IETF 91

OAuth SPOP

(Symmetric Proof of Possession for Code)

draft-ietf-oauth-spop-02

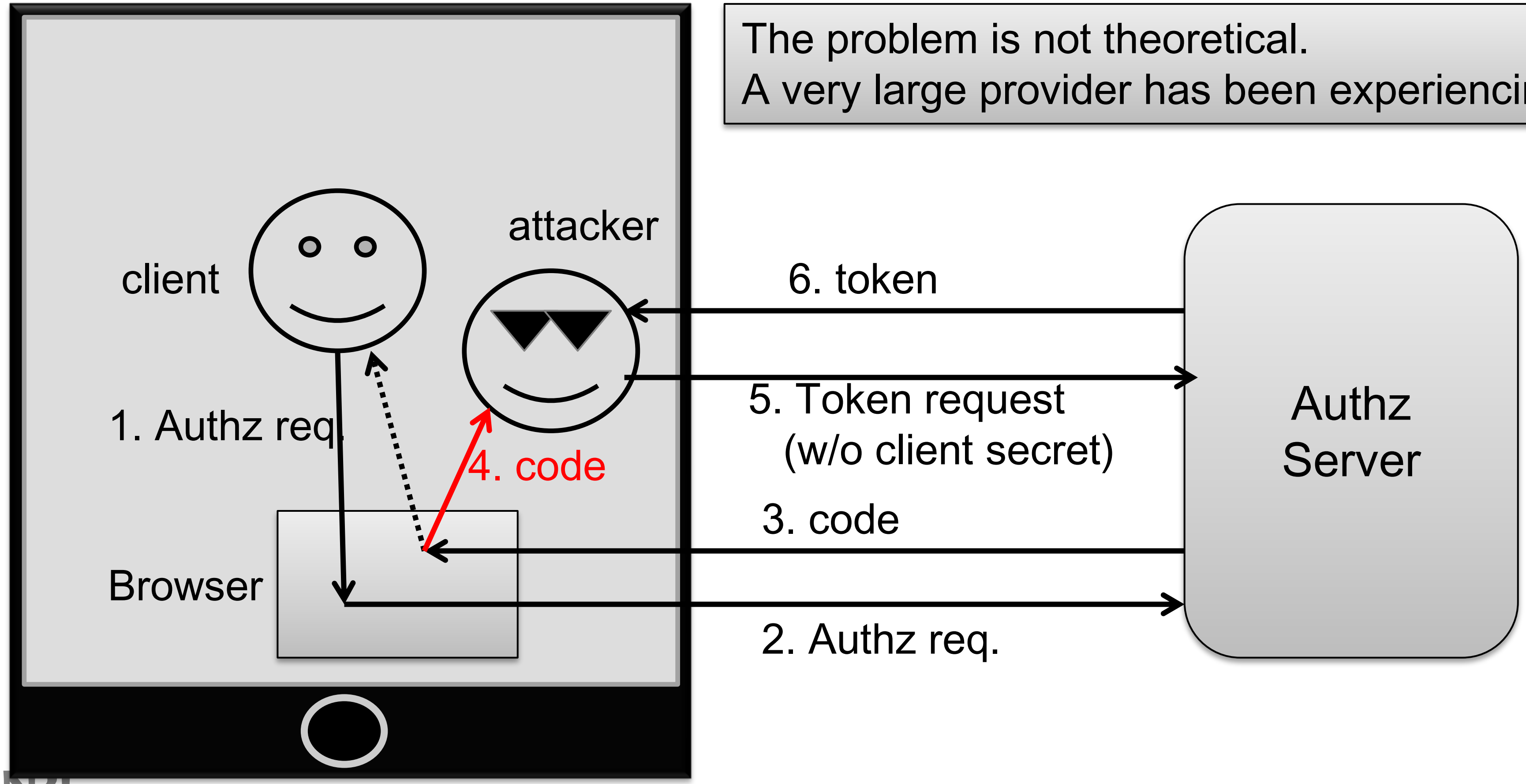
2014/11/12

Nat Sakimura
Nomura Research Institute, Ltd.
John Bradley
Ping Identity

Problem Statement 1

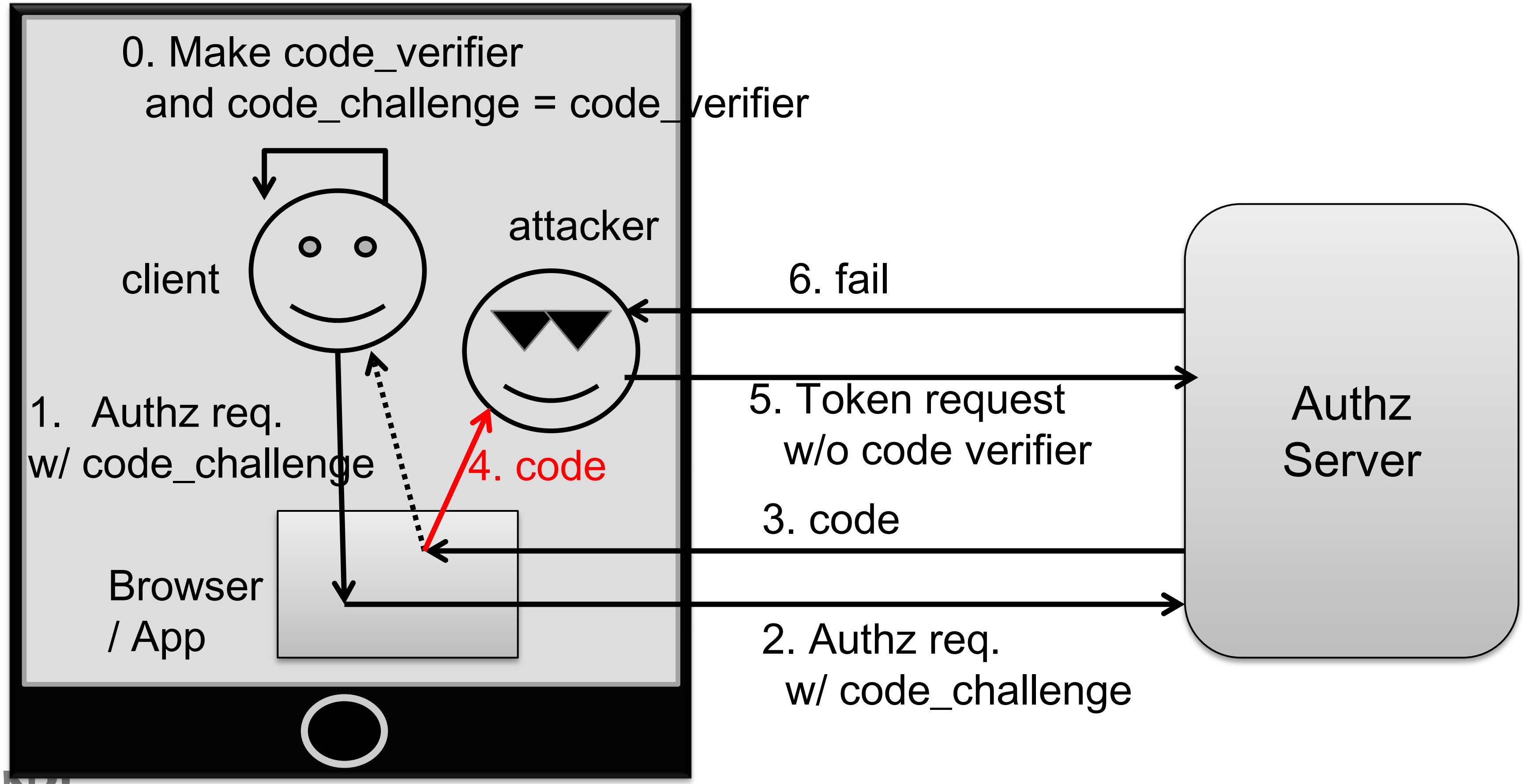
- Code interception attack (against public clients)
  - A malicious client gets the code instead of the client via registering the same scheme as the client, etc.

The problem is not theoretical.
A very large provider has been experiencing it.



