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

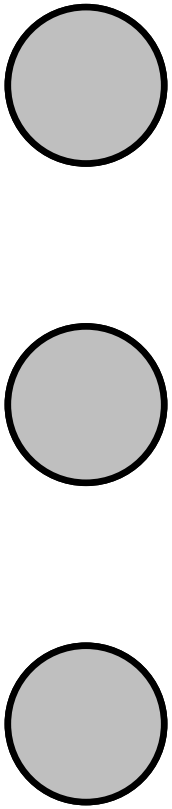
INTRODUCTION

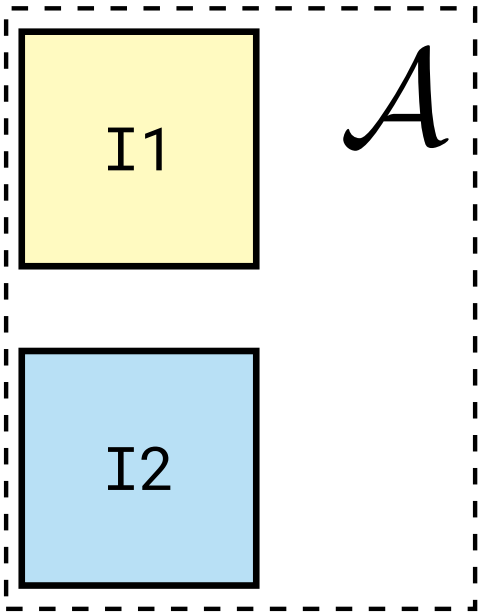
::: Unlinkability is determined in relation to the tokens that a client owns.

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

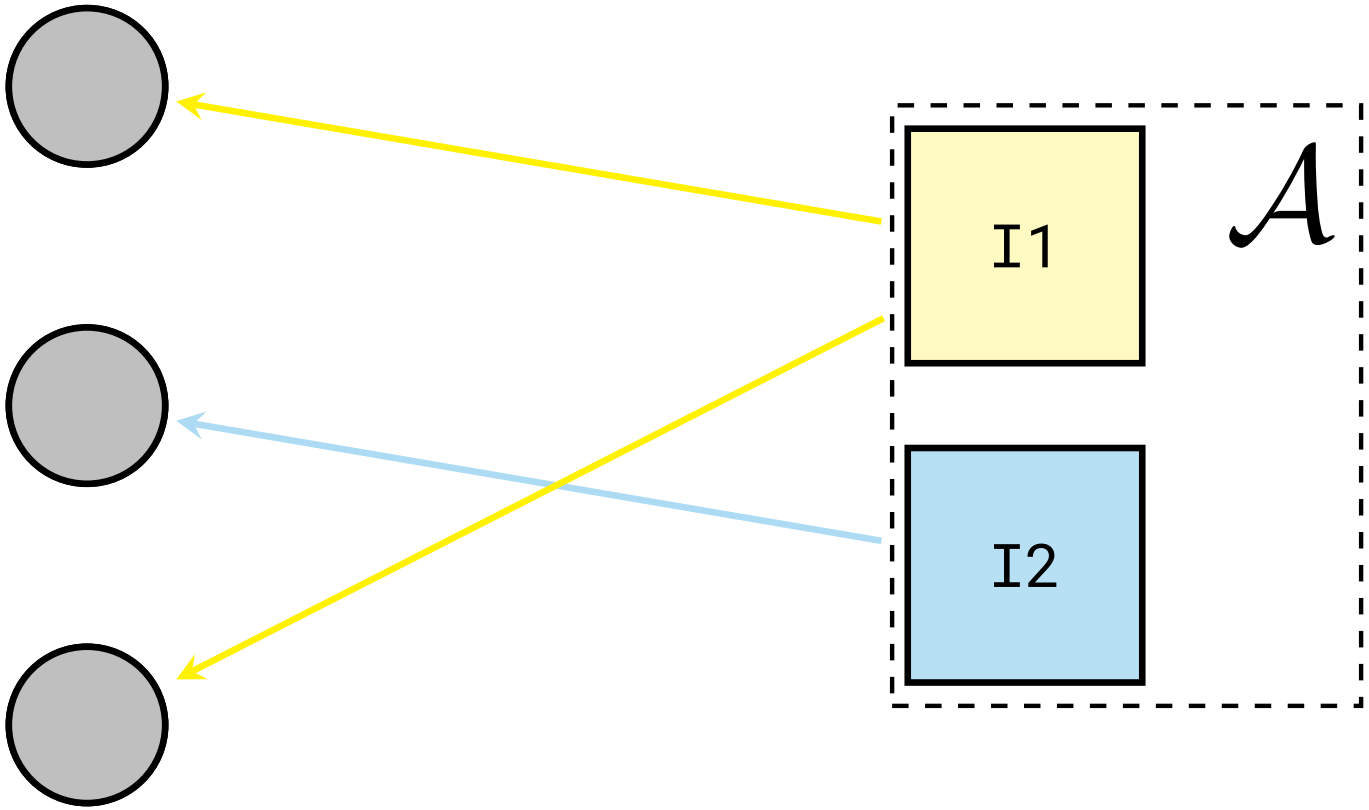
::: Third-party verification of redemptions reveals all of the previous issuances that a client has participated in.

