NTNU
Norwegian University of
Science and Technology

Towards Privacy Preserving Mobile Communications

George Petrides

(with Kristian Gjøsteen and Asgeir Steine)

8^{th} May 2012
Information Security Research School
Finse

Current Situation

(very loosely speaking)

Mobile Network Operators (MNOs) – e.g. Telenor, Netcom:

1. Maintain the communication infrastructure (base stations).
2. Subscribe users (SIM cards with embedded symmetric key & IMSI).
3. Bill subscribers and other MNOs for services.
   - Virtual Network Operators (MVNOs) – e.g. Chess.

Current Situation (Ctd.)

(still very loosely speaking)

When Alice switches on her phone:

1. Authenticates to $\mathcal{N}_A$ using IMSI and embedded key.

Current Situation (Ctd.)

(still very loosely speaking)

When Alice switches on her phone:

1. Authenticates to $\mathcal{N}_A$ using IMSI and embedded key.
   - $\mathcal{N}_A$ learns her identity & location (base station)

Current Situation (Ctd.)

(still very loosely speaking)

When Alice switches on her phone:

1. Authenticates to $\mathcal{N}_A$ using IMSI and embedded key.
   - $\mathcal{N}_A$ learns her identity & location (base station)
2. $\mathcal{N}_A$ sents her TMSIs for subsequent position updates.

Current Situation (Ctd.)

(still very loosely speaking)

When Alice switches on her phone:

1. Authenticates to $\mathcal{N}_A$ using IMSI and embedded key.
   - $\mathcal{N}_A$ learns her identity & location (base station)
2. $\mathcal{N}_A$ sents her TMSIs for subsequent position updates.
   - Eavesdroppers can't follow Alice around.

Current Situation (Ctd.)

(still very loosely speaking)

When Alice switches on her phone:

1. Authenticates to $\mathcal{N}_A$ using IMSI and embedded key.
   - $\mathcal{N}_A$ learns her identity & location (base station)
2. $\mathcal{N}_A$ sents her TMSIs for subsequent position updates.
   - Eavesdroppers can't follow Alice around.
   - $\mathcal{N}_A$ can!

Current Situation (Ctd.)

(still very loosely speaking)

When Alice switches on her phone:

1. Authenticates to $\mathcal{N}_A$ using IMSI and embedded key.
   - $\mathcal{N}_A$ learns her identity & location (base station)
2. $\mathcal{N}_A$ sents her TMSIs for subsequent position updates.
   - Eavesdroppers can't follow Alice around.
   - $\mathcal{N}_A$ can!
   - Active attackers can too! (IMSI-catchers)

Current Situation (Ctd.)

(still very loosely speaking)

If Alice wants to call Bob:

- Alice updates her position to $\mathcal{N}_A$ and asks to contact Bob -
- $\mathcal{N}_A$ contacts Bob through $\mathcal{N}_B$ -
- Alice and Bob exchange messages via $\mathcal{N}_A$ and $\mathcal{N}_B$ -

Current Situation (Ctd.)

(still very loosely speaking)

If Alice wants to call Bob:

- Alice updates her position to $\mathcal{N}_A$ and asks to contact Bob - $\mathcal{N}_A$ learns who she wants to talk to.
- $\mathcal{N}_A$ contacts Bob through $\mathcal{N}_B$ -
- Alice and Bob exchange messages via $\mathcal{N}_A$ and $\mathcal{N}_B$ -

Current Situation (Ctd.)

(still very loosely speaking)

If Alice wants to call Bob:

- Alice updates her position to $\mathcal{N}_A$ and asks to contact Bob - $\mathcal{N}_A$ learns who she wants to talk to.
- $\mathcal{N}_A$ contacts Bob through $\mathcal{N}_B$ - $\mathcal{N}_B$ learns Bob's location.
- Alice and Bob exchange messages via $\mathcal{N}_A$ and $\mathcal{N}_B$ -

Current Situation (Ctd.)

(still very loosely speaking)

If Alice wants to call Bob:

- Alice updates her position to $\mathcal{N}_A$ and asks to contact Bob - $\mathcal{N}_A$ learns who she wants to talk to.
- $\mathcal{N}_A$ contacts Bob through $\mathcal{N}_B$ - $\mathcal{N}_B$ learns Bob's location.
- Alice and Bob exchange messages via $\mathcal{N}_A$ and $\mathcal{N}_B$ - $\mathcal{N}_A$ and $\mathcal{N}_B$ listen to their conversation.

Current Situation (Ctd.)

