

**io-port 05871313**

**Maaser, Michael**

**Design and realization of privacy guaranteeing means for context-sensitive systems.**

Cottbus: Univ. Cottbus, Fakultät für Mathematik, Naturwissenschaften und Informatik (Diss.). vi, 161 p. (2010).

Summary: Privacy issues are becoming more and more important, especially since the cyber and the real world are converging up to certain extent when using mobile devices. Means that really protect privacy are still missing. The problem is, as soon as a user provides data to a service provider the user loses control over her/his data. The simple solution is not to provide any data but then many useful services, e.g., navigation applications, cannot be used. The dissertation addresses two aspects of privacy protection. The first aspect regards not producing private information if possible. Such unnecessary information are traces of access controlled service uses. Hence, one approach in this dissertation enables  $k$ -anonymous authorization for services uses. It equips the users of the system with trusted pseudonymous certificates reflecting their respective authorizations. Analogous to anonymous e-cash, the certificates are issued by a trusted authority with knowledge of the actual authorizations of an identified user. The certificates can be verified by any service supported by the trusted authority but without knowledge of the user's identity. Not even the issuing authority is able to reveal the users identity from the pseudonym of a certificate. Hence, service usage cannot be tracked, neither by the service nor by the authority. This protects the privacy of service usage behavior of users. The second aspect of privacy protection is to remain in control over private data released to others. Temporary release of private data is essential to context-sensitive services, which rely on these context data to provide or improve added value. Therefore, the dissertation designs a Privacy Guaranteeing Execution Container (PGEC), which enables applications to access private user data and guarantees that the user data is deleted as soon as the service or application is finished. Basically, the concept is that the application obtains access to the user data in a specially protected and certified environment, the PGEC. The PGEC also restricts the communication between the application and the service provider to what is explicitly allowed by the service user. In addition to those means, the PGEC also implements countermeasures against malicious attacks such as modified host systems and covert channel attacks, which might be misusing CPU load to signal data out of the PGEC. Thus, the PGEC guarantees a "one time use" of the provided private data.

<http://opus.kobv.de/btu/volltexte/2010/1959/>