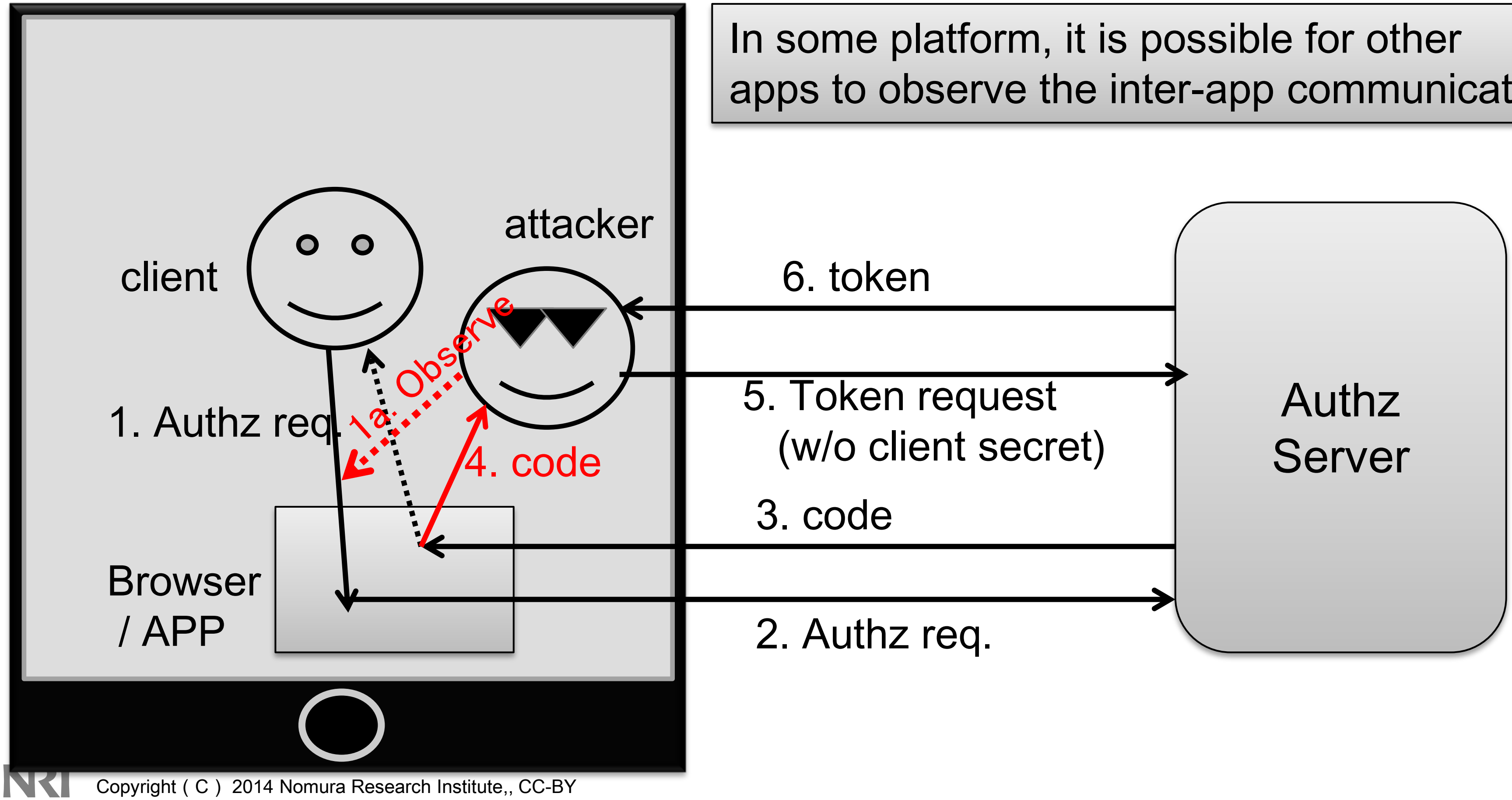
Solution 1

- Have the client create a one-time-credential and send it with the Authz req.
  - Based on the assumption that attacker cannot observe the request.



