IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)		
Title	**IEEE P802-15_TG3 NTRUEncrypt Security Suite**		
Date Submitted	[August 2, 2002]		
Source	[Daniel V. Bailey, Ari Singer, William Whyte] [NTRU] [5 Burlington Woods Burlington, MA 01803 USA]	Voice: Fax: E-mail:	[+1 781 418-2522] [+1 781 418-2532] [dbailey@ntru.com]
Re:	802.15.3 TG3 Letter Ballot Draft D10		
Abstract	[This document represents the text for the NTRUEncrypt security suite for inclusion in the 802.15.3 draft.]		
Purpose	[This document is intended to satisfy the requirements from 02/323r0 to provide an NTRUEncrypt security suite that includes a mode 2 sub-suite. This includes the text for the security suite itself along with changes that should be made to other portions of the standard if necessary.]		
Notice	This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.		
Release	The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.		

Author's note: Some changes to the main document that affect the integration of this security suite into the 802.15.3 standard are specified in the RSA Security Suite specification (02/363r0).

1. Security Suite Specifications

1.1 Security suite selections

Author's note: The OIDs and security services provided by the proposed NTRUEncrypt security suite are the same as the ones currently in the draft, so there should be no change to the text in 10.2.1 or 10.2.2 for this security suite

Author's note: The following sub-clause should replace clause 10.4 as the full text for the NTRUEncrypt 251-1 security suite.

1.2 NTRUEncrypt 251-1

The following subclauses define the security operations that are performed for the security suite NTRUEncrypt 251-1. The symmetric operations performed in this security suite are those specified in {xref 10.2.5}. The public key and authentication operations are specified in {xref 1.2.1}.

1.2.1 Public-key and authentication building blocks

The following cryptographic primitives and data elements are defined for use in all sub-suites of NTRUEncrypt 251-1.

1.2.1.1 NTRUEncrypt parameter set ees251ep1

All NTRUEncrypt objects and cryptographic operations used in this security suite shall use the parameter set ees251ep1 as specified in {xref EESS#1}. All transmitted NTRUEncrypt polynomials shall be sent in uncompressed form as specified in {xref EESS#1}.

1.2.1.2 NTRUEncrypt key pair

An NTRUEncrypt key pair consists of the private key, which is a small polynomial in the lattice and the public key, which is a large polynomial in the lattice as specified in {xref EESS#1}. All NTRUEncrypt public keys shall use the parameter set specified in {xref 10.4.1.1}.

1.2.1.3 NTRUEncrypt encryption and decryption

The NTRUEncrypt encryption algorithm used in this security suite shall be performed as specified in {xref EESS#1}.

1.2.1.4 SHA-1 cryptographic hash

The SHA-1 cryptographic hash algorithm used in this security suite shall be performed as specified in the FIPS 180-2 draft standard {xref FIP180}.

1.2.2 NTRUEncrypt raw 1 sub-suite

NTRUEncrypt raw 1 is a mode 2 sub-suite of the NTRUEncrypt 251-1 security suite. The cryptographic building blocks for the NTRUEncrypt raw 1 sub-suite are selected from the public-key cryptographic building blocks defined for the NTRUEncrypt 251-1 security suite. The OID for this sub-suite is specified in

{xref Table 79}. The following subclauses specify the public-key and authentication related objects for this sub-suite.

1.2.2.1 Public-key and authentication data formats

Table 1 specifies the length and meaning of the public-key cryptography and authentication related security suite specific data elements from Clause {xref 7}. The operations performed to obtain the variable data values are specified in 1.2.2.2.

Table 1—Public-key frame object formats

Notation	Length	Value	Description
PublicKeyObjectType	2	See {xref 7.5.2.1}	An NTRUEncrypt public key as specified in 1.2.1.2. The value is the entry for NTRUEncrypt raw 251 in table {xref 7.5.2.1}.
PublicKeyObjectLength	2	251	The length of the particular instance of the NTRUEncrypt public key.
PublicKeyObject	251	Variable	The particular instance of the NTRUEncrypt public key.
OIDLength	1	10	The length of the DER encoding of the OID ntruencrypt-raw-1 as specified in {xref Table 79}.
OID	10	OID Value	The DER encoding of the OID ecies-raw-1 as specified in {xref Table 79}.
Challenge	251	Variable	The result of the NTRUEncrypt encryption of the 21-octet challenge as specified in 1.2.1.3.
Auth response	8	Variable	The auth response consists of the encrypted integrity code that is the result of a CCM computation as specified in {xref - 10.2.4.3} with the encryption data being the empty string (NULL).
ChallengeResponse	8	Variable	The challenge response consists of the encrypted integrity code that is the result of a CCM computation as specified in {xref - 10.2.4.3} with the encryption data being the empty string (NULL).

1.2.2.2 Public key and authentication cryptographic operations

Table 2 specifies the public key cryptography and authentication related operations for the authentication protocol frames defined in Clause {xref 7}:

Table 2—Authentication related operations

Use	Operation
Verification of Public-Key	The ID and public-key received during the authentication protocol is verified by generating the SHA-1 hash of the device address concatenated with the public key of the device as specified in 1.2.1.4 and comparing it to the hash of the ID and public key stored in the MAC PIB. If the hash is not in the PIB, the public key is passed to the DME to establish trust by other means.
Challenge generation	The challenges generated during the authentication protocol are computed by performing an NTRUEncrypt encryption as specified in 1.2.1.3 on a fresh, randomly generated 21-byte challenge using the other device's public key.
Challenge decryption	The challenge decryption operation is performed using NTRUEncrypt decryption as specified in 1.2.1.3 on the received challenge.
Management key generation (for authentication protocol)	The 42-byte seed for the management key consists of the decrypted challenge from the security manager, concatenated with the decrypted challenge of the DEV. The management key for the relationship is generated from the seed by first calculation the SHA-1 hash as specified in 1.2.1.4 on the 42-byte seed and then setting the key to be the truncation of the result to the first 128-bits.
Challenge response generation	The challenge response is generated by computing the encrypted integrity code with the payload protection key using CCM authentication and encryption as specified in {xref - 10.2.4.3} with the entire authentication protocol up to that point as the authentication data input *a* and the empty string as the plaintext input *m* for encryption.
Authentication response generation	The authentication response is generated by computing the encrypted integrity code with the payload protection key using CCM authentication and encryption as specified in {xref - 10.2.4.3} with the entire authentication protocol up to that point as the authentication data input *a* and the empty string as the plaintext input *m* for encryption.