(still very loosely speaking)

If Alice wants to call Bob:

- Alice updates her position to $\mathcal{N}_A$ and asks to contact Bob - $\mathcal{N}_A$ learns who she wants to talk to.
- $\mathcal{N}_A$ contacts Bob through $\mathcal{N}_B$ - $\mathcal{N}_B$ learns Bob's location.
- Alice and Bob exchange messages via $\mathcal{N}_A$ and $\mathcal{N}_B$ - $\mathcal{N}_A$ and $\mathcal{N}_B$ listen to their conversation.

$\mathcal{N}_A$ and $\mathcal{N}_B$ (possibly one and the same) learn EVERYTHING there is to know: Who, Where and What.

New Privacy Preserving Setting

- We would prefer if $\mathcal{N}_A$ can't follow Alice around
  - but would still like to have authenticated seamless connection.
- Also, the identity of Bob and the contents of their conversation should be kept private.

New Privacy Preserving Setting

- We would prefer if $\mathcal{N}_A$ can't follow Alice around
  - but would still like to have authenticated seamless connection.
- Also, the identity of Bob and the contents of their conversation should be kept private.

Proposal: Split MNOs in two: MNOs and SPs (Service Providers)

1. MNOs
   - Maintain the communication infrastructure (base stations).
   - Bill SPs for services.
2. SPs
   - Subscribe users (SIM card with embedded symmetric key & identity token).
   - Bill subscribers for services.

This is not crazy - similar to MNO–MVNO case!

User-MNO Key Establishment

Alice establishes a secure channel with nearest $\mathcal{N}$.

- Diffie-Hellman key exchange.
- Anonymous by use of pseudonym ps_A.

User-MNO Key Establishment

Alice establishes a secure channel with nearest $\mathcal{N}$.

- Diffie-Hellman key exchange.
- Anonymous by use of pseudonym ps_A.

How does $\mathcal{N}$ know that user ps_A is a subscriber?

1. Alice (user ps_A) identifies herself to $\mathcal{SP}_A$ using token

$$\mathcal{T}_A = Enc\{Alice||smth\}_{\mathcal{K}_{\mathcal{SP}_A}}.$$

2. $\mathcal{SP}_A$ confirms to $\mathcal{N}$ that user ps_A is subscribed.

User-MNO Key Establishment

Alice establishes a secure channel with nearest $\mathcal{N}$.

- Diffie-Hellman key exchange.
- Anonymous by use of pseudonym ps_A.

How does $\mathcal{N}$ know that user ps_A is a subscriber?

1. Alice (user ps_A) identifies herself to $\mathcal{SP}_A$ using token

$$\mathcal{T}_A = Enc\{Alice||smth\}_{\mathcal{K}_{\mathcal{SP}_A}}.$$

2. $\mathcal{SP}_A$ confirms to $\mathcal{N}$ that user ps_A is subscribed.

– $\mathcal{N}$ only learns that a user ps_A at location loc_A is a subscriber of $\mathcal{SP}_A$.
– $\mathcal{SP}_A$ only learns that subscriber Alice is connecting to $\mathcal{N}$ from somewhere.

User-MNO Key Establishment

Alice establishes a secure channel with nearest $\mathcal{N}$.

- Diffie-Hellman key exchange.
- Anonymous by use of pseudonym ps_A.

How does $\mathcal{N}$ know that user ps_A is a subscriber?

1. Alice (user ps_A) identifies herself to $\mathcal{SP}_A$ using token

$$\mathcal{T}_A = Enc\{Alice||smth\}_{\mathcal{K}_{\mathcal{SP}_A}}.$$

2. $\mathcal{SP}_A$ confirms to $\mathcal{N}$ that user ps_A is subscribed.

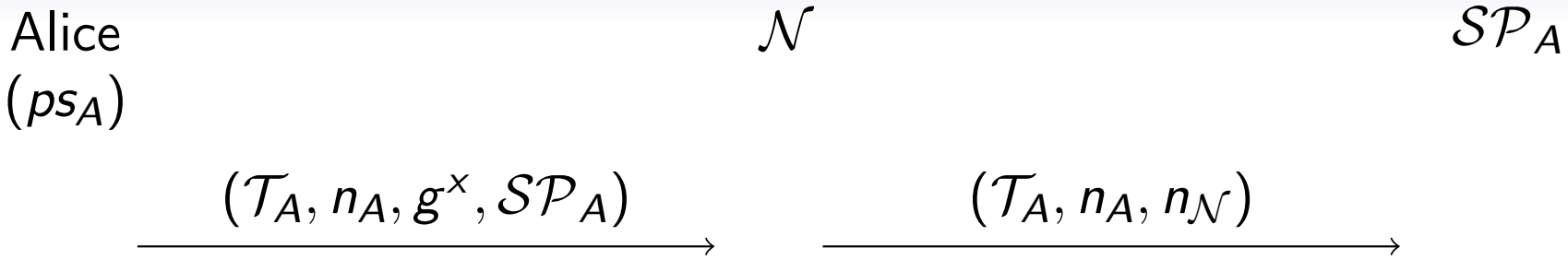
– $\mathcal{N}$ only learns that a user ps_A at location loc_A is a subscriber of $\mathcal{SP}_A$.
– $\mathcal{SP}_A$ only learns that subscriber Alice is connecting to $\mathcal{N}$ from somewhere.
$\mathcal{N}$–$\mathcal{SP}_A$ collusion leaks all!

