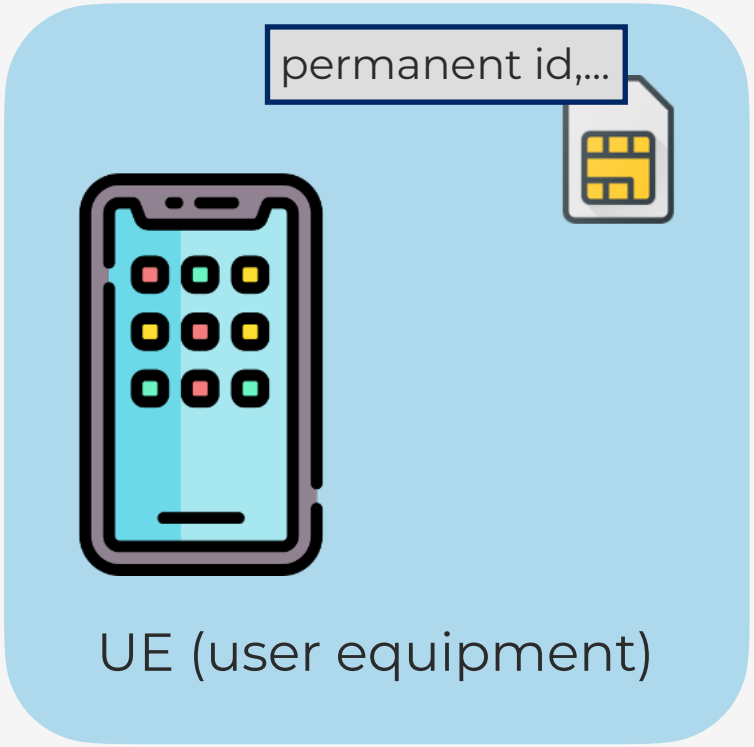
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

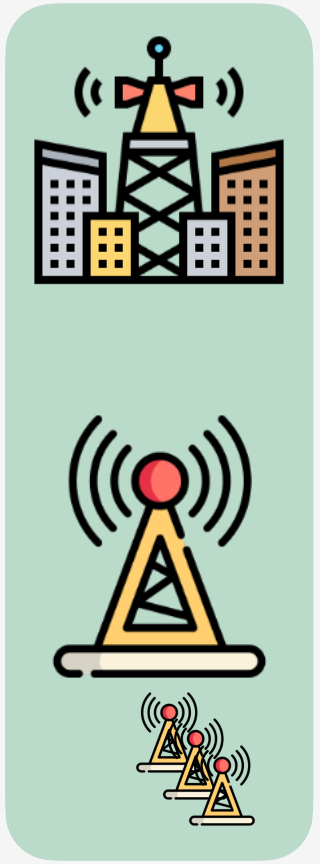
Anonymous Authentication and Key Agreement, Revisited

ACSAC 2025

Yanqi Zhao, **Xiangyu Liu**, Min Xie, Xiaoyi Yang, Jianting Ning, Baodong Qin, Haibin Zhang, Yong Yu
CISPA Helmholtz Center for Information Security

Mobile Systems



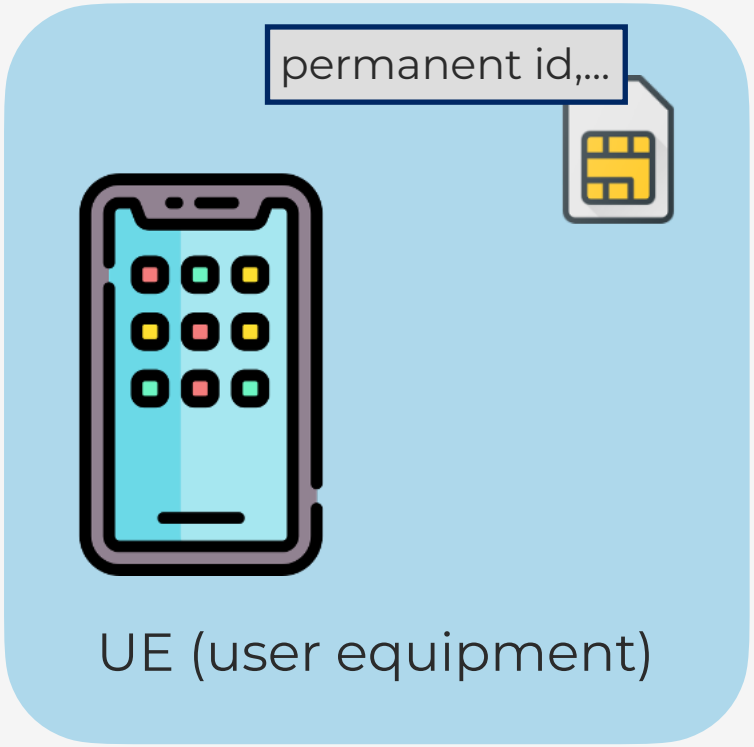


HN (home network)

MNO
(mobile network operators)

SN (serving network)

Mobile Systems



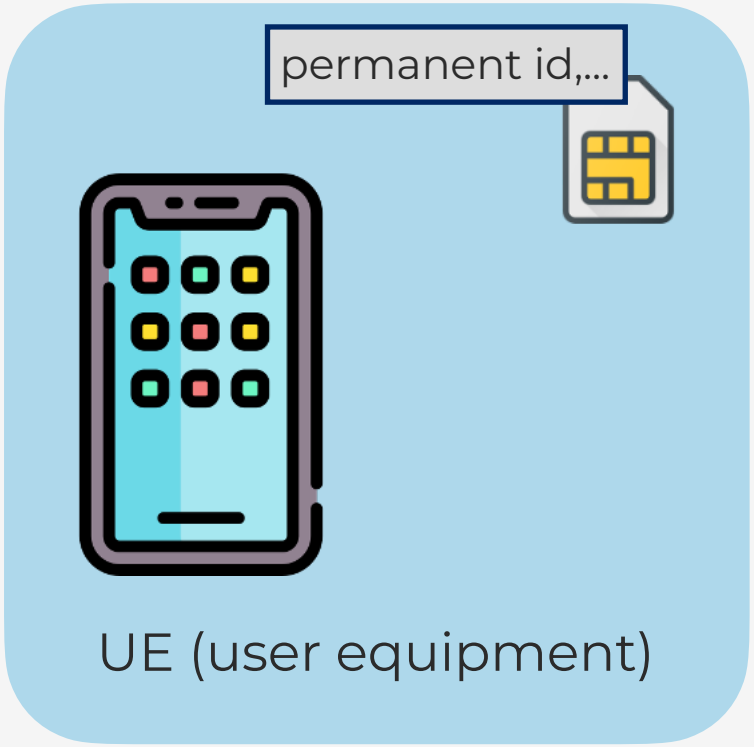
1. payment

HN (home network)

MNO
(mobile network operators)

SN (serving network)

Mobile Systems



1. payment

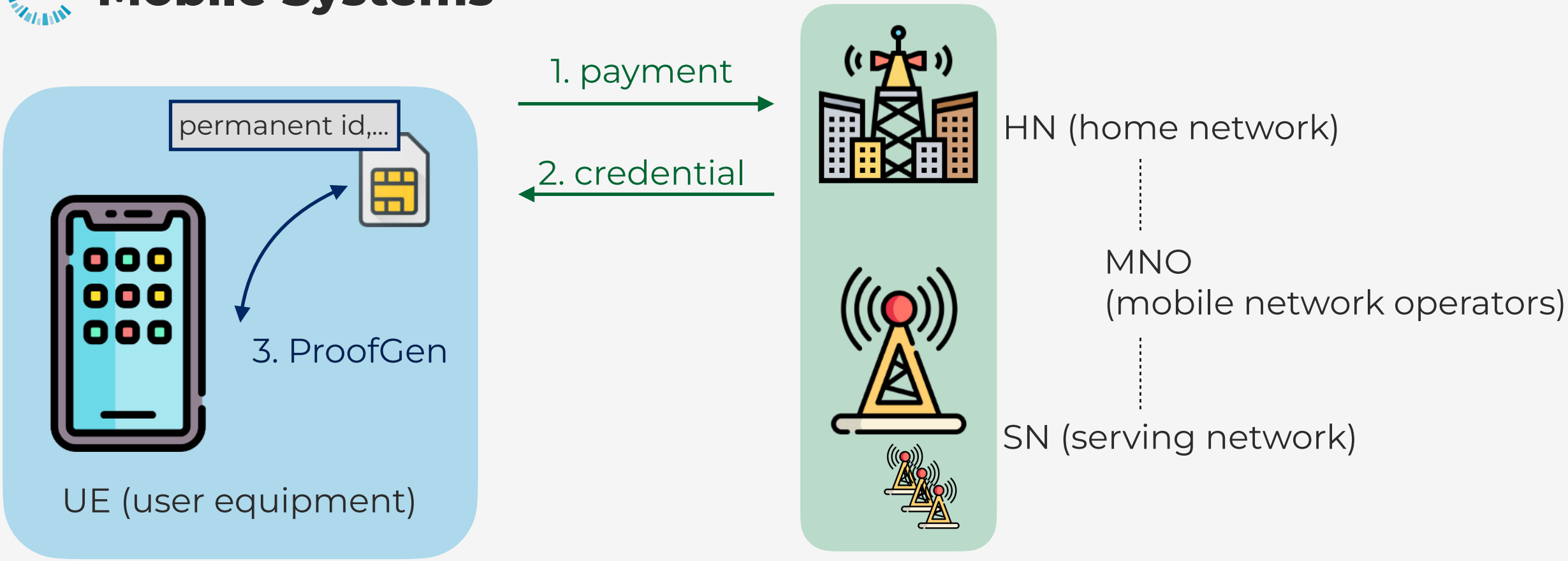
2. credential

HN (home network)

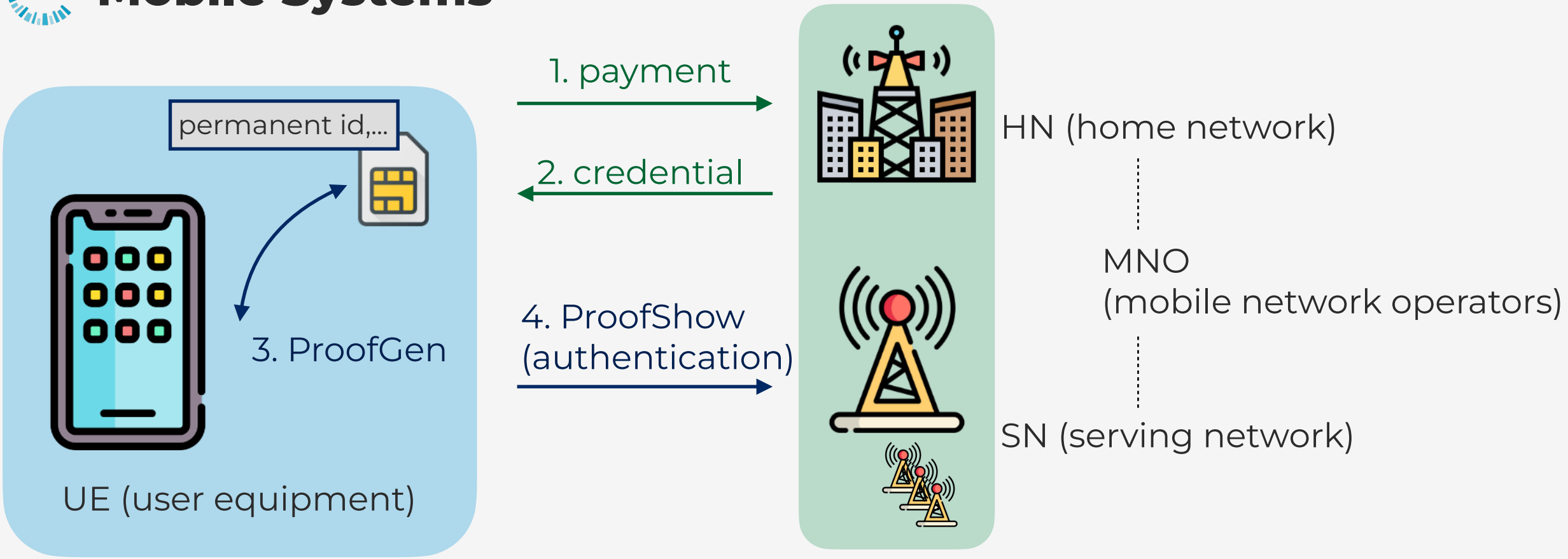
MNO
(mobile network operators)

SN (serving network)

