Private Access Tokens Crypto

draft-private-access-tokens-01
Setting

Problem statement

Client → Mediator → Issuer
Setting
Problem statement

Client

Mediator

Issuer

Fixed per-client private value

Fixed public value

Fixed private value
Requirements

Problem statement

Compute deterministic value $y$ over private Client input $x$ and private Issuer input $k$

$$y = F(k, x)$$

Such that

- The Mediator only learns $y$ if the client engages in the protocol with $x$;
- The Client cannot engage in the protocol for private input $x' \neq x$; and
- The Issuer does not learn $x$, nor when two requests have the same $x$. 
Assume prime-order group with generator $G$ and order $q$, where $x$ and $k$ are private scalars, and $X = xG$ a non-hiding commitment to $x$

$\pi = \text{NIZK}(\text{DL}(x, y) = z)$ is non-interactive Schnorr proof that $\log(z(x)) = y$

$\text{VerifyNIZK}(x, y, \pi)$ outputs 1 for $\pi = \text{NIZK}(\text{DL}(x, y) = z)$, and 0 otherwise
Protocol Overview

Solution sketch

Client $x$

$r \leftarrow Z_q$

$P = rX$

Mediator $X$

$(r, P)$

Issuer $k$

$V = kP = krX = krxG$

$y = r^{-1}V = xkG$
Protocol Overview

Solution sketch

Malicious, acts as client to learn $y$

Client $x$

Mediator $X$

Issuer $k$

$r \leftarrow Z_q$

$P = rX$

$P$

$V = kP = krX = krxG$

$V$

$y = r^{-1}V = xkG$
Protocol Overview
Solution sketch

\[
\begin{align*}
\text{Client} & \quad \text{Mediator} & \quad \text{Issuer} \\
r & \leftarrow Z_q \\
P &= rX \\
\pi &= \text{NIZK}(\text{DL}(P, x) = rG) \\
(r, \pi) &\quad \text{VerifyNIZK}(rG, P, \pi) \\
V &\quad \text{VerifyNIZK}(rG, P, \pi) \\
y &= r^{-1}V = xkG \\
V &= kP = krX = krxG
\end{align*}
\]
Protocol Overview

Solution sketch

\[ r \leftarrow Z_q \]
\[ P = rX \]
\[ \pi = \text{NIZK}(\text{DL}(P, x) = rG) \]

\[ (r, \pi) \rightarrow \text{VerifyNIZK}(rG, P, \pi) \]

\[ V = kP = krX = krxG \]

\[ y = r^{-1}V = xkG \]
Questions

Future work

Does the problem make sense?

Is the security model sensible?

Does the sketched protocol meet the desired security goals?