User-MNO Key Establishment - The Protocol

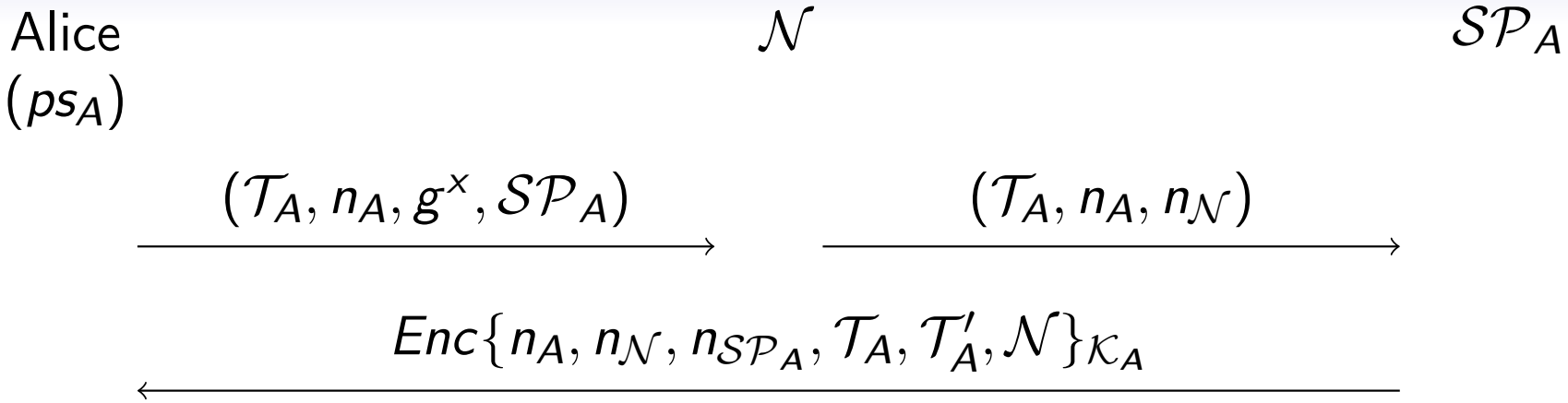
Alice (ps_A) $\mathcal{N}$ $\mathcal{SP}_A$

