Token Binding over HTTP

Dirk Balfanz, Google

IETF 92, 03/2015

Protecting Bearer Tokens over HTTP

- Goal: Strengthen credentials like
  - Cookies
  - OAuth Tokens

  so only authorized clients can use them

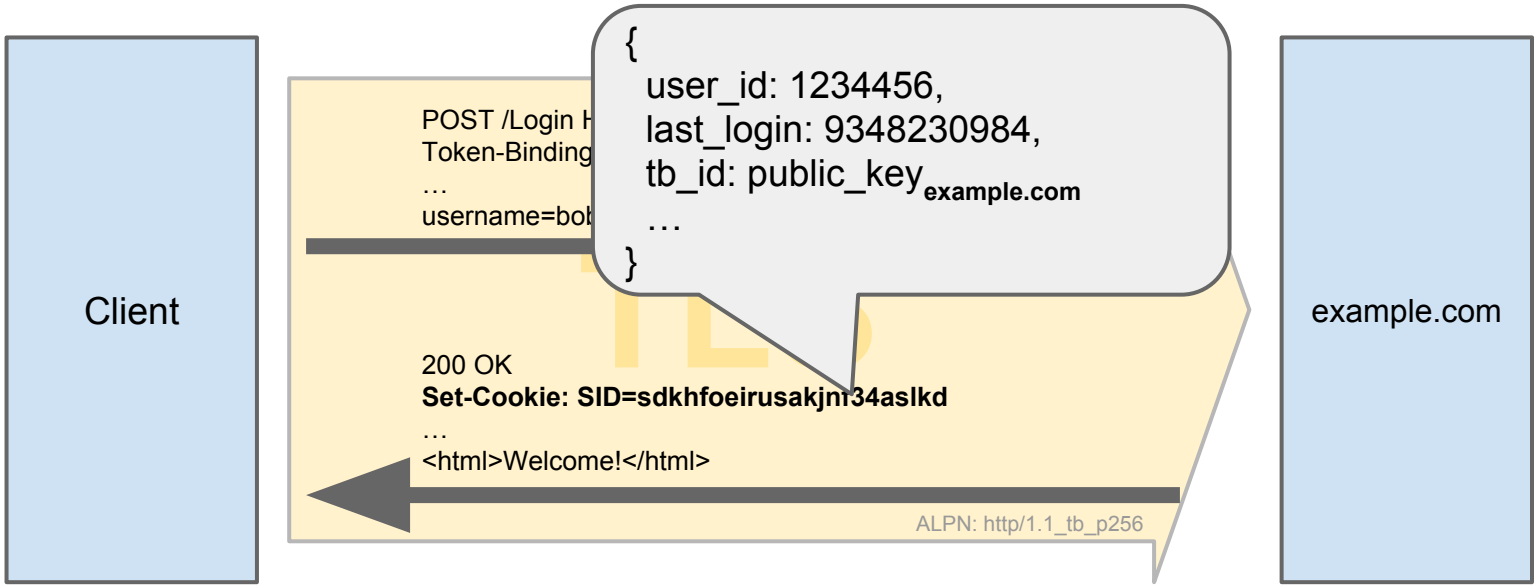
- Recap from draft-popov-token-binding:
  - Client signs tls_unique to prove possession of private key
  - Uses different Token Binding Key per eTLD

- HTTP Client discloses Token Binding Id to HTTP Server
  - via **new HTTP Header**

Token Binding Header

Example: Binding Cookies

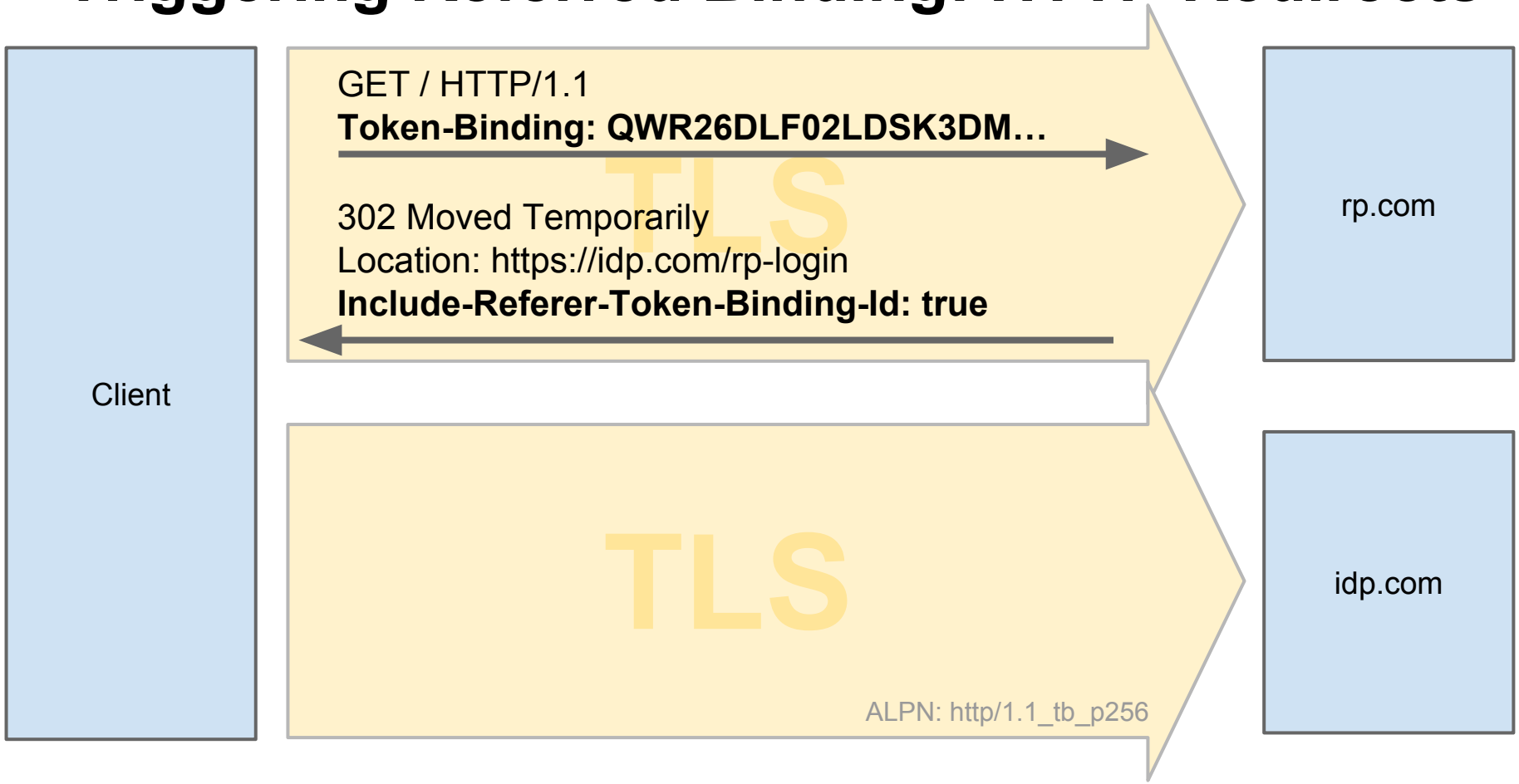
- Server can then bind tokens to Token Binding ID