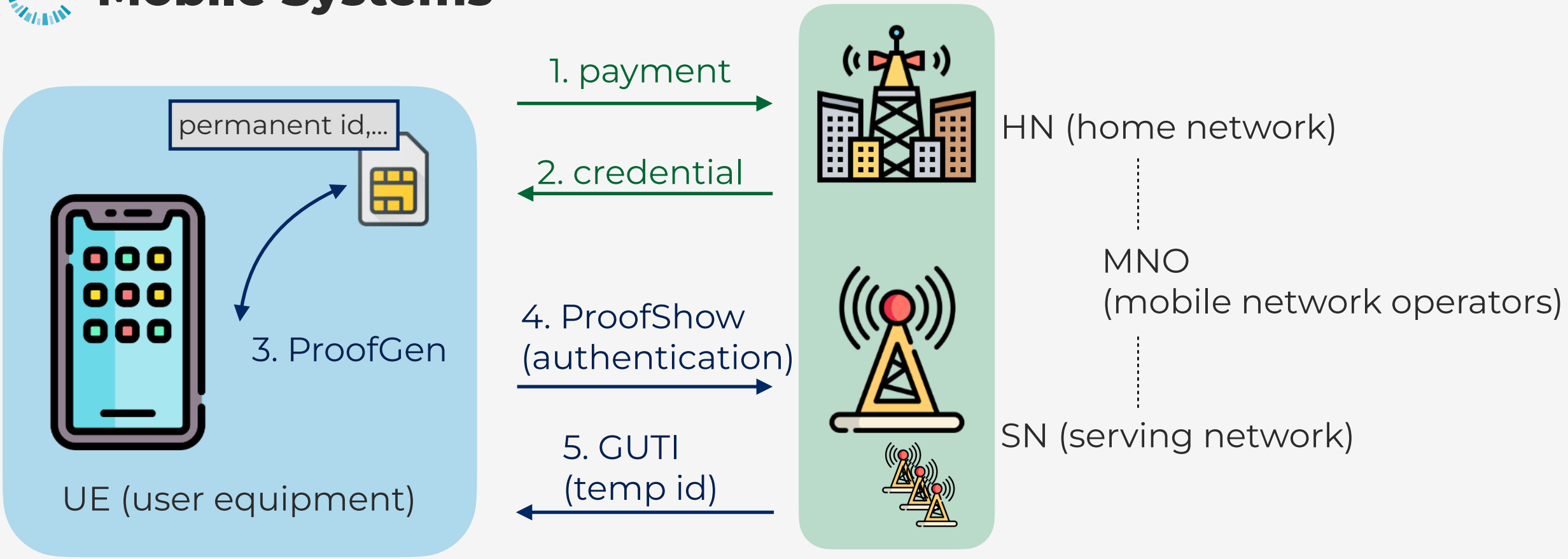
Mobile Systems



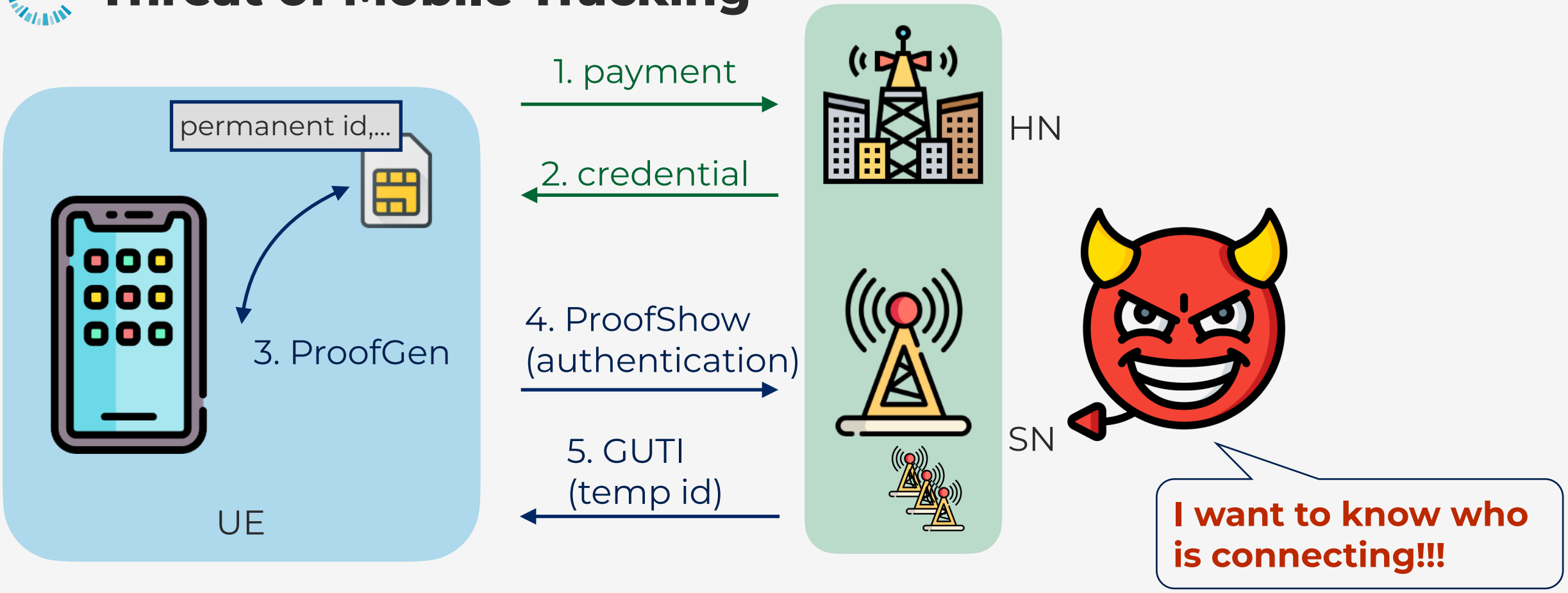
Mobile Systems



Mobile Systems

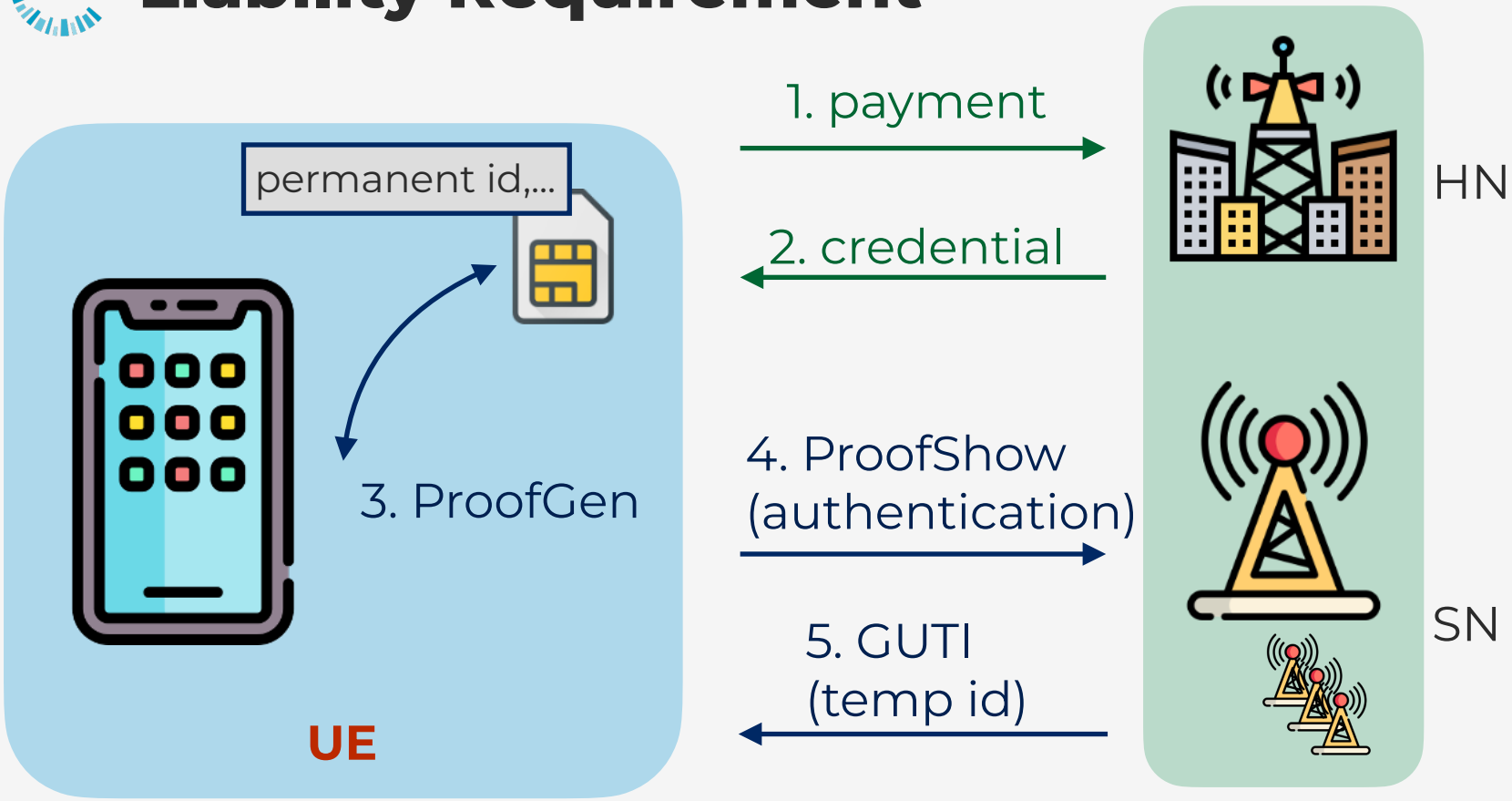


Threat of Mobile Tracking

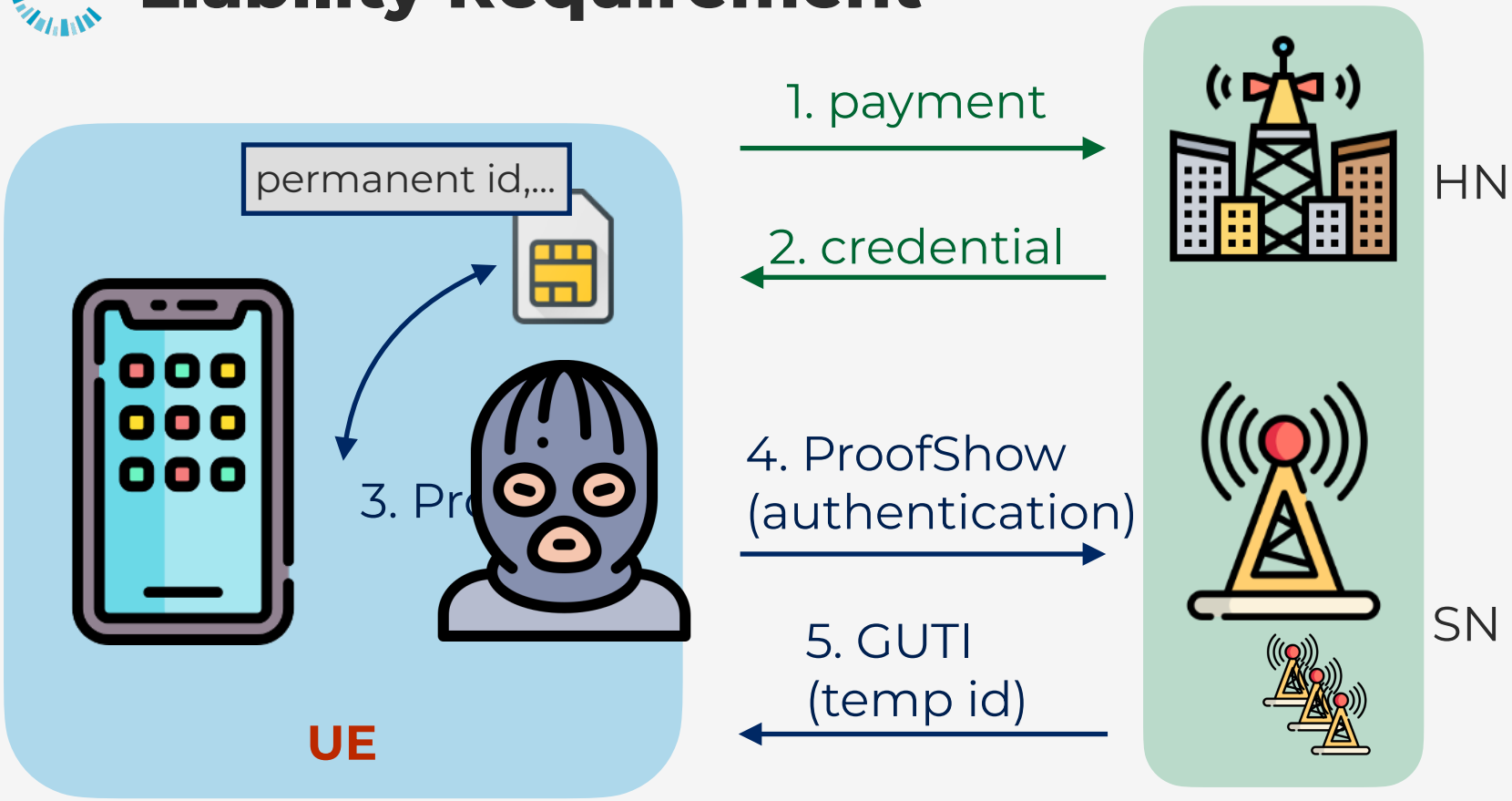


Mobile carriers may sell users' location history to third parties!