$$\xrightarrow{(\mathcal{T}_A, n_A, g^x, \mathcal{SP}_A)}$$

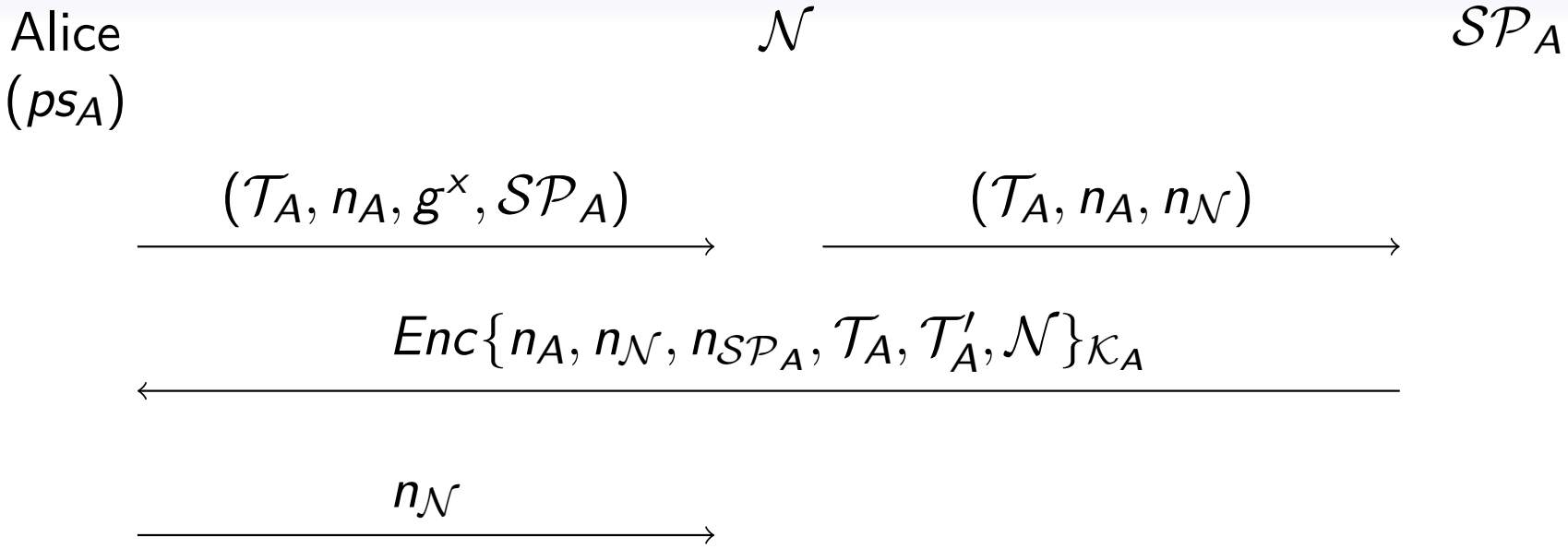
User-MNO Key Establishment - The Protocol



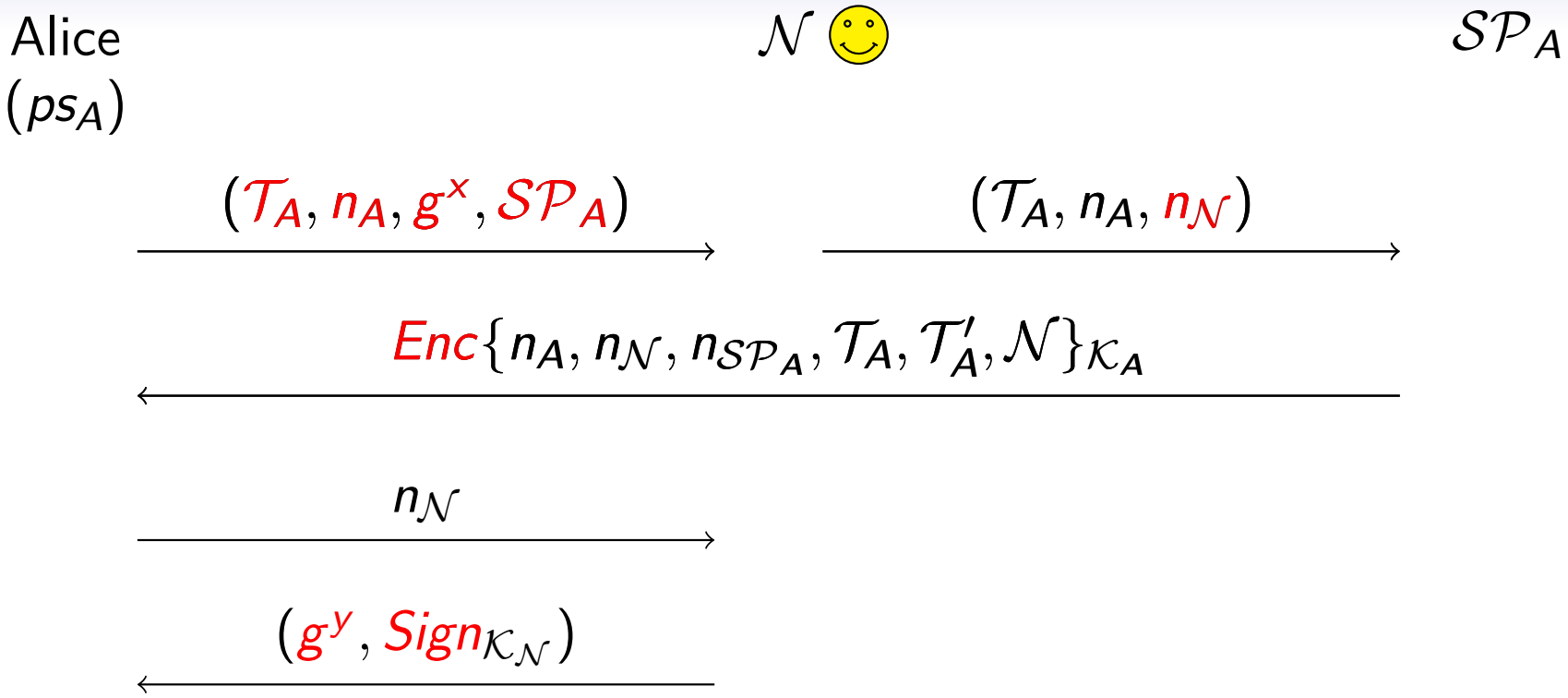
User-MNO Key Establishment - The Protocol



