “`cnf`”

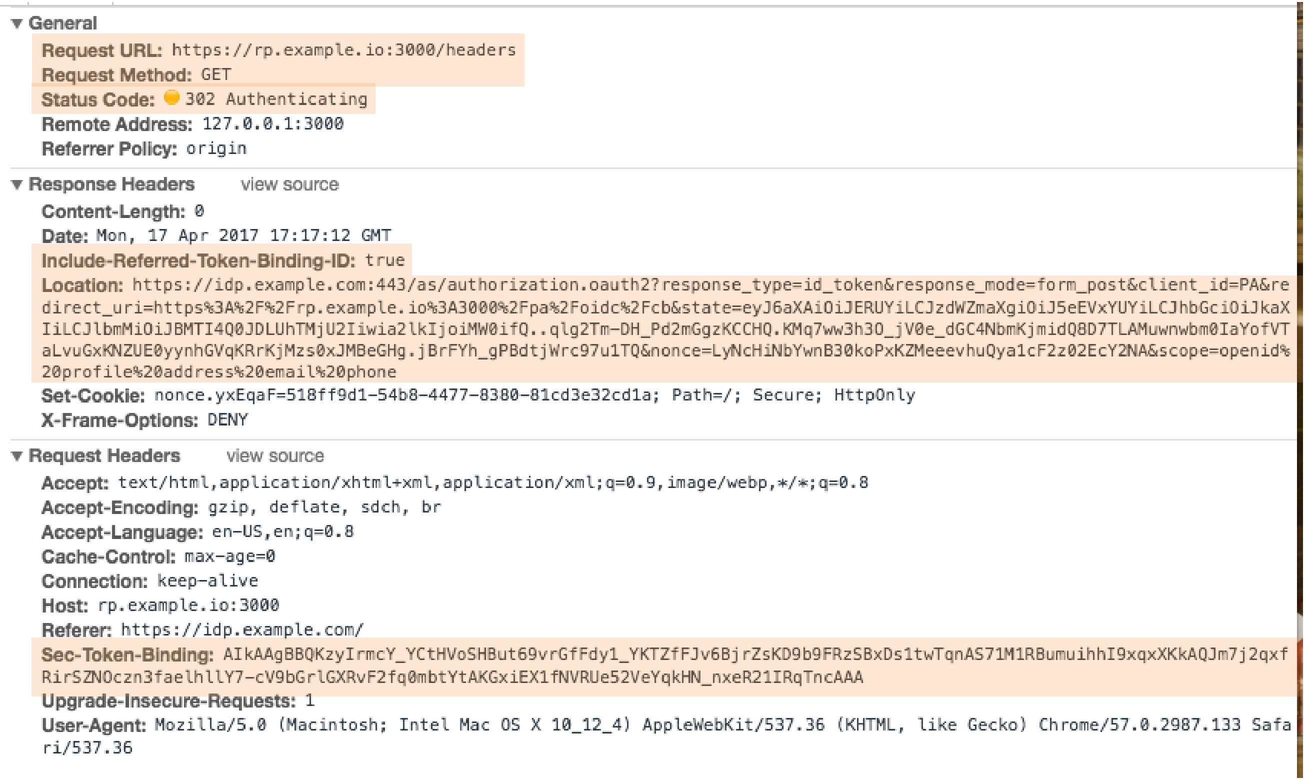
“Demo”



- Showing a bound:
  - ID Token SSO
  - Session Cookie

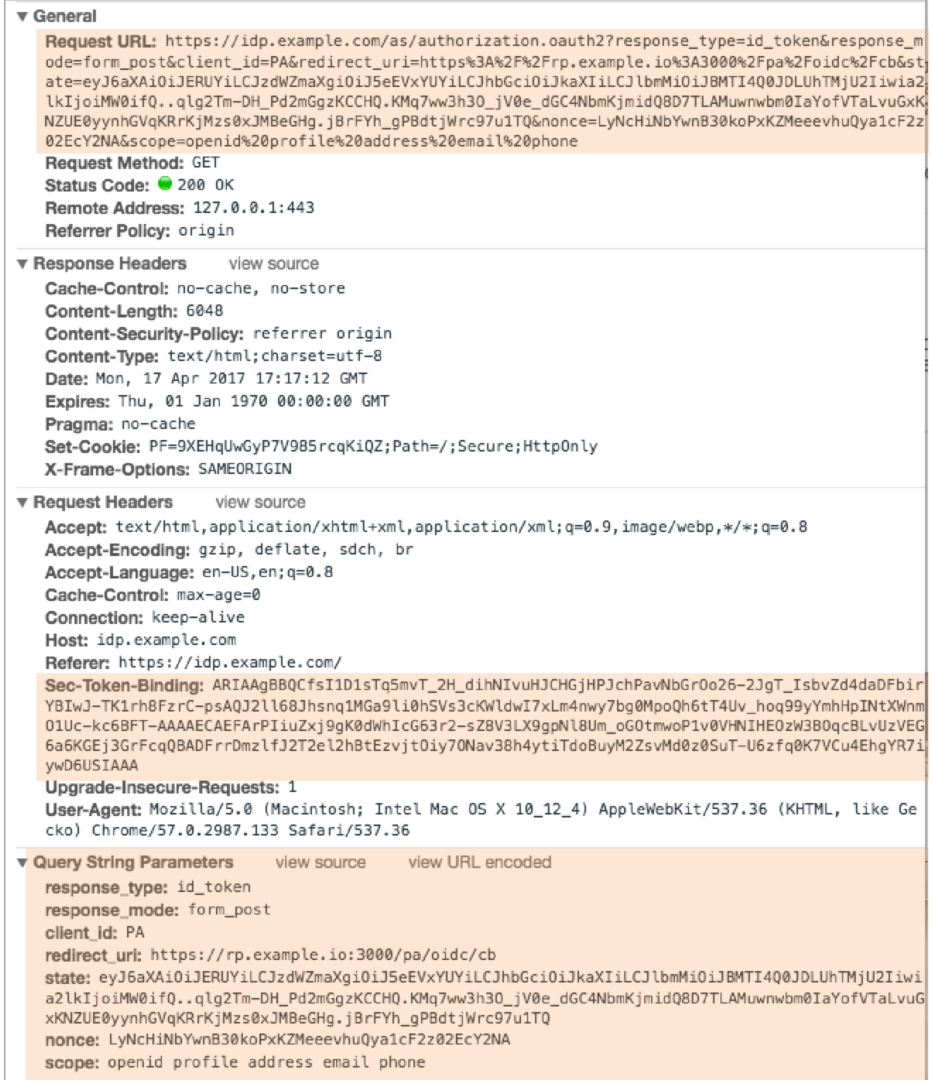
Unauthenticated access request to RP is redirected for SSO



