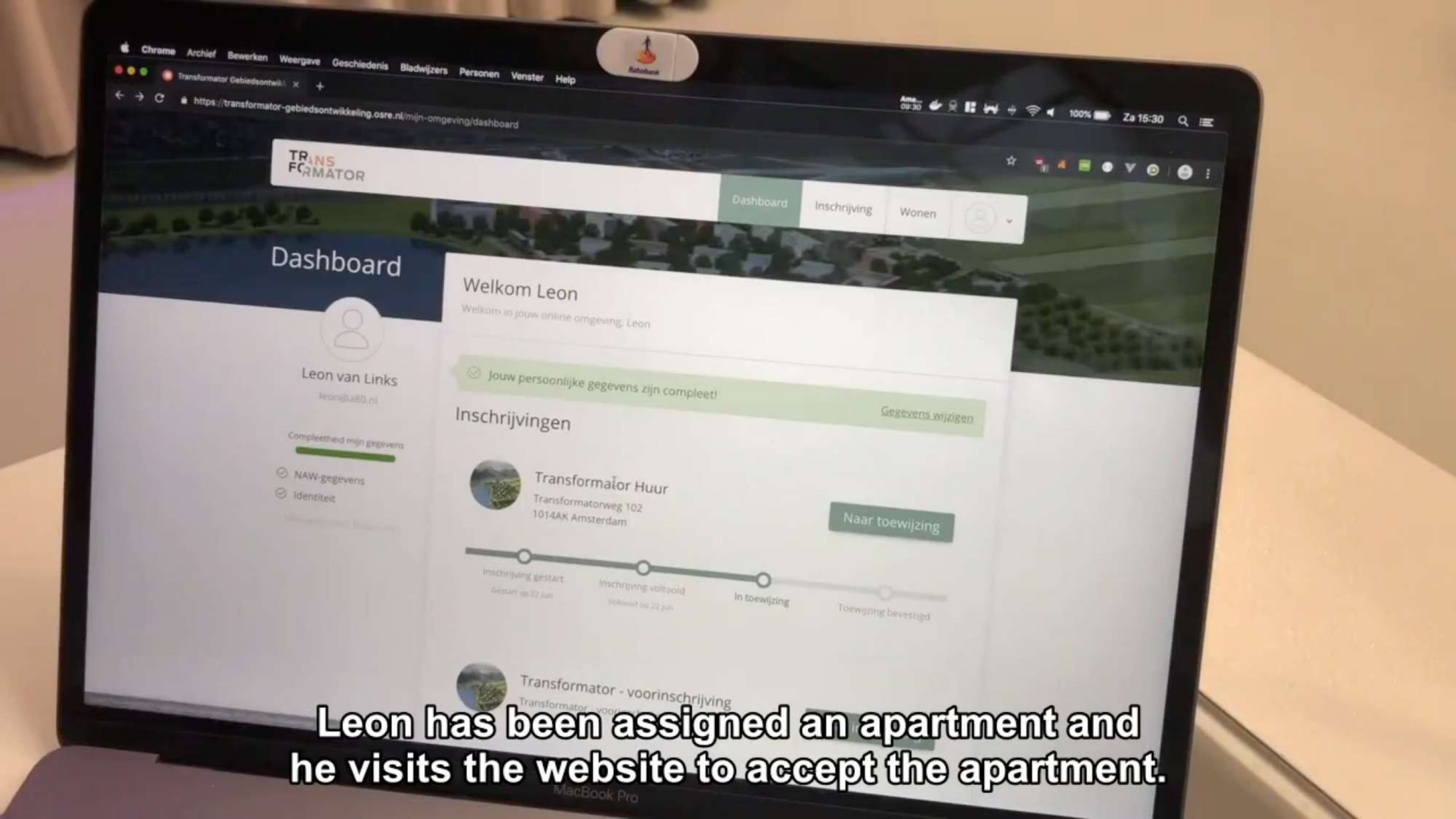
Zero Knowledge Proofs for Income Statements

Pepijn Overbeeke, Deloitte



Leon has been assigned an apartment and he visits the website to accept the apartment.

Questions?