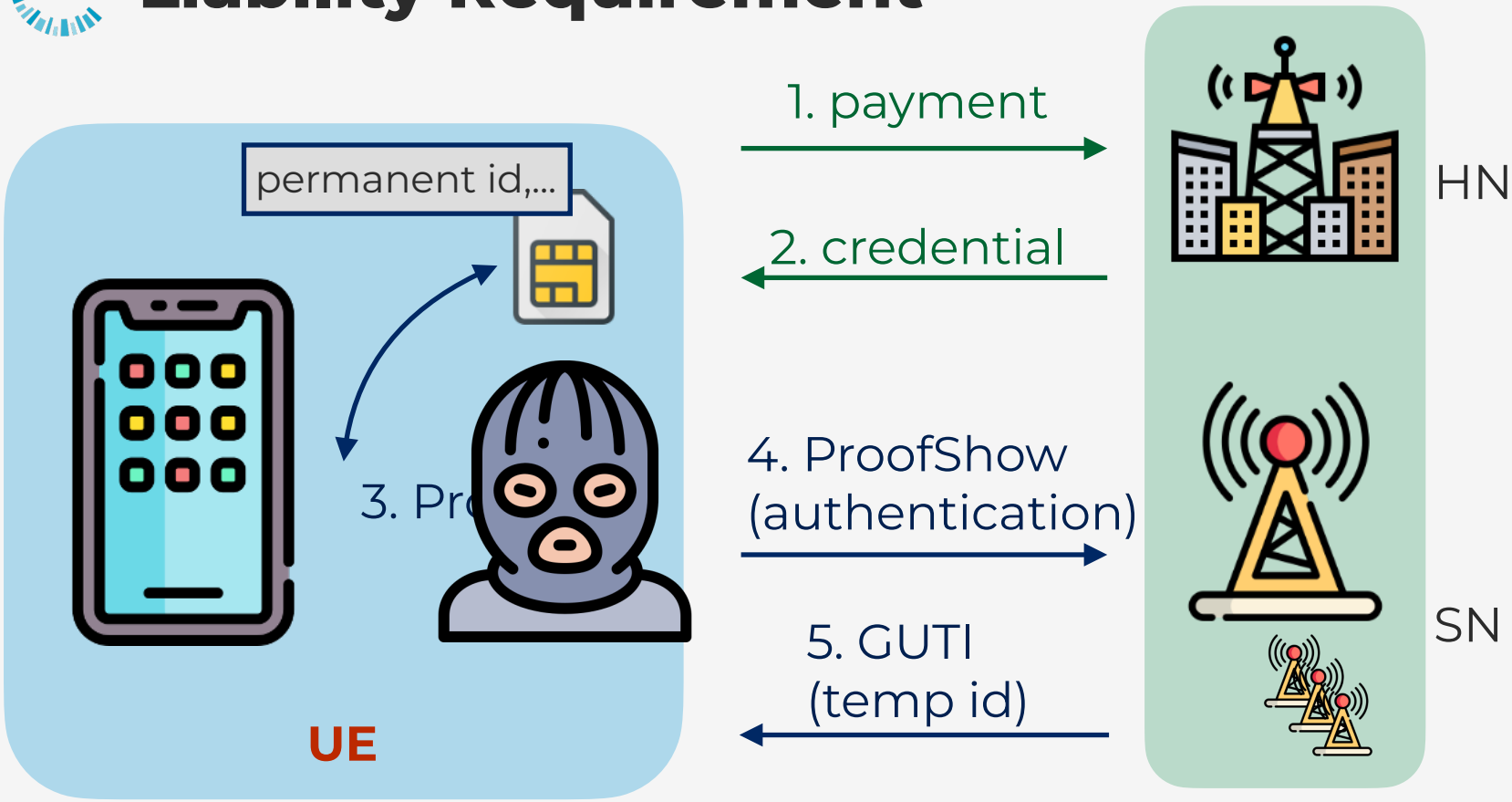
Liability Requirement



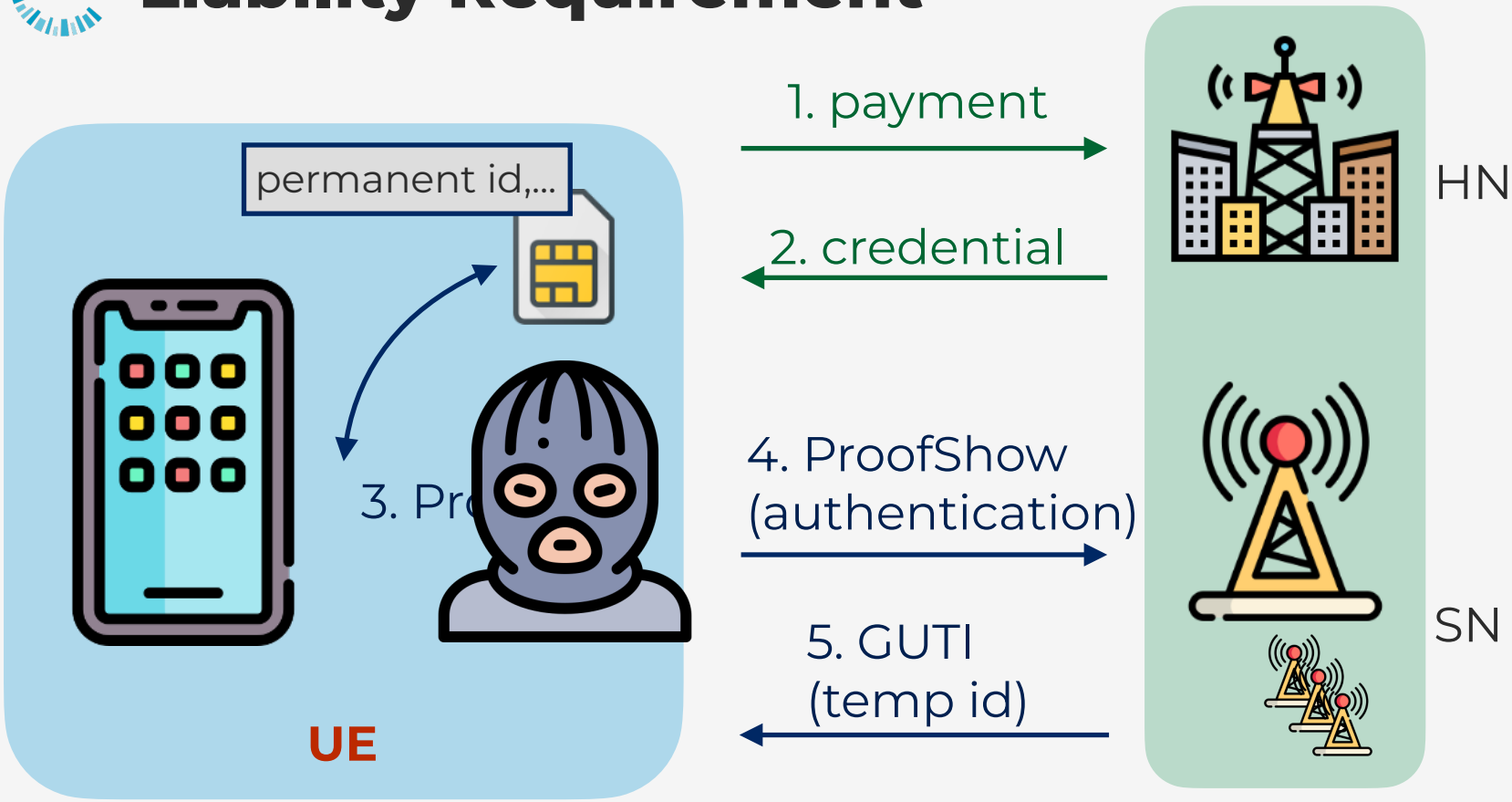
Liability Requirement



Liability Requirement



Liability Requirement



- privacy?
- anti-counterfeiting?
- traceability?
- reliability?

AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, “AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials,” in NDSS 2024.

AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

- anti-tracking privacy (unlinkability)

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, “AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials,” in NDSS 2024.

AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

- anti-tracking privacy (unlinkability)
- anti-counterfeiting protection (unforgeability)

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, “AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials,” in NDSS 2024.

AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

- anti-tracking privacy (unlinkability)
- anti-counterfeiting protection (unforgeability)
- lawful de-anonymization

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, “AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials,” in NDSS 2024.

AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

- anti-tracking privacy (unlinkability)
- anti-counterfeiting protection (unforgeability)
- lawful de-anonymization
- non-interactive roaming support

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, “AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials,” in NDSS 2024.

AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

- anti-tracking privacy (unlinkability)
- anti-counterfeiting protection (unforgeability)
- lawful de-anonymization
- non-interactive roaming support
- lightweight on user side

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, “AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials,” in NDSS 2024.

AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

- anti-tracking privacy (unlinkability)
- anti-counterfeiting protection (unforgeability)
- lawful de-anonymization
- non-interactive roaming support
- lightweight on user side
- compatibility and practicality

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, “AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials,” in NDSS 2024.

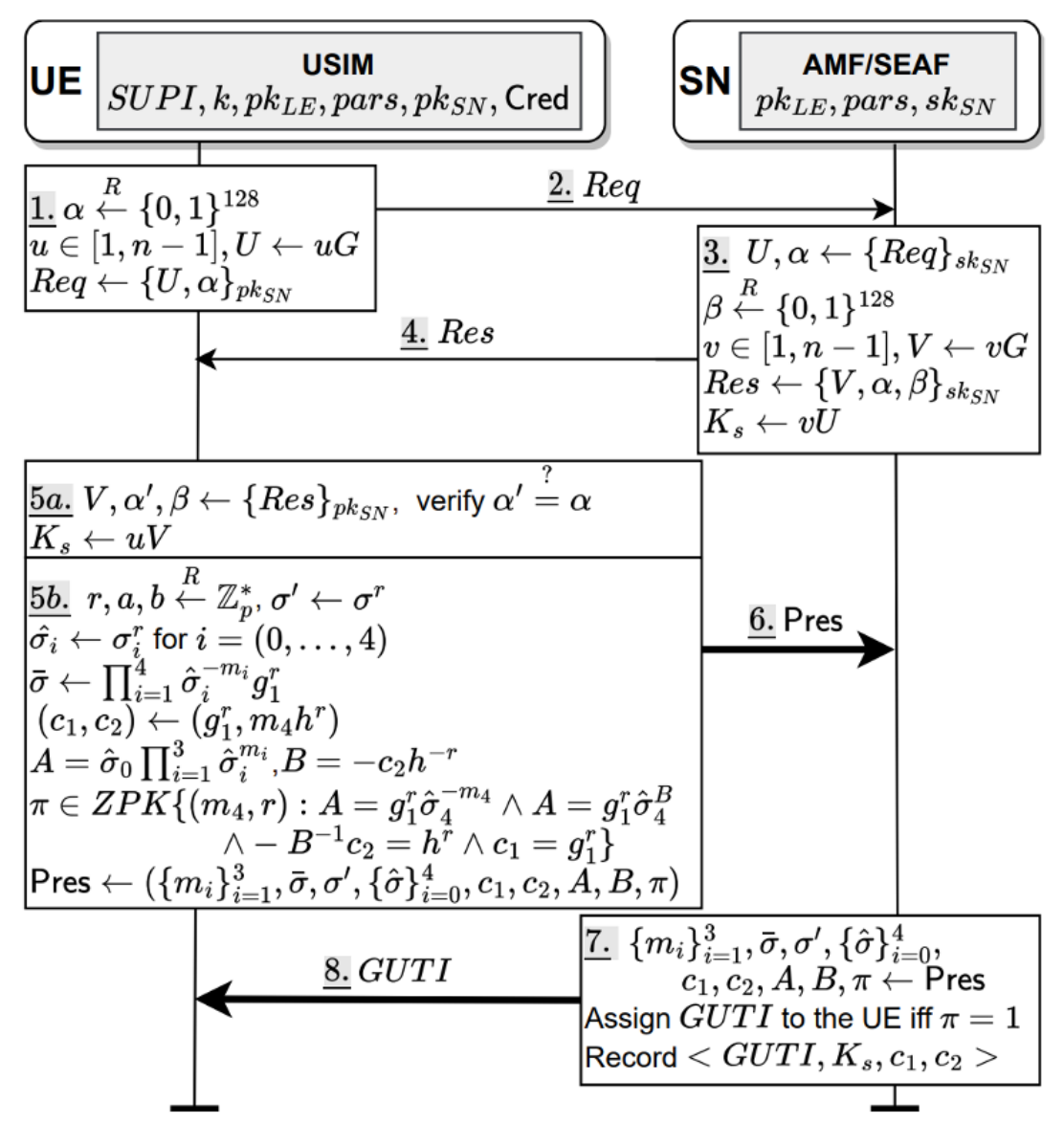
AAKA

AAKA: Anonymous Authentication and Key Agreement [YZZ+24]

- **anti-tracking privacy (unlinkability)** 
- **anti-counterfeiting protection (unforgeability)** 
- lawful de-anonymization
- non-interactive roaming support
- lightweight on user side
- compatibility and practicality

[YZZ+24] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, "AAKA: An anti-tracking cellular authentication scheme leveraging anonymous credentials," in NDSS 2024.

