IEEE P802.15
Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)
Title	**IEEE P802-15_TG3 RSA Security Suite Proposal**
Date Submitted	[May 13, 2002]
Source	[Daniel V. Bailey, Ari Singer, William Whyte] [NTRU] [5 Burlington Woods Burlington, MA 01803 USA] Voice: [+1 781 418-2522] Fax: [+1 781 418-2532] E-mail: [dbailey@ntru.com]
Re:	802.15.3 TG3 Letter Ballot Draft D0A,
Abstract	[This document is offered as a submission for an alternate security suite implementing techniques from the RSA family of algorithms.]
Purpose	[This document is intended as a proposal for an RSA security suite to be included in the 802.15.3 draft standard. The goal of this submission is to provide an alternative to the security suites currently specified in the draft using the RSA algorithm.]
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.

1. Security Suite Specifications

1.1 Security suite selections

1.1.1 OID selections

Author's note: The following entry should be added to the security suites table in clause 10.2.1.

Table 1—Security suites

Security Suite Name	OID Name	OID Number	DER Encoding
RSA-OAEP 1024-1	rsa-oaep-sec-suite-1	id-802-15-3-security-suites 3	0x060728C4620F030103

Author's note: The following entry should be added to the OIDs for sub-suites table in clause 10.2.1.

Table 2—OIDs for sub-suites

Sub-suite Name	OID Name	OID Number	DER Encoding
RSA-OAEP Raw 1	rsa-oaep-raw-1	rsa-oaep-sec-suite-1 1	0x060828C4620F03010301
RSA-OAEP X509 1	rsa-oaep-x509-1	rsa-oaep-sec-suite-1 2	0x060828C4620F03010302

Author's note: The security services provided by the proposed RSA security suite is the same as the other proposals, so there should be no change to the text in 10.2.2

Author's note: The following sub-clause should be added to clause 10 as the full text for the RSA-OAEP 1024-1 security suite.

1.2 RSA-OAEP 1024-1 security suite

The following sub-clauses define the security operations that are performed for the security suite RSA-OAEP 1024-1. The symmetric operations performed in this security suite are those specified in sub-clause {xref 10.2.4}. The public key and authentication operations are specified in the following sub-clause {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 RSA-OAEP 1024-1.

1.2.1.1 RSA domain parameters

All RSA objects and cryptographic operations used in this security suite shall use the following parameters as described in {xref PKCS#1}. The RSA modulus is defined to be an integer of length k = 128 octets, or 1024-bits.

1.2.1.2 RSA key pair

An RSA public key in this security suite consists of the modulus *n* and the public exponent *e* . The modulus *n* shall be an integer of length *k* as specified in sub-clause {xref 1.2.1.1}. The public exponent *e* shall be an integer less than 2^{32}. The private key is information that allows its owner to find e^{th} roots mod *n*. The private key may take one of a number of forms; see {xref PKCS#1} for more details. The choice of representation of the private key does not affect interoperability and is out of scope.

Author's note: Common values for the RSA public exponent are $2^{16} + 1$ and 3. The maximum value for the public exponent is selected to allow all public exponents to be represented in 4 bytes.

1.2.1.3 RSA raw public key

An RSA raw public key in this security suite is defined to be the octet string consisting of the modulus *n*, converted to an octet string using I2OSP as specified in {xref PKCS#1} parameterized with output length *k* as defined in subclause {xref 1.2.1.1}, concatenated with the public exponent *e*, converted to an octet string using I2OSP as specified in {xref PKCS#1} parameterized with output length 4.

1.2.1.4 RSA-OAEP encryption and decryption

The RSA-OAEP encryption scheme in this security suite shall be performed as specified in {xref PKCS#1}. The encryption and decryption operations shall be parameterized by the following inputs. The label *L* shall be the empty string. The hash function Hash shall be SHA-1 as specified in sub-clause {xref 1.2.1.5}. The mask generation function MGF shall be MGF1 as specified in sub-clause {xref 1.2.1.6}. The output of the encryption operation shall be an octet string of length *k* as defined in sub-clause {xref 1.2.1.1} and as described in {xref PKCS#1}.