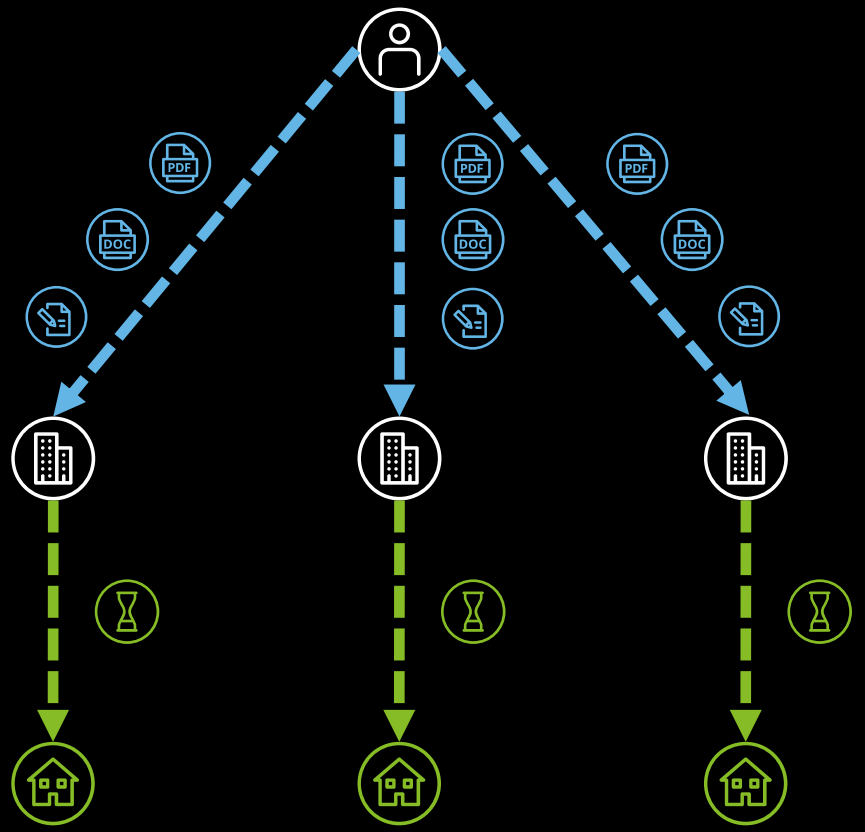
Outline

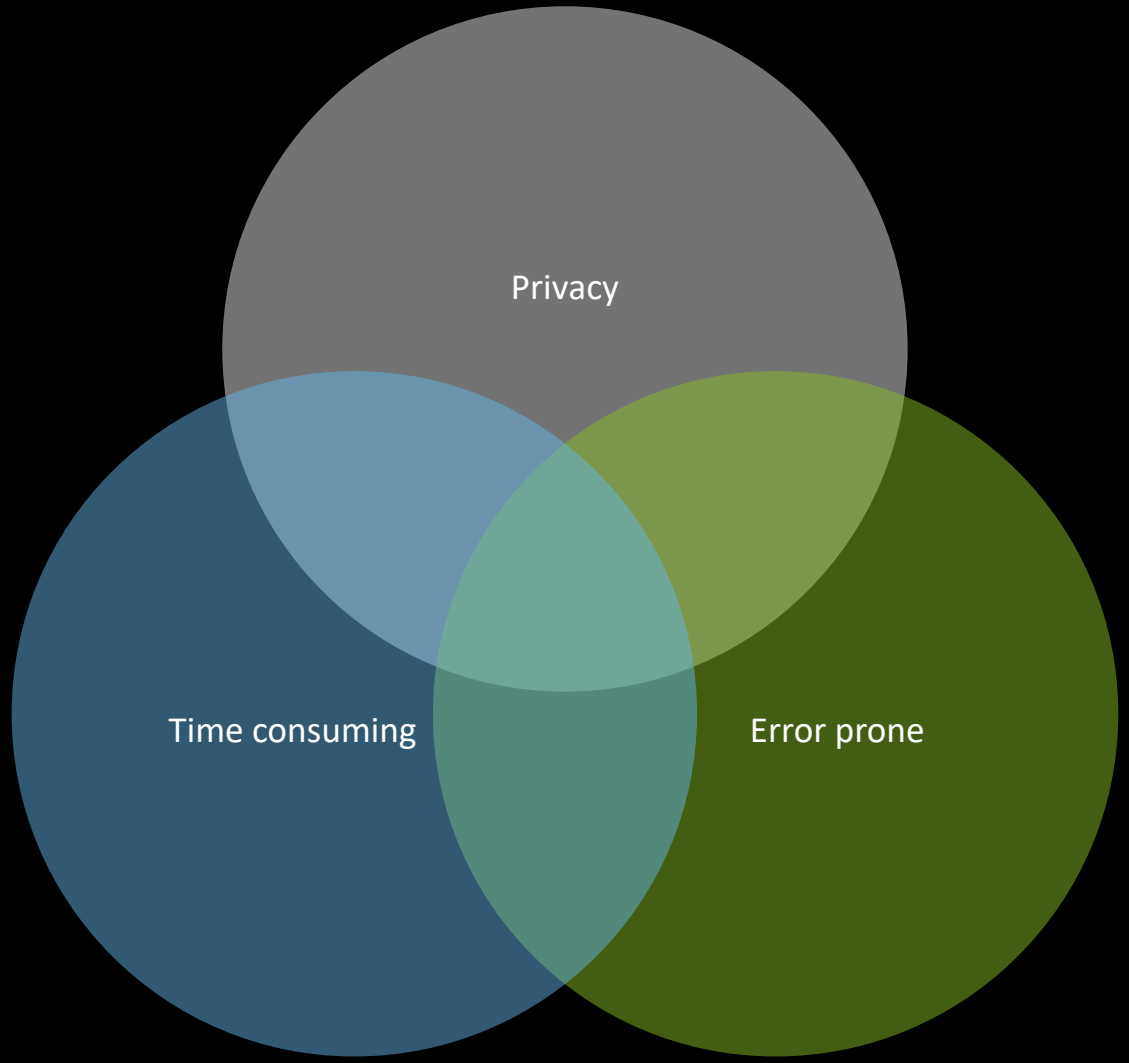
- Overview of problem and our solution
- Component overview and ZKP explanation

