Network Working Group J. Schaad
Request for Comments: 4055 Soaring Hawk Consulting
Updates: 3279 B. Kaliski
Category: Standards Track RSA Laboratories
R. Housley
Vigil Security
June 2005

Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Status of This Memo

Copyright Notice

Abstract

This document supplements RFC 3279. It describes the conventions for using the RSA Probabilistic Signature Scheme (RSASSA-PSS) signature algorithm, the RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) key transport algorithm and additional one-way hash functions with the Public-Key Cryptography Standards (PKCS) #1 version 1.5 signature algorithm in the Internet X.509 Public Key Infrastructure (PKI). Encoding formats, algorithm identifiers, and parameter formats are specified.