Problem Statement 2

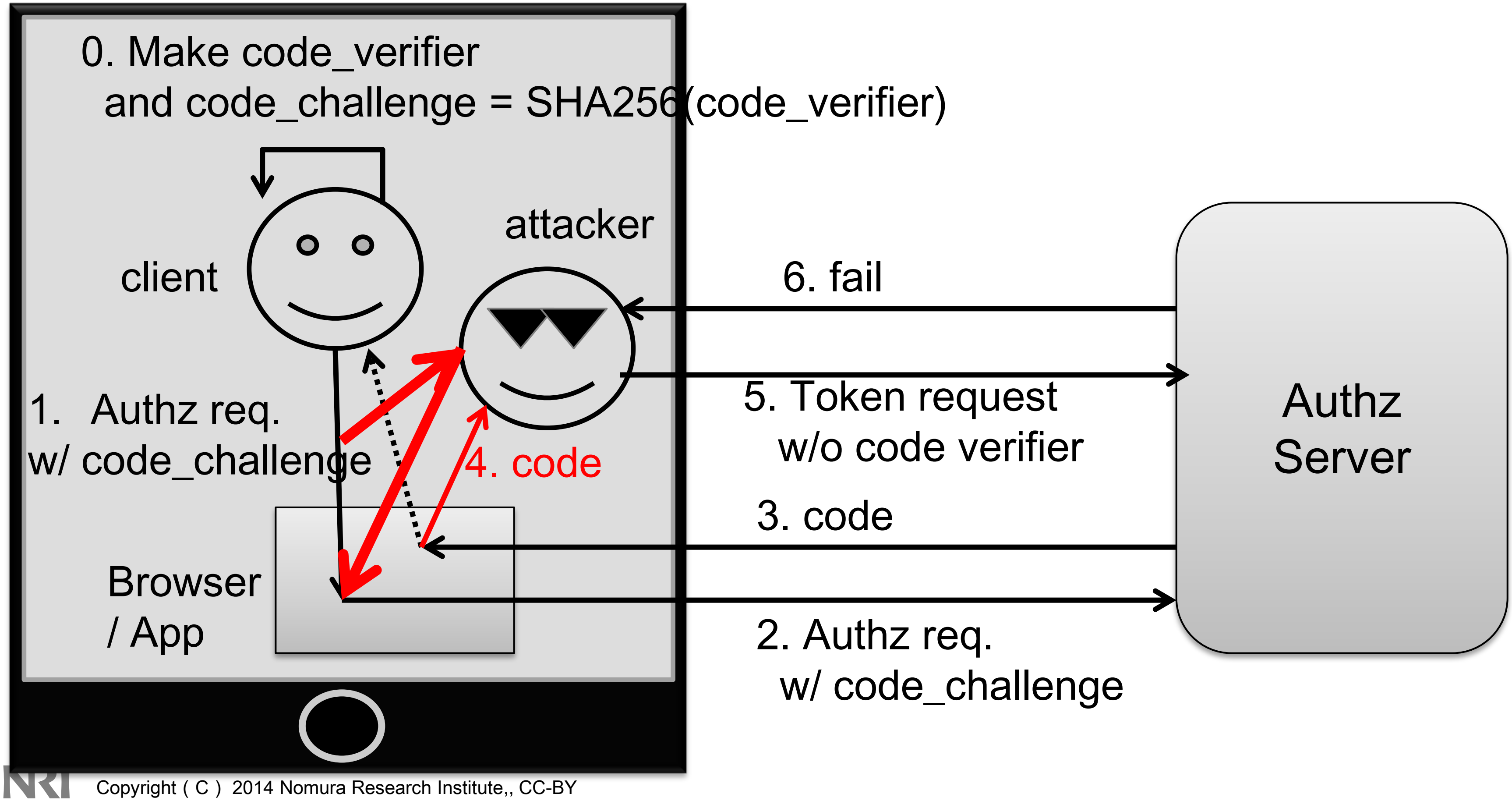
- Code interception attack (against public clients) + Authz req Observation
  - In addition to the code interception, he can actually see the AuthZ request, so it can see the code_challenge.



In some platform, it is possible for other apps to observe the inter-app communication.

Solution 2

- Have the client create a one-time-credential and send it with the Authz req.
  - Based on the assumption that attacker cannot observe the request.



Current Proposal

- Server MUST:
  - plain
  - S256 (sha256)
- MAY support:
  - none – plain OAuth
    - for compatibility with existing clients

