# Caught in the Maze of Security Standards

Jan Meier and Dieter Gollmann

Hamburg University of Technology
Harburger Schloßstr. 20 (HS20), 1st floor, room 123
Hamburg, 21079 Germany
diego@tu-harburg.de

**Abstract.** We analyze the interactions between several national and international standards for smart card based applications, noting deficiencies in those standards, or at least deficiencies in the documentation of their dependencies. We show that currently smart card protocols are specified in a way that standard compliant protocol implementations may be vulnerable to attacks. We further show that attempts to upgrade security by increasing the length of cryptographic keys may fail when message formats in protocols are not re-examined at the same time[1].

[1] A full version of this paper appears in LNCS 6345 — ESORICS 2010, pages 441–454.

B. Christianson and J. Malcolm (Eds.): Security Protocols 2010, LNCS 7061, p. 3, 2014.