Intrusion Detection and User Privacy - A Natural Contradiction?

Roland Büschkes, Dogan Kesdogan
Aachen University of Technology - Department of Computer Science
D-52056 Aachen, Germany
roland@i4.informatik.rwth-aachen.de

The Task

User demands:
- privacy

IDS demands:
- monitor the network
- detect anomalies
- detect misuse
- identify attackers

Contradiction?

Our approach: Design ***multilateral secure*** IDS by using ***pseudonyms*** to protect the user's privacy.

The Questions

1. **Where** to introduce the pseudonym?

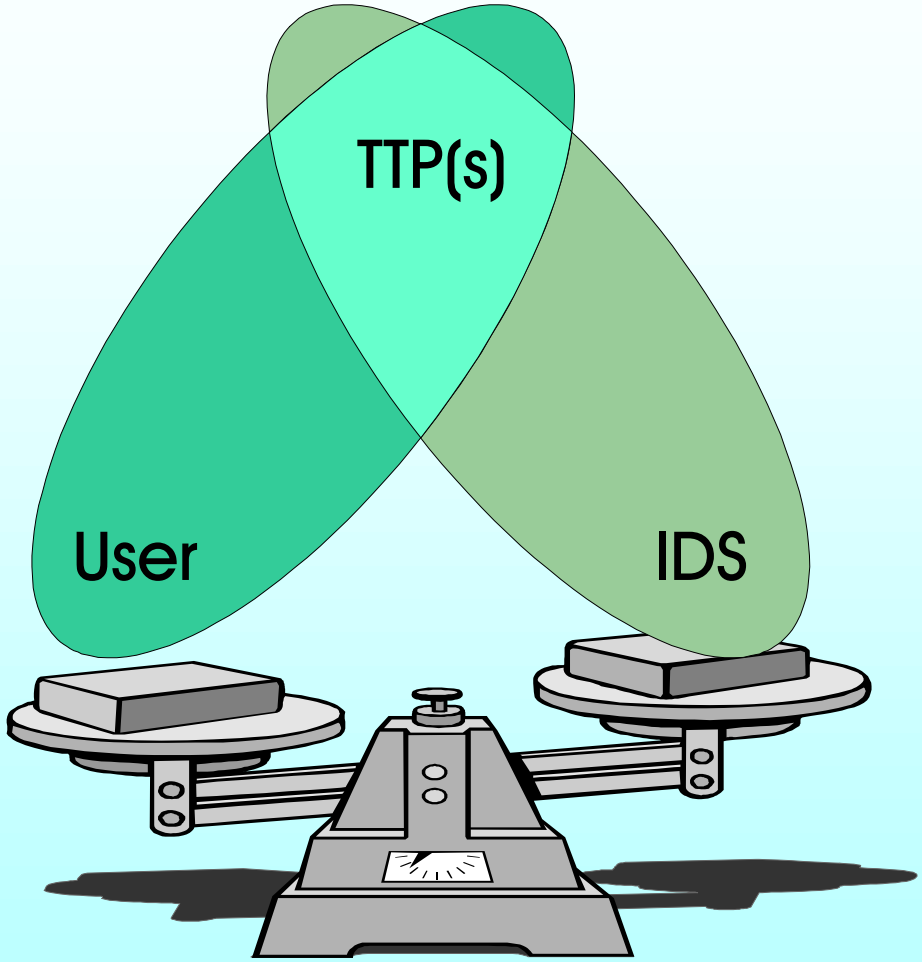
2. **When** to introduce the pseudonym for a user?

3. **How** to generate the pseudonym?

4. **How** to reveal the pseudonym in case of an intrusion?

