               The NSA (No Secrecy Afforded) Certificate Extension

Abstract

   This document defines the NSA (No Secrecy Afforded) certificate
   extension appropriate for use in certain PKIX (X.509 Pubic Key
   Certificates) digital certificates. Historically, clients and
   servers strived to maintain the privacy of their keys; however, the
   secrecy of their private keys cannot always be maintained. In
   certain circumstances, a client or a server might feel that they will
   be compelled in the future to share their keys with a third party.
   Some clients and servers also have been compelled to share their keys
   and wish to indicate to relying parties upon certificate renewal that
   their keys have in fact been shared with a third party.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This is a contribution to the RFC Series, independently of any other
   RFC stream. The RFC Editor has chosen to publish this document at
   its discretion and makes no statement about its value for
   implementation or deployment. Documents approved for publication by
   the RFC Editor are not a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7169.

1. Introduction

   Insecurity abounds when clients and servers are unable to keep their
   private keys private. Situations exist nonetheless where client and
   servers have shared their private keys with a third party. An
   example of over-sharing might be lawful intercept.

   Just because the private key has been shared does not mean that the
   private key holder wants to conceal the fact they have shared their
   private key with a third party. Overtly indicating that the private
   key may be or has been shared with a third party is the best way to
   indicate to relying parties that this sharing has occurred.
   Knowledge is power, after all. Extensions for certificates [RFC5280]
   offer an excellent mechanism to indicate that the entities key(s)
   have been shared, and this document specifies one such certificate
   extension for use by entities that have shared their private key: the
   NSA (No Secrecy Afforded) certificate extension.

2. The NSA Certificate Extension

   In order to allow entities that have shared their keys with a third
   party, the NSA certificate extension is defined herein. ASN.1
   [X.680] for the extension follows:

   ext-KeyUsage EXTENSION ::= { SYNTAX
        BOOLEAN   IDENTIFIED BY id-pe-nsa }

   id-pe-nsa OBJECT IDENTIFIER ::= { id-pe 23 }

   Making the boolean TRUE indicates that the key has been shared with a
   third party, and making the extension FALSE indicates that the key
   may have also been shared with a third party but the signer does not
   want to overtly indicate that the key has been shared. This
   extension is always marked critical.

3. Security Considerations

   Having to disclose keys is sometimes unavoidable. Explicitly
   indicating that the keys have been shared is one way to mitigate the
   risk that the relying party might be unaware of this over share.
   Whatever the case for having shared the keys, the certificate signer
   needs to careful consider whether to include this extension.

   Any key with this extension must be trusted with care. Lengthy
   deliberations about whether to trust the keys is necessary. Rushing
   a security analysis is never a good thing. Ultimately, the keys need
   not be trusted. Secrecy is hard.

4. Normative References

   [RFC5280]   Cooper, D., Santesson, S., Farrell, S., Boeyen, S.,
               Housley, R., and W. Polk, "Internet X.509 Public Key
               Infrastructure Certificate and Certificate Revocation List
               (CRL) Profile", RFC 5280, May 2008.

   [X.680]   ITU-T, "Information technology - Abstract Syntax Notation
               One (ASN.1): Specification of basic notation", ITU-T
               Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, 2002.

Author's Address

   Sean Turner
   IECA, Inc.
   3057 Nutley Street, Suite 106
   Fairfax, VA 22031
   USA

   EMail: turners@ieca.com
   XMPP: sean.turner@jabber.psg.com