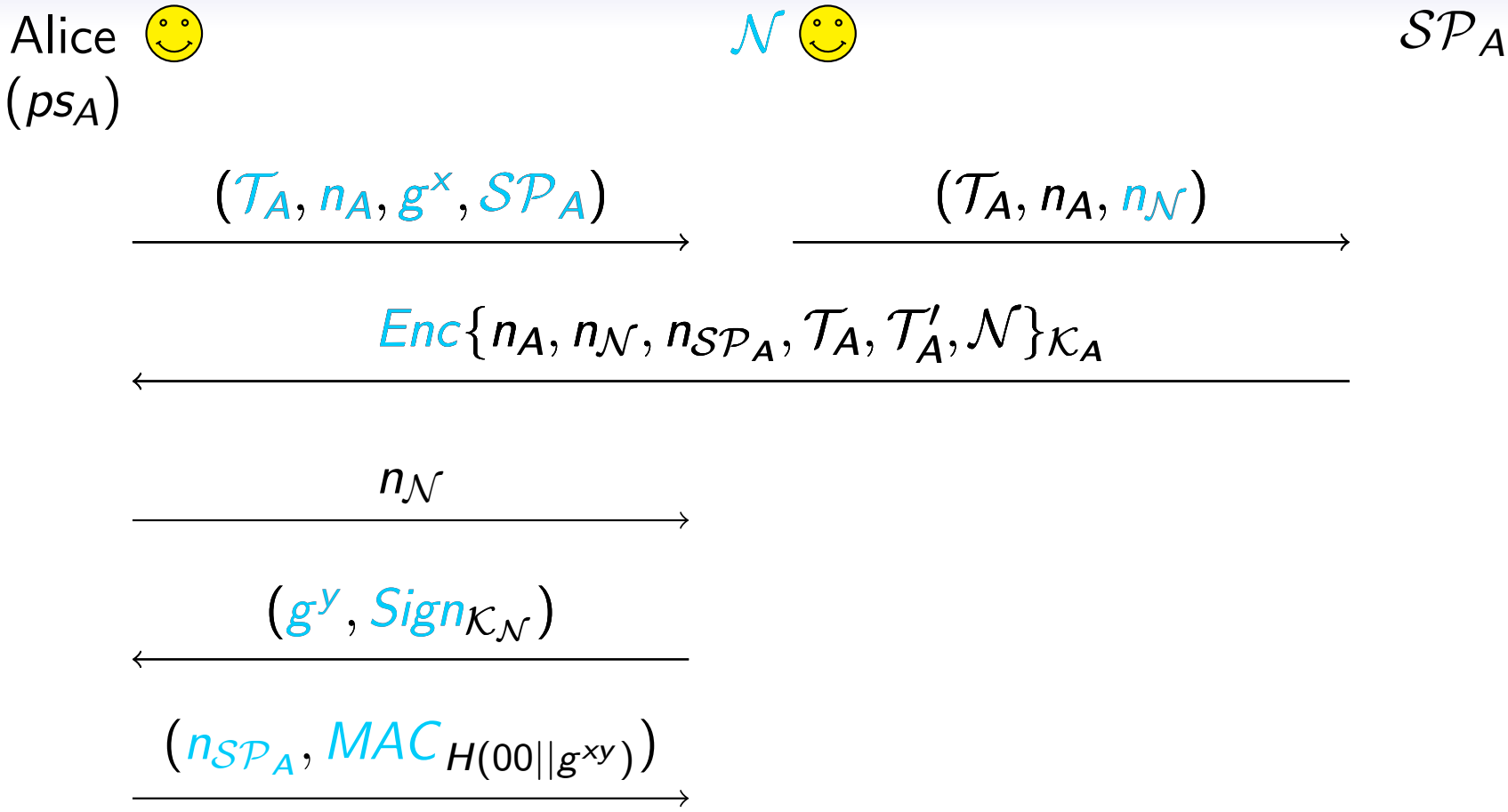
User-MNO Key Establishment - The Protocol