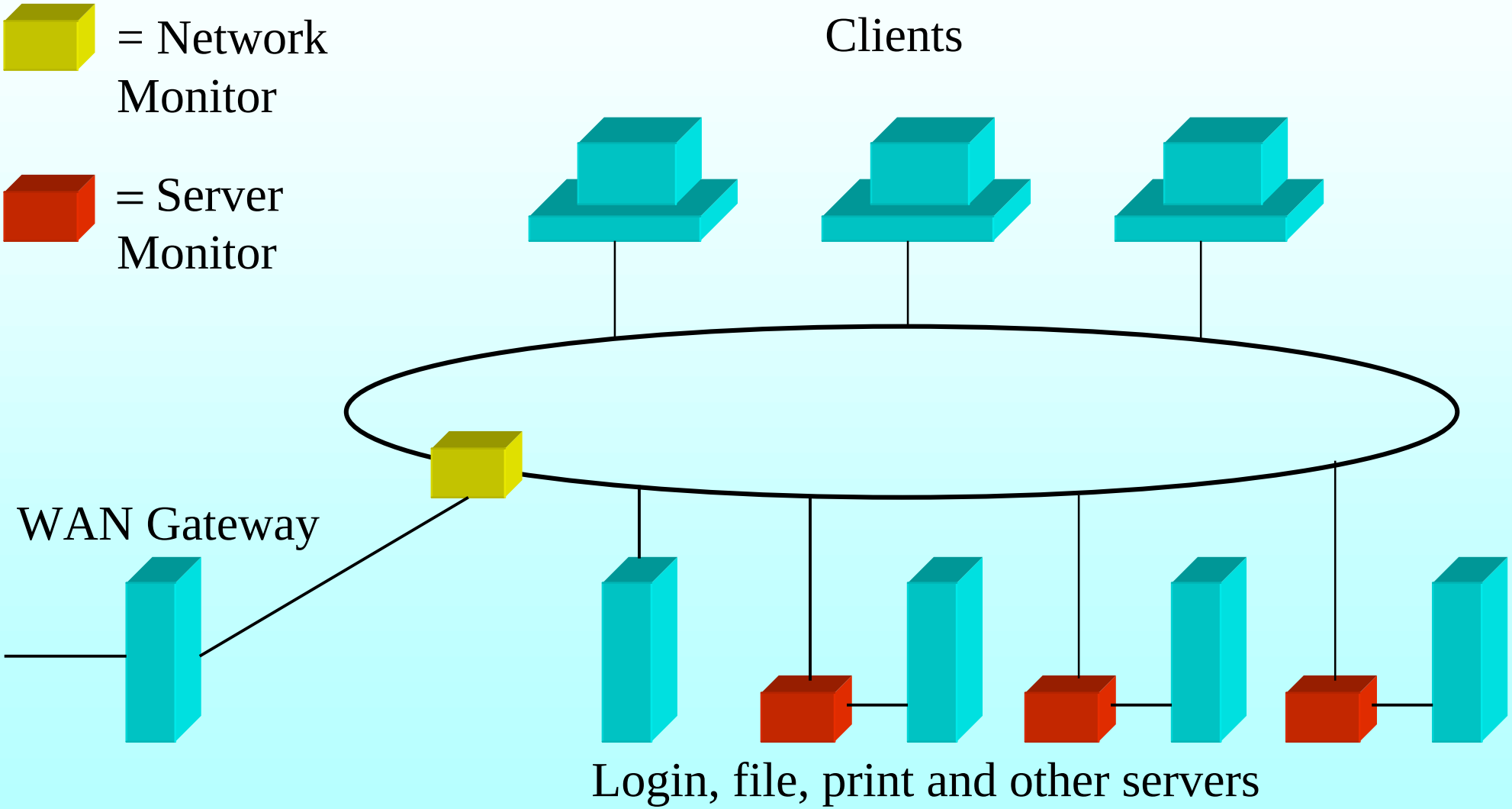
5. **What** additional data must be treated in a special way in order to prevent unwanted revelation of a pseudonym?

Where?



Where? At a *Trusted Third Party* (TTP)!

When?



When? At login time!

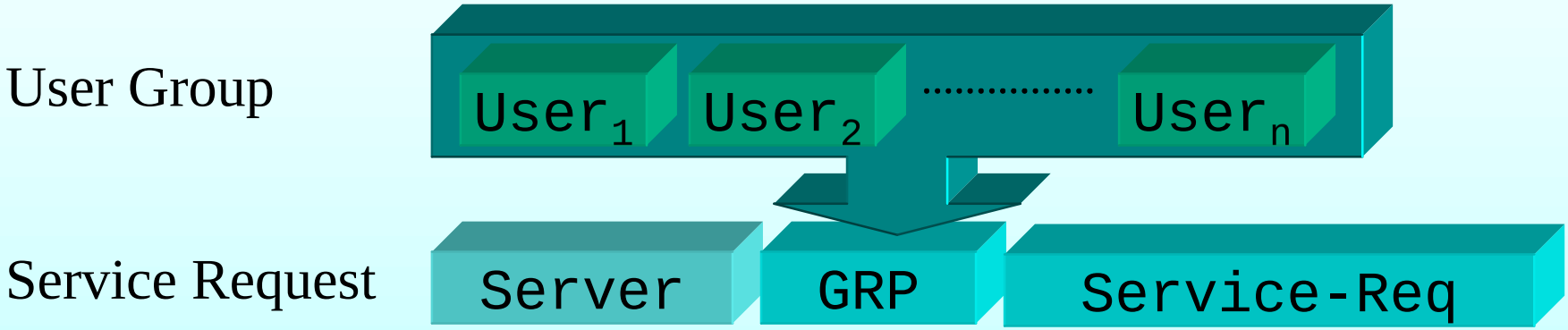
How? - Pseudonym Techniques

1. Quality criteria
   - time of deployment
   - stability concerning re-identification
   - cardinality of the anonymity set
   - possibility to relate single transactions of a user to each other
   - possible identification of users through a single data item in log files or transactions
   - frequency of pseudonym change