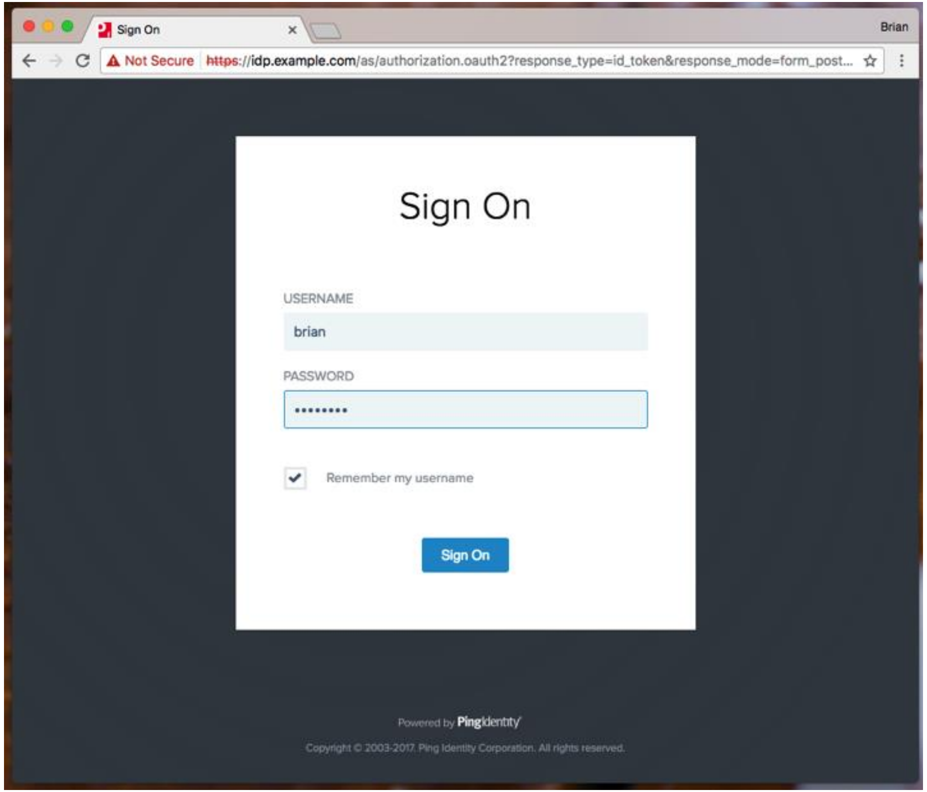


```
▼ General
    Request URL: https://rp.example.io:3000/headers
    Request Method: GET
    Status Code: ● 302 Authenticating
    Remote Address: 127.0.0.1:3000
    Referrer Policy: origin
▼ Response Headers      view source
    Content-Length: 0
    Date: Mon, 17 Apr 2017 17:17:12 GMT
    Include-Referred-Token-Binding-ID: true
    Location: https://idp.example.com:443/as/authorization.oauth2?response_type=id_token&response_mode=form_post&client_id=PA&re
    direct_uri=https%3A%2F%2Frp.example.io%3A3000%2Fpa%2Foidc%2Fcb&state=eyJ6aXAiOiJERUYiLCJzdWZmaXgiOiJ5eEVxYUYiLCJhbGciOiJkaX
    IiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2Iiwia2lkIjoiMW0ifQ..qlg2Tm-DH_Pd2mGgzKCCHQ.KMq7ww3h3O_jV0e_dGC4NbmKjmidQ8D7TLAMuwnwbm0IaYofVT
    aLvuGxKNZUE0yynhGVqKRrKjMzs0xJMBeGHg.jBrFYh_gPBdtjWrc97u1TQ&nonce=LyNcHiNbYwnB30koPxKZMeeevhuQya1cF2z02EcY2NA&scope=openid%
    20profile%20address%20email%20phone
    Set-Cookie: nonce.yxEqaF=518ff9d1-54b8-4477-8380-81cd3e32cd1a; Path=/; Secure; HttpOnly
    X-Frame-Options: DENY
▼ Request Headers      view source
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch, br
    Accept-Language: en-US,en;q=0.8
    Cache-Control: max-age=0
    Connection: keep-alive
    Host: rp.example.io:3000
    Referer: https://idp.example.com/
    Sec-Token-Binding: AIkAAgBBQKzyIrmcY_YCtHVoSHBut69vrGfFdy1_YKTZfFJv6BjrZsKD9b9FRzSBxDs1twTqnAS71M1RBumuihhI9xqxXKkAQJm7j2qxf
    RirSZNOczn3faelhllY7-cV9bGrlGXRvF2fq0mbtYtAKGxiEX1fNVRUe52VeYqkHN_nxeR21IRqTncAAA
    Upgrade-Insecure-Requests: 1
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safa
    ri/537.36
```

