Using IRMA for (small scale) digital elections

J.J.J. Doesburg

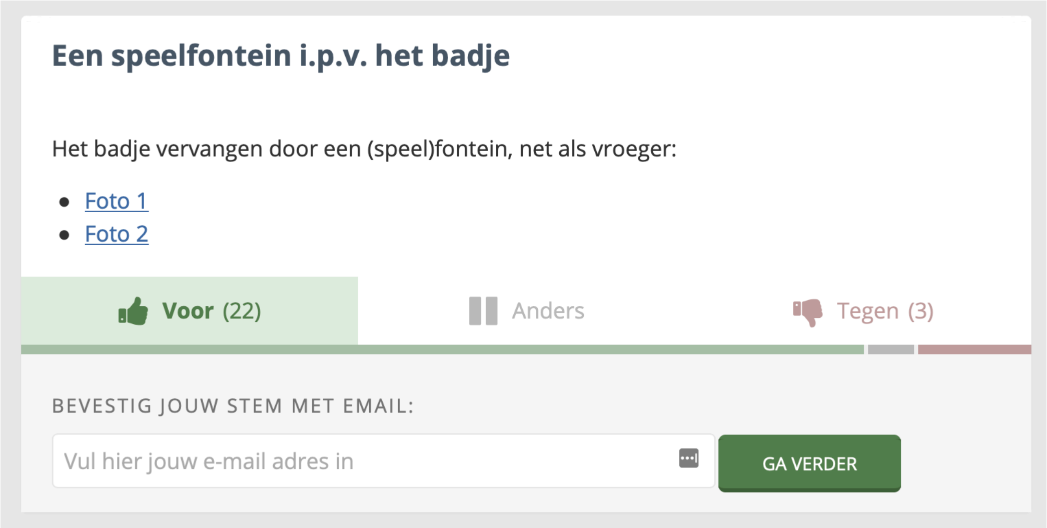
January 20th, 2020

Supervisor: prof. dr. B.P.F. Jacobs, dr. S. Ringers

Amsterdam OpenStad + Amsterdam Digitale Stad

- Citizen participation

  OpenStad makes digital tools for accessible participation, so that more people in Amsterdam can think along and decide on what is happening in the city.



Een speelfontein i.p.v. het badje

Het badje vervangen door een (speel)fontein, net als vroeger:

- Foto 1
- Foto 2

BEVESTIG JOUW STEM MET EMAIL:

Vul hier jouw e-mail adres in

- Relevant for our research:
  - Digital elections
  - Small scale, very local elections

- Current solution(s): sending voting codes per (paper) mail to houses, vote via internet with email, etc...
  - Expensive, unreliable, inaccessible, no privacy *by design*

Gemeente
Amsterdam
+
IRMA

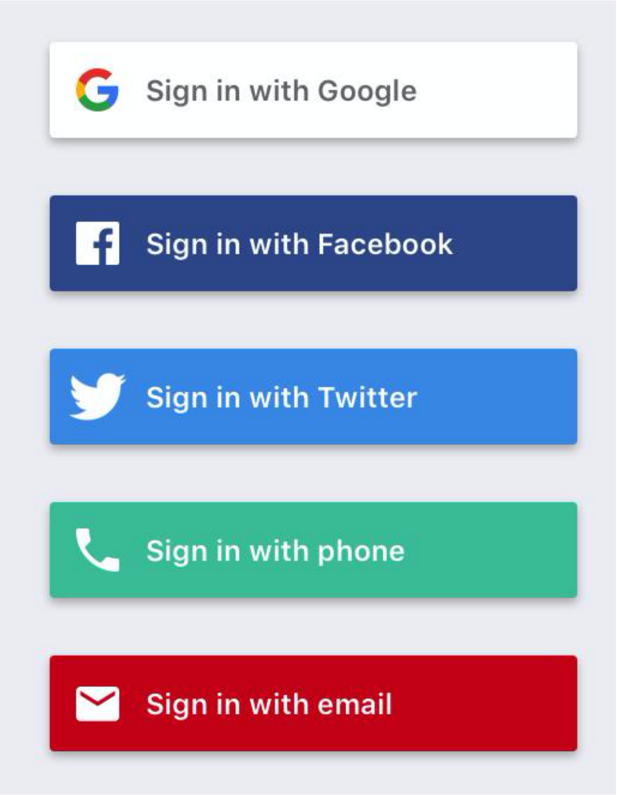
IRMA: an alternative to classic identity management

- Attribute-based credential system (IBM Idemix)

- Attributes: minimal pieces of information about a user
  - Name, 18+, date of birth, email address, town, nationality
  - Not necessarily identifying
  - Electronically signed by some issuer
  - Users can selectively disclose their attributes and signatures, maintaining their privacy