About me

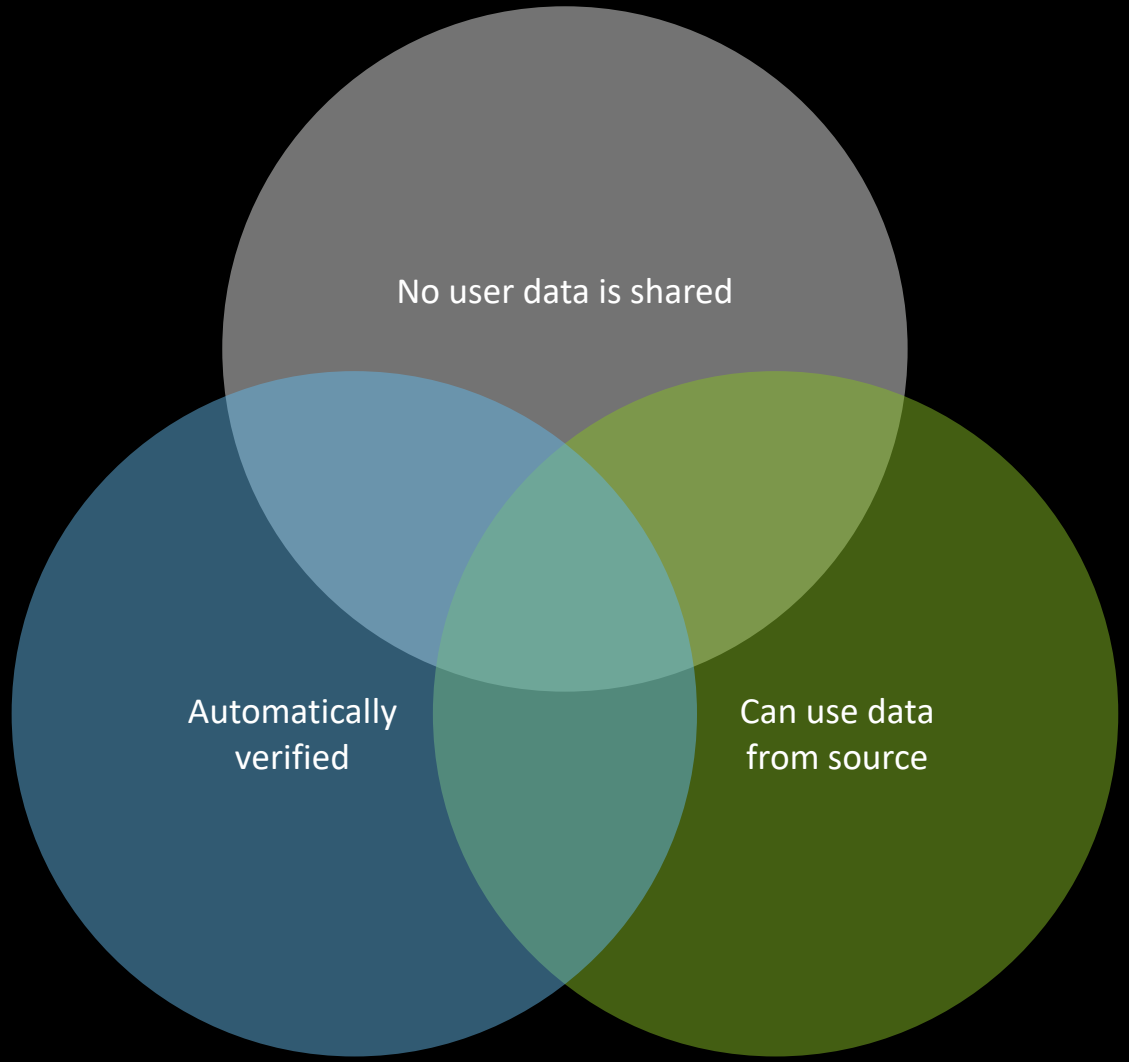
History

Current process





Problems



Why ZKP?