Authentication request to the IDP



```
▼ General
    Request URL: https://idp.example.com/as/authorization.oauth2?response_type=id_token&response_m
    ode=form_post&client_id=PA&redirect_uri=https%3A%2F%2Frp.example.io%3A3000%2Fpa%2Foidc%2Fcb&st
    ate=eyJ6aXAiOiJERUYiLCJzdWZmaXgiOiJ5eEVxYUYiLCJhbGciOiJkaXIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2Iiwia2
    lkIjoiMW0ifQ..qlg2Tm-DH_Pd2mGgzKCCHQ.KMq7ww3h3O_jV0e_dGC4NbmKjmidQ8D7TLAMuwnwbm0IaYofVTaLvuGxK
    NZUE0yynhGVqKRrKjMzs0xJMBeGHg.jBrFYh_gPBdtjWrc97u1TQ&nonce=LyNcHiNbYwnB30koPxKZMeeevhuQya1cF2z
    02EcY2NA&scope=openid%20profile%20address%20email%20phone
    Request Method: GET
    Status Code: ● 200 OK
    Remote Address: 127.0.0.1:443
    Referrer Policy: origin
▼ Response Headers     view source
    Cache-Control: no-cache, no-store
    Content-Length: 6048
    Content-Security-Policy: referrer origin
    Content-Type: text/html;charset=utf-8
    Date: Mon, 17 Apr 2017 17:17:12 GMT
    Expires: Thu, 01 Jan 1970 00:00:00 GMT
    Pragma: no-cache
    Set-Cookie: PF=9XEHqUwGyP7V985rcqKiQZ;Path=/;Secure;HttpOnly
    X-Frame-Options: SAMEORIGIN
▼ Request Headers     view source
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch, br
    Accept-Language: en-US,en;q=0.8
    Cache-Control: max-age=0
    Connection: keep-alive
    Host: idp.example.com
    Referer: https://idp.example.com/
    Sec-Token-Binding: ARIAAgBBQCfsI1D1sTq5mvT_2H_dihNIvuHJCHGjHPJchPavNbGrOo26-2JgT_IsbvZd4daDFbir
    YBIwJ-TK1rh8FzrC-psAQJ2ll68Jhsnq1MGa9li0hSVs3cKWldwI7xLm4nwy7bg0MpoQh6tT4Uv_hoq99yYmhHpINtXWnm
    O1Uc-kc6BFT-AAAAECAEFArPIiuZxj9gK0dWhIcG63r2-sZ8V3LX9gpNl8Um_oGOtmwoP1v0VHNIHEOzW3BOqcBLvUzVEG
    6a6KGEj3GrFcqQBADFrrDmzlfJ2T2el2hBtEzvjtOiy7ONav38h4ytiTdoBuyM2ZsvMd0z0SuT-U6zfq0K7VCu4EhgYR7i
    ywD6USIAAA
    Upgrade-Insecure-Requests: 1
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Ge
    cko) Chrome/57.0.2987.133 Safari/537.36
▼ Query String Parameters     view source     view URL encoded
    response_type: id_token
    response_mode: form_post
    client_id: PA
    redirect_uri: https://rp.example.io:3000/pa/oidc/cb
    state: eyJ6aXAiOiJERUYiLCJzdWZmaXgiOiJ5eEVxYUYiLCJhbGciOiJkaXIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2Iiwi
    a2lkIjoiMW0ifQ..qlg2Tm-DH_Pd2mGgzKCCHQ.KMq7ww3h3O_jV0e_dGC4NbmKjmidQ8D7TLAMuwnwbm0IaYofVTaLvuG
    xKNZUE0yynhGVqKRrKjMzs0xJMBeGHg.jBrFYh_gPBdtjWrc97u1TQ
    nonce: LyNcHiNbYwnB30koPxKZMeeevhuQya1cF2z02EcY2NA
    scope: openid profile address email phone
```



https://idp.example.com/as/authorization.oauth2?response_type=id_token&response_mode=form_post...