YZZ+ AAKA

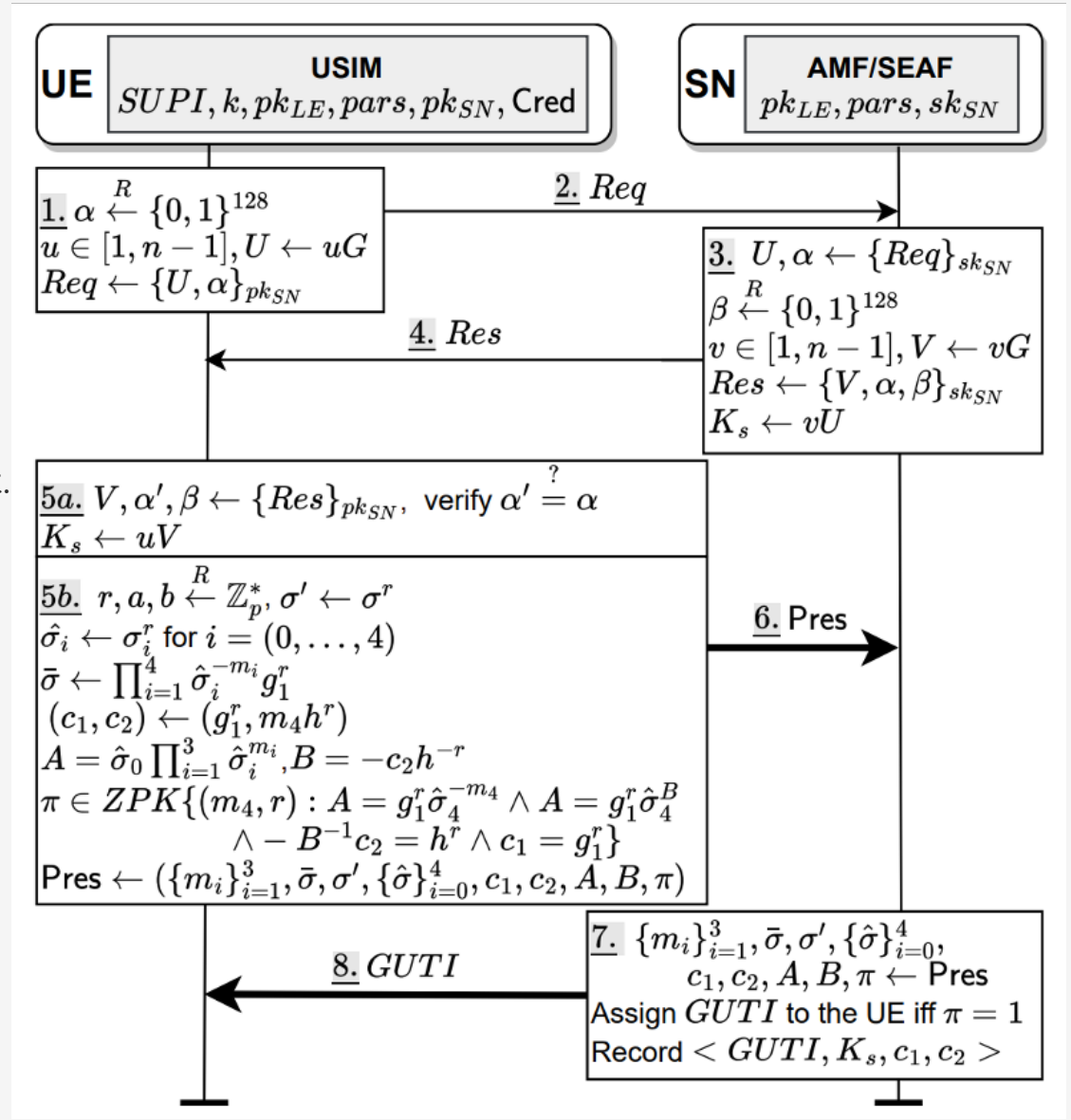


the Presentation and Verification protocol in YZZ+ AAKA

YZZ+ AAKA

m_1, m_2, m_3: public info (subscription)
m_4: private info (permanent id)

$X_0, \ldots, X_4$: public key of HN
h: public key of LEA
(c_1, c_2): ElGamal encryption of m_4
π: zero-knowledge proof for (m_4, r) s.t.
$\ldots, -B^{-1}c_2 = h^r, \ldots$



the Presentation and Verification protocol in YZZ+ AAKA

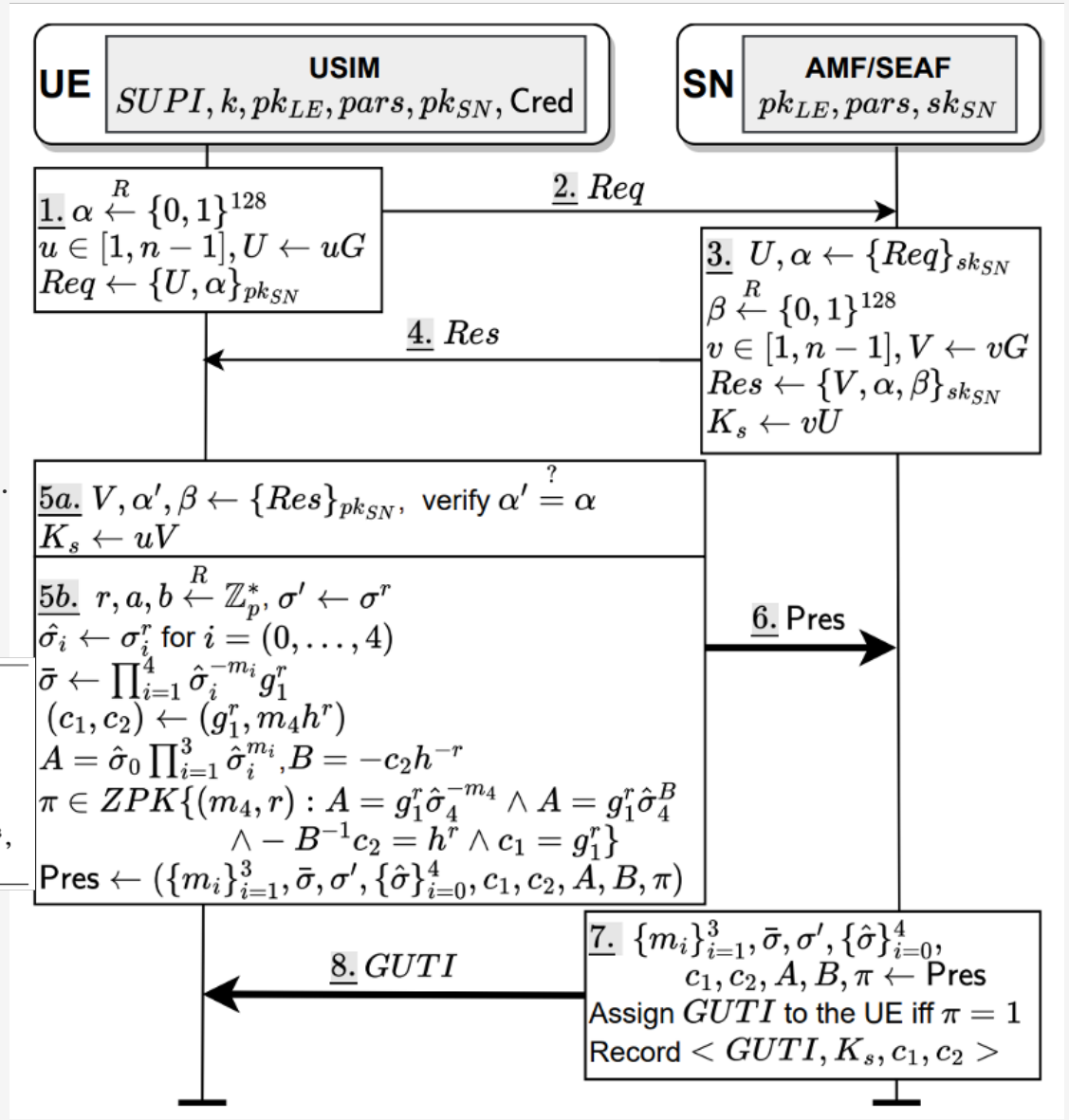
YZZ+ AAKA

m_1, m_2, m_3: public info (subscription)
m_4: private info (permanent id)

$X_0, \ldots, X_4$: public key of HN
h: public key of LEA
(c_1, c_2): ElGamal encryption of m_4
π: zero-knowledge proof for (m_4, r) s.t.
$\ldots, -B^{-1}c_2 = h^r, \ldots$

Let $y_3 = -B^{-1}c_2$. UE executes the following steps:
1) Randomly takes $a_3 \in Z_p^*$
2) Choose challenge $C_3 = H(\bar{y_3})$
3) Compute $\bar{a_3} = a_3 + C_3 r$
4) Sends $(y_3, C_3, \bar{a_3})$ to the SN

SN then computes $\bar{y_3} = h^{\bar{a_3}} y_3^{-C_3} = h^{a_3 + C_3 r} h^{-C_3 r} = h^{a_3}$, and check if $C_3 = H(\bar{y_3})$



the Presentation and Verification protocol in YZZ+ AAKA

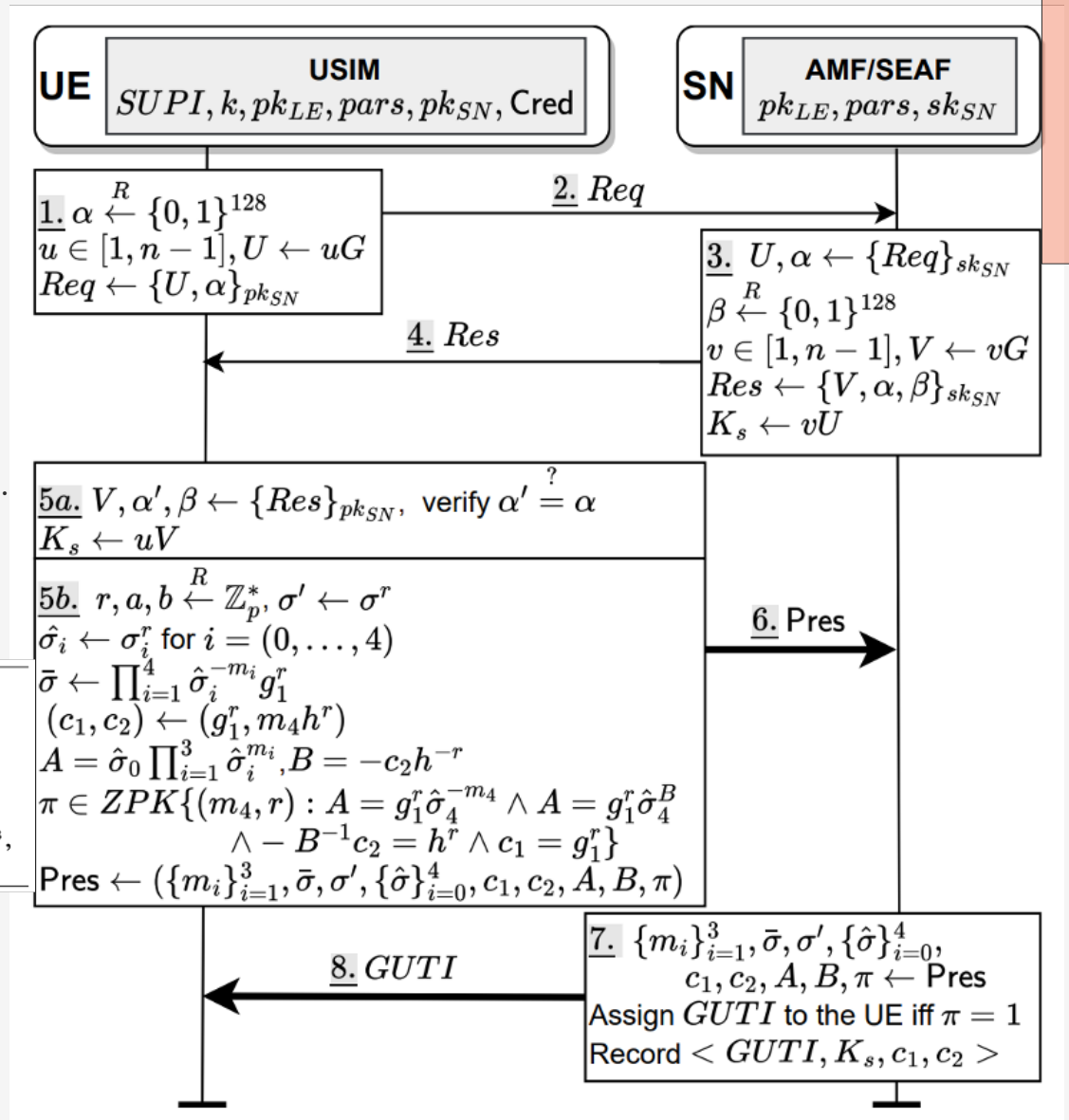
YZZ+ AAKA

m_1, m_2, m_3: public info (subscription)
m_4: private info (permanent id)

$X_0, \ldots, X_4$: public key of HN
h: public key of LEA
(c_1, c_2): ElGamal encryption of m_4
π: zero-knowledge proof for (m_4, r) s.t.
$\ldots, -B^{-1}c_2 = h^r, \ldots$

Let $y_3 = -B^{-1}c_2$. UE executes the following steps:
1) Randomly takes $a_3 \in Z_p^*$
2) Choose challenge $C_3 = H(\bar{y_3})$
3) Compute $\bar{a_3} = a_3 + C_3 r$
4) Sends $(y_3, C_3, \bar{a_3})$ to the SN

SN then computes $\bar{y_3} = h^{\bar{a_3}} y_3^{-C_3} = h^{a_3 + C_3 r} h^{-C_3 r} = h^{a_3}$, and check if $C_3 = H(\bar{y_3})$