No IRMA

DigiD



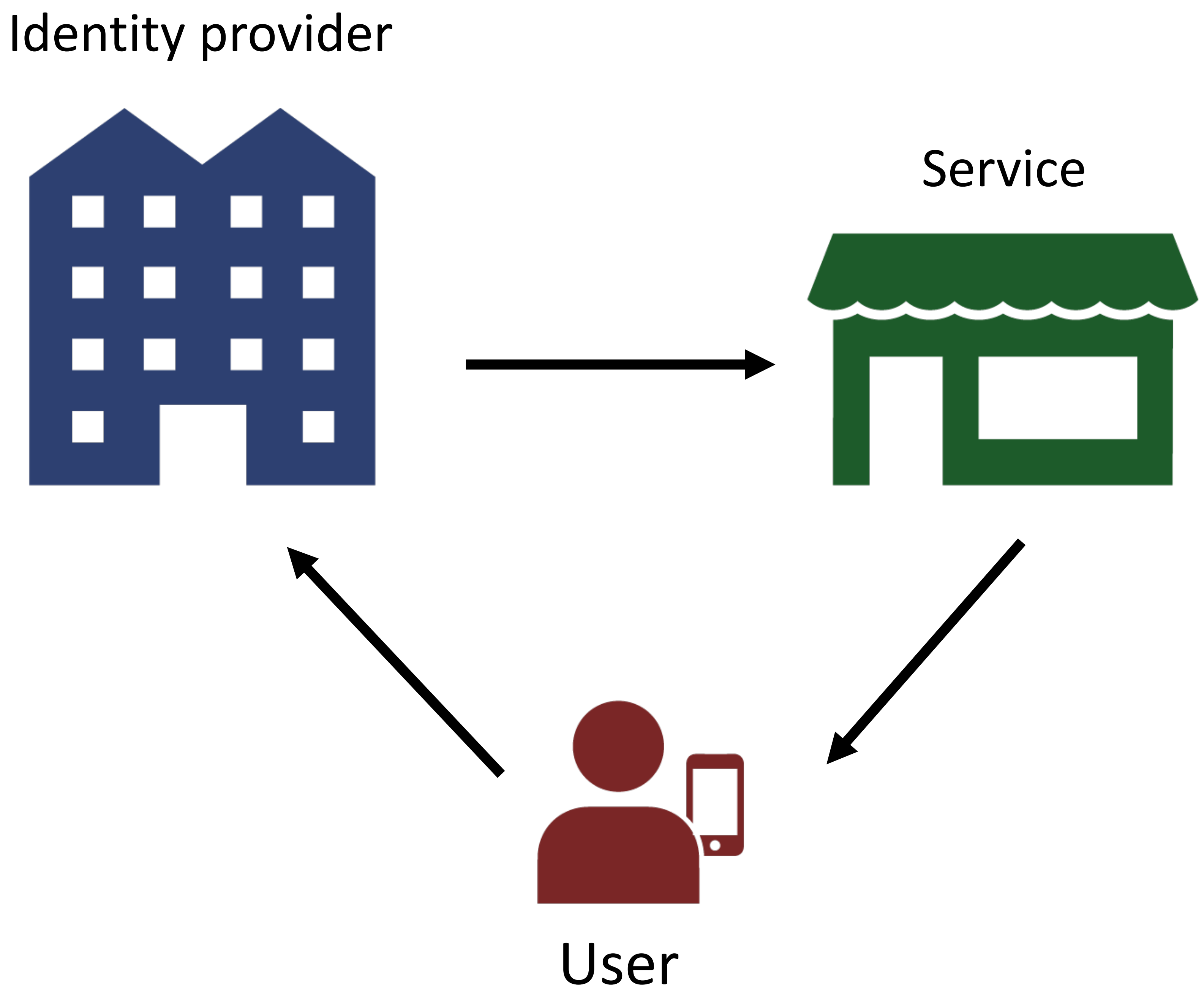
Sign in with Google

Sign in with Facebook

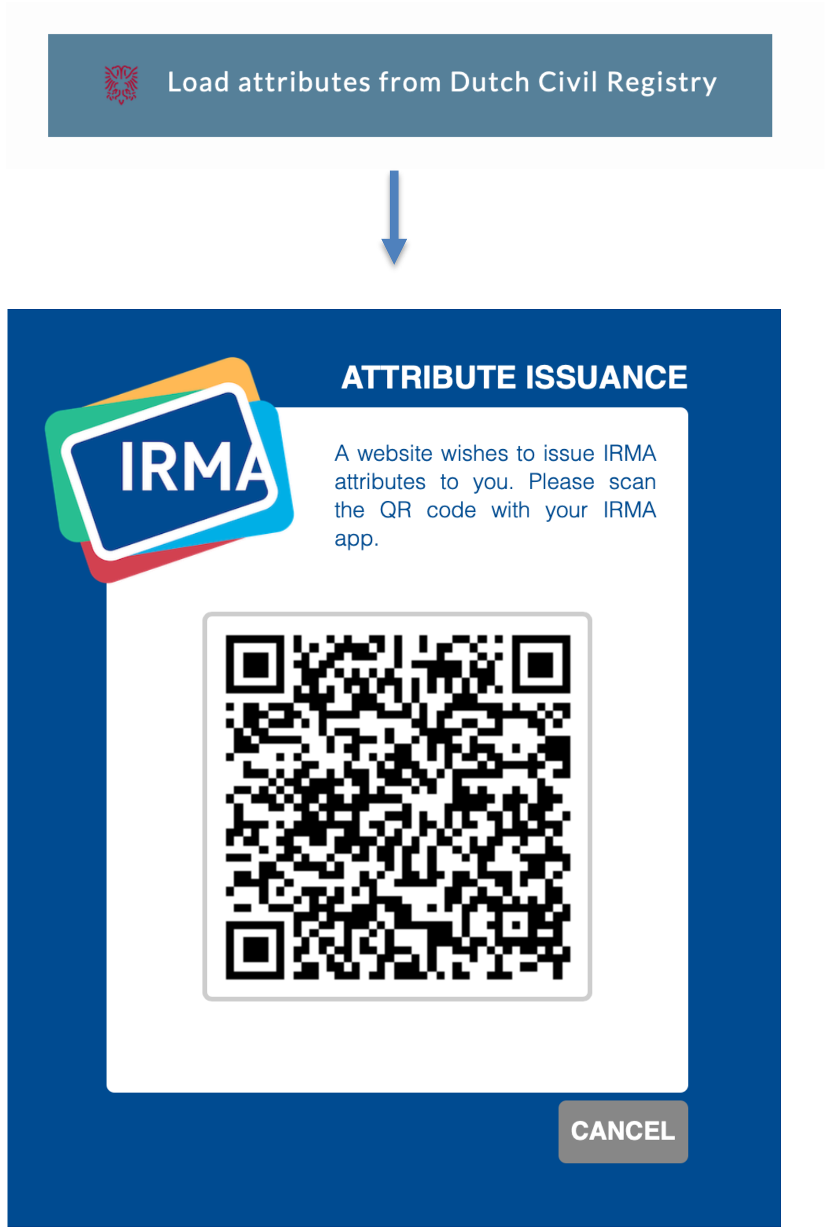
Sign in with Twitter

Sign in with phone