FAQ

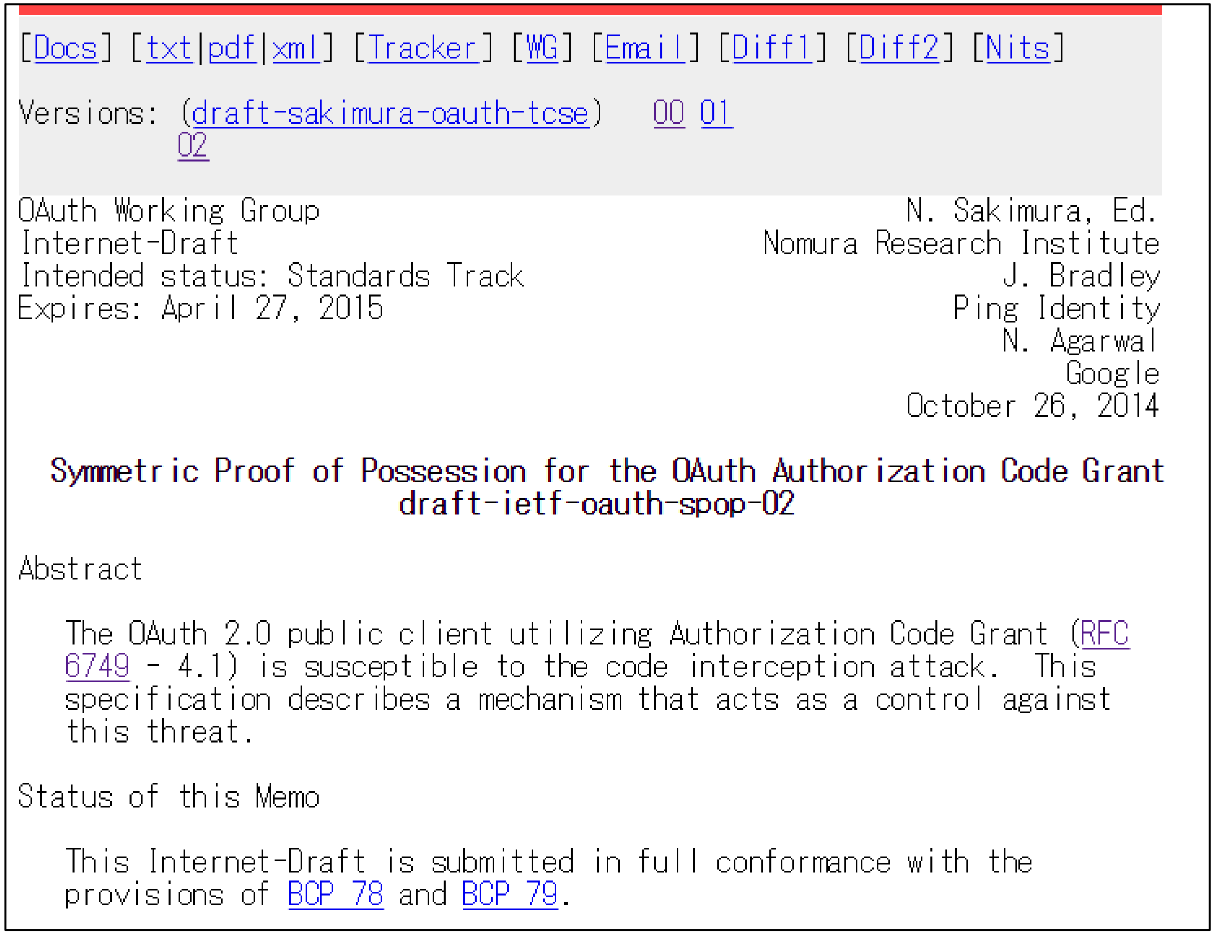
- Why does it not use asymmetric crypto?
  - Discovery of key and crypto algs, protocols, etc. .
  - Complexity.
- Why not only support SHA256?
  - Some client has no access to crypto libraries OR hard for them to use.
  - Clients can select based on the risk profile of the OS.
    - Simplifies the code.
  - (Graceful fallback and backward compatibility)
- Why not re-use the client secret field?
  - It is not the transient client secret. It is a secret for code, so semantically, it is different and we should not overload the field.

Draft is available as:

- https://tools.ietf.org/html/draft-ietf-oauth-spop-02

- WG LAST CALL

- Send comments NOW!



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

Versions: (draft-sakimura-oauth-tcse)    00 01
          02

OAuth Working Group                                      N. Sakimura, Ed.
Internet-Draft                                Nomura Research Institute
Intended status: Standards Track                             J. Bradley
Expires: April 27, 2015                                   Ping Identity
                                                             N. Agarwal
                                                                 Google
                                                       October 26, 2014


  Symmetric Proof of Possession for the OAuth Authorization Code Grant
                        draft-ietf-oauth-spop-02

Abstract

   The OAuth 2.0 public client utilizing Authorization Code Grant (RFC
   6749 - 4.1) is susceptible to the code interception attack.  This
   specification describes a mechanism that acts as a control against
   this threat.

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.
```

Todo: define error responses.

- Error response to authorization request
  - Returns `invalid_request` with additional error param `spop_error` with the following values:
    - `S256_unsupported`
    - `none_unsupported`
    - `invalid_code_challenge`

clients MUST NOT accept the downgrade request through this as it may be a downgrade attack by a MITM.

- Error response to token request
  - Returns `invalid_request` with additional error param `spop_error` with the following values:
    - `invalid _code_verifier`
    - `verifier_challenge_mismatch`
- Authorization server should return more descriptive information on
  - `error_description`
  - `error_uri`

ToDo: text clarifications

- It should make it clear that it is trying to mitigate the communication that is not protected by TLS: the inter-app communication.
- It should make it clear that for the “request”, it is not about MITM but the “observer” that it is trying to protect.
- It should make it clear that it is about transient secret for “code”, that it is authenticating the “code”.