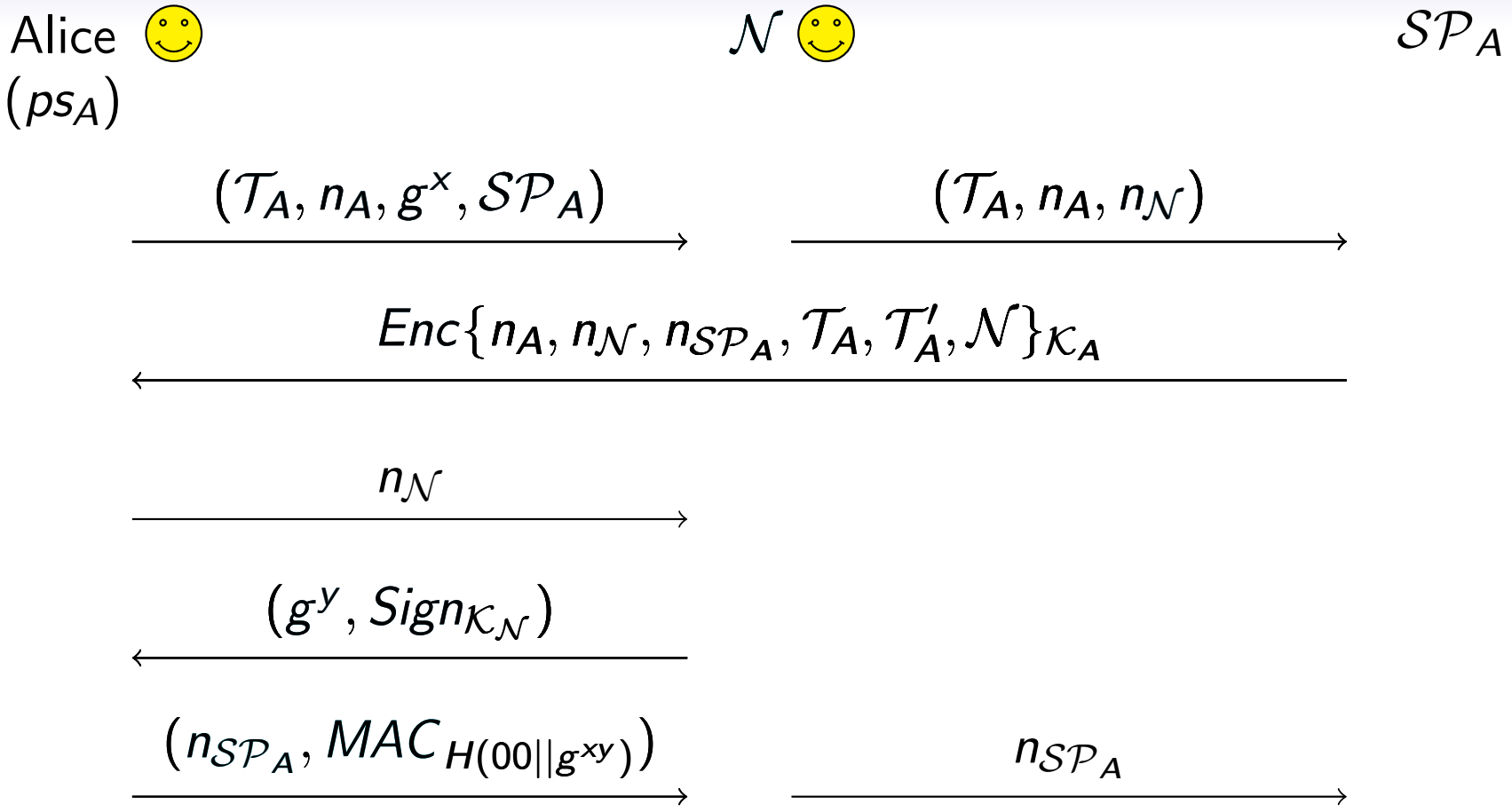
User-MNO Key Establishment - The Protocol