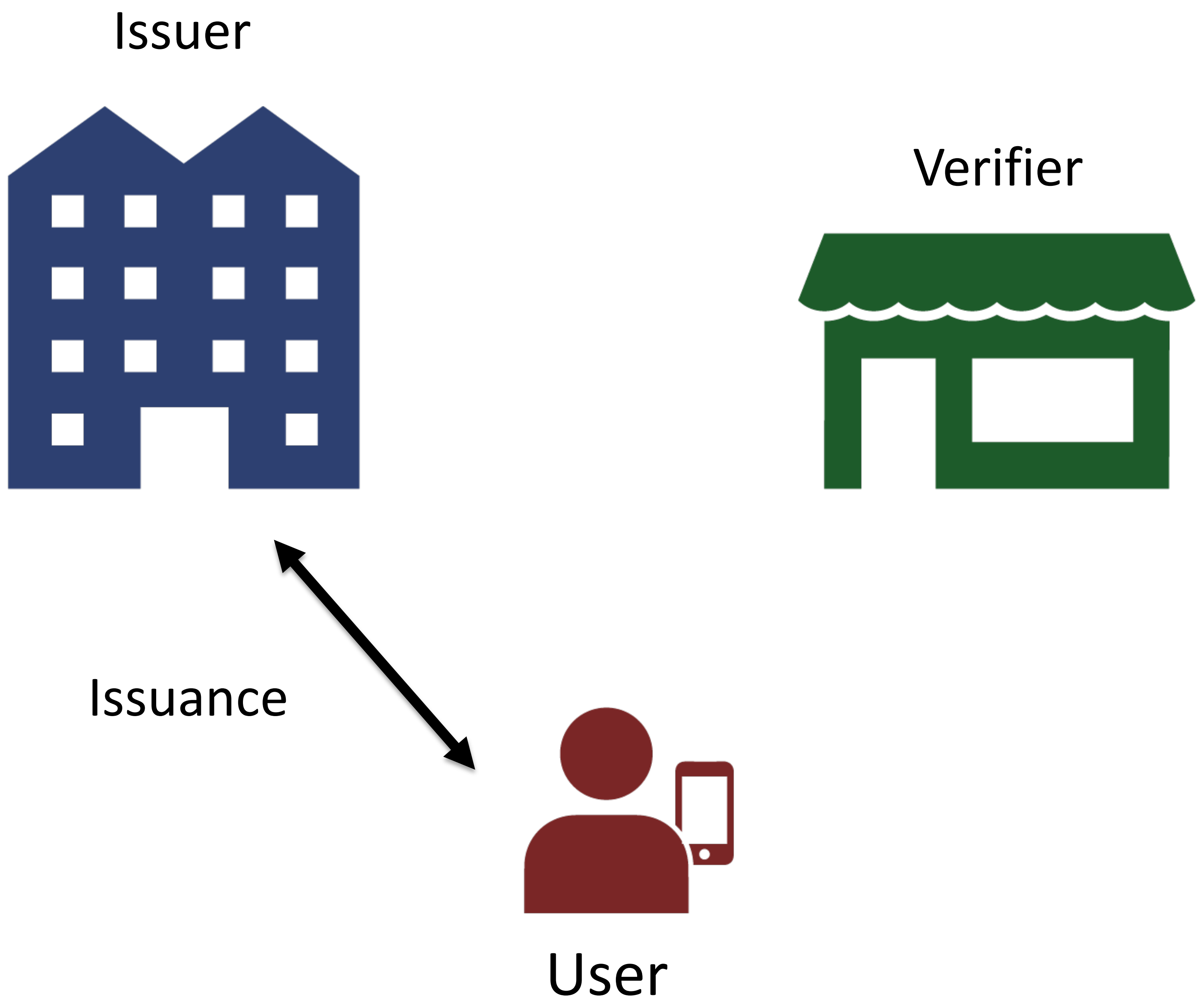
Sign in with email



IRMA



A website wishes to issue IRMA attributes to you. Please scan the QR code with your IRMA app.