Sign On

USERNAME

brian

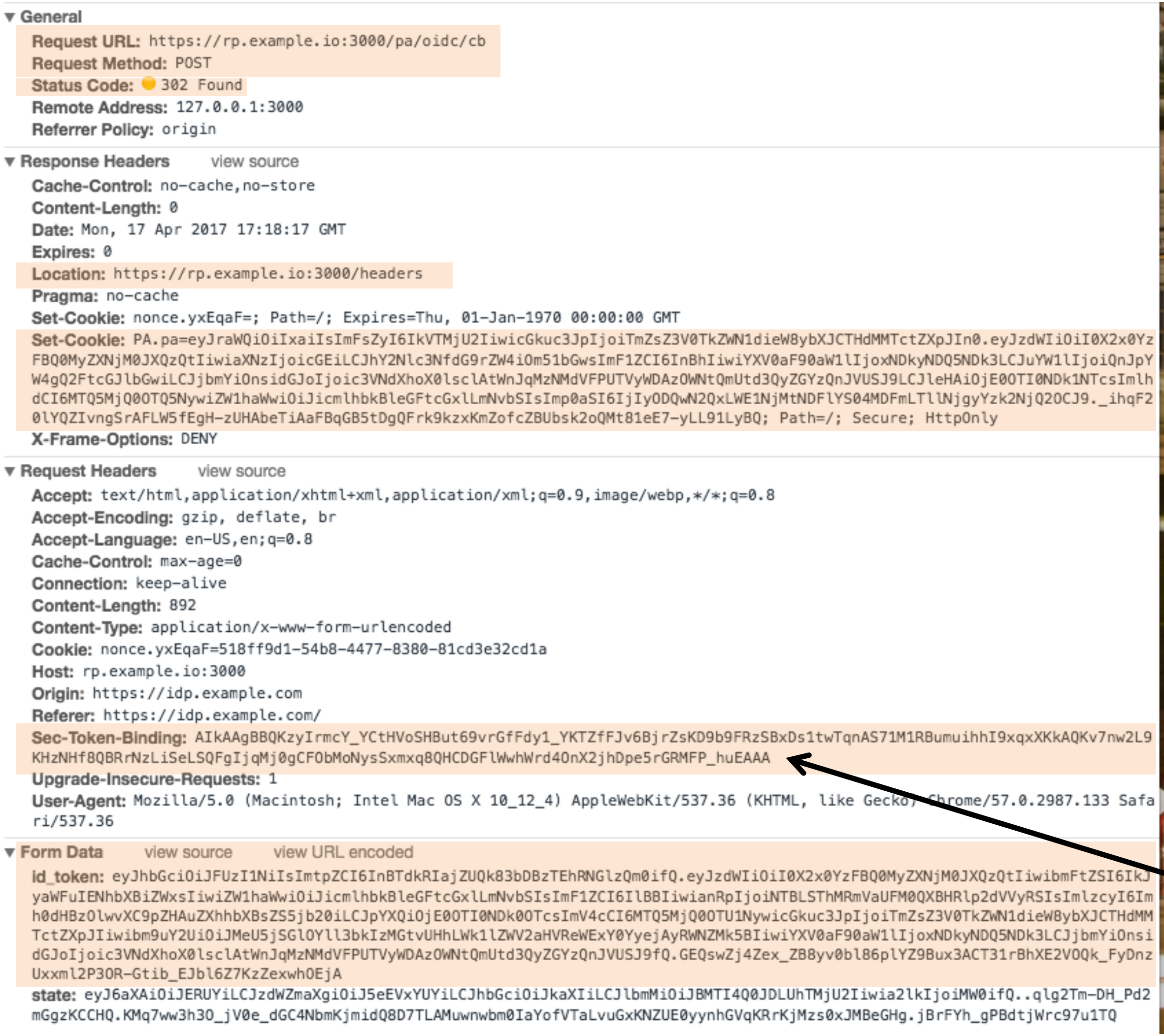
PASSWORD

•••••••••

☑ Remember my username

Copyright © 2003-2017 Ping Identity Corporation. All rights reserved.

ID Token delivered to RP



▼ **General**

Request URL: https://rp.example.io:3000/pa/oidc/cb
Request Method: POST
Status Code: ● 302 Found
Remote Address: 127.0.0.1:3000
Referrer Policy: origin