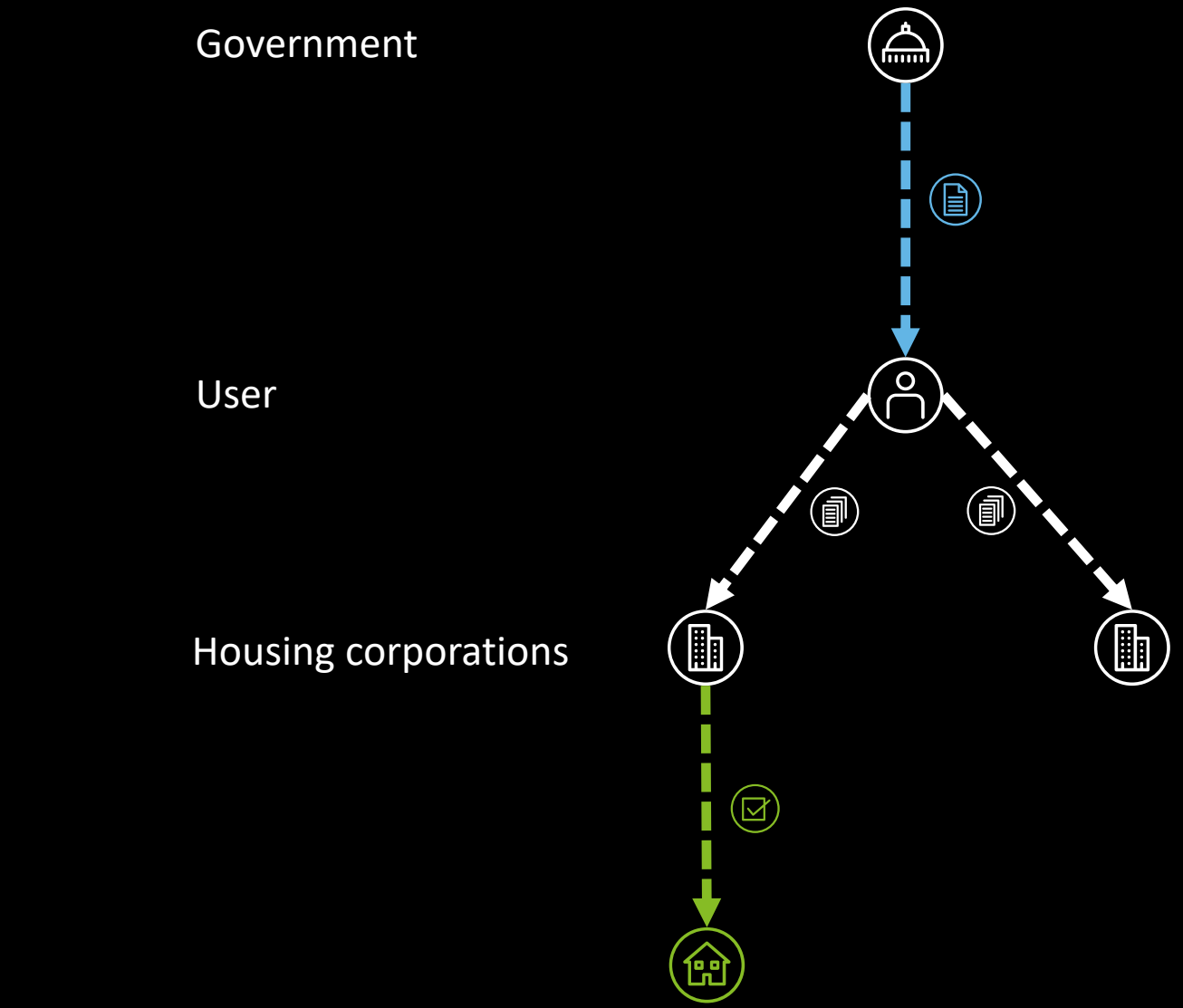
Hackathon

- Data minimalization
- Applicability
- People focused
- Inclusive

Ecosystem partners

- Deloitte
- Rabobank
- De Alliantie

Our solution

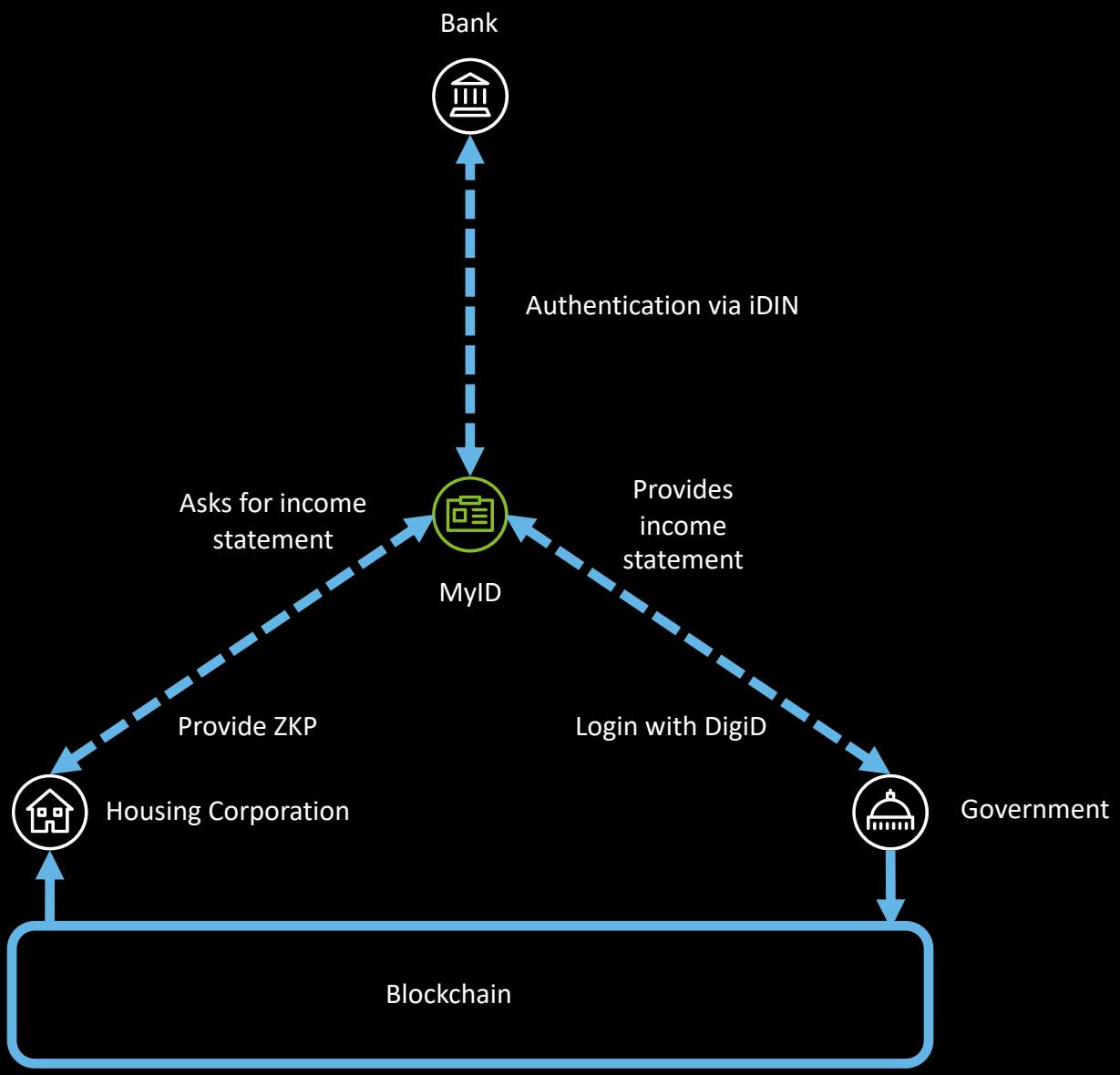


Implications

Government

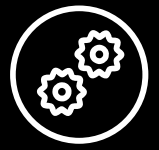
User

Housing corporations



Component overview

MyID app



Range Proof

Boudot, Fabrice. "Efficient proofs that a committed number lies in an interval." *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 2000.