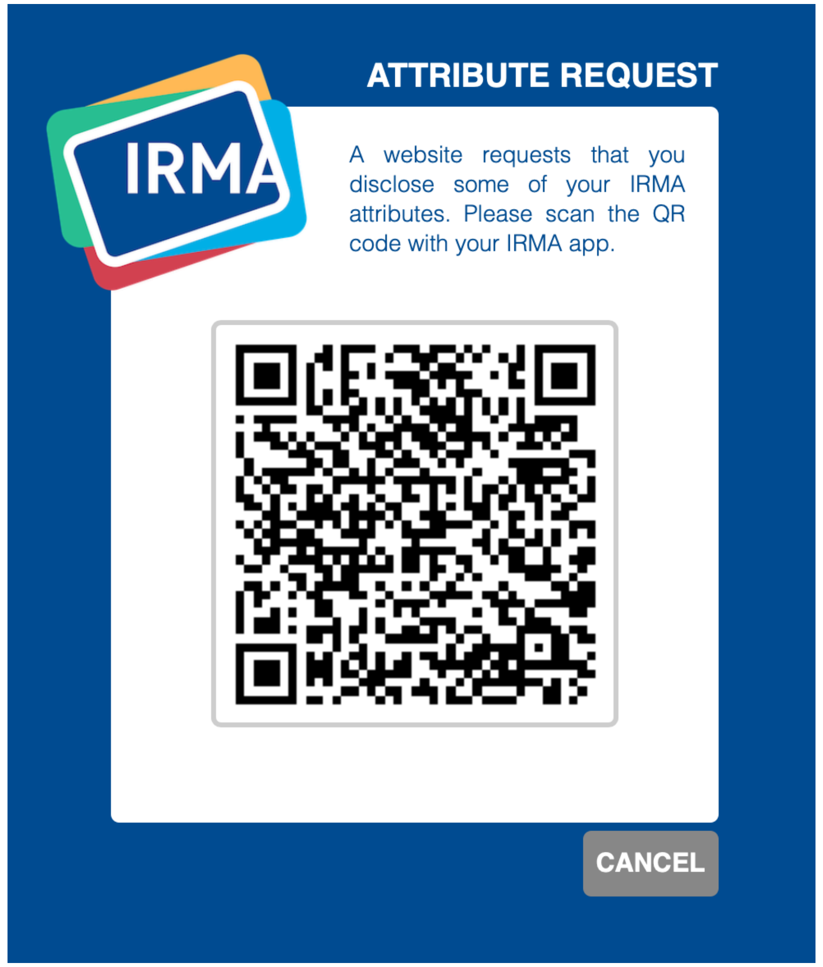
Issuer

Verifier

Issuance

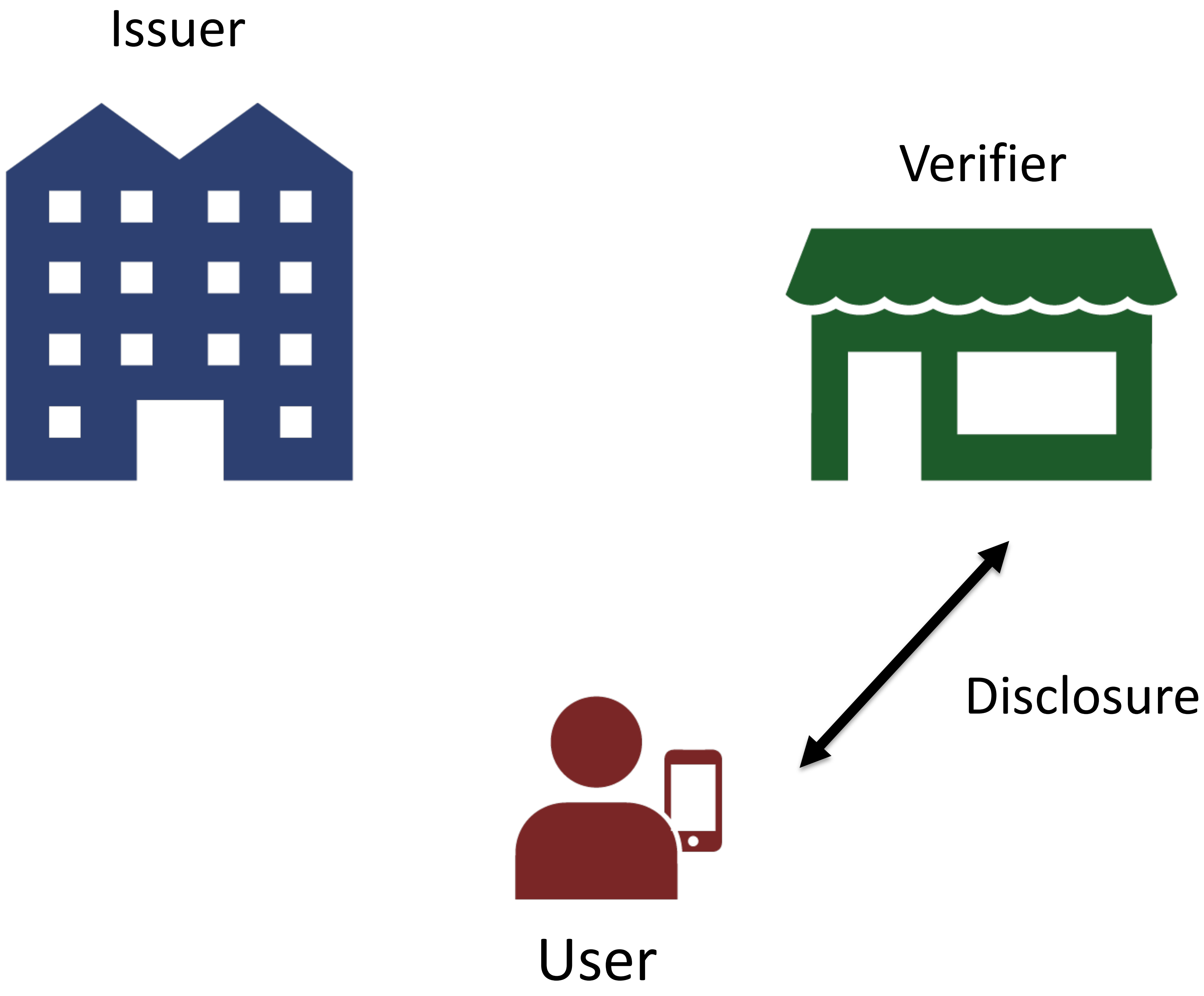
User

IRMA



ATTRIBUTE REQUEST

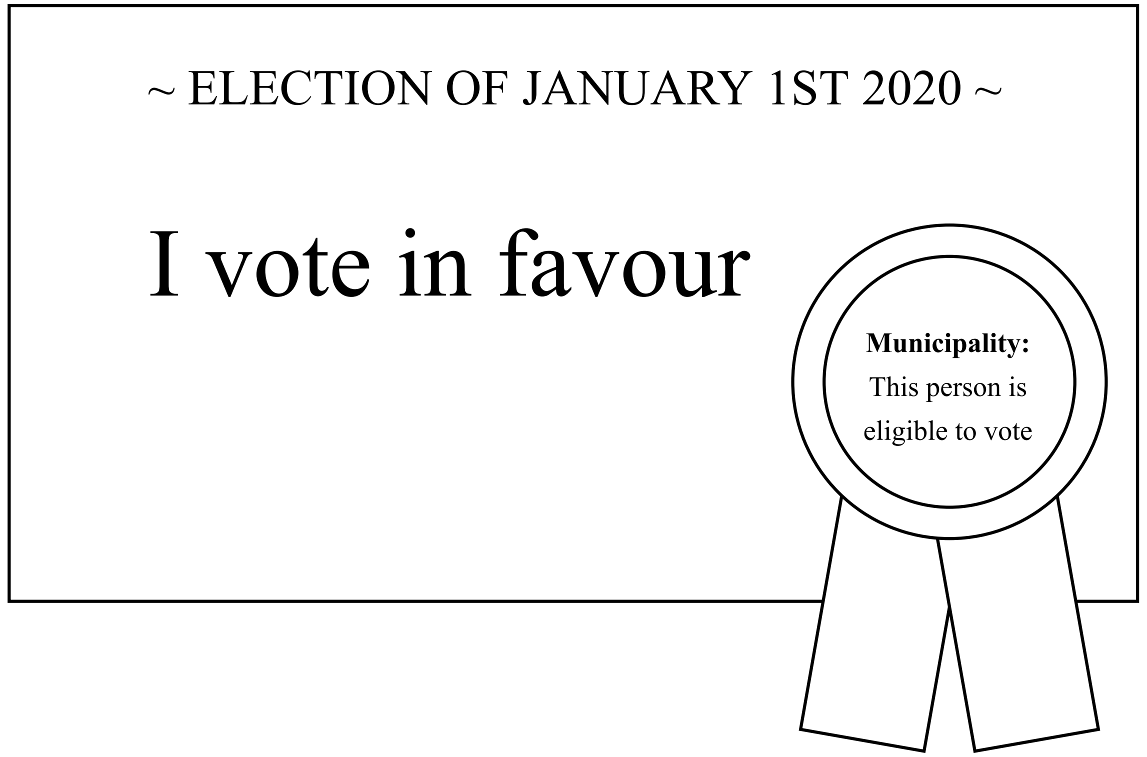
A website requests that you disclose some of your IRMA attributes. Please scan the QR code with your IRMA app.



