

IBM Research Division, Zurich Research Laboratory
Säumerstrasse 4
CH-8803 Rüschlikon
Switzerland

March 3, 2000

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e. V.
10772 Berlin
Germany

To the Secretariat:

This letter is to inform ISO SC27 of IBM's patent licensing practices as related to standardization activities. It is the belief of IBM that the IBM patent application listed in Attachment A is relevant to the "ACE Encrypt" algorithm submitted in response to the ISO SC27 New Work Item Proposal on "Encryption algorithms."

In the event that this algorithm is adopted as a standard, and the standard can not be practiced without the use of the aforementioned patent, IBM agrees upon request to grant a non-exclusive license under this patent on a nondiscriminatory basis and on reasonable terms and conditions including its then current royalty rates and provided a similar grant under licensee's patents within the scope of the license granted to licensee is made available upon request to IBM. Should other IBM patents be required to implement the standard, they will be licensed under the same nondiscriminatory, reasonable terms and conditions.

Any requests for license information may be directed to:

Gerald Rosenthal
Director of Licensing
International Business Machines Corporation
North Castle Drive
Armonk, NY 10504
USA

e-mail: jerry@us.ibm.com
tel: +1 (914) 765-4260
fax: +1 (914) 765-4390

IBM is pleased to make this offer in support of the standardization activities in

ISO SC27. If you have any questions, please let me know.

Sincerely,

Victor Shoup, for IBM Corporation

Attachment A: SUBJECT PATENT APPLICATIONS

Ronald Cramer, Victor Shoup, "Practical non-malleable public-key cryptosystem," Filed February 16, 1999.