Requirements

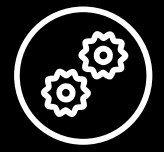
$g \in \mathbb{Z}_n^*$ and h element of group generated by g.

Fujisaki-Okamoto Commitment: $E(x, r) = g^x h^r$, where $r \in [-2^s n + 1, 2^s n - 1]$. Note that $E(x + y, r + s) = E(x, r)E(y, s)$.

Proof that a commitment $E(x^2, r)$ hides a square.

CFT proof, which proves that $x \in [0, b]$ is in $[-2^{t+l} b, 2^{t+l} b]$.

Range Proof

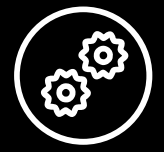


Proof that x $\in [a, b]$ is in $[a - \theta, b + \theta]$ where $\theta = 2^{t+l+1}\sqrt{b-a}$. Let $E = E(x, r)$.

1. Set $\tilde{E} = E/g^a$, $\bar{E} = g^b/E$, $\tilde{x} = x - a$ and $\bar{x} = b - x$.
2. Let $\tilde{x}_1 = \lfloor\sqrt{x-a}\rfloor$, $\tilde{x}_2 = \tilde{x} - {\tilde{x}_1}^2$, $\bar{x}_1 = \lfloor\sqrt{b-x}\rfloor$ and $\bar{x}_2 = \bar{x} - {\bar{x}_1}^2$.
3. Select $\tilde{r}_1$, $\tilde{r}_2$, $\bar{r}_1$ and $\bar{r}_2$ such that $\tilde{r}_1 + \tilde{r}_2 = r$ and $\bar{r}_1 + \bar{r}_2 = -r$.
4. Compute $\tilde{E}_1 = E({\tilde{x}_1}^2, \tilde{r}_1)$ and $\bar{E}_1 = E({\bar{x}_1}^2, \bar{r}_1)$. Let $\tilde{E}_2 = E(\tilde{x}_2, \tilde{r}_2)$ and $\bar{E}_2 = E(\bar{x}_2, \bar{r}_2)$. Note that $\tilde{E}_2 = \tilde{E}/\tilde{E}_1$ and $\bar{E}_2 = \bar{E}/\bar{E}_1$.
5. Create proofs that $\tilde{E}_1$ and $\bar{E}_1$ hide squares and create CFT proofs that $\tilde{x}_2 \in [-\theta, \theta]$ and $\bar{x}_2 \in [-\theta, \theta]$.

Verifier is convinced that $\tilde{E}$ and $\bar{E}$ are greater than $-\theta$ and since $\tilde{E}$ hides $x - a$ and $\bar{E}$ hides $b - x$, verifier is convinced $x \in [a - \theta, b + \theta]$.

Range Proof Cont.



Proof that x ∈ $[a, b]$ is in $[a, b]$.

Let $T = 2(t + l + 1) + |b - a|$ and $x' = 2^T x$. Then $E' = E^{2^T}$.

Execute range proof proving $x' \in [2^T a - \theta', 2^T b + \theta']$ where $\theta' = 2^{t+l+T/2+1}\sqrt{b-a}$. It can be shown that $\theta' < 2^T$.

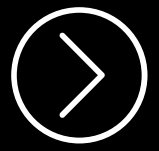
Verifier is convinced $x' \in [2^T a - \theta', 2^T b + \theta']$ and thus $x' \in]2^T a - 2^T, 2^T b + 2^T[$ and $x \in]a - 1, b + 1[$.

Messages

Government sends the MyID app:
- The income x
- The committed income $E(x, r)$ and r
- Government signature $sig(E(x, r))$
- n, g and h

MyID app sends housing corporation:
- Range proof which includes $E(x, r)$
- Signature $sig(E(x, r))$
- n, g and h

Blockchain



Next steps

Questions?