▼ **Response Headers** view source

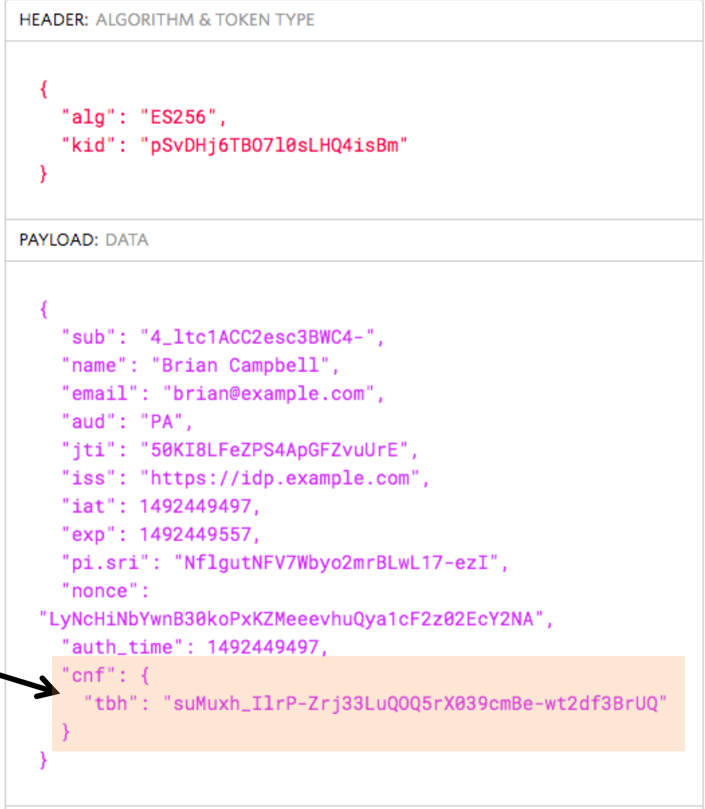
Cache-Control: no-cache,no-store
Content-Length: 0
Date: Mon, 17 Apr 2017 17:18:17 GMT
Expires: 0
Location: https://rp.example.io:3000/headers
Pragma: no-cache
Set-Cookie: nonce.yxEqaF=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT
Set-Cookie: PA.pa=eyJraWQiOiIxaiIsImFsZyI6IkVTMjU2IiwicGkuc3JpIjoiTmZsZ3V0TkZWN1dieW8ybXJCTHdMMTctZXpJIn0.eyJzdWIiOiI0X2x0YzFBQ0MyZXNjM0JXQzQtIiwiaXNzIjoicGEiLCJhY2Nlc3NfdG9rZW4iOm51bGwsImF1ZCI6InBhIiwiYXV0aF90aW1lIjoxNDkyNDQ5NDk3LCJuYW1lIjoiQnJpYW4gQ2FtcGJlbGwiLCJjbmYiOnsidGJoIjoic3VNdXhoX0lsclAtWnJqMzNMdVFPUTVyWDAzOWNtQmUtd3QyZGYzQnJVUSJ9LCJleHAiOjE0OTI0NDk1NTcsImlhdCI6MTQ5MjQ0OTQ5NywiZW1haWwiOiJicmlhbkBleGFtcGxlLmNvbSIsImp0aSI6IjIyODQwN2QxLWE1NjMtNDFlYS04MDFmLTllNjgyYzk2NjQ2OCJ9._ihqF20lYQZIvngSrAFLW5fEgH-zUHAbeTiAaFBqGB5tDgQFrk9kzxKmZofcZBUbsk2oQMt81eE7-yLL91LyBQ; Path=/; Secure; HttpOnly
X-Frame-Options: DENY

▼ **Request Headers** view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 892
Content-Type: application/x-www-form-urlencoded
Cookie: nonce.yxEqaF=518ff9d1-54b8-4477-8380-81cd3e32cd1a
Host: rp.example.io:3000
Origin: https://idp.example.com
Referer: https://idp.example.com/
Sec-Token-Binding: AIkAAgBBQKzyIrmcY_YCtHVoSHBut69vrGfFdy1_YKTZfFJv6BjrZsKD9b9FRzSBxDs1twTqnAS71M1RBumuihhI9xqxXKkAQKv7nw2L9KHzNHf8QBRrNzLiSeLSQFgIjqMj0gCFObMoNysSxmxq8QHCDGFlWwhWrd4OnX2jhDpe5rGRMFP_huEAAA
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36

▼ **Form Data** view source view URL encoded

id_token: eyJhbGciOiJFUzI1NiIsImtpZCI6InBTdkRIajZUQk83bDBzTEhRNGlzQm0ifQ.eyJzdWIiOiI0X2x0YzFBQ0MyZXNjM0JXQzQtIiwibmFtZSI6IkJyaWFuIENhbXBiZWxsIiwiZW1haWwiOiJicmlhbkBleGFtcGxlLmNvbSIsImF1ZCI6IlBBIiwianRpIjoiNTBLSThMRmVaUFM0QXBHRlp2dVVyRSIsImlzcyI6Imh0dHBzOlwvXC9pZHAuZXhhbXBsZS5jb20iLCJpYXQiOjE0OTI0NDk0OTcsImV4cCI6MTQ5MjQ0OTU1NywicGkuc3JpIjoiTmZsZ3V0TkZWN1dieW8ybXJCTHdMMTctZXpJIiwibm9uY2UiOiJMeU5jSGlOYll3bkIzMGtvUHhLWk1lZWV2aHVReWExY0YyejAyRWNZMk5BIiwiYXV0aF90aW1lIjoxNDkyNDQ5NDk3LCJjbmYiOnsidGJoIjoic3VNdXhoX0lsclAtWnJqMzNMdVFPUTVyWDAzOWNtQmUtd3QyZGYzQnJVUSJ9fQ.GEQswZj4Zex_ZB8yv0bl86plYZ9Bux3ACT31rBhXE2VOQk_FyDnzUxxml2P3OR-Gtib_EJbl6Z7KzZexwhOEjA
state: eyJ6aXAiOiJERUYiLCJzdWZmaXgiOiJ5eEVxYUYiLCJhbGciOiJkaXIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2Iiwia2lkIjoiMW0ifQ..qlg2Tm-DH_Pd2mGgzKCCHQ.KMq7ww3h3O_jV0e_dGC4NbmKjmidQ8D7TLAMuwnwbm0IaYofVTaLvuGxKNZUE0yynhGVqKRrKjMzs0xJMBeGHg.jBrFYh_gPBdtjWrc97u1TQ



