Public chromium.org document // davidvc@chromium.org, July 2021

What's TrustTokenV3?

"TrustTokenV3" is a collection of backwards-incompatible changes to Chromium's Trust Tokens implementation arriving starting in Chrome 92, which will reach Beta (small number of users) in early June and Stable towards the end of July.

The changes are:

1. In **Chrome 92**, the key commitment format will change for better future backwards-compatibility. (ISSUER_PROTOCOL.md in the Trust Token API GitHub repo describes the specifics of the changes to the key commitment format.) In particular, issuer servers will be able to serve key commitments for multiple Trust Tokens versions concurrently, and Chrome will select the right commitment based on which version(s) it supports.
2. In **Chrome 93**, the request signing operation's signature scheme is changing from Ed25519 to P-256 ECDSA, somewhat improving server-side compatibility at the cost of slightly worse performance. Additionally, the signed request signature header's schema is changing slightly, to bring the structure better in line with signature payload formats in related cryptographic features.
3. Just like for any new Trust Tokens version, Chrome will send a different `Sec-Trust-Token-Version` header along with its issuance and redemption requests, and it will use a new domain separator string when defining its signed requests' signing data. Additionally, Chrome will begin sending the `Sec-Trust-Token-Version` header alongside signed requests, in contrast to the prior behavior of only sending the header alongside issuance and redemption requests.

Updating an end-to-end Trust Tokens integration to support Chrome 92 and 93

Here's how to update a full suite of key commitment, token issuance, redemption, and signed request consumption systems to be compatible with these new changes.

- For **Chrome 92**, the key commitment endpoint should start serving TrustTokenV3-format key commitments, and the issuance and redemption services should be able to handle requests bearing `Sec-Trust-Token-Version: TrustTokenV3` request headers.
- For **Chrome 93**, the signed request consumption system should be able to validate TrustTokenV3 signed requests. Recapping from above, the changes to signed requests coming in Chrome 93 are:

1. Signed requests' domain separator string changes from `TrustTokenV2` to `TrustTokenV3`.
2. Signed requests' public keys change to be P-256 points in the standard (uncompressed) point encoding.
3. Signed requests' signatures become DER-encoded ECDSA-Sig-Value objects containing P-256 (SHA-256) ECDSA signatures.
4. The `alg` field in signed requests' `Sec-Signature` header moves into the `signatures` field, as in the golden request below.
5. The `alg` field's value becomes `"ecdsa_secp256r1_sha256"`, to indicate that the signature comes from P-256 ECDSA.

"Golden" post-Chrome 92 key commitment result

Here's a Chrome 92+ key commitment result, reflecting the TrustTokenV3 key commitment format changes of (1) nesting commitments by their Trust Tokens version, and (2) embedding keys in a new `"keys"` member, rather than at the same level as the per-commitment metadata fields like `"batchsize"` and `"id"`.


```
{
   "TrustTokenV3VOPRF" : {
      "batchsize" : 25,
      "id" : 5,
      "keys" : {
         "9" : {
            "Y" :
"AAAACQRl13pTAyCF21Y6Xk130/WKwvtsL8PjNd+HWG4kQ9wjbMC9NWFy6ZNsJ4MUxpr9XMA6sAAcBDLUI6uJ6dtbe6Rn4Oaeeb5SzY
OMKiVozW2IxGSAoJcFGaIGimNQUnOa7eU=",
            "expiry" : "1628182800000000"
         }
      },
      "protocol_version" : "TrustTokenV3VOPRF",
   }
}
```


"Golden" post-Chrome 93 signed request

Here's a Chrome 93+ signed request, complete with all five changes: a signature computed over the new domain separator string; P-256 signature, public key, and algorithm identifier; and the version header.


```
Sec-Redemption-Record:
"https://a.test:39135";redemption-record=:Ym9keT06cEdodFpYUmhaR0YwWWFKbWNIVmliR2xqQUdkd2NtbDJZWFJsQUdwM
GIydGxiaTFvWVhOb1dDQXlSWnJWdUhJYzBYYjlPRzNxZFZLcmdoYncxeUlnSklLTGtGQjl4Qllob1d0amJHbGxiblF0WkdGMFlhTm9h
MlY1TFdoaGMyaFlJRzdoV1FmSG5lVS9YcjVyVlRJeTlWeXN1MGorY203dWl0UkdSUXpnMW5SYmNISmxaR1ZsYldsdVp5MXZjbWxuYVc
1MGFIUjBjSE02THk5aExuUmxjM1E2TXpreE16VjBjbVZrWlcxd2RHbHZiaTEwYVcxbGMzUmhiWEFhWVA5RVJuQmxlSEJwY25rdGRHbH
```

```
RaWE4wWVcxd0FBPT06LCBzaWduYXR1cmU9OktWR0tzWnoyVXV1bzhCZ0hnSmtyVmRmdTg5R2J0V1VIME1HVG1tQWJWSWtHdWRqMXVKb
TVVbVFHQS83Y09LenB2V1E4L2M1REdBNEFqQW9SQnJ1TENRPT06:

Sec-Signature:
signatures=("https://a.test:39135";public-key=:BCGEjkKZJuBqMIcpOkPh7pUYLSHUfVHJHTET/aBfsCY6GOAEY2lEILA1
HTPFl7Sk4Mbr6BLbMOx9i/SXEXb08dE=:;sig=:MEUCIBMpY10dGkgFwEYtBydjHIKuqcUwFJpGXArQ+Lbssii5AiEA9twtv8vXAPQo
Cc/9BVBQSI6SOvN/yBmKFq58X7HOsaY=:;alg="ecdsa_secp256r1_sha256"), sign-request-data=include

Sec-Trust-Token-Version: TrustTokenV3
```