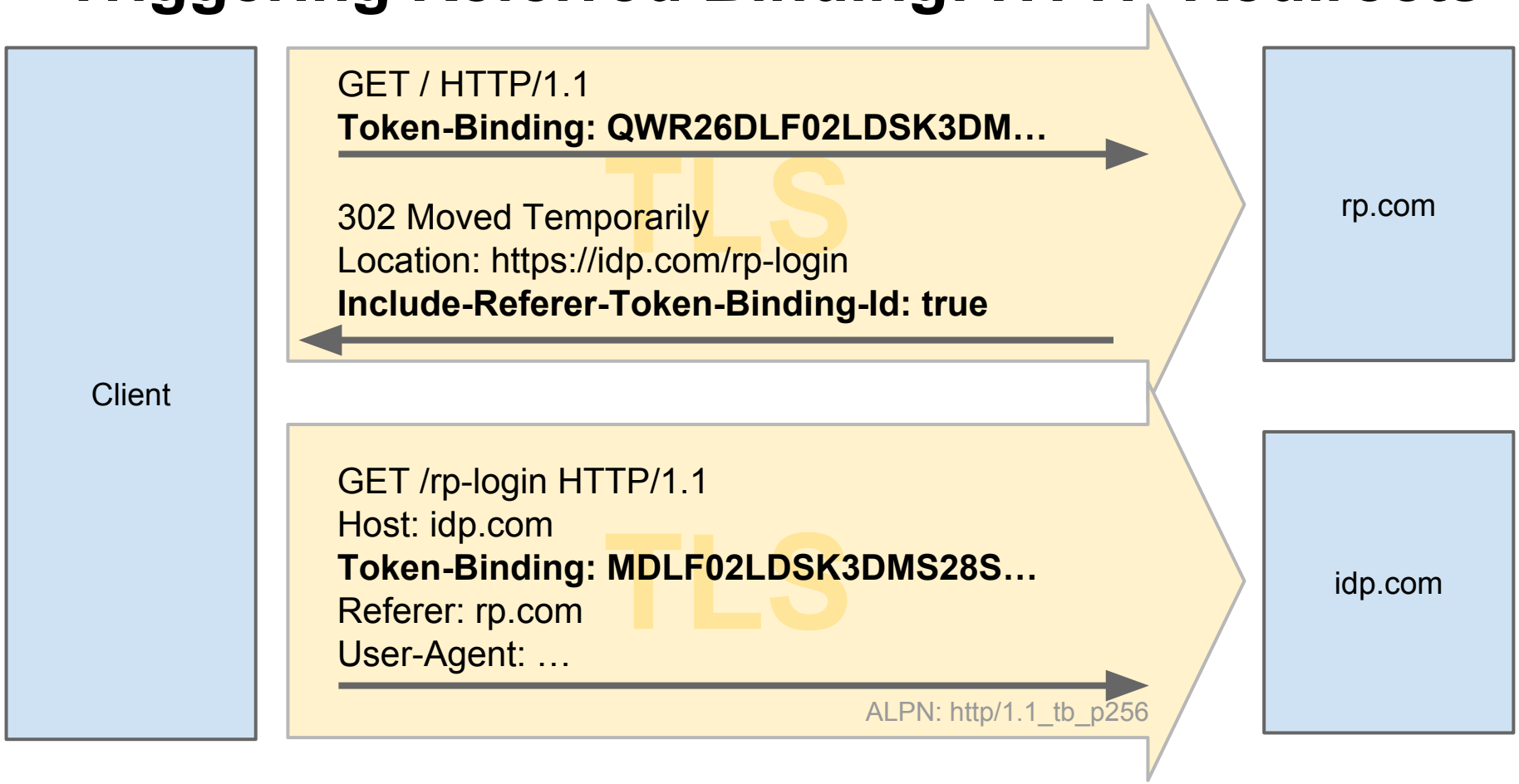
Federation Support

- Problem: Client uses different Token-Binding IDs with RP and IdP; IdP wants to issue bound tokens.
- RP allows client to reveal RP-associated (public) key to IdP
  - client still proves possession of corresponding private key
- IdP can then bind tokens to RP-associated key
- We define two mechanisms for RP:
  - HTTP response header
  - Javascript API