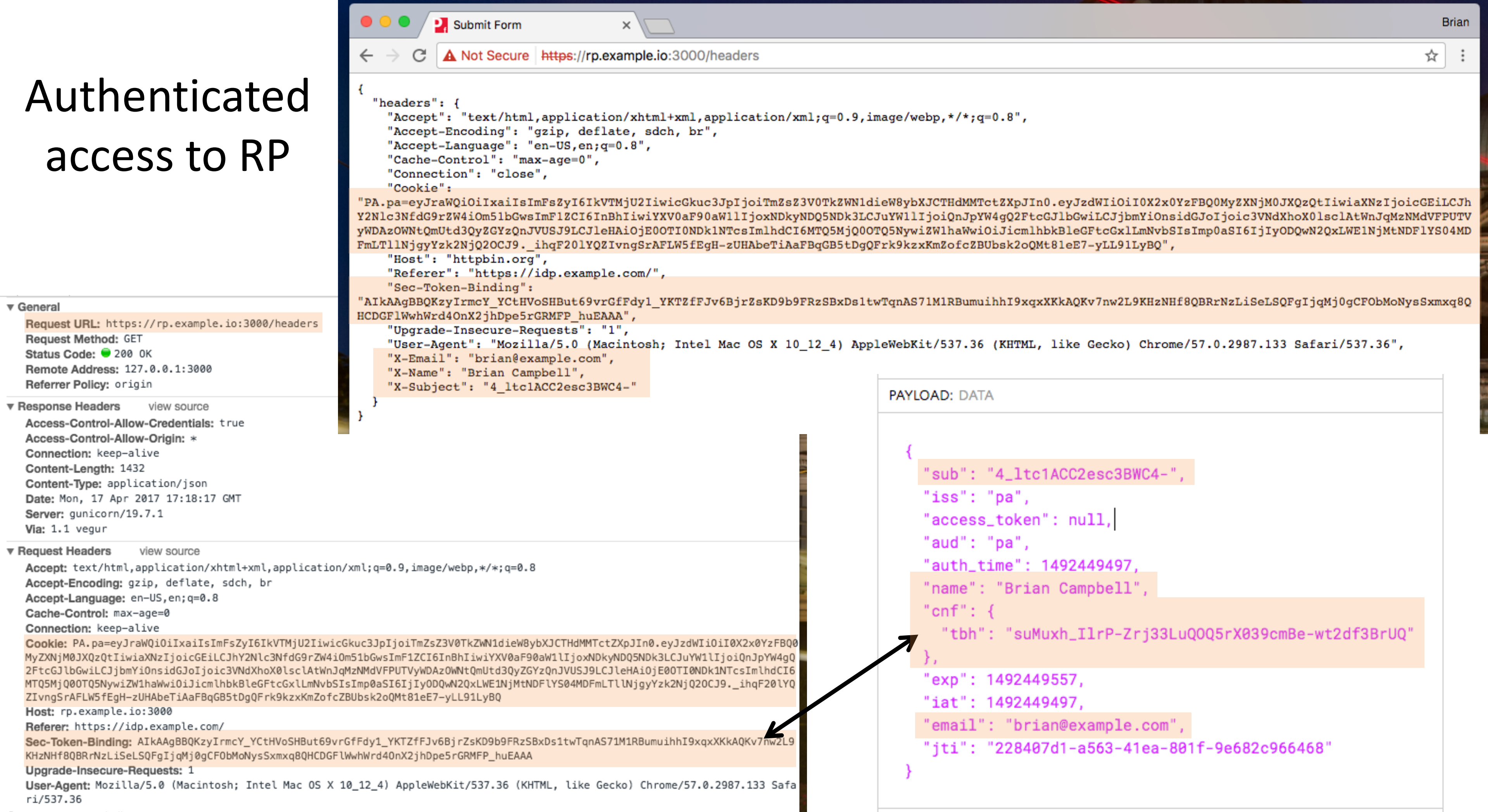
HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "ES256",
  "kid": "pSvDHj6TBO7l0sLHQ4isBm"
}
```

PAYLOAD: DATA

```
{
  "sub": "4_ltc1ACC2esc3BWC4-",
  "name": "Brian Campbell",
  "email": "brian@example.com",
  "aud": "PA",
  "jti": "50KI8LFeZPS4ApGFZvuUrE",
  "iss": "https://idp.example.com",
  "iat": 1492449497,
  "exp": 1492449557,
  "pi.sri": "NflgutNFV7Wbyo2mrBLwL17-ezI",
  "nonce":
"LyNcHiNbYwnB30koPxKZMeeevhuQya1cF2z02EcY2NA",
  "auth_time": 1492449497,
  "cnf": {
    "tbh": "suMuxh_IlrP-Zrj33LuQOQ5rX039cmBe-wt2df3BrUQ"
  }
}
```

Authenticated access to RP



