Authenticity and Provability - a Formal Framework *

Sigrid Gürgens, Peter Ochsenschläger, and Carsten Rudolph

Fraunhofer – Institute for Secure Telecooperation SIT
Rheinstrasse 75, D-64295 Darmstadt, Germany
{guergens,ochsenschlaeger,rudolphc}@sit.fraunhofer.de

Abstract. This paper presents a new formalisation of authenticity and proof of authenticity. These security properties constitute essential requirements for secure electronic commerce and other types of binding telecooperation. Based on the notions of formal language theory, authenticity and proof of authenticity are defined relative to the agents' knowledge about the system. Abstraction by language homomorphisms satisfying particular properties preserves the respective security properties from a higher to a lower level of abstraction. Thus, the new formalisation is suitable for a top-down security engineering method. The approach is demonstrated by a typical e-commerce example, a price-offer transaction. We present specifications of this example on two different abstraction levels. On the lower of these abstraction levels, Asynchronous Product Automata (APA) are used to model cryptographic protocols, and properties of cryptographic algorithms are formally described by abstract secure channels.

* Full paper to appear in *Proceedings of INFRASEC 2002*,