IRMA attribute-based signatures

- Include attributes in an electronic signature
- Privacy friendly signed statements

- Can be used to record votes
  - Signatures for integrity
  - IRMA for privacy



~ ELECTION OF JANUARY 1ST 2020 ~

I vote in favour

Municipality:
This person is
eligible to vote

B. Hampiholi, G. Alpár, F. van den Broek & B. Jacobs (2015). Towards practical attribute-based signatures. In *Proceedings of the 5th International Conference on Security, Privacy, and Applied Cryptography Engineering - Volume 9354*, page 310–328. Springer-Verlag, 2015.

To what extent can IRMA be used in digital elections?

- So far, existing (cryptographic) schemes for electronic elections often turn out to be impractical and remained merely academic.[1]
- No attempts to solve the ‘e-voting’ problem with attribute-based credential systems
- IRMA could, as versatile ecosystem with many applications, be rather accessible
- Attribute-based signatures are a perfect fit for recording votes

[1] K. Krips and J. Willemson. On practical aspects of coercion-resistant remote voting systems. In *Electronic Voting*, pages 216–232. Springer International Publishing, 2019.

Overview

- Introduction
  - Amsterdam OpenStad elections
  - IRMA
- Requirements for elections
- Elections in IRMA
- Limitations & details
- Conclusion

Requirements for elections

- Key features:
  - Eligibility
  - Unicity
  - Secrecy
  - Integrity
  - Verifiability

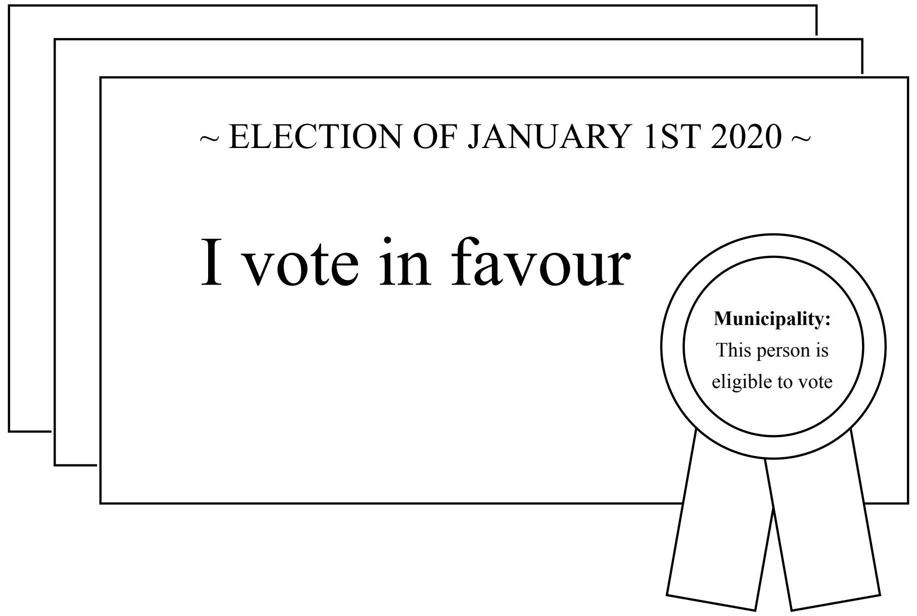
- Additional features: transparency, liberty, accessibility

Adviescommissie inrichting verkiezingsproces. Stemmen met vertrouwen. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2007.

IRMA voting scheme: partial solution

- Intuitive approach
  - Attribute-based signature (ABS) on a voting statement
  - Eligibility-attribute included in the 'attribute-based vote'
  - Publish publicly for anyone to verify *(not covered in this research)*

  - Problem: unlinkability of IRMA enables people to vote multiple times, violating unicity