```
{
  "headers": {
    "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8",
    "Accept-Encoding": "gzip, deflate, sdch, br",
    "Accept-Language": "en-US,en;q=0.8",
    "Cache-Control": "max-age=0",
    "Connection": "close",
    "Cookie":
"PA.pa=eyJraWQiOiIxaiIsImFsZyI6IkVTMjU2IiwicGkuc3JpIjoiTmZsZ3V0TkZWN1dieW8ybXJCTHdMMTctZXpJIn0.eyJzdWIiOiI0X2x0YzFBQ0MyZXNjM0JXQzQtIiwiaXNzIjoicGEiLCJh
Y2Nlc3NfdG9rZW4iOm51bGwsImF1ZCI6InBhIiwiYXV0aF90aW1lIjoxNDkyNDQ5NDk3LCJuYW1lIjoiQnJpYW4gQ2FtcGJlbGwiLCJjbmYiOnsidGJoIjoic3VNdXhoX0lsclAtWnJqMzNMdVFPUTV
yWDAzOWNtQmUtd3QyZGYzQnJVUSJ9LCJleHAiOjE0OTI0NDk1NTcsImlhdCI6MTQ5MjQ0OTQ5NywiZW1haWwiOiJicmlhbkBleGFtcGxlLmNvbSIsImp0aSI6IjIyODQwN2QxLWE1NjMtNDFlYS04MD
FmLTllNjgyYzk2NjQ2OCJ9._ihqF20lYQZIvngSrAFLW5fEgH-zUHAbeTiAaFBqGB5tDgQFrk9kzxKmZofcZBUsk2oQMt8leE7-yLL91LyBQ",
    "Host": "httpbin.org",
    "Referer": "https://idp.example.com/",
    "Sec-Token-Binding":
"AIkAAgBBQKzyIrmcY_YCtHVoSHBut69vrGfFdy1_YKTZfFJv6BjrZsKD9b9FRzSBxDs1twTqnAS71M1RBumuihhI9xqxXKkAQKv7nw2L9KHzNHf8QBRrNzLiSeLSQFgIjqMj0gCFObMoNysSxmxq8Q
HCDGFlWwhWrd4OnX2jhDpe5rGRMFP_huEAAA",
    "Upgrade-Insecure-Requests": "1",
    "User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36",
    "X-Email": "brian@example.com",
    "X-Name": "Brian Campbell",
    "X-Subject": "4_ltc1ACC2esc3BWC4-"
  }
}
```

▼ General

Request URL: https://rp.example.io:3000/headers
Request Method: GET
Status Code: ● 200 OK
Remote Address: 127.0.0.1:3000
Referrer Policy: origin

▼ Response Headers   view source

Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: *
Connection: keep-alive
Content-Length: 1432
Content-Type: application/json
Date: Mon, 17 Apr 2017 17:18:17 GMT
Server: gunicorn/19.7.1
Via: 1.1 vegur

▼ Request Headers   view source

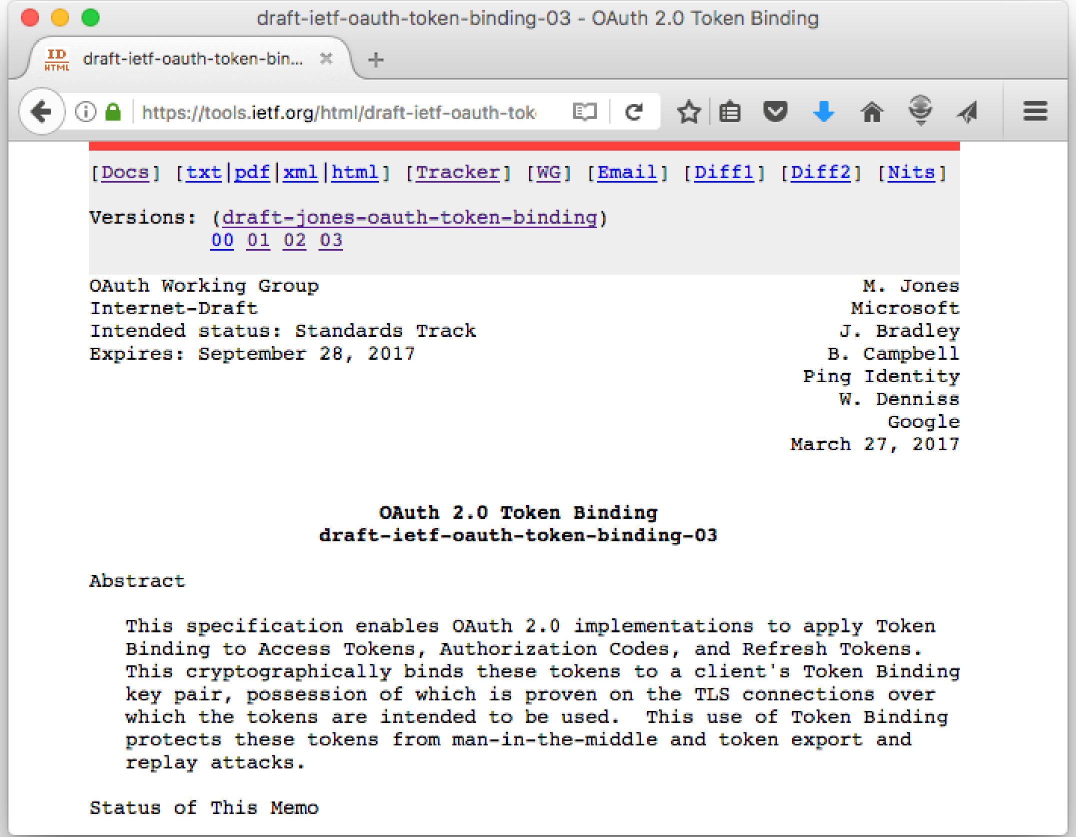
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-US,en;q=0.8
Cache-Control: max-age=0
Connection: keep-alive
Cookie: PA.pa=eyJraWQiOiIxaiIsImFsZyI6IkVTMjU2IiwicGkuc3JpIjoiTmZsZ3V0TkZWN1dieW8ybXJCTHdMMTctZXpJIn0.eyJzdWIiOiI0X2x0YzFBQ0MyZXNjM0JXQzQtIiwiaXNzIjoicGEiLCJhY2Nlc3NfdG9rZW4iOm51bGwsImF1ZCI6InBhIiwiYXV0aF90aW1lIjoxNDkyNDQ5NDk3LCJuYW1lIjoiQnJpYW4gQ2FtcGJlbGwiLCJjbmYiOnsidGJoIjoic3VNdXhoX0lsclAtWnJqMzNMdVFPUTVyWDAzOWNtQmUtd3QyZGYzQnJVUSJ9LCJleHAiOjE0OTI0NDk1NTcsImlhdCI6MTQ5MjQ0OTQ5NywiZW1haWwiOiJicmlhbkBleGFtcGxlLmNvbSIsImp0aSI6IjIyODQwN2QxLWE1NjMtNDFlYS04MDFmLTllNjgyYzk2NjQ2OCJ9._ihqF20lYQZIvngSrAFLW5fEgH-zUHAbeTiAaFBqGB5tDgQFrk9kzxKmZofcZBUsk2oQMt81eE7-yLL91LyBQ
Host: rp.example.io:3000
Referer: https://idp.example.com/
Sec-Token-Binding: AIkAAgBBQKzyIrmcY_YCtHVoSHBut69vrGfFdy1_YKTZfFJv6BjrZsKD9b9FRzSBxDs1twTqnAS71M1RBumuihhI9xqxXKkAQKv7nw2L9KHzNHf8QBRrNzLiSeLSQFgIjqMj0gCFObMoNysSxmxq8QHCDGFlWwhWrd4OnX2jhDpe5rGRMFP_huEAAA
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36

PAYLOAD: DATA