Attack on Privacy:
SN obtains
$y_3 = -B^{-1}c_2 = h^r$
$c_2 = m_4 / h^r$
so, $m_4 = c_2 / y_3$

the Presentation and Verification protocol in YZZ+ AAKA

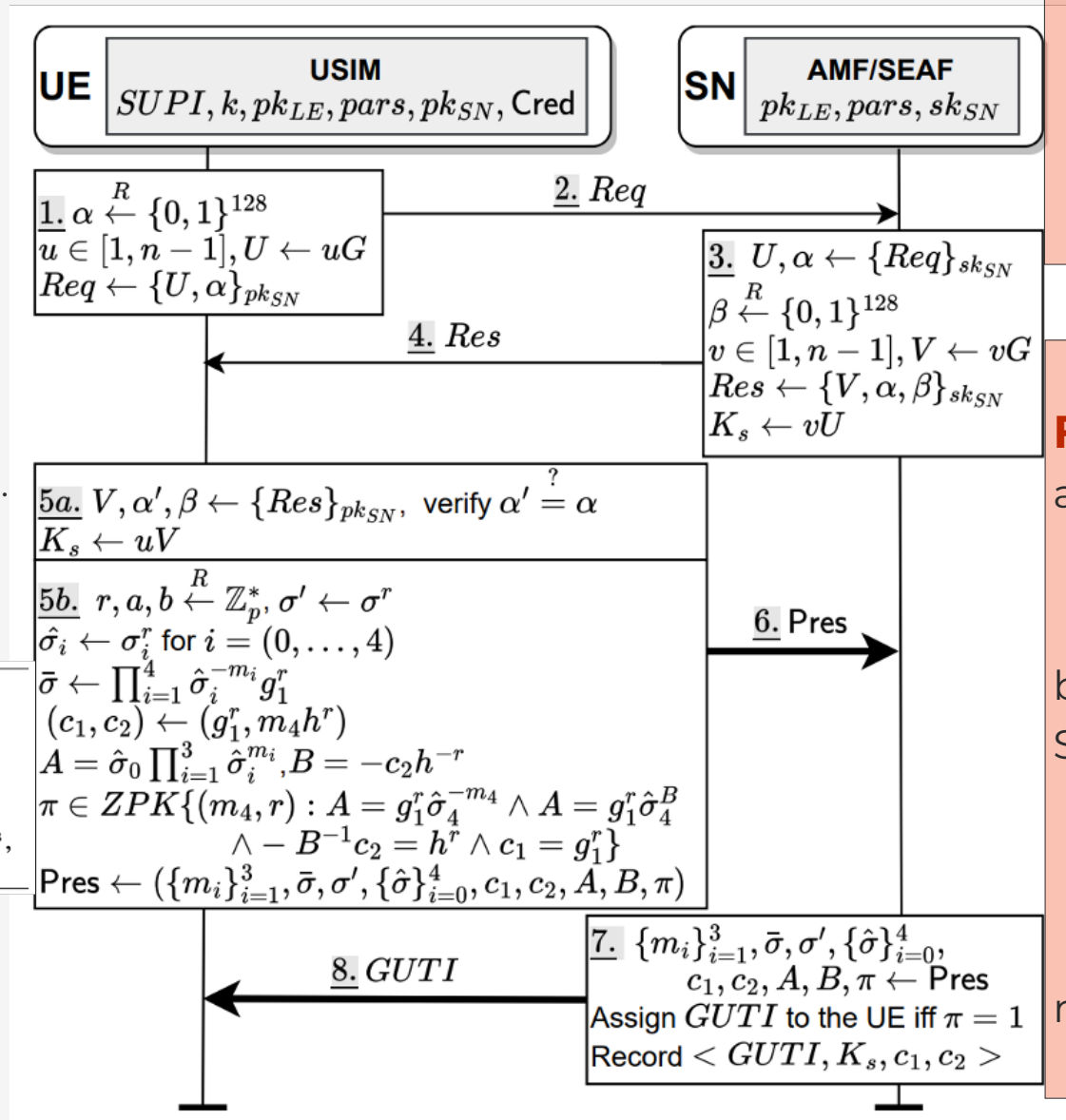
YZZ+ AAKA

m_1, m_2, m_3: public info (subscription)
m_4: private info (permanent id)

$X_0, \ldots, X_4$: public key of HN
h: public key of LEA
(c_1, c_2): ElGamal encryption of m_4
π: zero-knowledge proof for (m_4, r) s.t.
$\ldots, -B^{-1}c_2 = h^r, \ldots$

Let $y_3 = -B^{-1}c_2$. UE executes the following steps:
1) Randomly takes $a_3 \in Z_p^*$
2) Choose challenge $C_3 = H(\bar{y_3})$
3) Compute $\bar{a_3} = a_3 + C_3 r$
4) Sends $(y_3, C_3, \bar{a_3})$ to the SN

SN then computes $\bar{y_3} = h^{\bar{a_3}} y_3^{-C_3} = h^{a_3 + C_3 r} h^{-C_3 r} = h^{a_3}$, and check if $C_3 = H(\bar{y_3})$



Attack on Privacy:
SN obtains
$y_3 = -B^{-1}c_2 = h^r$
$c_2 = m_4 / h^r$
so, $m_4 = c_2 / y_3$

Flaw in Correctness:
a credential is a BB signature σ s.t.
$$e(\sigma, X_0 \prod_{i=1}^4 X_i) = e(g_1, g_2)$$
but in Verification,
SN checks $(\hat{\sigma}_0, \ldots, \hat{\sigma}_4, \hat{\sigma}, \sigma', \pi')$ s.t.
$$e(\hat{\sigma}, g_2) = e(\sigma', X_0)$$
$$\pi' : \ \hat{\sigma}_0 \prod_{1}^{3} \hat{\sigma}_i^{m_i} = g_1^r \hat{\sigma}_4^{-m_4}$$
no use of public keys $X_1, \ldots, X_4$

the Presentation and Verification protocol in YZZ+ AAKA

Revisiting AAKA

BB: the Boneh-Boyen signature scheme
PS: the Pointcheval-Sanders signature scheme

Revisiting AAKA

- Identify the insecurity of YZZ+ AAKA

BB: the Boneh-Boyen signature scheme
PS: the Pointcheval-Sanders signature scheme

Revisiting AAKA

- Identify the insecurity of YZZ+ AAKA
- Formalize the model and redesign AAKA

BB: the Boneh-Boyen signature scheme
PS: the Pointcheval-Sanders signature scheme

Revisiting AAKA

- Identify the insecurity of YZZ+ AAKA
- Formalize the model and redesign AAKA
- AAKA+: verifier-local revocation

BB: the Boneh-Boyen signature scheme
PS: the Pointcheval-Sanders signature scheme

Revisiting AAKA

- Identify the insecurity of YZZ+ AAKA
- Formalize the model and redesign AAKA
- AAKA+: verifier-local revocation
- Two schemes AAKA+BB and AAKA+PS

BB: the Boneh-Boyen signature scheme
PS: the Pointcheval-Sanders signature scheme

Revisiting AAKA

- Identify the insecurity of YZZ+ AAKA
- Formalize the model and redesign AAKA
- AAKA+: verifier-local revocation
- Two schemes AAKA+BB and AAKA+PS
- Practice evaluation

BB: the Boneh-Boyen signature scheme
PS: the Pointcheval-Sanders signature scheme

Boneh-Boyen Signatures

[BB04] D. Boneh and X. Boyen, “Short signatures without random oracles,” in EUROCRYPT 2004.

Boneh-Boyen Signatures

- signing on multiple messages $m_1, \cdots, m_i, \cdots$

[BB04] D. Boneh and X. Boyen, “Short signatures without random oracles,” in EUROCRYPT 2004.

Boneh-Boyen Signatures

- signing on multiple messages $m_1, \cdots, m_i, \cdots$

- public key $X_0 = g_2^{x_0}, X_1 = g_2^{x_1}, \cdots$
- secret key $x_0, x_1, \ldots$
- signature on $m_1, \cdots, m_i, \cdots$
- $\sigma = g_1^{\frac{1}{x_0 + \sum_i x_i m_i}}$
- verification checks if

$$e(\sigma, X_0 \prod_i X_i^{m_i}) = e(g_1, g_2)$$

[BB04] D. Boneh and X. Boyen, “Short signatures without random oracles,” in EUROCRYPT 2004.