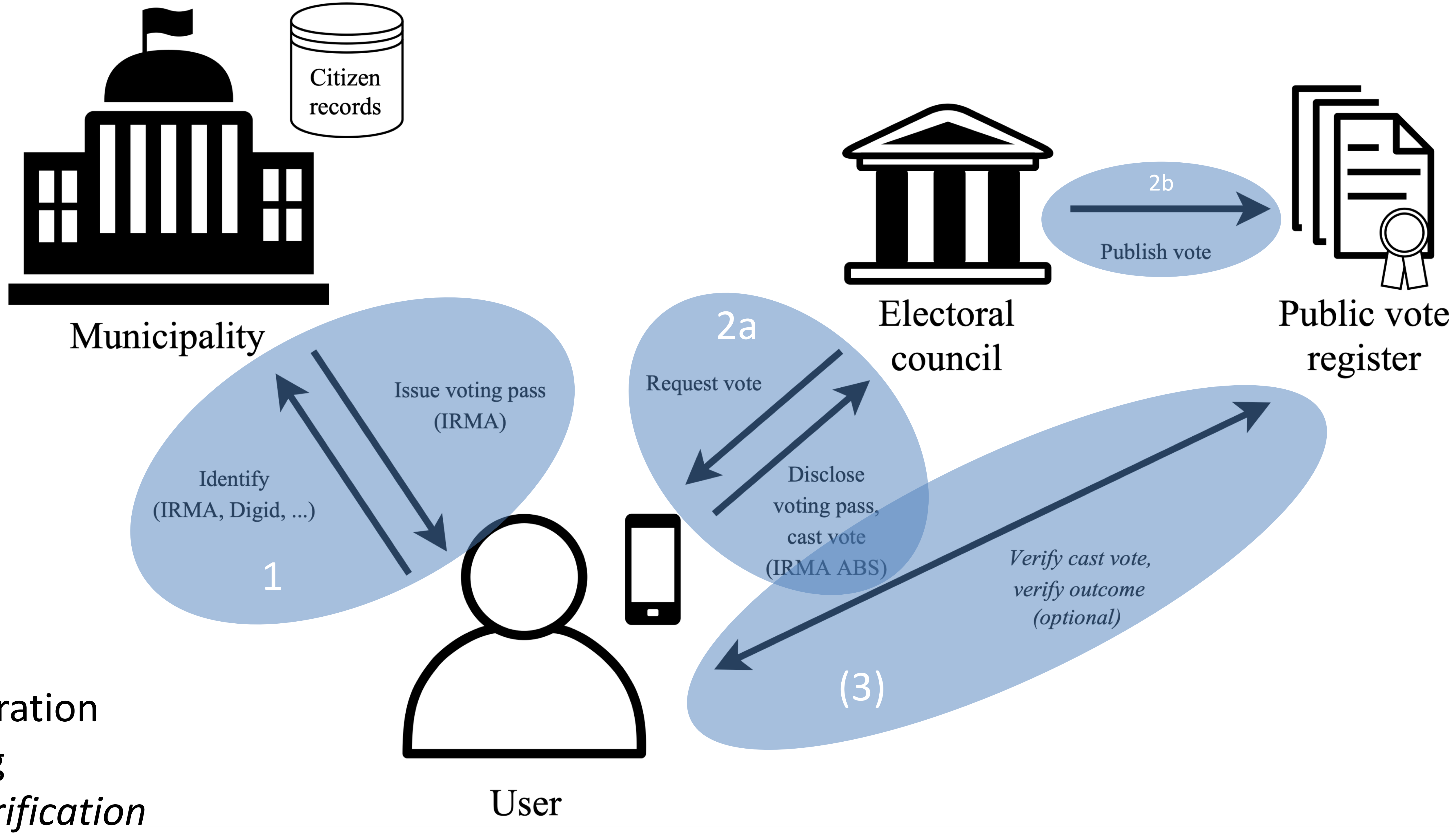
IRMA voting scheme: blindly issued voting numbers

- We must include a voting number!
- But a voting number issued by the municipality, identifies a user and violates secrecy
- We need blindly issued credentials – blind signatures on voting numbers
    - Municipality must sign the number, but…
    - … municipality cannot know the number

- My thesis describes two small changes to scheme for IRMA issuance to enable this

The person with this number may now vote

Overview of the scheme



1: voter registration

2: vote casting

3: optional verification

Limitations & details

- Voting phases do not really need to be fully separate
  - Voter registration can be done last-minute, but timing can violate anonymity

- Proving what you voted makes you coercible
  - Solve partially by allowing change/retraction of votes

