Agreement for Mix Operators

Revision: Sep 24 2003

This agreement aims at ensuring resp. increasing the trustworthiness of the anonymity service. To reach this goal, the operators have to take technical and organisational precautions for a high degree of privacy and security.

The signatory operates an anonymity host (in the following: mix). Together with other mixes, it forms a sequence called mix cascade. A cascade consists of a first mix, a last mix, and optionally several middle mixes. In particular, the nature of cascades implies that each mix has at most one predecessor-mix and one successor-mix. Mixes are connected, e.g., over the Internet.

Agreement of the Operator

With respect to the operation of the mix, the operator ensures the following:

* The mix operator is bound to the provisions of law.

* Neither log files containing information of the anonymised connections nor the internal states (e.g., the permutation of messages, session keys) are created or stored.

* Exchange and forwarding of data between the mixes is restricted to what is required by the communication protocol specified in the mix software. The mix software is operated only in the way described in the specification.

* The operator prevents unauthorised access to the hardware used for the mix. Physical access to the hardware is restricted by constructional, infrastructural, and organisational means to the persons required for the operation. Using authentication mechanisms (e.g., password protection, possibly biometrics), it is ensured that authorised persons can only access data that they have right to access. Administrative network access to the mix – if necessary – makes use of encrypted connections (e.g., SSH).

* The operator ensures that staff for system administration has the skills, reliability, and time necessary for fulfilling their tasks.

* The hardware and software is configured and maintained according to the state of the art of security and privacy, i.e., in particular spying on data by third parties (e.g., by means of computer viruses, Trojan horses) is prevented. Known security leaks are fixed as soon as possible.

* The signatory agrees that the fulfilment of these agreements can be verified by an independent privacy protection control organisation at any time even without concrete reason.

Digital unterschrieben von JAP-Team
CN: CN = JAP-Team, C = DE, L = Dresden, S = Saxony, O = Dresden, University of Technology, OU = Department of Computer Science, Institute for System Architecture
Datum: 2004.03.04 11:41:50 +01'00'