2. Techniques
   - self generated pseudonyms
   - reference pseudonyms
   - one-way pseudonyms

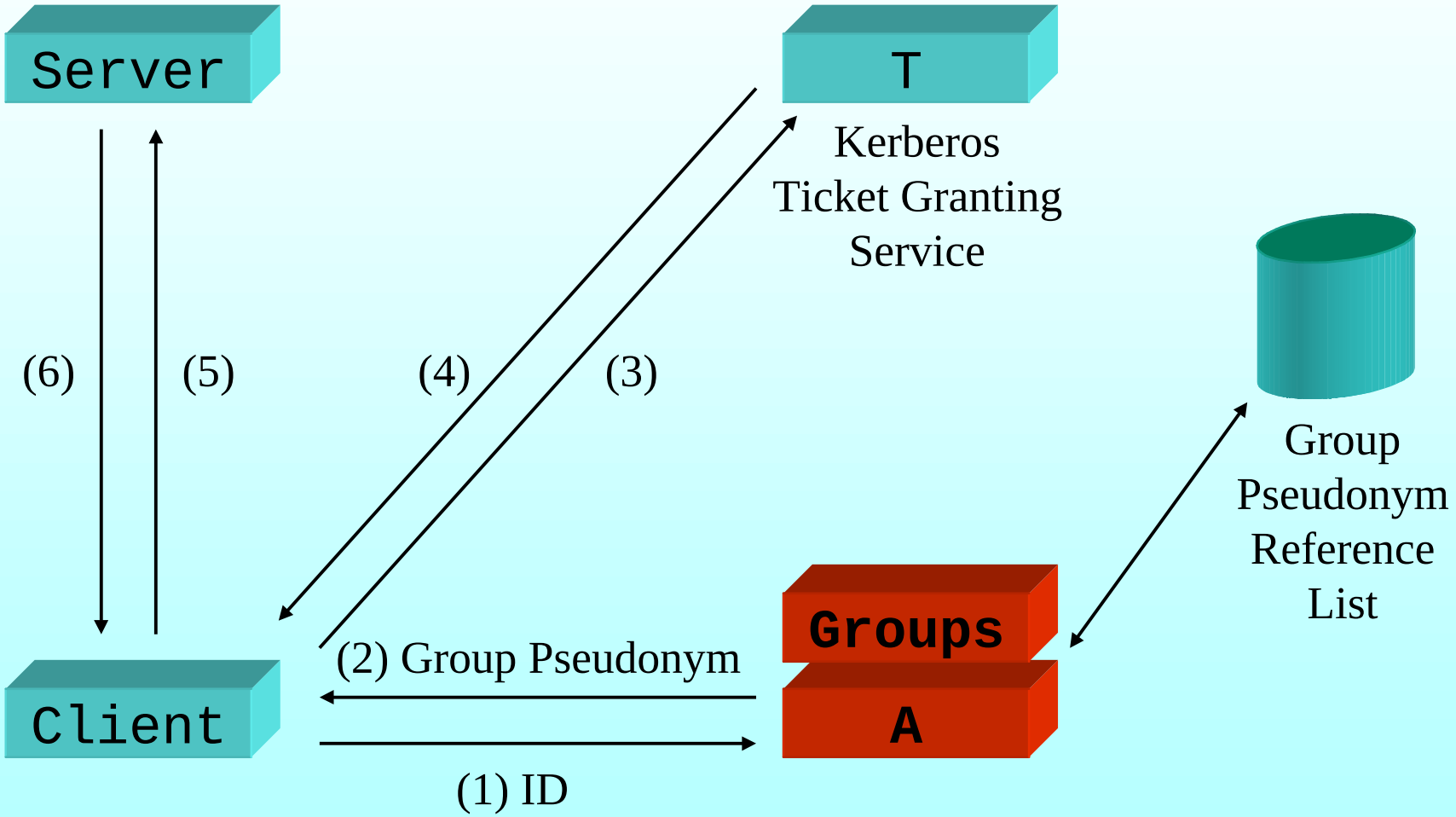
How? - Group Reference Pseudonyms (GRPs)

A GRP contains information about the group to which a user belongs:

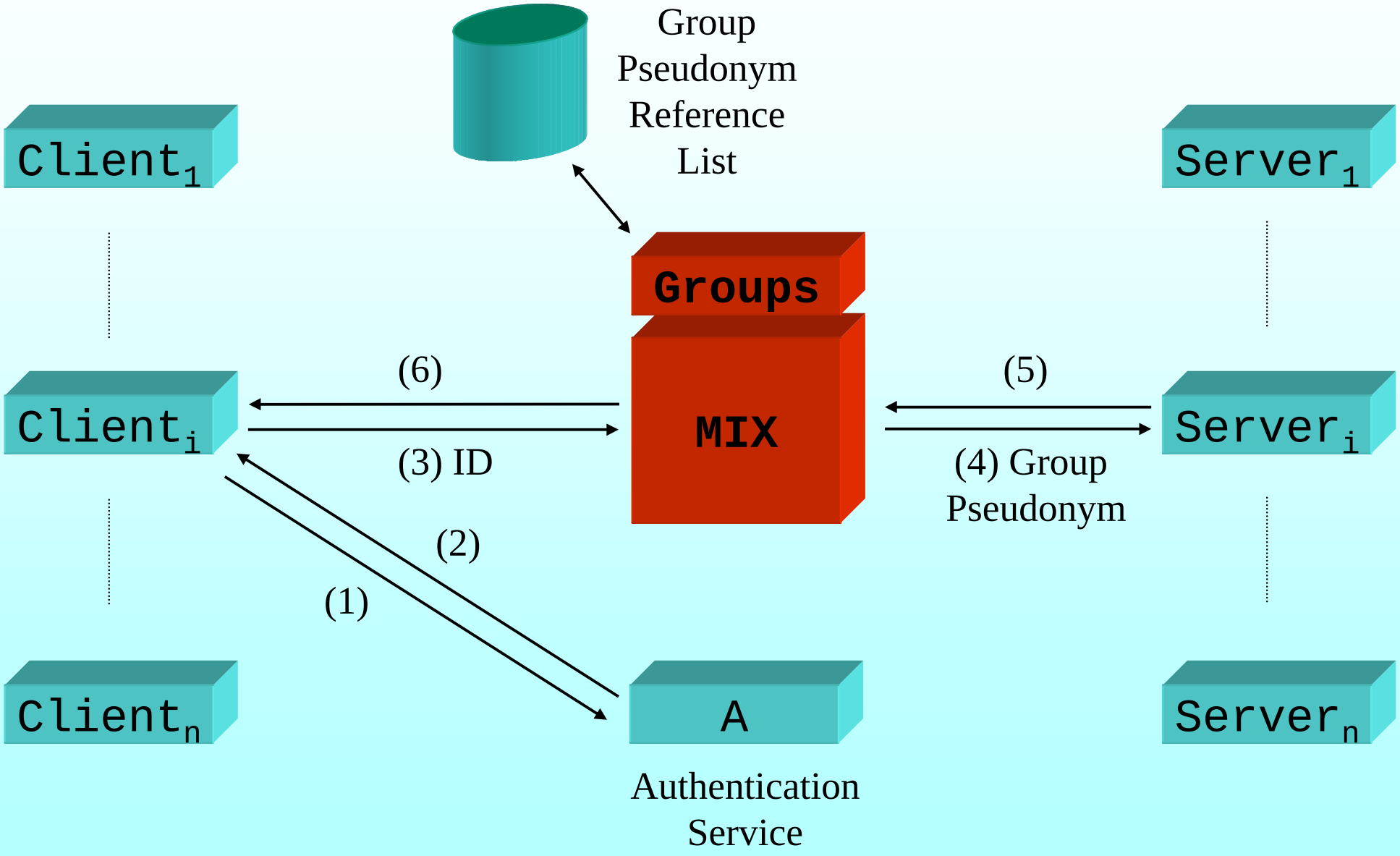


- created by TTP(s)
- defines anonymity set of a user
- base for verification of a user's access rights
- base for profiling through an anomaly detection component
- base for misuse detection

Solution 1 - Ticket Based



Solution 2 - MIX Based



IDS and GRPs

1. Anomaly Detection
   - natural embedding of users into groups
   - single user cannot fool the anomaly detection component by slowly modifying his standard behavior
   - attack only possible if the majority of a group cooperates
   - individual profiling possible, although dependent on validity of GRP

2. Misuse Detection
   - misuse detection can operate on individual groups
   - identifies group as origin of an attack
   - attacker can generally always change his identity and current location during an attack, so no expected additional profit from periodical change of pseudonyms

Conclusions & Future Works

1. Conclusions
   - future ID systems must be embedded in the general network (network management) and operating system environments
   - cooperation with general authentication and access control mechanisms enables the design of multilateral secure IDS
   - proposed solutions do not easily integrate with legacy systems

2. Future works
   - validation of technical feasibility from the viewpoint of operating system
   - validation of technical feasibility from the viewpoint of IDS
   - treatment of special data, which uniquely identifies a user
   - real-time identification of attackers
   - validity period of GRPs