ISSUER CARDINALITY & PRIVACY

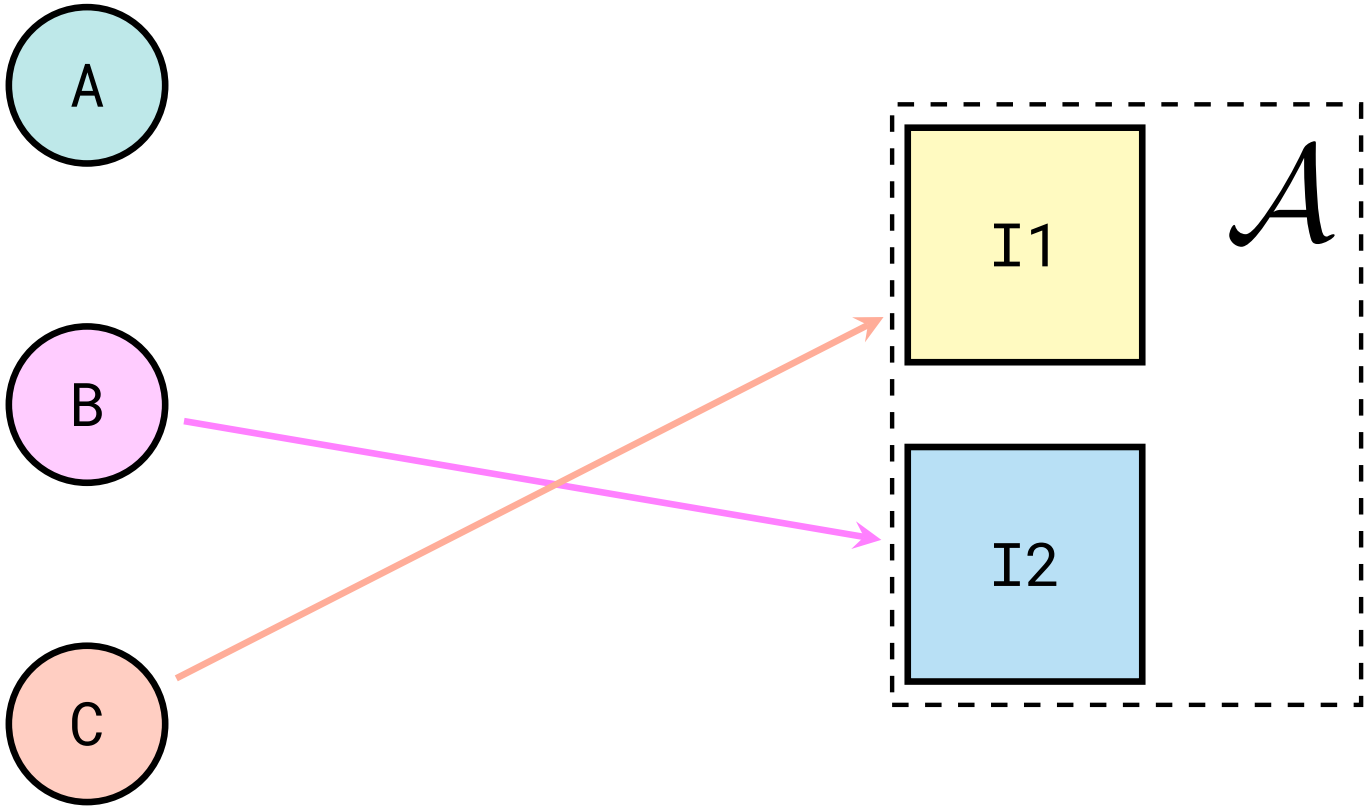




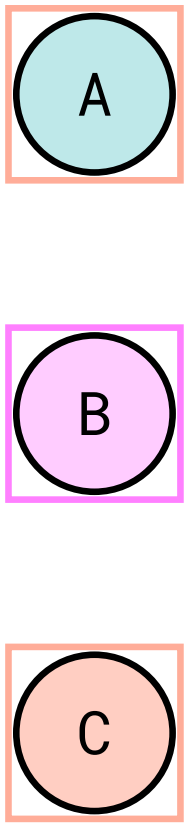
ISSUER CARDINALITY & PRIVACY

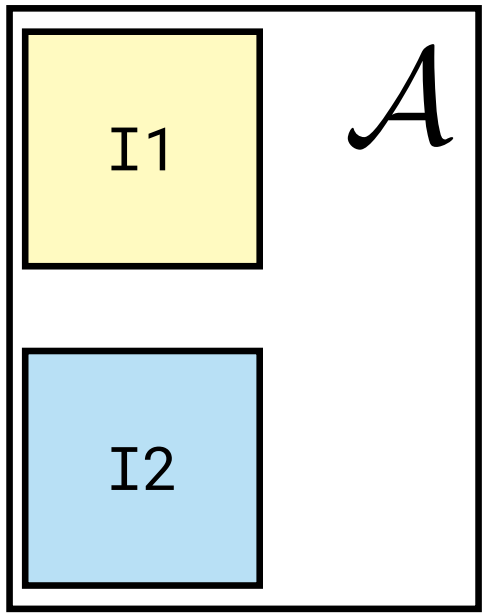


ISSUER CARDINALITY & PRIVACY



ISSUER CARDINALITY & PRIVACY





ISSUER CARDINALITY & PRIVACY

:: **MAIN TAKEAWAY** ::

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:

$$\approx \frac{log_2\left(\frac{|users|}{min(|anon\_set\_size|)}\right) - max(metadata\_bits)}{2}$$

ENFORCING LOW NUMBER OF ISSUERS

::: Section 10 discusses the parametrization of a generic ecosystem.

::: Equation for `# issuers` (Table 1) is:

$$\approx \frac{log_2\left(\frac{|\text{users}|}{\min(|\text{anon\_set\_size}|)}\right) - \max(\text{metadata\_bits})}{2}$$

::: ($|\text{users}| = \mathbf{1\ billion} \approx 2^{30}$) and ($\min(\text{anon\_set\_size}) = \mathbf{5000} \approx 2^{12}$) implies # issuers $\leq$ **17**.

ENFORCING LOW NUMBER OF ISSUERS

::: Small numbers of issuers are impractical (higher impact for smaller ecosystems).

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

REDUCING REDEMPTION EVENTS

::: 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.

REDUCING REDEMPTION EVENTS

::: 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).

REDUCING REDEMPTION EVENTS

::: 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.

REDUCING REDEMPTION EVENTS

::: 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?

OPEN QUESTIONS