1.2.1.5 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].

1.2.1.6 MGF1 cryptographic mask generation function

The MGF1 cryptographic mask generation function used in this security suite shall be performed as specified in Annex B.2.1 of {xref PKCS#1}. This operation shall be parameterized by the hash function SHA-1 as specified in sub-clause {xref 1.2.1.5}

1.2.1.7 RSA X.509 certificate

The X.509 digital certificate format and verification used in this security suite shall be as specified by the PKIX RFC 3280 {xref PKIX}. These certificates shall contain an RSA public key as specified in clause {xref 1.2.1.2}. These certificates shall be signed using the RSASSA-PKCS1-v1_5 signature algorithm as specified in clause {xref 1.2.1.8}. The ASN.1 encoding for the public key and signature shall be as specified in {xref PKCS#1}. The subject field of the X.509 certificate shall be NULL and the subjectAltName shall consist of the PrintableString encoding of the hexadecimal representation of the 48-bit IEEE MAC address of the device.

1.2.1.8 RSASSA-PKCS1-v1_5 digital signatures and verification

The RSASSA-PKCS1-v1_5 digital signature algorithm used in this security suite shall be performed as specified in {xref PKCS#1}. The RSASSA-PKCS1-v1_5 signature algorithm operations shall be performed using the domain parameters specified in clause {xref 1.2.1.1} and RSA key pairs as specified in clause {xref 1.2.1.2}. The RSASSA-PKCS1-v1_5 signature and verification algorithms shall be parameterized by the following input. The hash function Hash shall be SHA-1 as specified in sub-clause {xref 1.2.1.5}.

1.2.2 RSA-OAEP Raw 1 sub-suite

RSA-OAEP Raw 1 is a mode 2 sub-suite of the RSA-OAEP 1024-1 security suite. The cryptographic building blocks for the RSA-OAEP Raw 1 sub-suite are selected from the public-key cryptographic building blocks defined for the RSA-OAEP 1024-1 security suite. The OID for this sub-suite is specified in {xref Table 2}. The following sub-clauses specify the public-key and authentication related objects for this sub-suite.

1.2.2.1 Public-key and authentication data formats

The following table specifies the length and meaning of the public-key cryptography and authentication related security suite specific data elements from clause 7{xref}. The operations performed to obtain the variable data values are specified in a separate sub-clause.

Table 3—Public-key frame object formats

Notation	Length	Value	Description
PublicKeyObjectType	2	See 7.4.1.1{xref}	An RSA raw public key as specified in clause {xref 1.2.1.3}. The value is the entry for RSA-OAEP Raw 1024 in table 7.4.1.1{xref}.
PublicKeyObjectLength	2	132	The length of the RSA raw public key.
PublicKeyObject	132	Variable	The particular instance of the RSA raw public key.
OIDLength	1	10	The length of the DER encoding of the OID rsa-oaep-raw-1 as specified in {xref Table 2}.
OID	10	OID Value	The DER encoding of the OID rsa-oaep-raw-1 as specified in {xref Table 2}.
ChallengeType	2	See table 7.4.1.3{xref}	The challenge type is an RSA-OAEP encryption of a 16-octet challenge as specified in clause {xref 1.2.1.4.}. The value is the entry for RSA-OAEP 1024 encrypted seed in 7.4.1.3{xref}.
ChallengeLength	2	128	The length of an RSA-OAEP encryption of a 16-octet challenge as specified in clause {xref 1.2.1.4.}.
Challenge	128	Variable	The result of the RSA-OAEP encryption of the 16-octet challenge as specified in clause {xref 1.2.1.4.}.

1.2.2.2 Public key and authentication cryptographic operations

The following table specifies the public key cryptography and authentication related operations for the authentication protocol frames defined in clause 7{xref}.:

Table 4—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 RSA raw public key of the device as specified in sub-clause {xref 1.2.1.5}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 RSA-OAEP encryption as specified in sub-clause {xref 1.2.1.4} on a fresh, randomly generated 16-byte challenge using the other device's public key.
Challenge decryption	The challenge decryption operation is performed using RSA-OAEP decryption as specified in sub-clause {xref 1.2.1.4} on the received challenge.
Seed generation (for authentication protocol)	The 32-byte seed for the authentication protocol consists of the decrypted challenge from the security manager, concatenated with the decrypted challenge of the DEV.