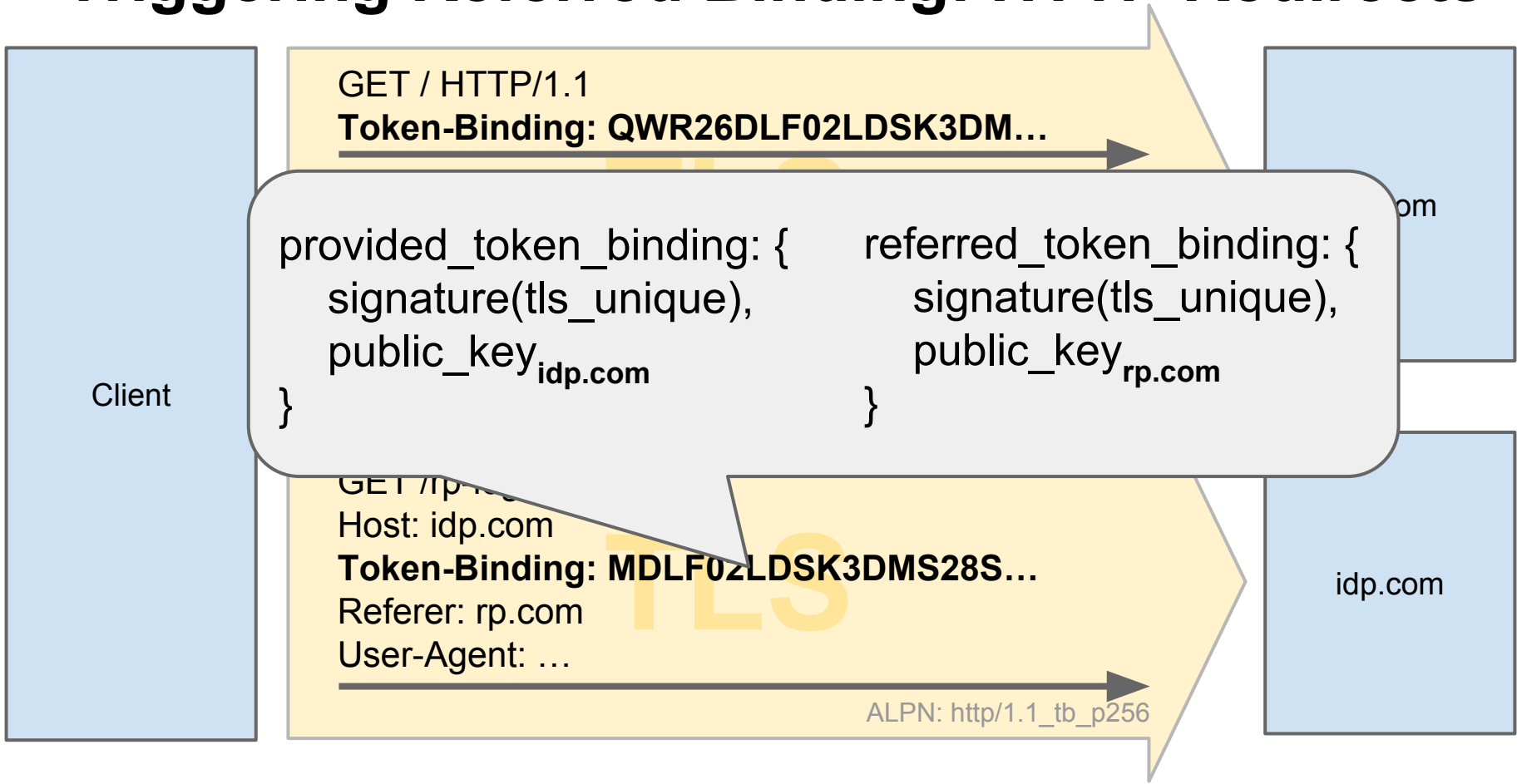
Triggering Referred Binding: HTTP Redirects



Triggering Referred Binding: HTTP Redirects



Triggering Referred Binding: HTTP Redirects



Triggering Referred Binding: XHR

- RP uses new property of XmlHttpRequest to make client ask IdP for RP-bound token

```
var xhr = new XmlHttpRequest();
xhr.withCredentials = true; // send cookies
xhr.withRefererTokenBindingId = true;
xhr.open(method, url, async);
```

- If property is true, Client includes `referred_token_binding` in `Token-Binding` header to IdP

Open Issues

- XmlHttpRequest vs. fetch()
  - which one to extend?

- Other ways for RP to signal to client
  - What other mechanisms do federation protocols use?
  - WebSockets? others?

Links and Contact Information

The Token Binding Protocol Version 1.0:
http://tools.ietf.org/html/draft-popov-token-binding-00