Anonymous Credentials

Anonymous Credentials

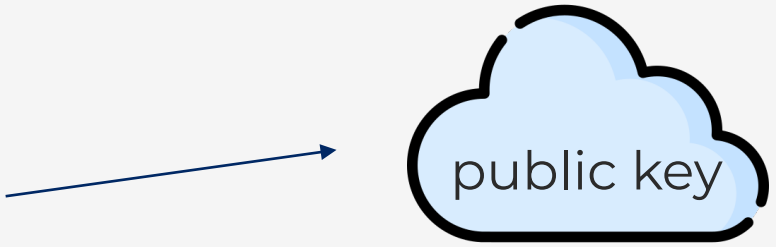
Authority

User

Verifier

Anonymous Credentials

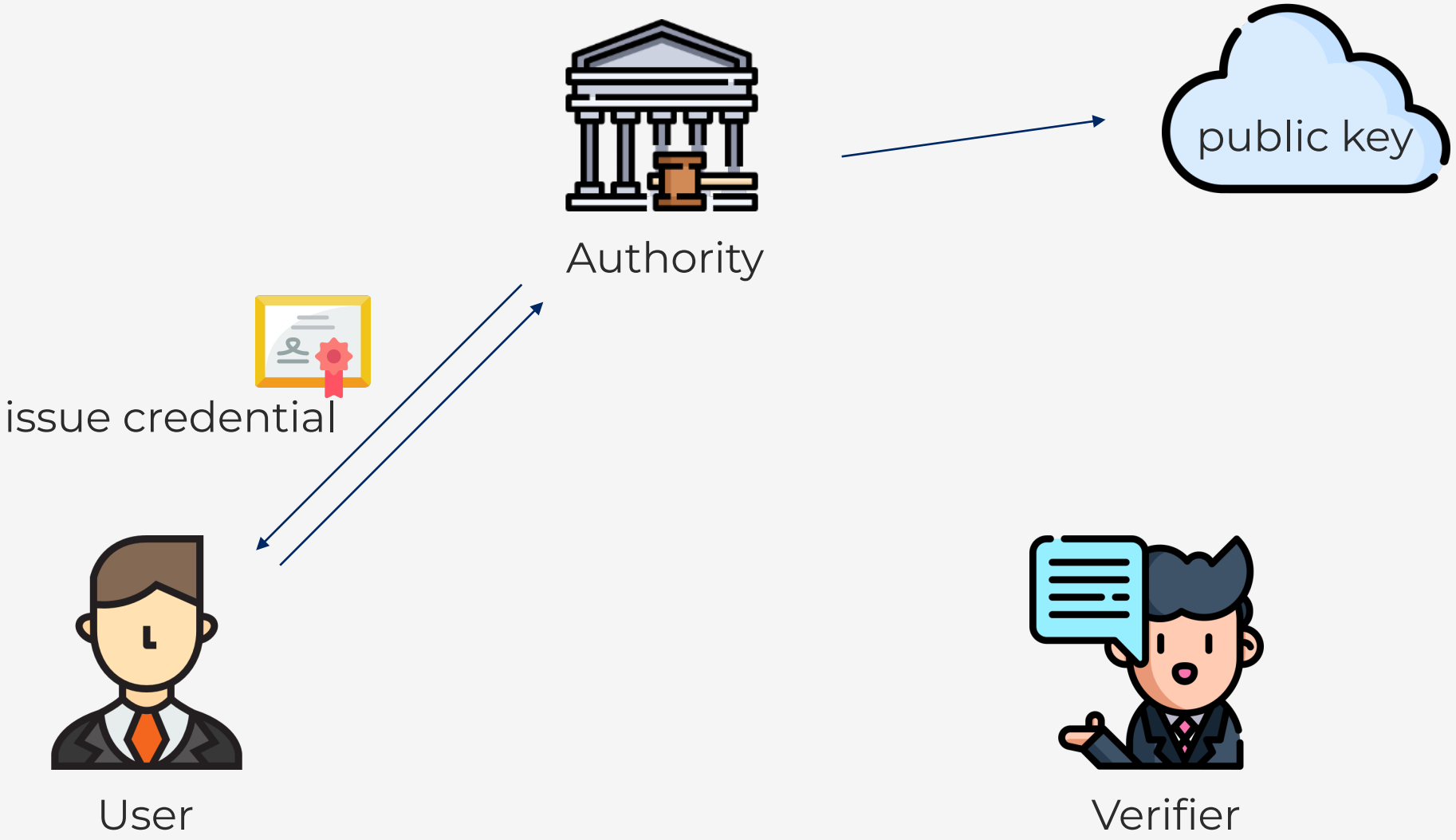
Authority



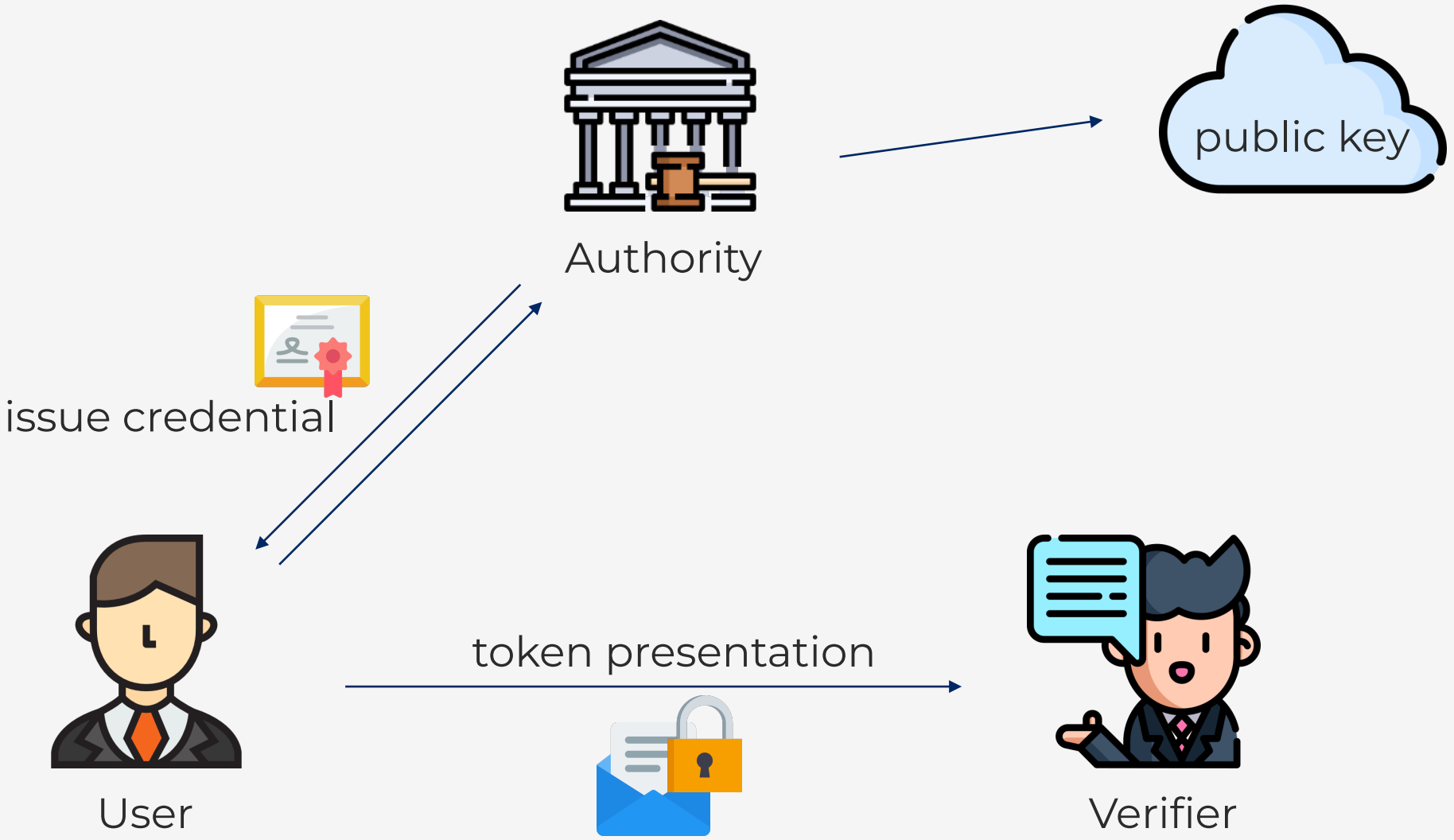
User

Verifier

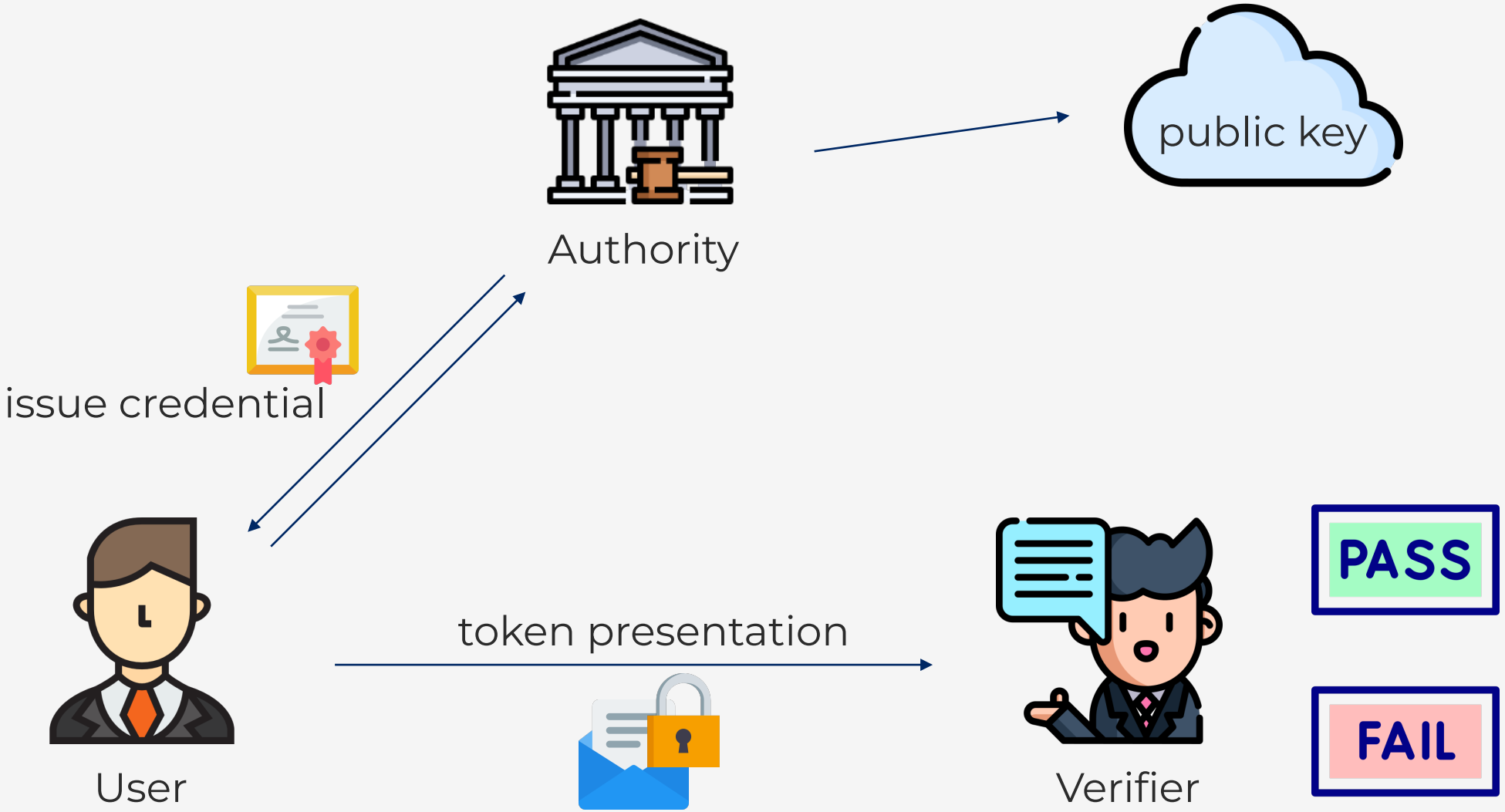
Anonymous Credentials



Anonymous Credentials



Anonymous Credentials



Anonymous Credential for BB Signatures

- D. Boneh and X. Boyen, “Short signatures without random oracles,” in EUROCRYPT 2004.
- J. Camenisch, M. Drijvers, P. Dzurenda, and J. Hajny, “Fast keyed-verification anonymous credentials on standard smart cards,” in SEC 2019.

Anonymous Credential for BB Signatures

- public key $X_0 = g_2^{x_0}, X_1 = g_2^{x_1}, X_2 = g_2^{x_2}$
- m: public message
- pm: private message
- $\sigma = g_1^{\frac{1}{x_0 + x_1 m_1 + x_2 pm}}$
- verification: $e(\sigma, X_0 X_1^m X_2^{pm}) = e(g_1, g_2)$

- D. Boneh and X. Boyen, “Short signatures without random oracles,” in EUROCRYPT 2004.
- J. Camenisch, M. Drijvers, P. Dzurenda, and J. Hajny, “Fast keyed-verification anonymous credentials on standard smart cards,” in SEC 2019.

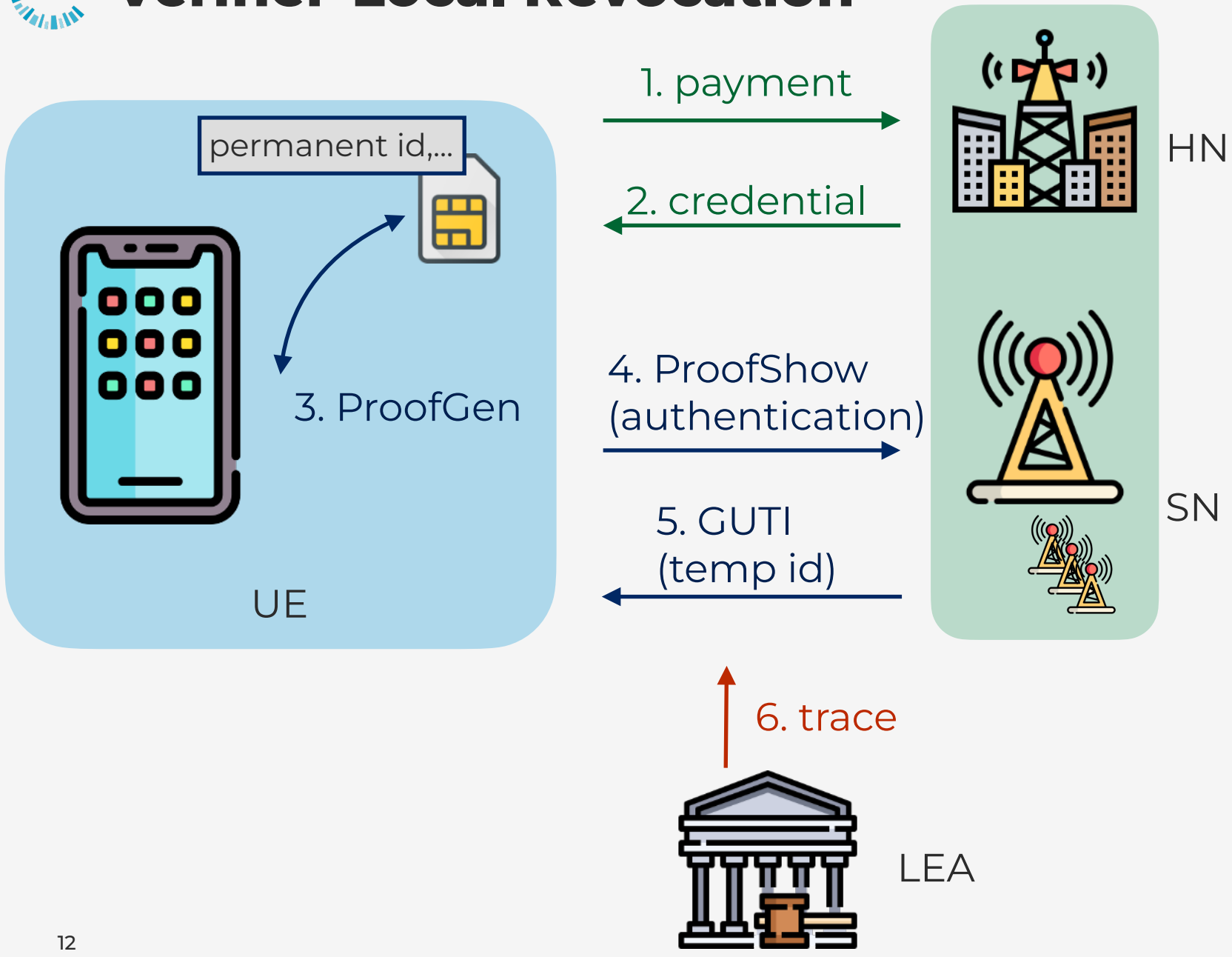
Anonymous Credential for BB Signatures

- public key $X_0 = g_2^{x_0}, X_1 = g_2^{x_1}, X_2 = g_2^{x_2}$
- m: public message
- pm: private message
- $\sigma = g_1^{\frac{1}{x_0 + x_1 m_1 + x_2 pm}}$
- verification: $e(\sigma, X_0 X_1^m X_2^{pm}) = e(g_1, g_2)$

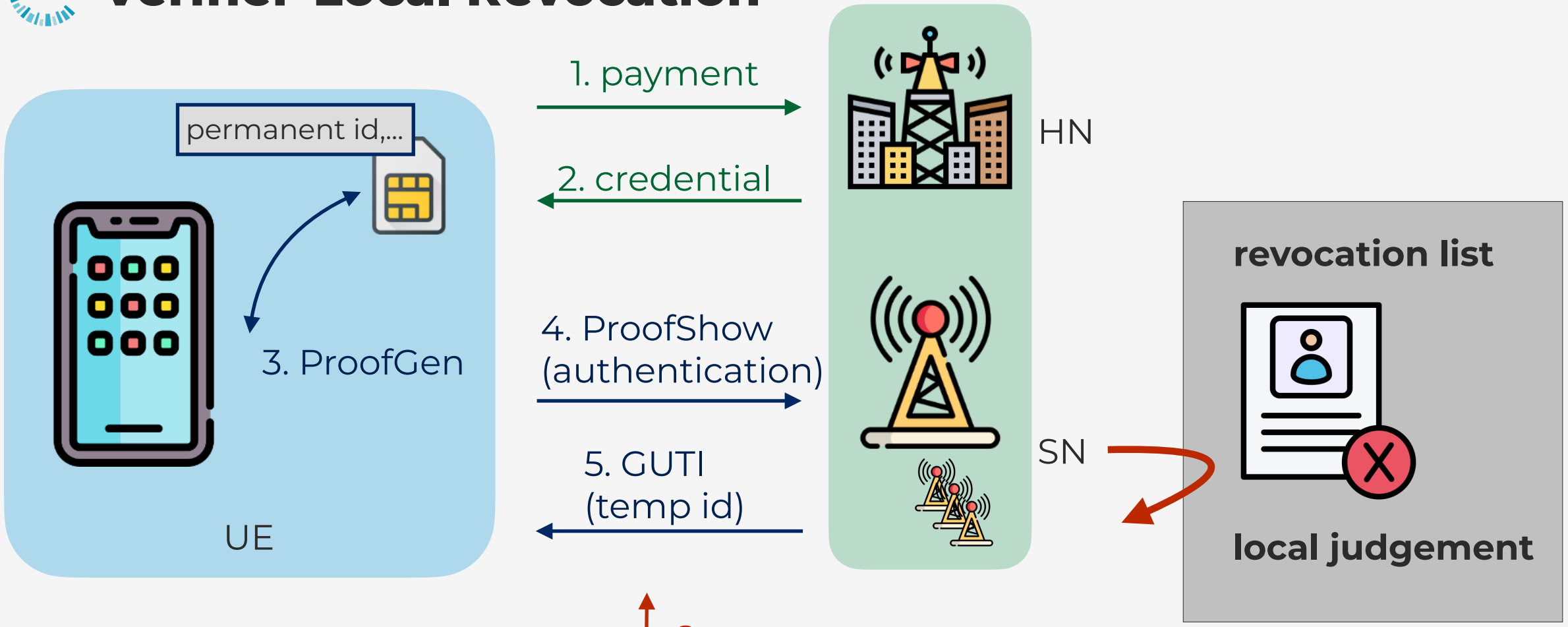
- $\hat{\sigma} = \sigma^r, C_1 = X_0 X_1^m X_2^{pm} g^t, C_2 = g_1^r \hat{\sigma}^t$
- π: zero-knowledge for the witness (pm, r, t)
- Verify $e(\hat{\sigma}, C_1) = e(C_2, g_2)$ and π

- D. Boneh and X. Boyen, “Short signatures without random oracles,” in EUROCRYPT 2004.
- J. Camenisch, M. Drijvers, P. Dzurenda, and J. Hajny, “Fast keyed-verification anonymous credentials on standard smart cards,” in SEC 2019.

