ARCHITECTURE: ISSUER CARDINALITY

Alex Davidson

privacypass WG IETF110 ::: 2021-03-12
::: Architectural framework for analysing anonymity of users in multi-dimensional ecosystem

::: Minor changes from -00: clarifying token metadata and expiration discussions
::: Unlinkability is determined in relation to the tokens that a client owns.

::: Every successful redemption reveals the issuer of the token.

::: Third-party verification of redemptions reveals all of the previous issuances that a client has participated in.
ISSUER CARDINALITY & PRIVACY
ISSUER CARDINALITY & PRIVACY
WORST-CASE: each issuer in the system reduces the privacy of a client by 1 bit (≡ an exponential decrease).
:: MAIN TAKEAWAY ::

**WORST-CASE**: each issuer in the system reduces the privacy of a client by 1 bit (≡ an exponential decrease).

Independent of any other privacy-reducing features, e.g. appending token metadata.
Section 10 discusses the parametrization of a generic ecosystem.

Equation for \# issuers (Table 1) is:

$$\approx \log_2 \left( \frac{|\text{users}|}{\min(|\text{anon_set_size}|)} \right) - \max(\text{metadata_bits})$$

|users| = 1 billion \approx 2^{30} \text{ and } \min(\text{anon_set_size}) = 5000 \approx 2^{12} \text{ implies } \# \text{ issuers} \leq 17.$$
Section 10 discusses the parametrization of a generic ecosystem.

Equation for \# issuers (Table 1) is:

\[
\log_2 \left( \frac{|\text{users}|}{\min(|\text{anon_set_size}|)} \right) - \max(\text{metadata_bits}) \approx \frac{\log_2(\min(|\text{anon_set_size}|))}{2}
\]

\(|\text{users}| = 1 \text{ billion} \approx 2^{30}\) and \((\min(\text{anon_set_size}) = 5000 \approx 2^{12})\) implies \# issuers \(\leq 17\).
Small numbers of issuers are impractical (higher impact for smaller ecosystems).

Privacy bits are only lost when redemptions occur.
::: Small numbers of issuers are impractical (higher impact for smaller ecosystems).

::: Privacy bits are only lost when redemptions occur.

::: Alternative option is to reduce occurrences of redemptions.
::: Small numbers of issuers are impractical (higher impact for smaller ecosystems).

::: Privacy bits are only lost when redemptions occur.

::: Alternative option is to reduce occurrences of redemptions.

::: Or, limit the number of issuers that a client redeems with (Section 10.3).
::: Client redemption tokens should only be held for a small number of issuers within each ecosystem.

::: Or, client only redeems tokens for a small subset.

::: Allows moving privacy consideration to # tokens, instead of # issuers.
::: How does a client manage which issuers it should interact with?
   ▶ e.g. what happens when a client receives tokens from a new issuer?

::: How can client redemption contexts be practically enforced?
   ▶ (See Steven’s talk).

::: Are these questions application-specific?

::: What architectural guidance is suitable?