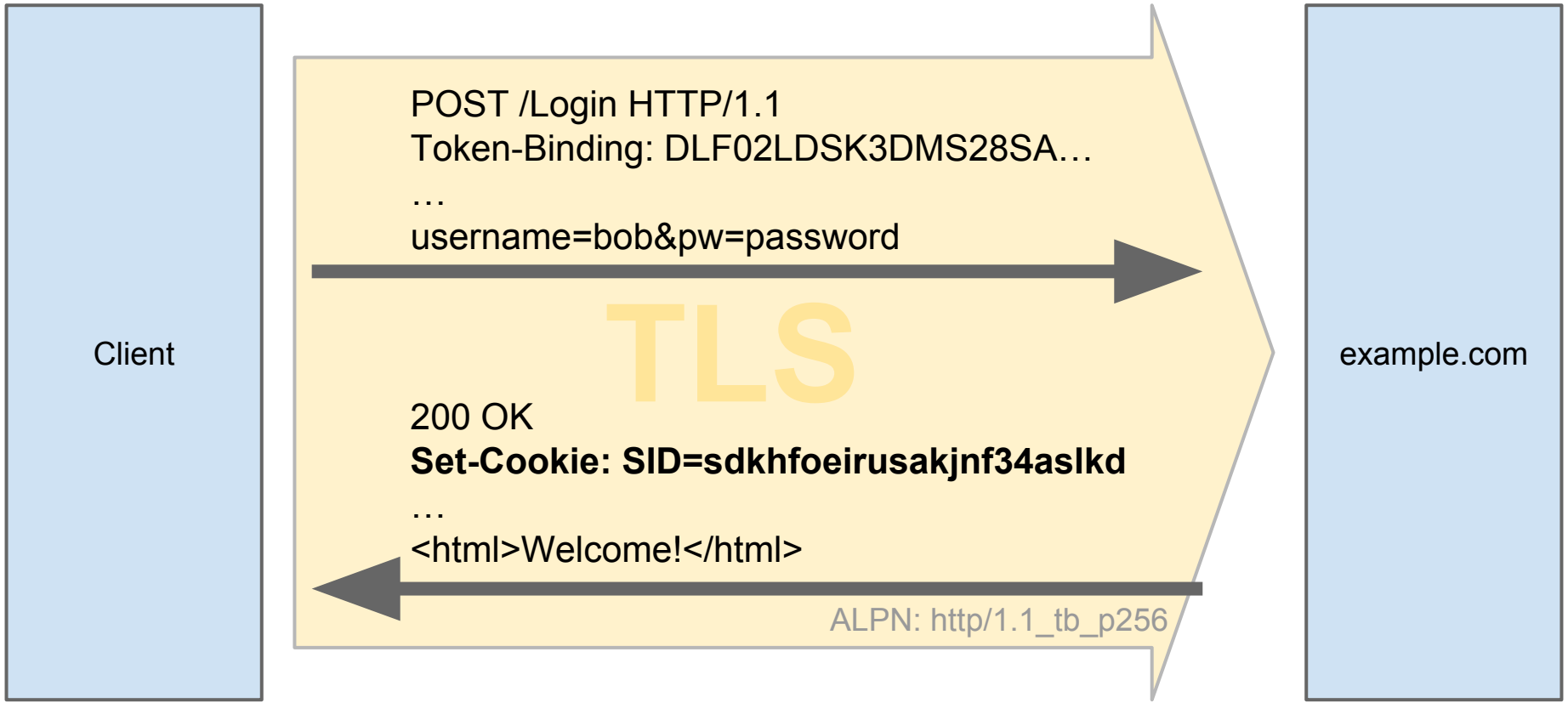
Token Binding over HTTP:
http://tools.ietf.org/html/draft-balfanz-https-token-binding-00

On GitHub:
https://github.com/TokenBinding/Internet-Drafts

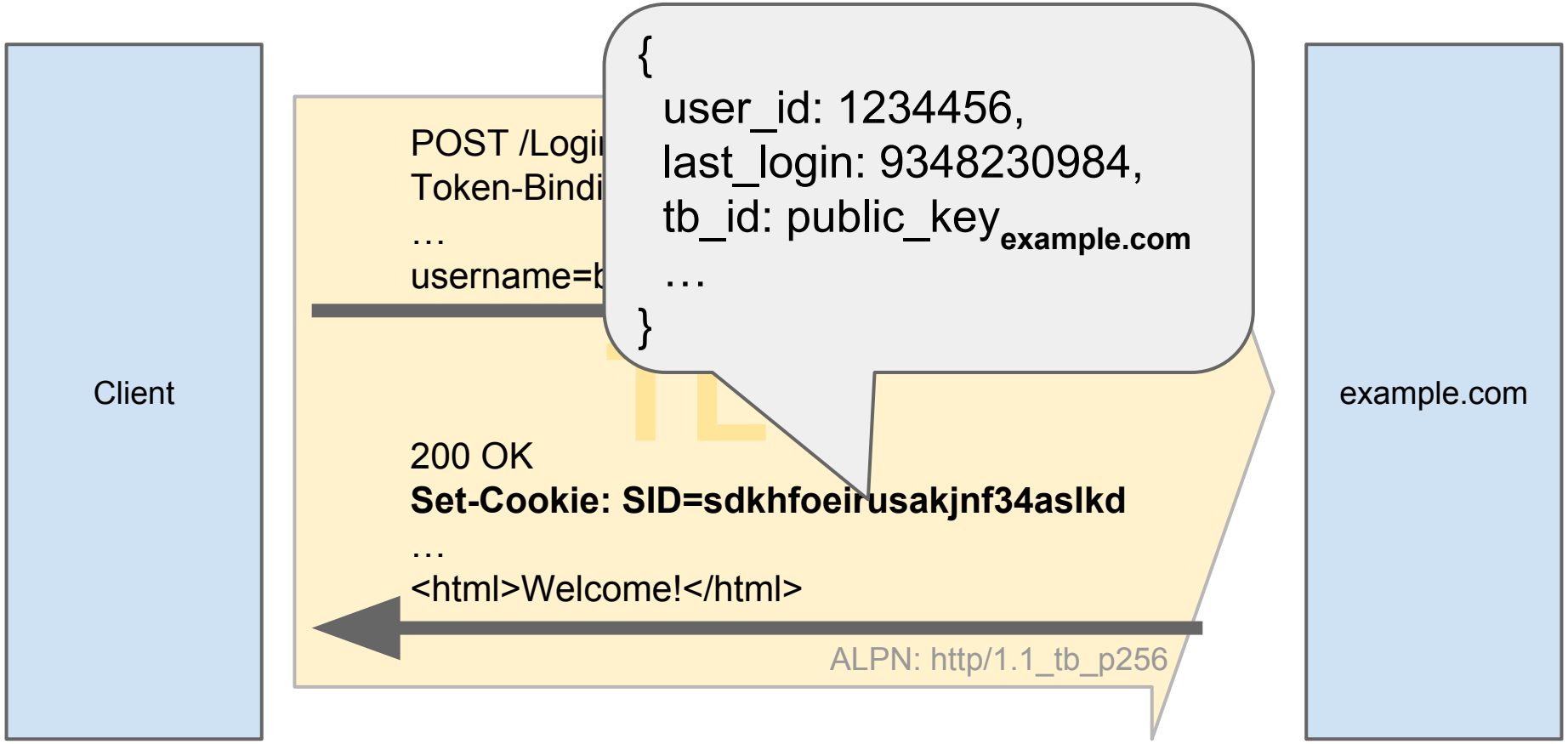
Dirk Balfanz balfanz@google.com
Vinod Anupam vanupam@google.com
Andrei Popov andreipo@microsoft.com