- Network-layer (IP addresses etc.) violates privacy

- Devices must be secure

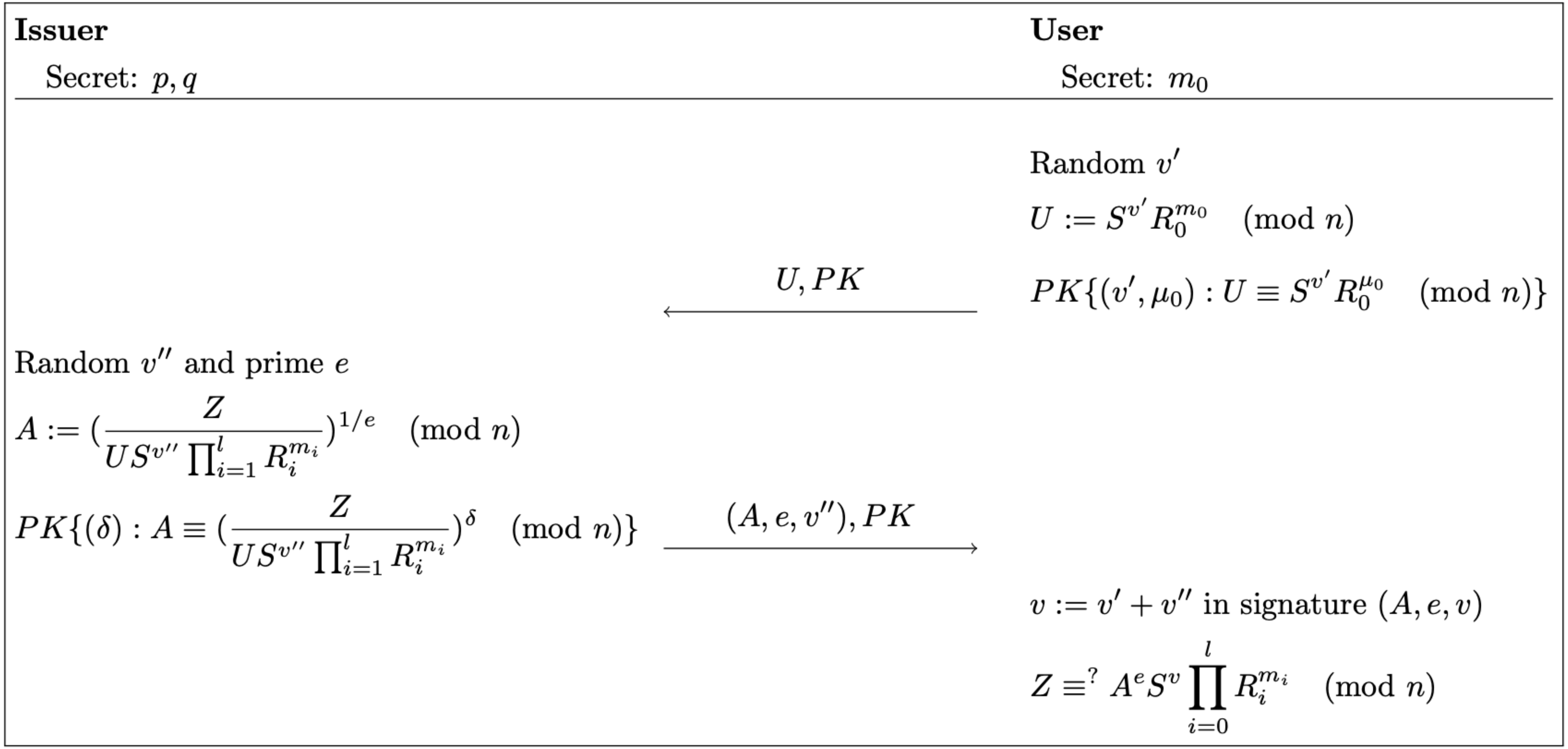
Conclusion

- Blindly issued attributes are required to organize digital elections in IRMA

- Online remote elections have fundamental problems
  - Coercion, secure devices and networks, (D)DoS
- Not recommendable for large scale, high impact elections

- For small scale, low influence elections, we consider the benefits to outweigh these problems
- IRMA allows for rather simple/accessible online voting
  - Ultimately verifiable
  - Privacy by design
- We have described a good way to start the development of proof of concept digital elections with IRMA

Extra: Overview of IRMA / Idemix issuance



Issuer

Secret: p, q

User

Secret: m_0

Random v'

$U := S^{v'} R_0^{m_0} \pmod{n}$

$PK\{(v', \mu_0) : U \equiv S^{v'} R_0^{\mu_0} \pmod{n}\}$

$\xleftarrow{U, PK}$

Random v'' and prime e

$$A := \left(\frac{Z}{U S^{v''} \prod_{i=1}^{l} R_i^{m_i}}\right)^{1/e} \pmod{n}$$

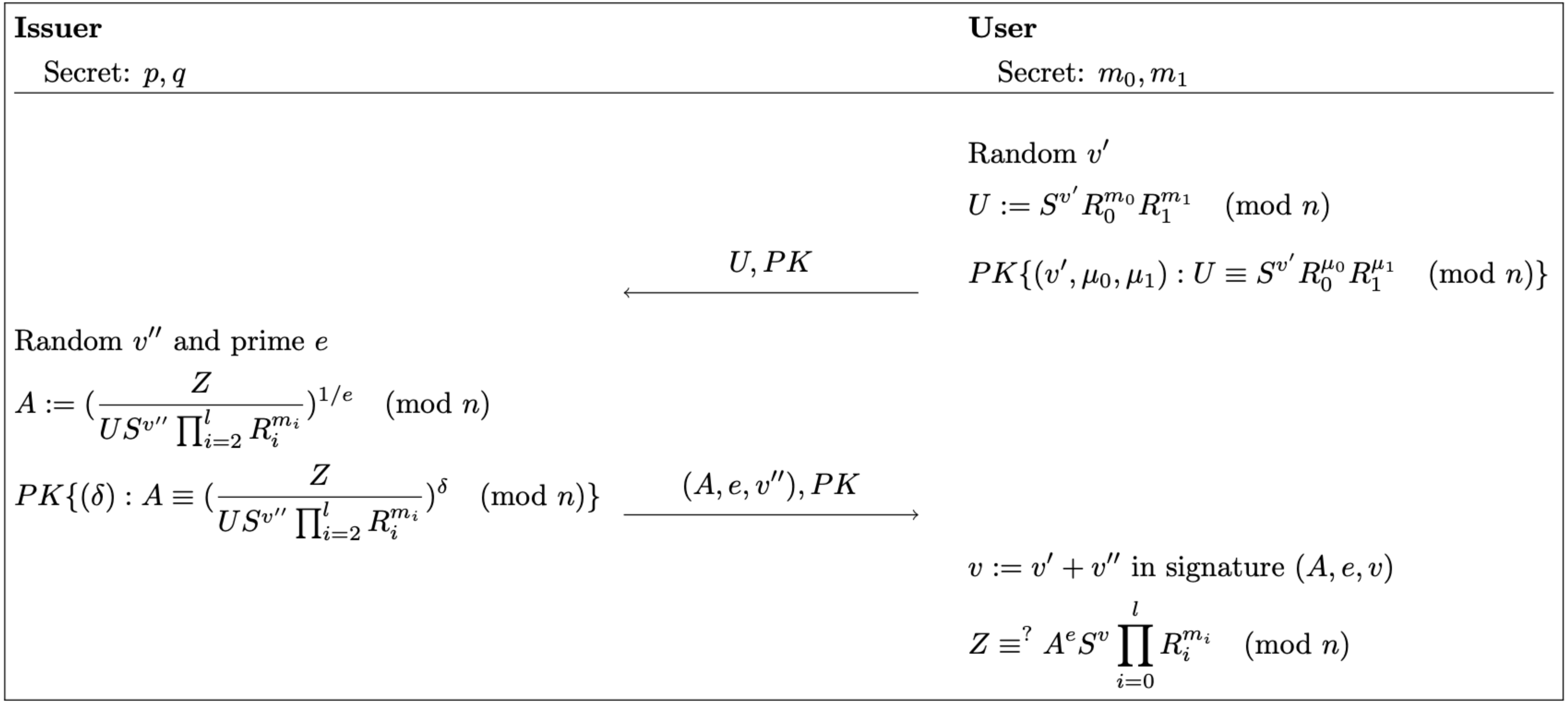
$$PK\{(\delta) : A \equiv \left(\frac{Z}{U S^{v''} \prod_{i=1}^{l} R_i^{m_i}}\right)^{\delta} \pmod{n}\}$$