1.2.3 RSA-OAEP X509 1 sub-suite

RSA-OAEP X509 1 is a mode 3 sub-suite of the RSA-OAEP 1024-1 security suite. The cryptographic building blocks for RSA-OAEP X509 1 sub-suite are selected from the public-key cryptographic building blocks defined for the RSA-OAEP 1024-1 security suite. The OID for this sub-suite is specified in {xref Table 2}. The following sub-clauses specify the public-key and authentication related objects for this sub-suite.

1.2.3.1 Public-key and authentication data formats

The following table specifies the length and meaning of the public-key cryptography and authentication related security suite specific data elements from clause 7{xref}. The operations performed to obtain the variable data values are specified in a separate sub-clause.

Table 5—Public-key frame object formats

Notation	Length	Value	Description
PublicKeyObjectType	2	See 7.4.1.2{xref}	An RSA X.509 certificate as specified in clause {xref 1.2.1.7}. The value is the entry for RSA X.509 1024 in table 7.4.1.2{xref}.

Table 5—Public-key frame object formats

PublicKeyObjectLength	2	Variable	The length of the particular instance of the X.509 certificate.
PublicKeyObject	Variable	Variable	The particular instance of the X.509 certificate.
OIDLength	1	10	The length of the DER encoding of the OID rsa-oaep-x509-1 as specified in {xref Table 2}.
OID	10	OID Value	The DER encoding of the OID rsa-oaep-x509-1 as specified in {xref Table 2}.
ChallengeType	2	See table 7.4.1.3{xref}	The challenge type is an RSA-OAEP encryption of a 16-octet challenge as specified in clause {xref 1.2.1.4.}. The value is the entry for RSA-OAEP 1024 encrypted seed in 7.4.1.3{xref}.
ChallengeLength	2	128	The length of an RSA-OAEP encryption of a 16-octet challenge as specified in clause {xref 1.2.1.4.}.
Challenge	128	Variable	The result of the RSA-OAEP encryption of the 16-octet challenge as specified in clause {xref 1.2.1.4.}.

1.2.3.2 Public key and authentication cryptographic operations

The following table specifies the public key cryptography and authentication related operations for the authentication protocol frames defined in clause 7{xref}.:

Table 6—Authentication related operations

Use	Operation
Verification of Public-Key	The X.509 certificate received during the authentication protocol is verified by retrieving the appropriate CA key and verifying the RSASSA-PKCS1-v1_5 signature as specified in clause {xref 1.2.1.8}on the certificate. The device shall verify that the MAC address in the subjectAltName of the certificate matches the MAC address that the certificate was received from. The device shall extract the public key for use in the authentication protocol. There are several other checks that should be performed by the device if possible to ensure the security properties of the certificate including a CRL check, validity period verification and the key use field check. In addition, the device shall check that the device in the certificate is included in the MAC PIB. If the device is not in the PIB, the certificate 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 RSA-OAEP encryption as specified in sub-clause {xref 1.2.1.4} on a fresh, randomly generated 16-byte challenge using the other device's public key.

Table 6—Authentication related operations

Challenge decryption	The challenge decryption operation is performed using RSA-OAEP decryption as specified in sub-clause {xref 1.2.1.4} on the received challenge.
Seed generation (for authentication protocol)	The 32-byte seed for the authentication protocol consists of the decrypted challenge from the security manager, concatenated with the decrypted challenge of the DEV.

2. References

Author’s note: The following normative references should be included.

PKCS#1v2.1: RSA Cryptography Standard, RSA Laboratories, Draft 3, April 19, 2002[1]

R. Housley, et. al., RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[1]PKCS standards are available from RSA Security at 174 Middlesex Turnpike, Bedford, MA 01730, USA and online at http://www.rsasecurity.com/rsalabs/pkcs/index.html.