Experience With Google Chrome's Trust Tokens

Yahoo

W3C Privacy CG - June 2022

yahoo!

Who are we?

- Jaime Perez - Sr Principal Architect, Identity Systems, Yahoo
- Sumit Kapoor - Sr Principal Architect, Identity Systems, Yahoo
- Wendell Baker - VP Architect, Advertising Systems, Yahoo

There are others off-stage and in devops & product.

yahoo!

Agenda

1. **Why we did this?** → What was our motivation?
   What questions we wanted to answer?
2. **What did we do?** → What we built. How it all works.
3. **What we learned?** → The limitations & areas of concern

yahoo!

What we found?

- Successfully built Proof of Concept internally
- Unable to determine clear Proof of Value being $-value < $$$-cost
  But this could change.
- Found areas of concern in operational complexity.
  Work is needed to simplify and publish “standard components”
- Found areas of concern in protocol evolution.
  Unknown effect of multiple proto versions while under $$$ urgency.

yahoo!

Motivation – Why we did all this?

- Google is building features to replace some aspects of 3rd party cookies.
  - Deprecate cross-site tracking, making 3rd party cookies obsolete by 2023→2026.
  - The Trust Tokens are addressing spam and fraud in the Google Privacy Sandbox initiatives.

  Our question: Does the technology scheme work in a functional sense?

  "Does the math work out in code?"

- As Yahoo, we want to [...use case...] Chrome Trust Tokens to [...goal...]
  - Understand how it works End to End; where it works; where it fails; how costly to operate.
  - Identify Use Cases for the business, the $$-benefit to offset all the devops, opex & capex.
  - Identify any limitations and security concerns.

  Our question: What is the feasibility of Trust Tokens as a gatekeeper to our business?

  "What if it breaks?"
  "What if they change the T&C?"
  "What if they change the proto and we can't?"

yahoo!

What did we do?

- We built a Proof of Concept (POC) in Q4 2021.
- We operated it Q4-Q1 to a friendly population.
- We fixed on protocol version TrustTokenPMBV2.
- We were able to issue and redeem Trust Tokens between our own services
  Among a small panel of pre-consented pre-disposed users
  The convenience sample + snowballing → employees plus more.

What did we NOT do?

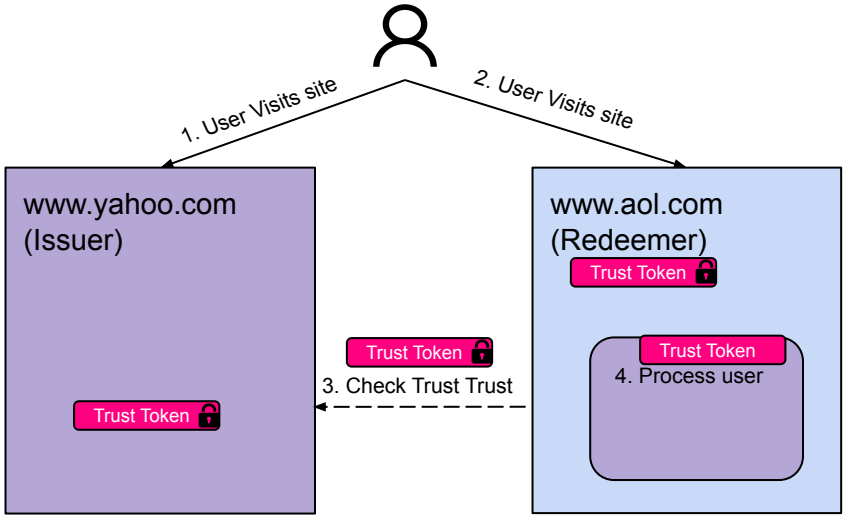
- Tested “at scale” with the full fire hose; *e.g.* frontpage.
- Operated through two full protocol evolutions v1→v2→v3 across the full serving surface.
- Dress rehearsal of a P0-$$$ event plus outages (think: Black Friday + forced protocol upgrade ratchet)