Appendix

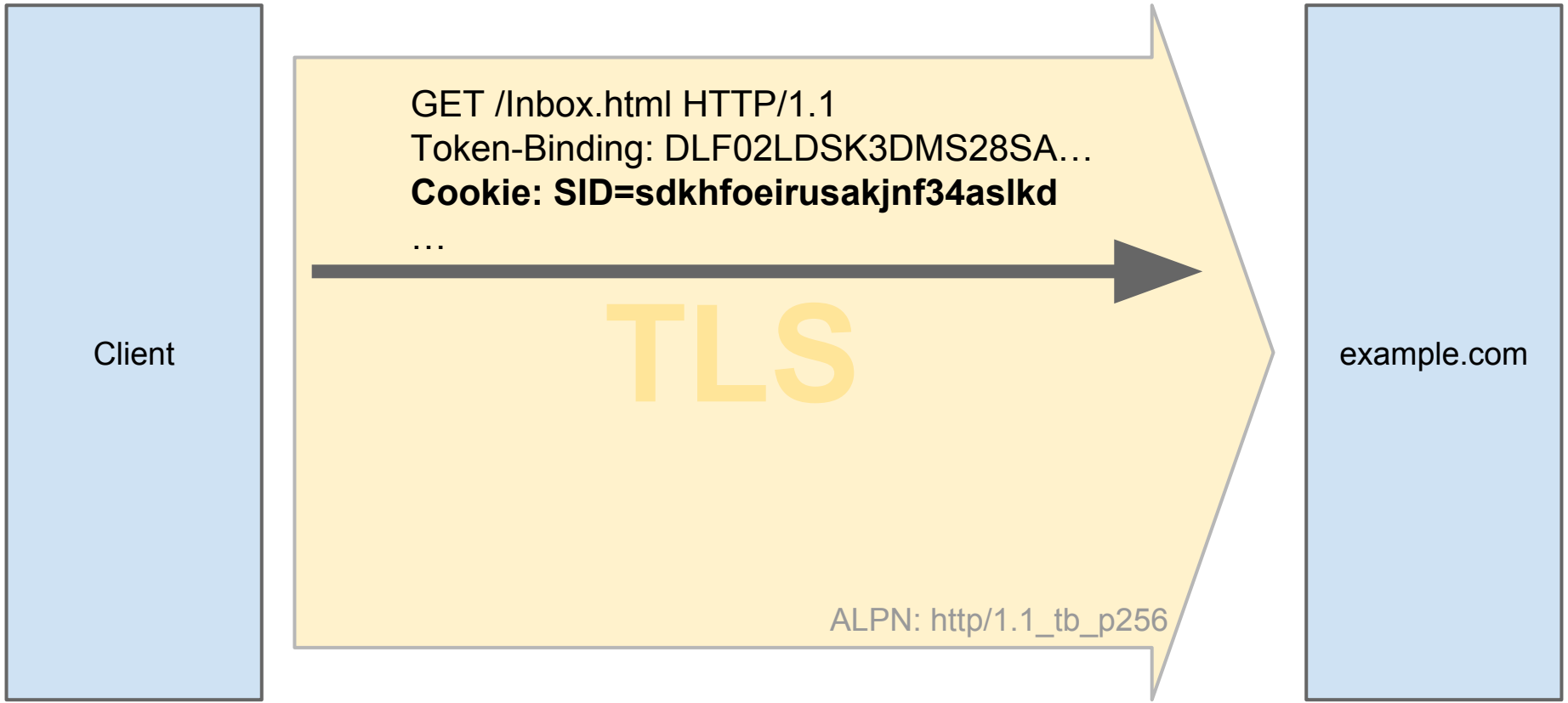
First-Party Binding



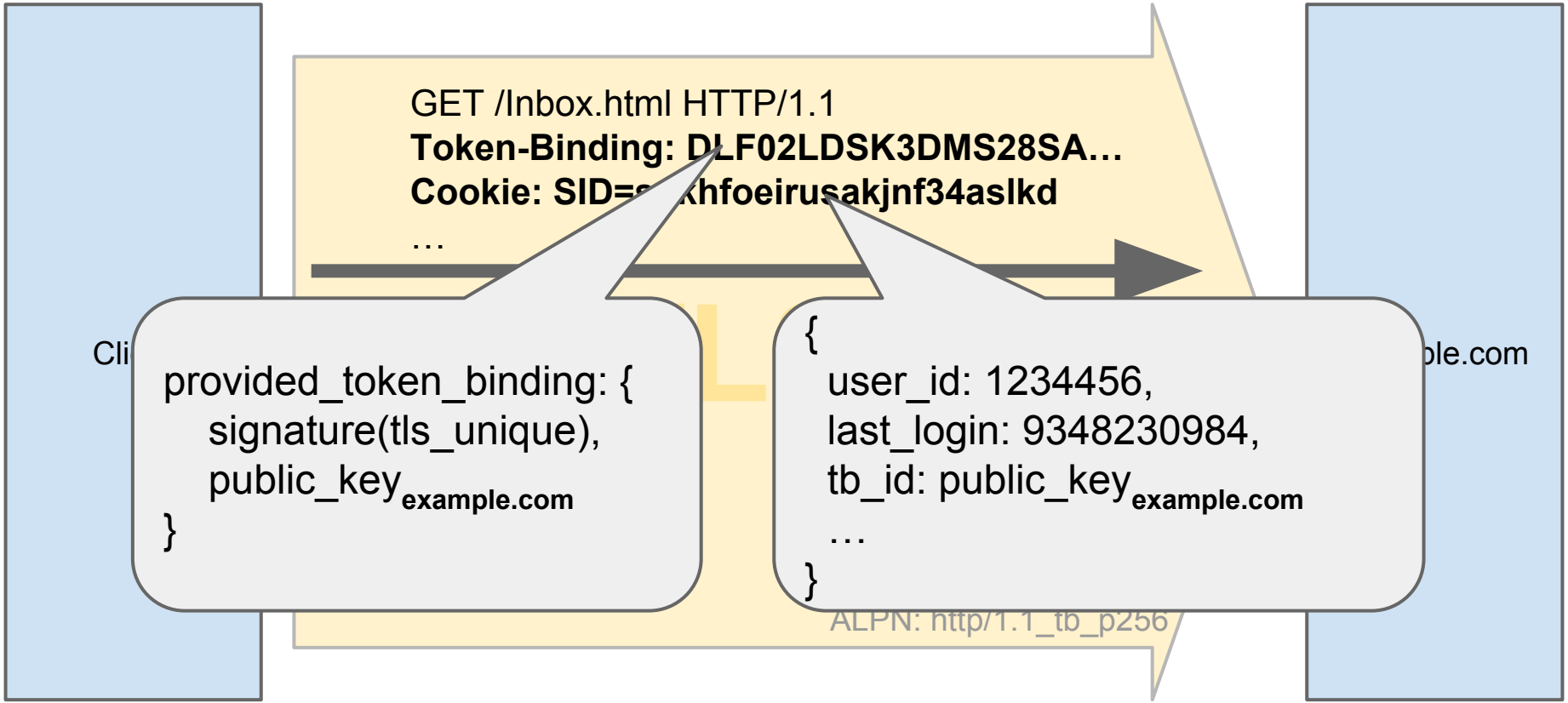
First-Party Binding



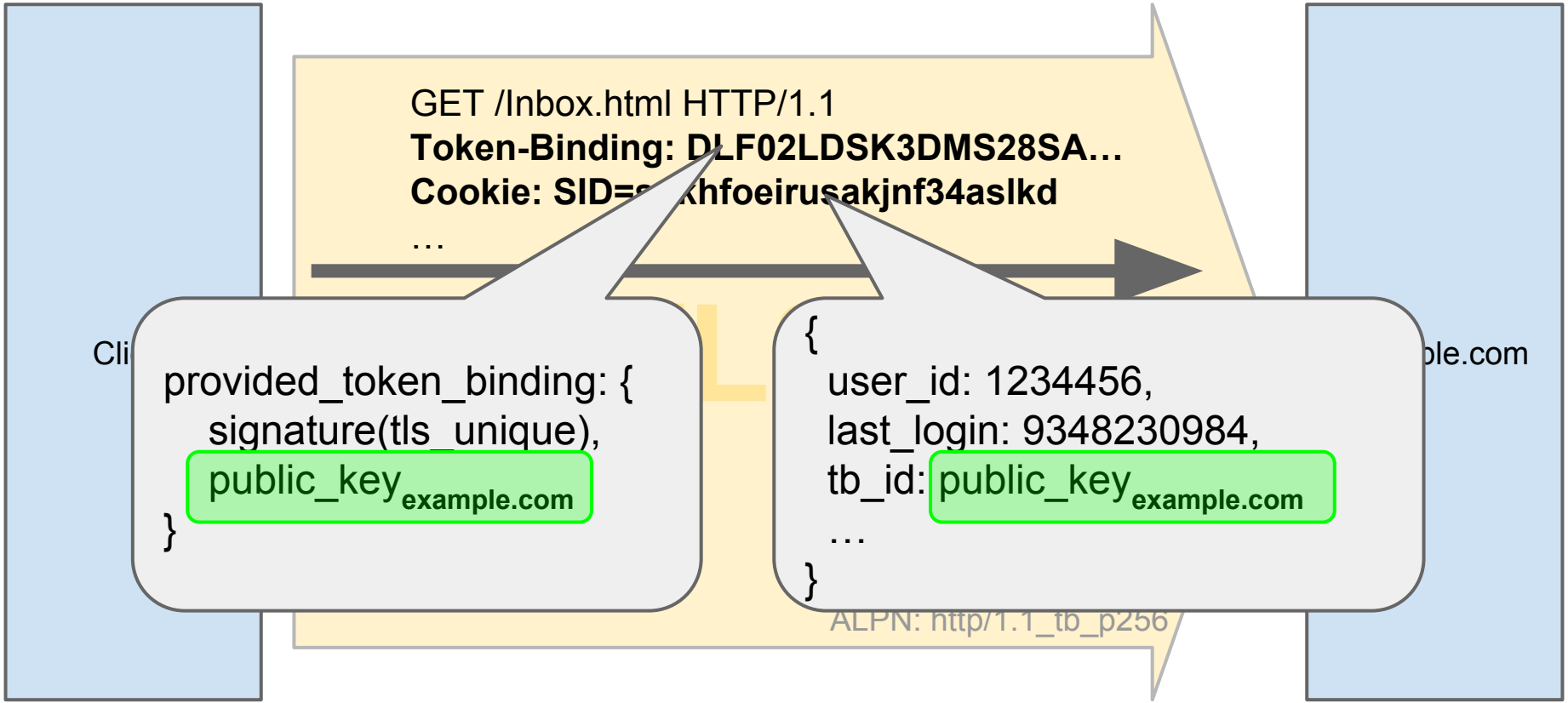
First-Party Binding



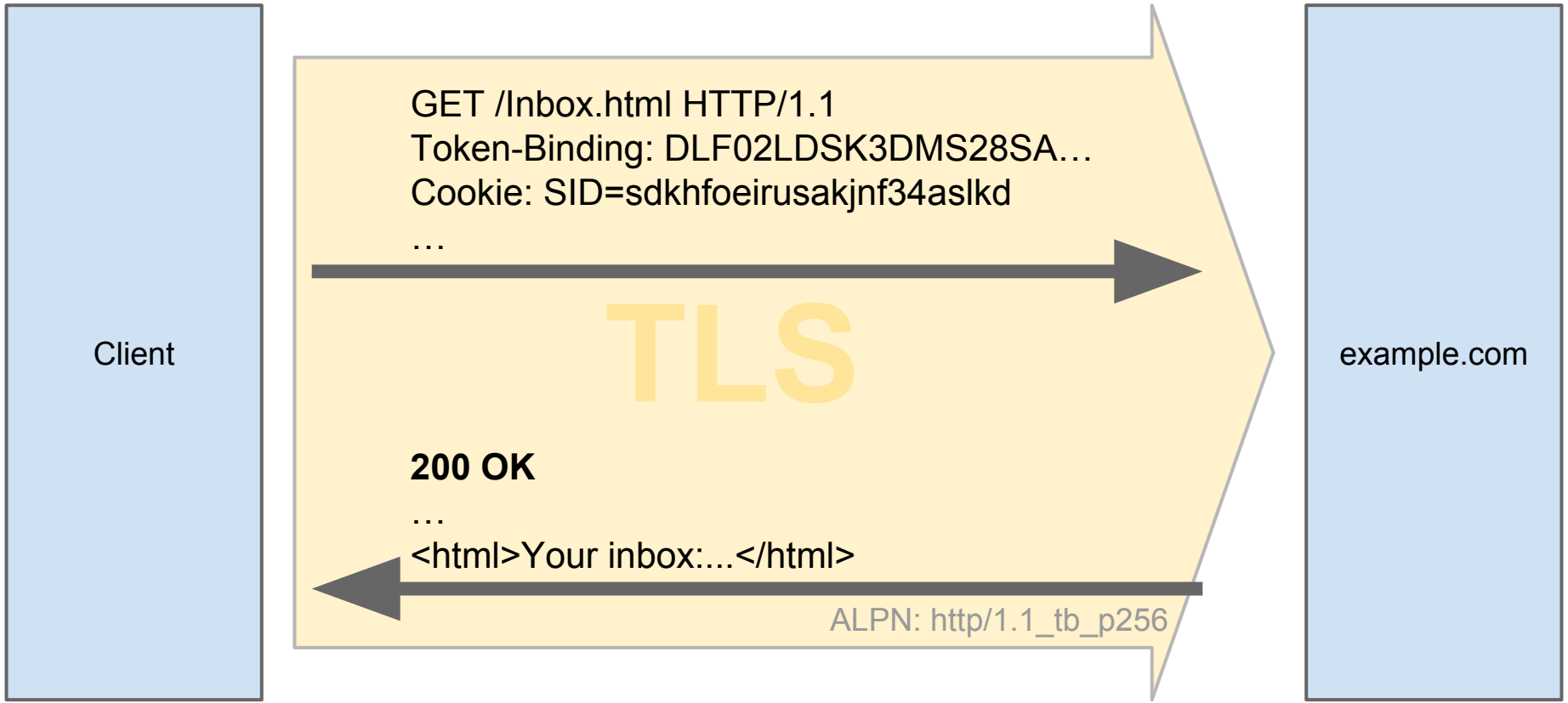
First-Party Binding



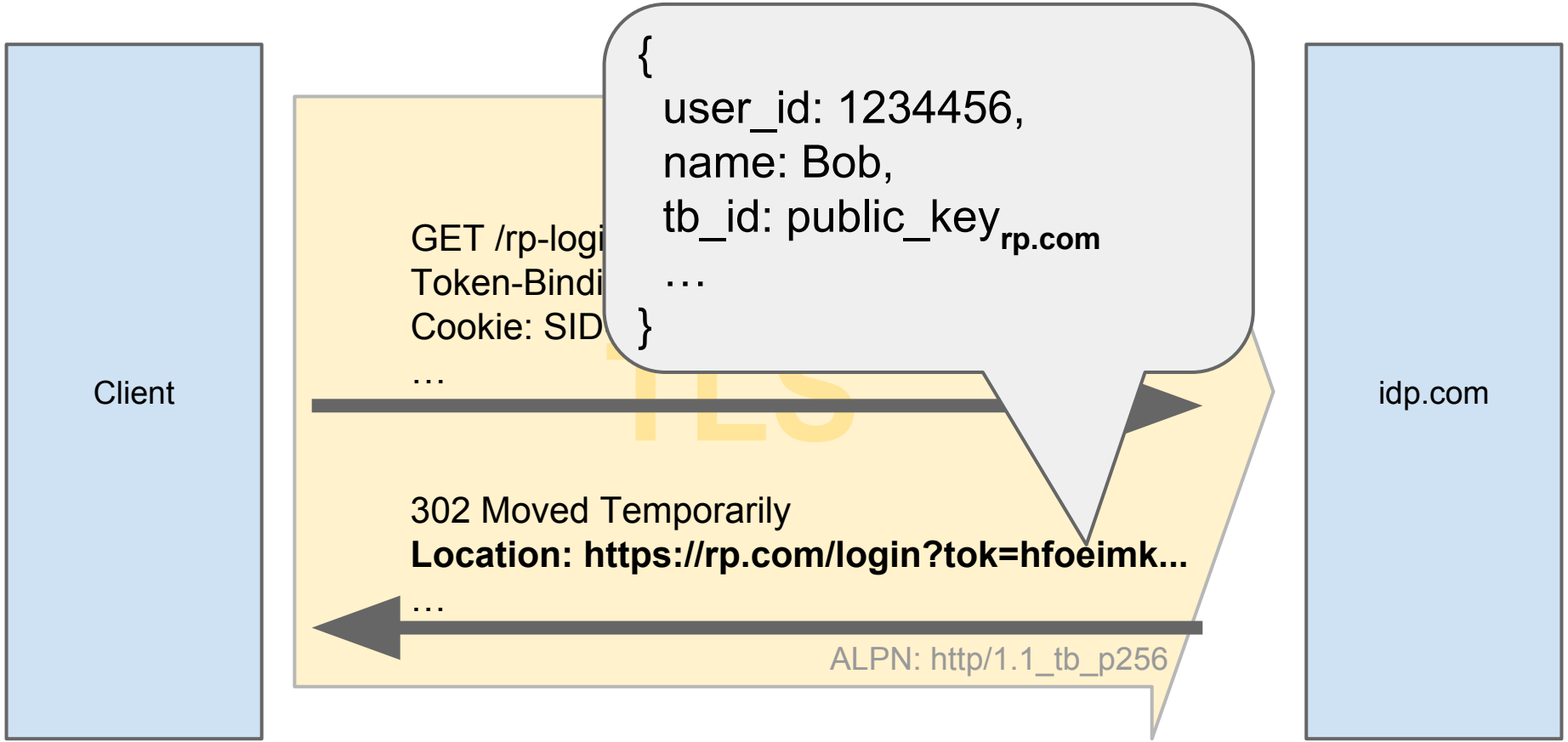
First-Party Binding



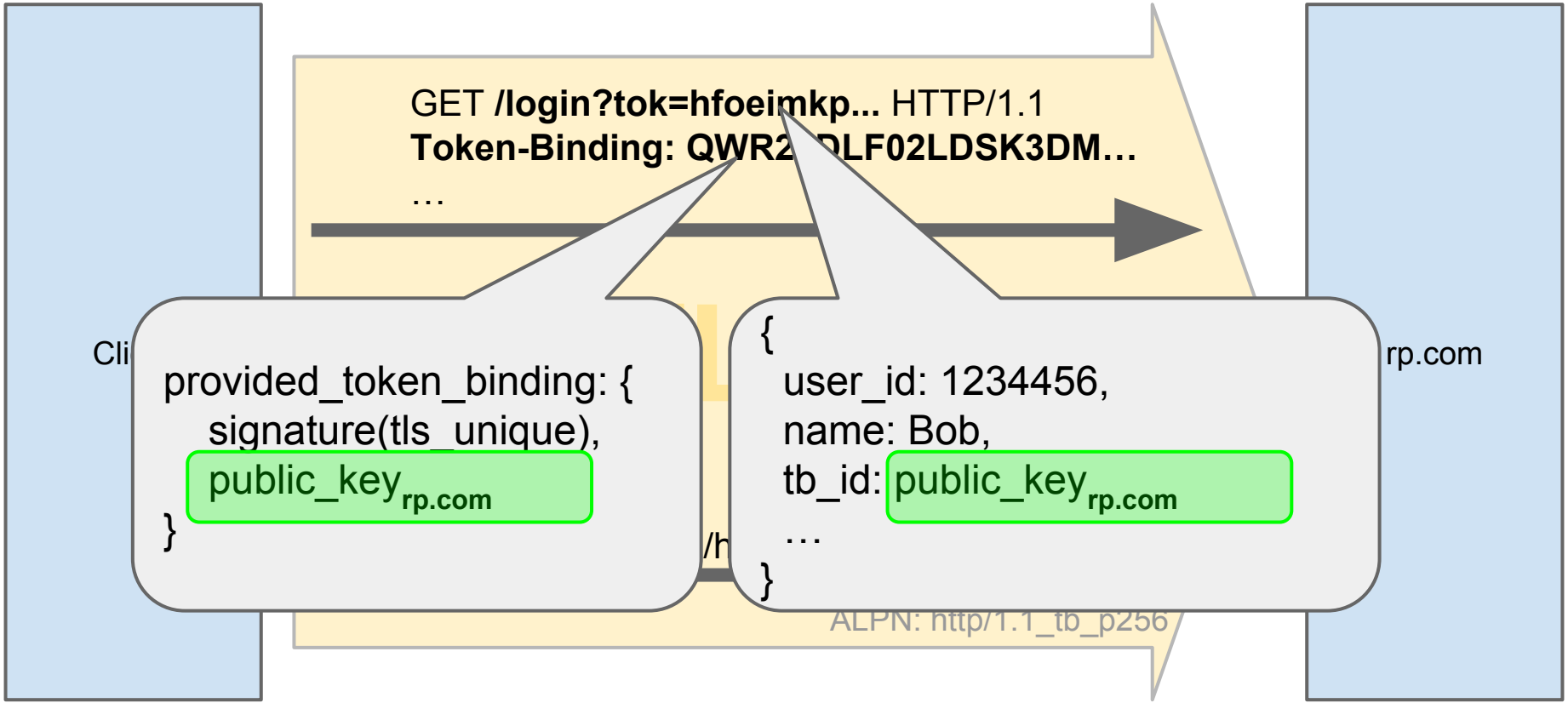
First-Party Binding



Federated Binding



Federated Binding



Privacy Considerations

Clients must

- use different Token Binding Ids for different eTLDs
  - Protects against cross-domain linking of user identities
- let users manage TB Ids like cookies
  - Must obey all user-specified cookie control settings
  - Must allow them to be cleared by user at any time
- not transmit TB Ids in the clear
  - They are persistent identifiers
    automatically presented by clients to identify themselves to servers

Security Considerations

Clients must

- negotiate Enhanced Master Secret Extn
  - Protocol uses `tls_unique` to create Token Binding Ids
  - EMS Extension protects against Triple Handshake Attack which
    - allows propagation of `tls_unique` value into other TLS connections
    - thus could allow bound tokens to be used over such connections
- protect Token Binding private keys
  - Bound tokens cannot be used by clients without right private keys

Clients *should* use hardware security modules

- to prevent stealing of private keys