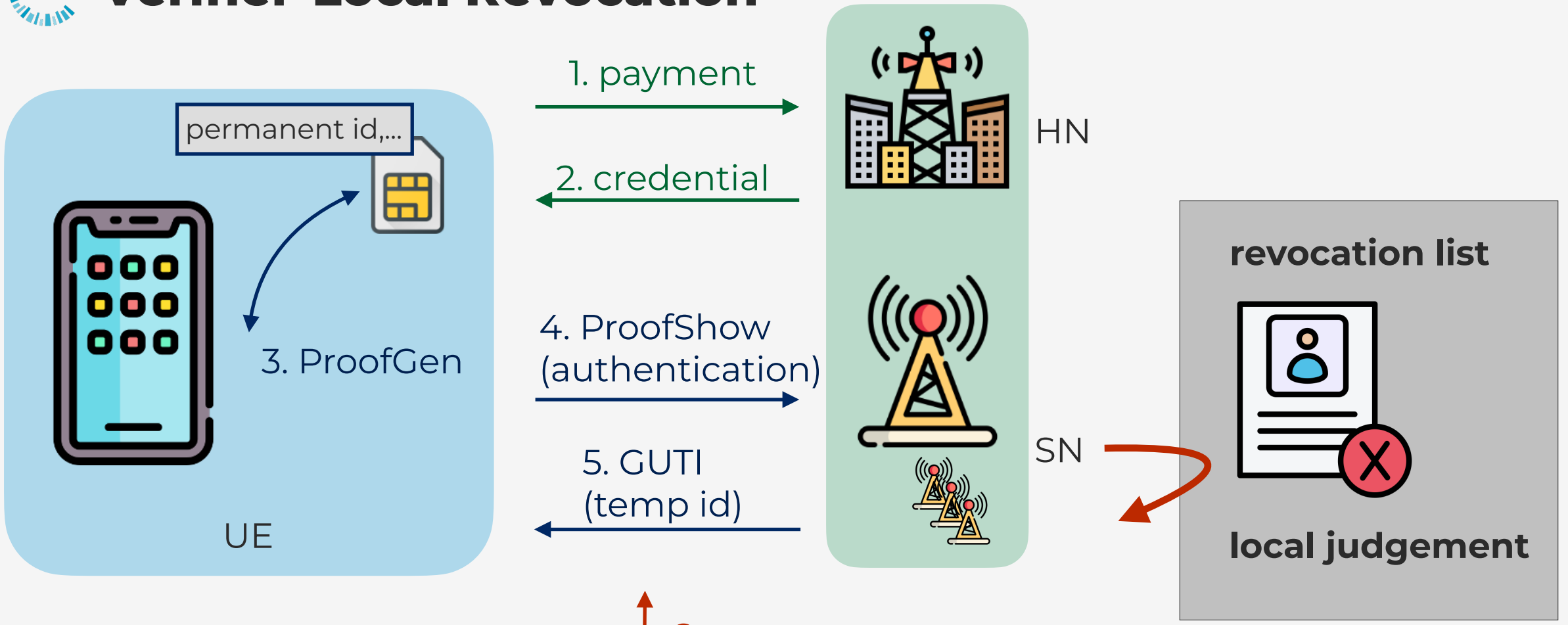
Verifier-Local Revocation



Verifier-Local Revocation



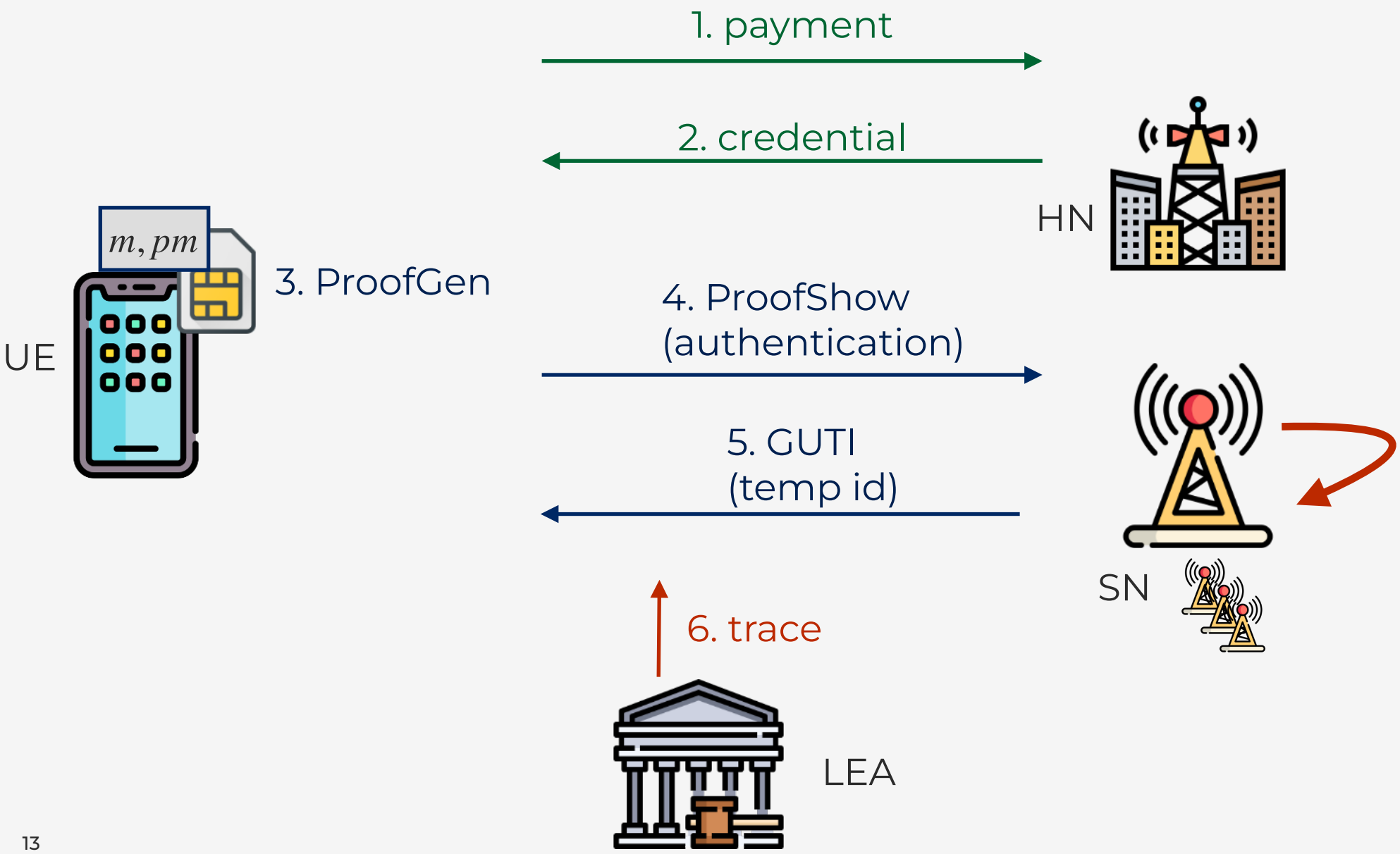
Verifier-Local Revocation



Determine if UE has been revoked immediately (without querying HN)

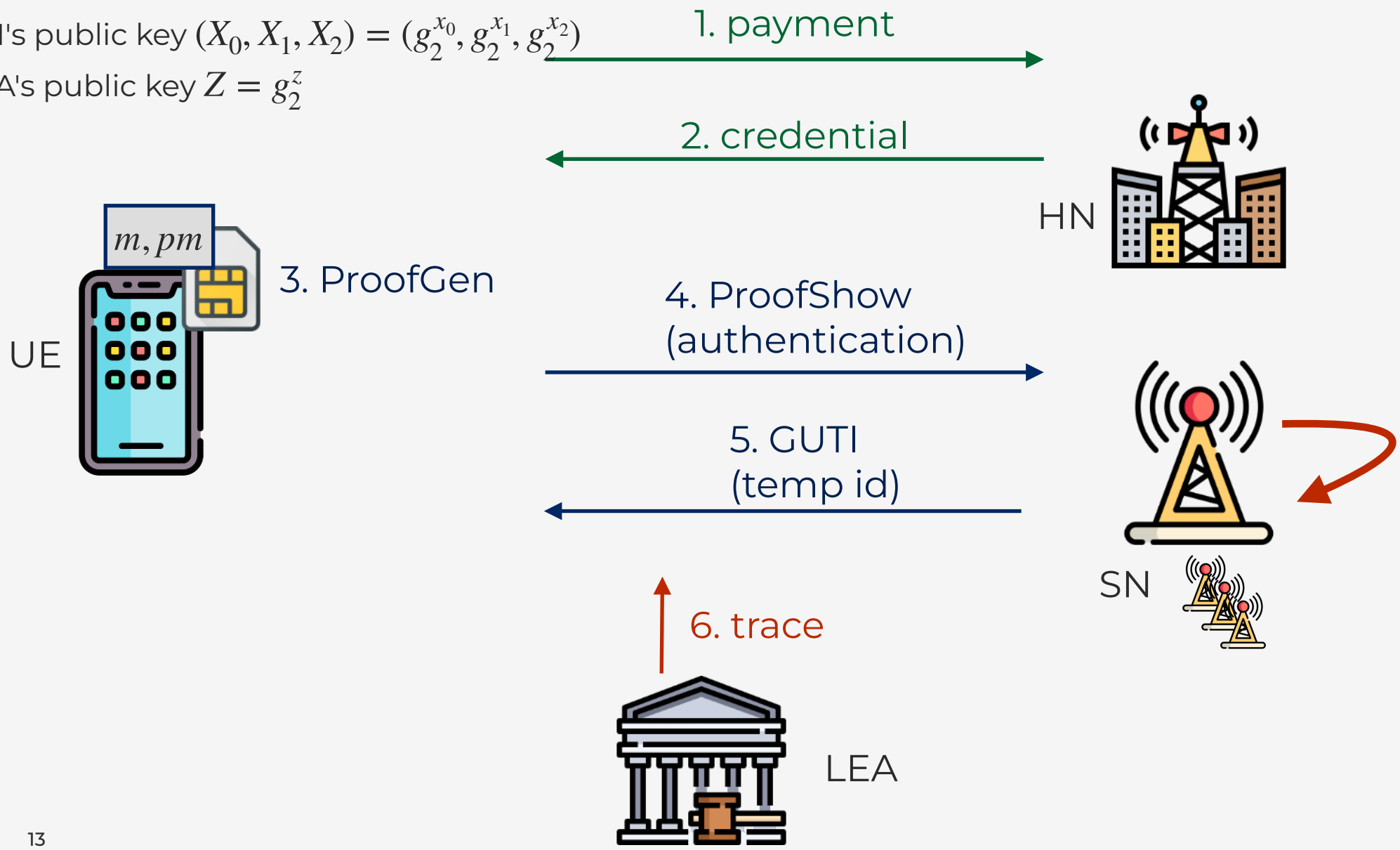
All Together, AAKA+BB

All Together, AAKA+BB



All Together, AAKA+BB

- HN's public key $(X_0, X_1, X_2) = (g_2^{x_0}, g_2^{x_1}, g_2^{x_2})$
- LEA's public key $Z = g_2^z$



All Together, AAKA+BB

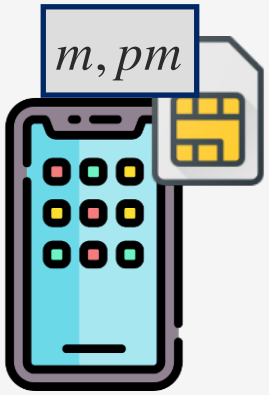
- HN's public key $(X_0, X_1, X_2) = (g_2^{x_0}, g_2^{x_1}, g_2^{x_2})$
- LEA's public key $Z = g_2^z$

BB signature $\sigma = g_2^{\frac{1}{x_0 + x_1 m + x_2 pm}}$

1. payment

2. credential

HN

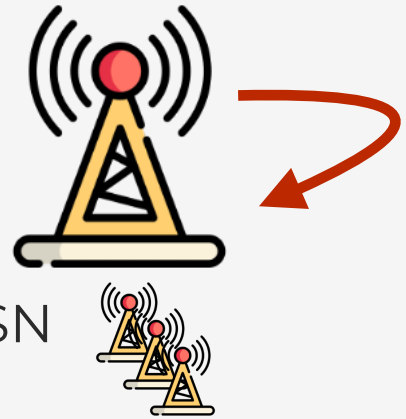


UE

3. ProofGen

4. ProofShow
(authentication)

5. GUTI
(temp id)



SN

6. trace

LEA

All Together, AAKA+BB

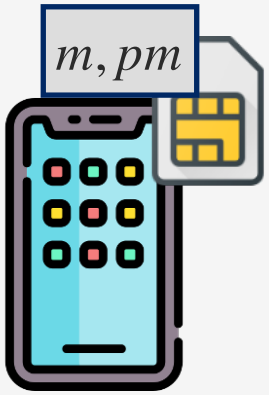
- HN's public key $(X_0, X_1, X_2) = (g_2^{x_0}, g_2^{x_1}, g_2^{x_2})$
- LEA's public key $Z = g_2^z$

BB signature $\sigma = g_2^{\frac{1}{x_0 + x_1 m + x_2 pm}}$

1. payment

2. credential

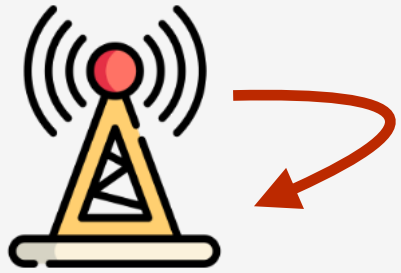
HN



UE

3. ProofGen

4. ProofShow
(authentication)



SN

5. GUTI
(temp id)

$\hat{\sigma} = \sigma^r,$
$C_1 = X_0 X_1^m X_2^{pm} g_2^t, C_2 = g_1^r \hat{\sigma}^t$
$C_3 = g_2^u, C_4 = Z^u \cdot g_2^{pm};$
$C_5 = h^{pm}$ s.t. $h = \text{Hash(context)}$
π : proof of well-formedness