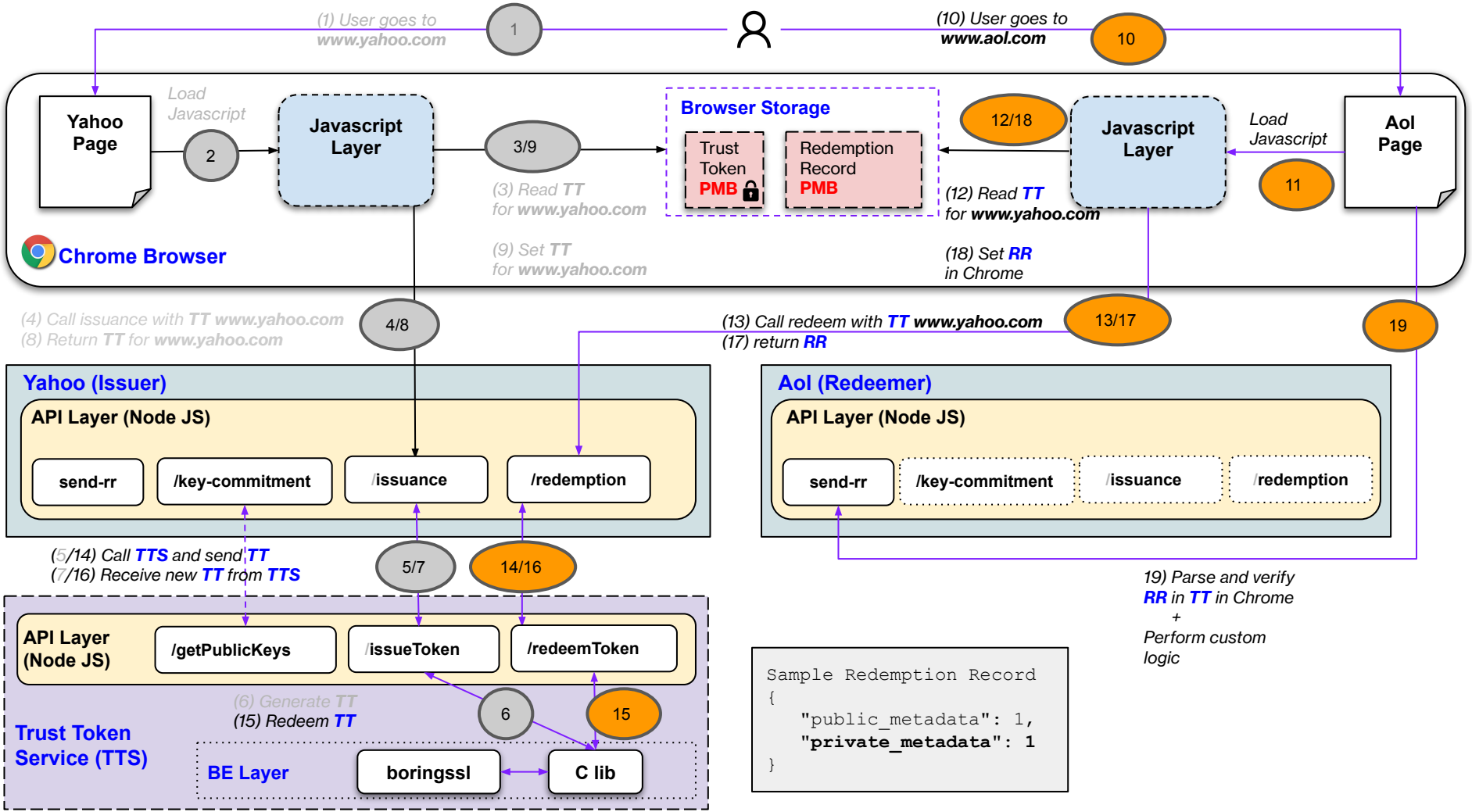
yahoo!

Use Case Explored

- Distinguish between a real user and an imposter.
  - When serving Ads
  - When user is trying to login or create an account

1. User visits www.yahoo.com and a **Trust Token** is generated
2. User goes to another site www.aol.com
3. AOL checks **Trust Token** from Yahoo
4. Based on **Trust Token** determine how to handle this user
   i. allow login?
   ii. how to handle Ads?




(1) User goes to www.yahoo.com
1
(10) User goes to www.aol.com
10
Yahoo Page
Load Javascript
2
Javascript Layer
3/9
Browser Storage
Trust Token PMB
Redemption Record PMB
12/18
Javascript Layer
Load Javascript
11
Aol Page
(3) Read TT for www.yahoo.com
(12) Read TT for www.yahoo.com
Chrome Browser
(9) Set TT for www.yahoo.com
(18) Set RR in Chrome
(4) Call issuance with TT www.yahoo.com
(8) Return TT for www.yahoo.com
4/8
(13) Call redeem with TT www.yahoo.com
(17) return RR
13/17
19
Yahoo (Issuer)
API Layer (Node JS)
send-rr
/key-commitment
/issuance
/redemption
Aol (Redeemer)
API Layer (Node JS)
send-rr
/key-commitment
/issuance
/redemption
(5/14) Call TTS and send TT
(7/16) Receive new TT from TTS
5/7
14/16
19) Parse and verify RR in TT in Chrome
+
Perform custom logic
API Layer (Node JS)
/getPublicKeys
/issueToken
/redeemToken
(6) Generate TT
(15) Redeem TT
6
15
Trust Token Service (TTS)
BE Layer
boringssl
C lib
Sample Redemption Record
{
"public_metadata": 1,
"private_metadata": 1
}

What we learned?

- We were able to Issue and Redeem Trust Tokens successfully.
- Proof of Concept(POC) worked but unable to determine Proof of Value (POV).

Areas of Concern

- Unclear if we are using Trust Tokens for the right Use Cases.
- Greater value comes when Trust can be shared with other companies.
- Redeemer sites can rely on at most 2 Issuers (avoids fingerprinting but not scalable).
- Presence of Trust Tokens can be seen by anyone (Security Risk).
- Maintenance overhead
  - BoringSSL C library, sole developer & maintainer is Google?
  - Trust Token protocol version cadence is Google's with no clear down-tempo plan.
  - Maintaining the Key commitments is fraught

    "and now you have yet another key management problem."
  - Failure modes & pathologies are unclear; hard to debug failures when PO-$$

yahoo!

Wrap up

- Third party cookies in Chrome to be problematic around 2023-2026
- Yahoo looking to use Trust Tokens for fraud prevention
- Successfully built Proof of Concept internally
- Unable to determine Proof of Value
- Found areas of concern in protocol, operations & TBD in business.

yahoo!

Thank You !!!

yahoo!

Q&A

yahoo!

Contact info

jaimeperez@yahooinc.com

wbaker@yahooinc.com

yahoo!