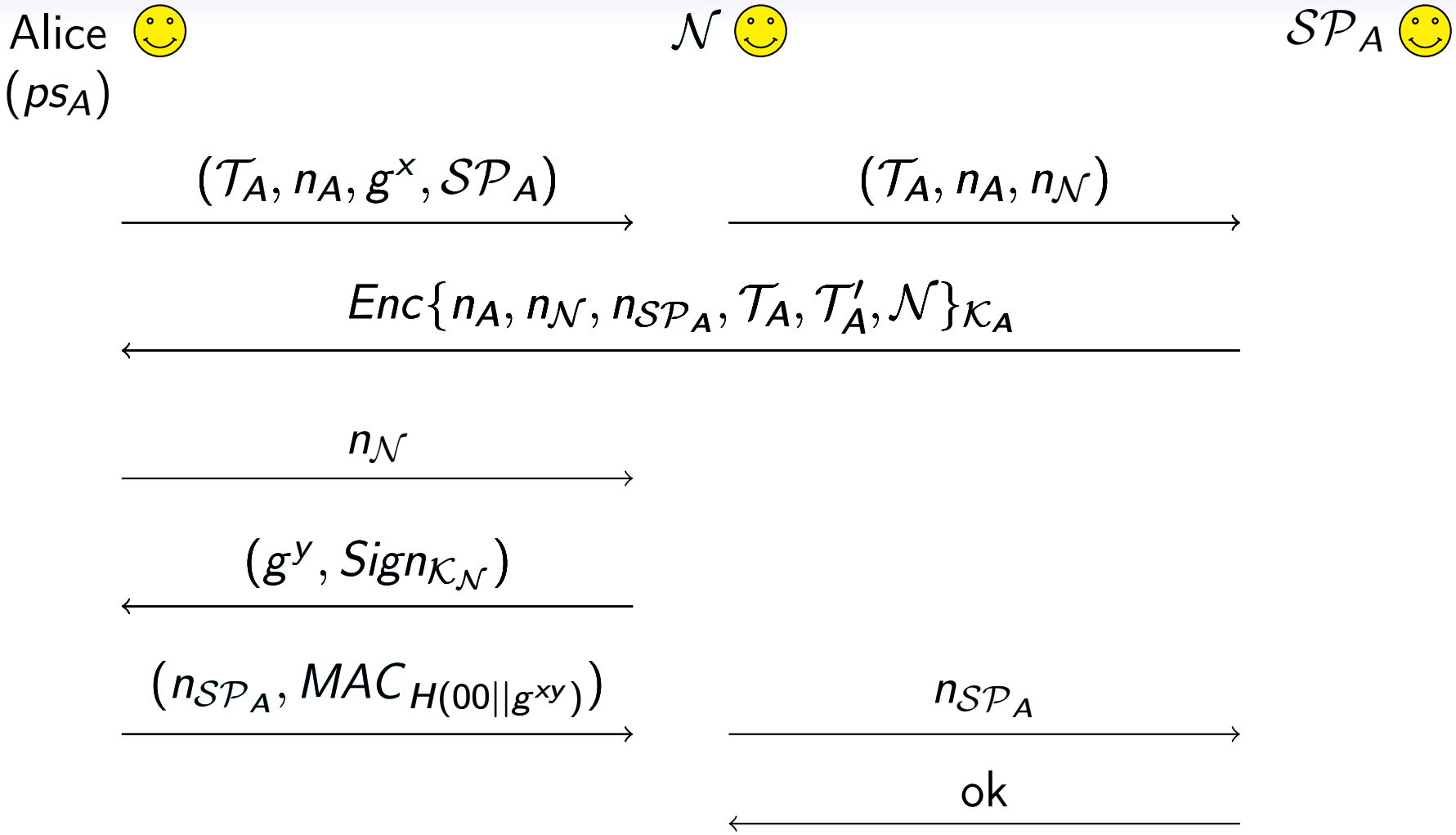
User-MNO Key Establishment - The Protocol