6. trace

LEA

All Together, AAKA+BB

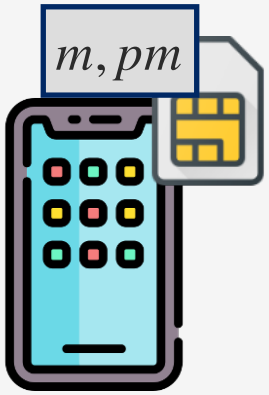
- HN's public key $(X_0, X_1, X_2) = (g_2^{x_0}, g_2^{x_1}, g_2^{x_2})$
- LEA's public key $Z = g_2^z$

BB signature $\sigma = g_2^{\frac{1}{x_0 + x_1 m + x_2 pm}}$

1. payment

2. credential

HN

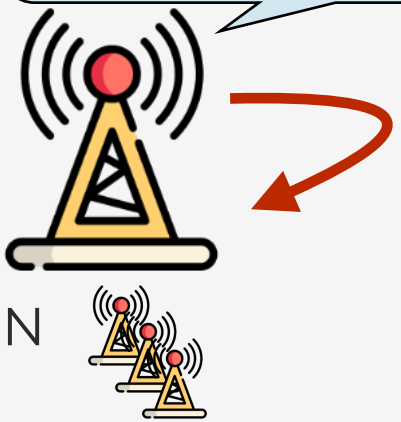


UE

3. ProofGen

4. ProofShow
(authentication)

verify $e(\hat{\sigma}, C_1) = e(C_2, g_2)$ and π



SN

5. GUTI
(temp id)

$\hat{\sigma} = \sigma^r$,
$C_1 = X_0 X_1^m X_2^{pm} g_2^t$, $C_2 = g_1^r \hat{\sigma}^t$
$C_3 = g_2^u$, $C_4 = Z^u \cdot g_2^{pm}$;
$C_5 = h^{pm}$ s.t. $h = \mathsf{Hash}(\text{context})$
π : proof of well-formedness

6. trace

LEA

All Together, AAKA+BB

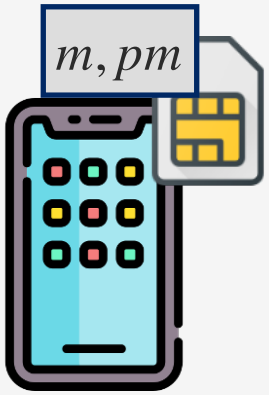
- HN's public key $(X_0, X_1, X_2) = (g_2^{x_0}, g_2^{x_1}, g_2^{x_2})$
- LEA's public key $Z = g_2^z$

BB signature $\sigma = g_2^{\frac{1}{x_0 + x_1 m + x_2 pm}}$

1. payment →

← 2. credential

HN 



UE

3. ProofGen

4. ProofShow (authentication) →

verify $e(\hat{\sigma}, C_1) = e(C_2, g_2)$ and π

SN 

local judgement checks if $e(h, W) = e(C_5, g_2)$ for $W = g_2^{pm'}$ in revocation list

← 5. GUTI (temp id)

$\hat{\sigma} = \sigma^r$,
$C_1 = X_0 X_1^m X_2^{pm} g_2^t, C_2 = g_1^r \hat{\sigma}^t$
$C_3 = g_2^u, C_4 = Z^u \cdot g_2^{pm}$;
$C_5 = h^{pm}$ s.t. $h = \text{Hash(context)}$
π : proof of well-formedness

↑ 6. trace

LEA

All Together, AAKA+BB

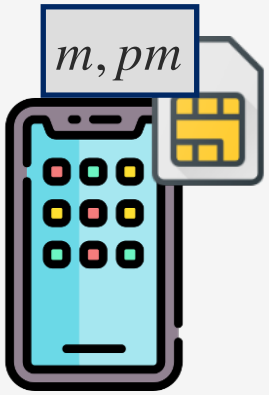
- HN's public key $(X_0, X_1, X_2) = (g_2^{x_0}, g_2^{x_1}, g_2^{x_2})$
- LEA's public key $Z = g_2^z$

BB signature $\sigma = g_2^{\frac{1}{x_0 + x_1 m + x_2 pm}}$

1. payment →

← 2. credential

HN 



UE

3. ProofGen

4. ProofShow (authentication) →

verify $e(\hat{\sigma}, C_1) = e(C_2, g_2)$ and π

SN 

local judgement checks if $e(h, W) = e(C_5, g_2)$ for $W = g_2^{pm'}$ in revocation list

← 5. GUTI (temp id)

$\hat{\sigma} = \sigma^r$,
$C_1 = X_0 X_1^m X_2^{pm} g_2^t$, $C_2 = g_1^r \hat{\sigma}^t$
$C_3 = g_2^u$, $C_4 = Z^u \cdot g_2^{pm}$;
$C_5 = h^{pm}$ s.t. $h = \text{Hash(context)}$
π : proof of well-formedness

6. trace ↑

LEA

trace $C_4 / C_3^z = g_2^{pm}$

Pointcheval-Sanders Signatures

- public key $X_0 = g_2^{x_0}, X_1 = g_2^{x_1}, \ldots$
- secret key $x_0, x_1, \cdots$
- signature on $m_1, \cdots, m_i, \cdots$
- $\sigma_1 \leftarrow \mathbb{G}_1^*, \sigma_2 = \sigma_1^{x_0 + \sum_i x_i m_i}$
- verification checks if

$$e(\sigma_1, X_0 \prod_i X_i^{m_i}) = e(\sigma_2, g_2)$$

D. Pointcheval and O. Sanders, “Short randomizable signatures,” in Topics in Cryptology - CT-RSA 2016.

AAKA+PS

- HN's public key $(X_0, X_1, X_2) = (g_2^{x_0}, g_2^{x_1}, g_2^{x_2})$
- LEA's public key $Z = g_2^z$

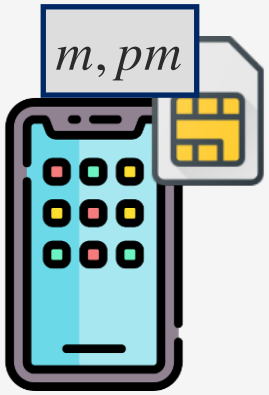
1. payment

PS signature $(\sigma_1, \sigma_2 = \sigma_1^{x_0+x_1 m+x_2 pm})$

2. credential

HN

UE



3. ProofGen

4. ProofShow
(authentication)

verify $e(\hat{\sigma}_1, C_1) = e(\hat{\sigma}_2, g_2)$ and π

SN

local judgement checks if
$e(h, W) = e(C_4, g_2)$
for $W = g_2^{pm'}$ in revocation list

5. GUTI
(temp id)

$\hat{\sigma}_1 = \sigma_1^r, \hat{\sigma}_2 = \sigma_2^r \cdot \hat{\sigma}_1^t$
$C_1 = X_0 X_1^m X_2^{pm} g_2^t,$
$C_2 = g_2^u, C_3 = Z^u \cdot g_2^{pm};$
$C_4 = h^{pm}$ s.t. $h = \mathsf{Hash}(\text{context})$
π : proof of well-formedness

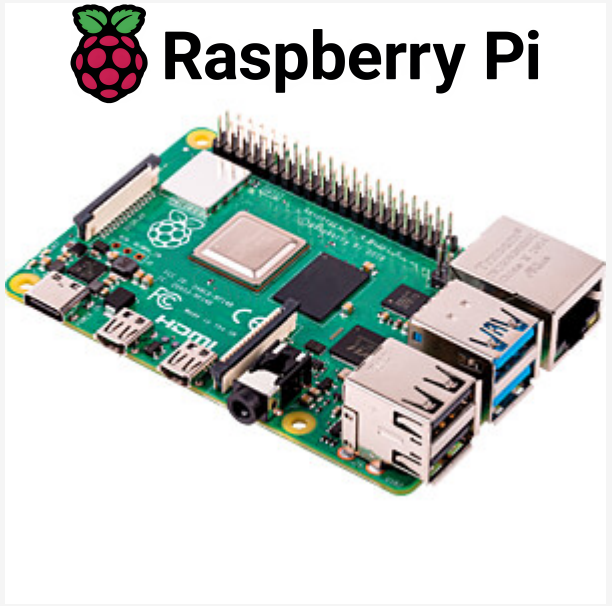
6. trace

LEA

trace $C_3 / C_2^z = g_2^{pm}$

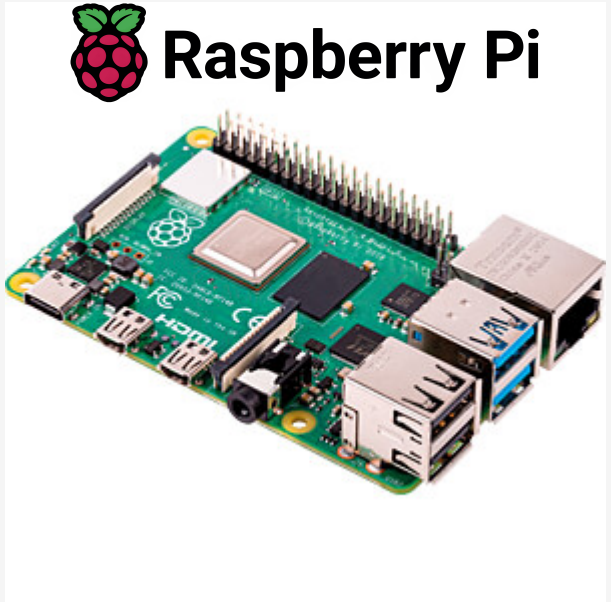
Evaluation

Evaluation



Raspberry Pi 4

Evaluation

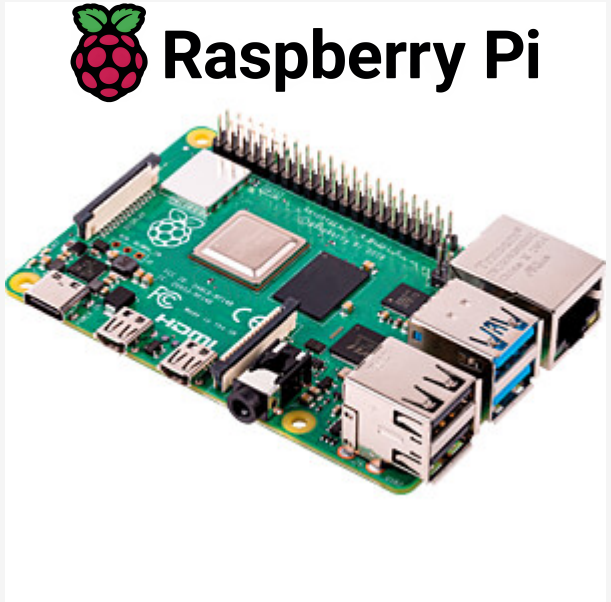


Raspberry Pi 4

Communication Complexity

Components	Size	
	AAKA+BB	AAKA+PS
CredIssue	$4([\mathbb{G}_1] + [\mathbb{Z}_q])$	$2[\mathbb{G}_1] + 4[\mathbb{Z}_q]$
Key Agreement (UE)	$1[\mathbb{G}_1]$	$1[\mathbb{G}_1]$
Key Agreement (SN/HN)	$1[\mathbb{G}_1] + \lambda$	$1[\mathbb{G}_1] + \lambda$
ProofShow	$3([\mathbb{G}_1] + [\mathbb{G}_2]) + 5[\mathbb{Z}_q]$	$3([\mathbb{G}_1] + [\mathbb{G}_2]) + 4[\mathbb{Z}_q]$
Trace	$1[\mathbb{G}_2]$	$1[\mathbb{G}_2]$

Evaluation



Raspberry Pi 4

Time Cost (ms)

Different stages	Entity	AAKA+BB	AAKA+PS
CredIssue	HN	6.82	3.98
CredVer	UE	38.82	12.17
Key Agreement	UE	∼4.30	∼4.30
Key Agreement	SN/HN	∼0.89	∼0.89
ProofShow	UE	18.40 (+29.45)	18.09(+26.10)
ProofVer	SN/HN	19.93	18.87
Trace	LEA	∼0.96	∼0.96

Communication Complexity

Components	Size	
	AAKA+BB	AAKA+PS
CredIssue	$4([\mathbb{G}_1] + [\mathbb{Z}_q])$	$2[\mathbb{G}_1] + 4[\mathbb{Z}_q]$
Key Agreement (UE)	$1[\mathbb{G}_1]$	$1[\mathbb{G}_1]$
Key Agreement (SN/HN)	$1[\mathbb{G}_1] + \lambda$	$1[\mathbb{G}_1] + \lambda$
ProofShow	$3([\mathbb{G}_1] + [\mathbb{G}_2]) + 5[\mathbb{Z}_q]$	$3([\mathbb{G}_1] + [\mathbb{G}_2]) + 4[\mathbb{Z}_q]$
Trace	$1[\mathbb{G}_2]$	$1[\mathbb{G}_2]$

Summary

- Identify the insecurity of YZZ+ AAKA
- Formalize the model and redesign AAKA
- AAKA+: verifier-local revocation
- Two schemes AAKA+BB and AAKA+PS
- Practice evaluation
- full paper: eprint.iacr.org/2025/1986

Summary

- Identify the insecurity of YZZ+ AAKA
- Formalize the model and redesign AAKA
- AAKA+: verifier-local revocation
- Two schemes AAKA+BB and AAKA+PS
- Practice evaluation
- full paper: eprint.iacr.org/2025/1986

Questions?