Cryptology ePrint Archive: Report 2011/058

Supplemental Access Control (PACE v2): Security Analysis of PACE Integrated Mapping

Jean-S\'ebastien Coron and Aline Gouget and Thomas Icart and Pascal Paillier

Abstract: We describe and analyze the password-based key establishment protocol PACE v2 Integrated Mapping (IM), an evolution of PACE v1 jointly proposed by Gemalto and Sagem S\'ecurit\'e. PACE v2 IM enjoys the following properties: patent-freeness3 (to the best of current knowledge in the field); full resistance to dictionary attacks, secrecy and forward secrecy in the security model agreed upon by the CEN TC224 WG16 group; optimal performances.

The PACE v2 IM protocol is intended to provide an alternative to the German PACE v1 protocol, which is also the German PACE v2 Generic Mapping (GM) protocol, proposed by the German Federal Office for Information Security (BSI). In this document, we provide a description of PACE v2 IM, a description of the security requirements one expects from a password-based key establishment protocol in order to support secure applications, and a security proof of PACE v2 IM in the so-called Bellare-Pointcheval-Rogaway (BPR) security model.

Category / Keywords: cryptographic protocols / public-key cryptography, password-based key exchange

Publication Info: This paper has not been submitted yet in a conference/workshop

Date: received 1 Feb 2011, last revised 7 Jun 2011

Contact author: aline gouget at gemalto com