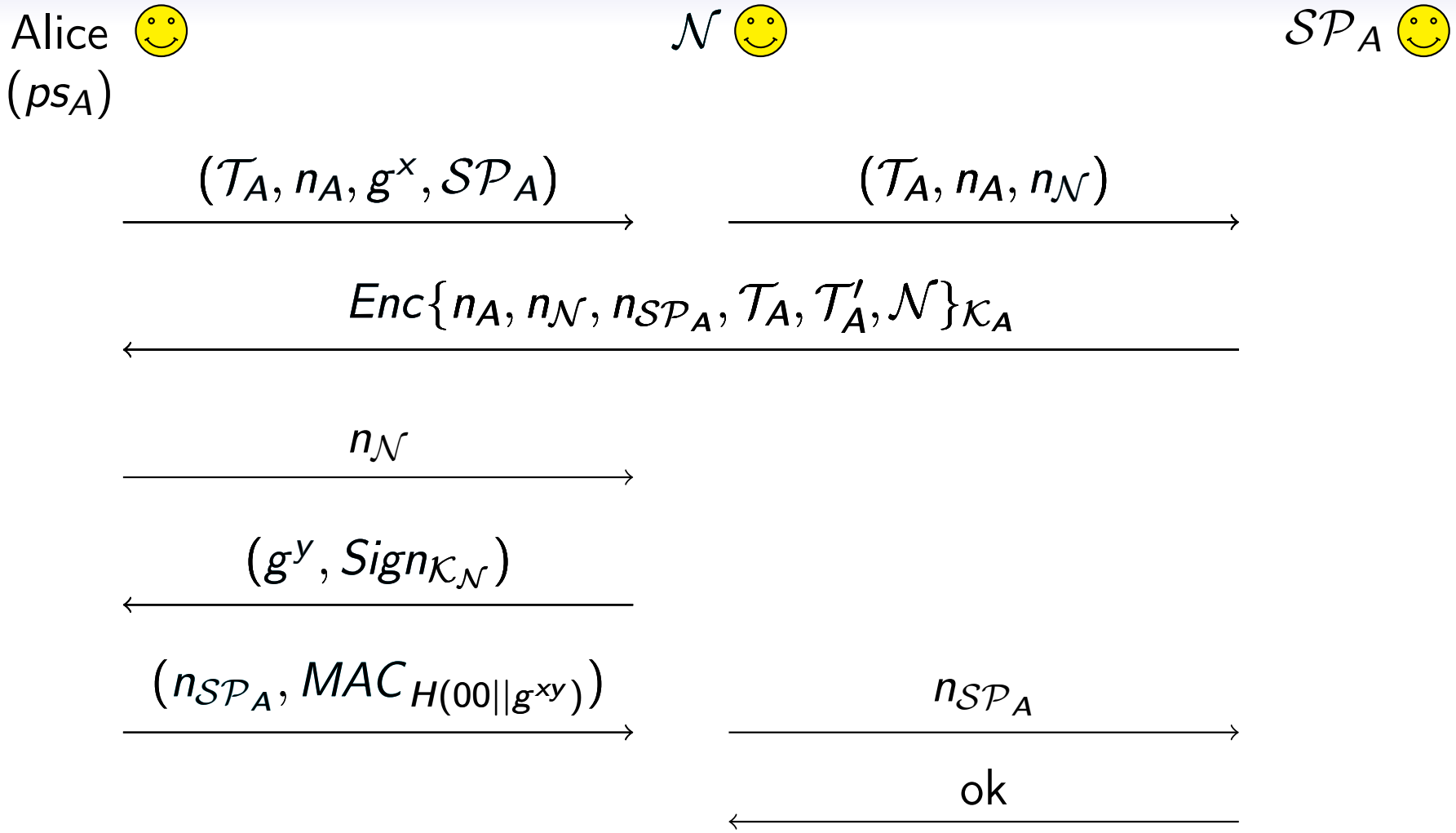
User-MNO Key Establishment - The Protocol



User-MNO Key Establishment - The Protocol



User-MNO Key Establishment - The Protocol



Shared: keys $H(01||g^{xy}), H(10||g^{xy})$, TMSI $H(11||g^{xy})$

Traceability Issues

Alice uses token $\mathcal{T}_A$ to verify that she is a subscriber.

- To avoid tracing, $\mathcal{SP}_A$ sends her a new token $\mathcal{T}_A$'.
- Still, traceable if denial of service before she receives $\mathcal{T}_A$'.
  - Only if she moves before connecting.
- Unconditional untraceability alternative: Public Key Crypto.
  - Too expensive to verify valid tokens - Denial of service attack!

Authenticated & Encrypted Radio Link

- Using the established keys and TMSI Alice secures the radio link with $\mathcal{N}$.
- $\mathcal{N}$ sends pseudonyms to Alice for communication with others.
- Alice can have persistent connection with content service providers.
  - Initial authentication with PKC (no DoS attacks as users are tied to TMSI via pseudonym).
  - Stay connected using tokens (if new token denied, go PKC again).
  - Protection against traffic analysis.
- Can contact Bob by requesting his pseudonym from his Telephony (content) Provider.
  - Again, initially PKC and then tokens.
  - No one knows who is calling who.
  - Can encrypt their communication using a symmetric key.

Legal Aspects

What about e.g. EU's Data Retention Directive?

- Judicial MNO–SP collaboration can reveal necessary info.
- Stored info is split and therefore leaks less about users.

Conclusions

- Don't expect implementation - mainly make a point.
- Designed to be Universally Composable Secure
  - We provide ideal functionalities for everything.
  - Proofs are quite long and complex (as the case usually is).

Thank You!