```
{
  "sub": "4_ltc1ACC2esc3BWC4-",
  "iss": "pa",
  "access_token": null,
  "aud": "pa",
  "auth_time": 1492449497,
  "name": "Brian Campbell",
  "cnf": {
    "tbh": "suMuxh_IlrP-Zrj33LuQOQ5rX039cmBe-wt2df3BrUQ"
  },
  "exp": 1492449557,
  "iat": 1492449497,
  "email": "brian@example.com",
  "jti": "228407d1-a563-41ea-801f-9e682c966468"
}
```

“Demo” Finished

OAuth Token Binding


draft-ietf-oauth-token-binding-03 - OAuth 2.0 Token Binding
draft-ietf-oauth-token-bin...
https://tools.ietf.org/html/draft-ietf-oauth-tok

[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

```
Versions: (draft-jones-oauth-token-binding)
          00 01 02 03

OAuth Working Group                                             M. Jones
Internet-Draft                                                 Microsoft
Intended status: Standards Track                              J. Bradley
Expires: September 28, 2017                                  B. Campbell
                                                           Ping Identity
                                                              W. Denniss
                                                                  Google
                                                          March 27, 2017
```

OAuth 2.0 Token Binding
draft-ietf-oauth-token-binding-03

Abstract

This specification enables OAuth 2.0 implementations to apply Token Binding to Access Tokens, Authorization Codes, and Refresh Tokens. This cryptographically binds these tokens to a client's Token Binding key pair, possession of which is proven on the TLS connections over which the tokens are intended to be used. This use of Token Binding protects these tokens from man-in-the-middle and token export and replay attacks.

Status of This Memo

- Access tokens with referred Token Binding ID
- Refresh tokens with provided Token Binding ID
- Authorization codes via PKCE
  - Native app clients
  - Web server clients

The Landscape

- Three IETF Token Binding specs soon to be RFCs
- Drafts supported in:
  - Edge, IE, and Chrome (but not on iOS)
  - On Google servers since January
  - .NET Framework 4.6 (for server side)
  - Open Source
    - OpenSSL (https://github.com/google/token_bind)
    - Apache (https://github.com/zmartzone/mod_token_binding)
    - NGINX (https://github.com/google/ngx_token_binding)
    - Java (Brian Campbell has mods he plans to submit…)

- OpenID Connect Token Bound Authentication spec maturing
  - Online Token Binding demo available
- OAuth 2.0 Token Binding spec also maturing

Privacy Considerations

- Token Binding is not a *supercookie* or new tracking mechanism
- Client generates a unique key pair per effective top-level domain + 1 (eTLD+1)
  - E.g., example.com, www.example.com, and etc.example.com share binding but not example.org or example.co.uk
- Same scoping rules and privacy implications as cookies

Workshop Discussion Topics

- Detecting and preventing downgrade attacks
- Status of platform and library support for Token Binding
- Implementations and deployments to date and what we’ve learned from them
- Practical steps needed to deploy Token Binding for OAuth and OpenID Connect end-to-end

Where can I participate & learn more?

- Online Token Binding Demo
  - https://www.ietf.org/mail-archive/web/unbearable/current/msg01385.html
- IETF Token Binding mailing list
  - https://www.ietf.org/mailman/listinfo/unbearable
- IETF OAuth mailing list
  - https://www.ietf.org/mailman/listinfo/oauth
- OpenID Enhanced Authentication Profile (EAP) mailing list
  - http://lists.openid.net/mailman/listinfo/openid-specs-eap
- My blog
  - http://self-issued.info/
- E-mail me
  - mbj@microsoft.com