$\xrightarrow{(A, e, v''), PK}$

$v := v' + v''$ in signature (A, e, v)

$$Z \equiv^{?} A^e S^v \prod_{i=0}^{l} R_i^{m_i} \pmod{n}$$

Extra: Blind (double) signature on voting number



Issuer

Secret: p, q

User

Secret: m_0, m_1

Random v'

$$U := S^{v'} R_0^{m_0} R_1^{m_1} \pmod{n}$$

$$PK\{(v', \mu_0, \mu_1) : U \equiv S^{v'} R_0^{\mu_0} R_1^{\mu_1} \pmod{n}\}$$

$$\xleftarrow{\quad U, PK \quad}$$

Random v'' and prime e

$$A := \left(\frac{Z}{US^{v''} \prod_{i=2}^{l} R_i^{m_i}}\right)^{1/e} \pmod{n}$$

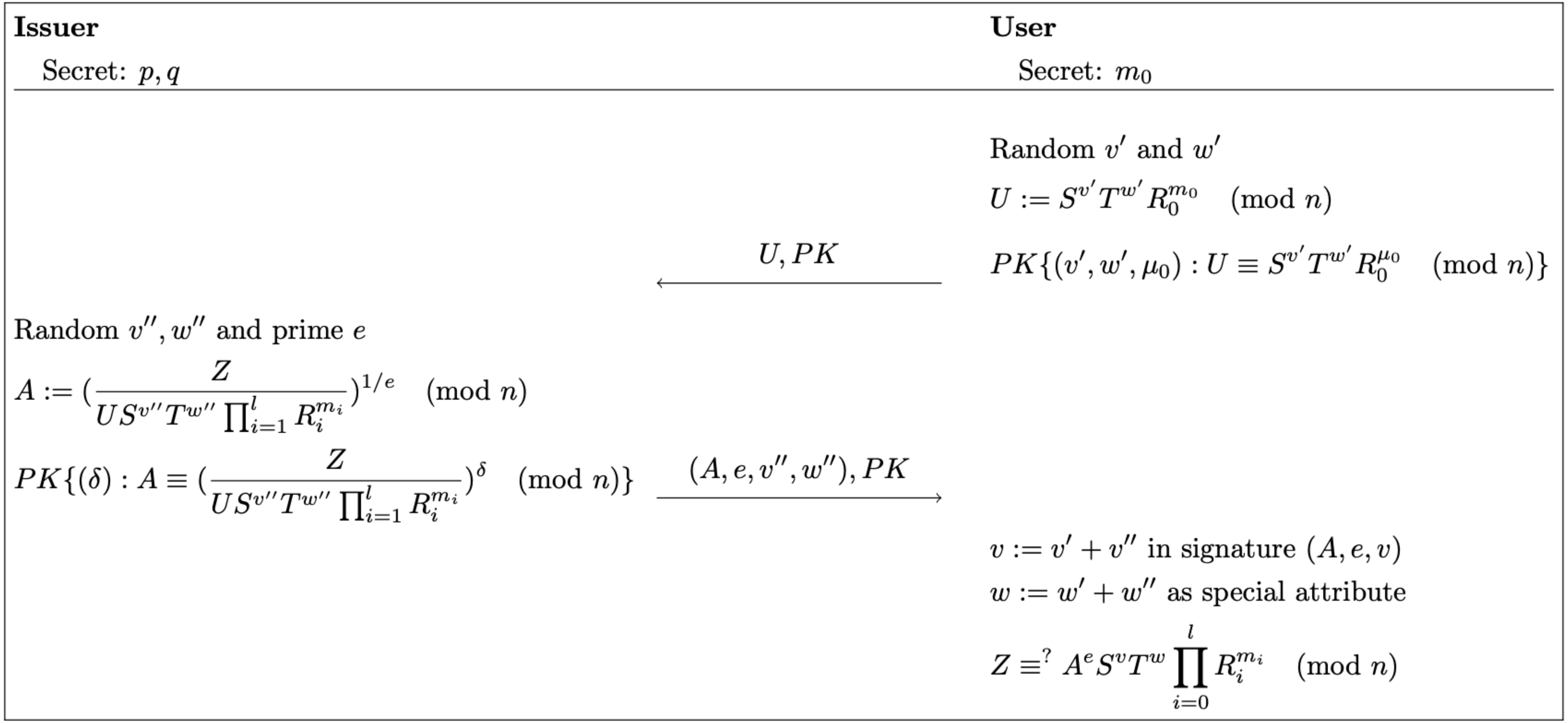
$$PK\{(\delta) : A \equiv \left(\frac{Z}{US^{v''} \prod_{i=2}^{l} R_i^{m_i}}\right)^{\delta} \pmod{n}\}$$

$$\xrightarrow{\quad (A, e, v''), PK \quad}$$

$v := v' + v''$ in signature (A, e, v)

$$Z \overset{?}{\equiv} A^e S^v \prod_{i=0}^{l} R_i^{m_i} \pmod{n}$$

Extra: Blind generation of voting number during issuance



Issuer

Secret: p, q

User

Secret: m_0

Random v' and w'

$$U := S^{v'} T^{w'} R_0^{m_0} \pmod{n}$$

$$PK\{(v', w', \mu_0) : U \equiv S^{v'} T^{w'} R_0^{\mu_0} \pmod{n}\}$$

$$\xleftarrow{\quad U, PK \quad}$$

Random v'', w'' and prime e

$$A := \left(\frac{Z}{U S^{v''} T^{w''} \prod_{i=1}^{l} R_i^{m_i}}\right)^{1/e} \pmod{n}$$

$$PK\{(\delta) : A \equiv \left(\frac{Z}{U S^{v''} T^{w''} \prod_{i=1}^{l} R_i^{m_i}}\right)^{\delta} \pmod{n}\}$$

$$\xrightarrow{\quad (A, e, v'', w''), PK \quad}$$

$v := v' + v''$ in signature (A, e, v)

$w := w' + w''$ as special attribute

$$Z \overset{?}{\equiv} A^e S^v T^w \prod_{i=0}^{l} R_i^{m_i} \pmod{n}$$