1.RSA AES KEY WRAP mechanism parameters

- **CK_RSA_AES_KEY_WRAP_PARAMS; CK_RSA_AES_KEY_WRAP_PARAMS_PTR**

CK_RSA_AES_KEY_WRAP_PARAMS is a structure that provides the parameters to the **CKM_RSA_AES_KEY_WRAP** mechanism. It is defined as follows:

```
typedef struct CK_RSA_AES_KEY_WRAP_PARAMS {
        CK_ULONG                        ulAESKeyBits;
        CK_RSA_PKCS_OAEP_PARAMS_PTR     pOAEPParams;
      } CK_RSA_AES_KEY_WRAP_PARAMS;
```

The fields of the structure have the following meanings:

ulAESKeyBits length of the temporary AES key in bits. Can be only 128, 192 or 256.

pOAEPParams pointer to the parameters of the temporary AES key wrapping. See also the description of PKCS #1 RSA OAEP mechanism parameters.

CK_RSA_AES_KEY_WRAP_PARAMS_PTR is a pointer to a **CK_RSA_AES_KEY_WRAP_PARAMS**.

2.RSA AES KEY WRAP

The RSA AES KEY WRAP mechanism, denoted **CKM_RSA_AES_KEY_WRAP** , is a mechanism based on the RSA public-key cryptosystem and the AES key wrap mechanism. It supports single-part key wrapping; and key unwrapping.

It has a parameter, a **CK_RSA_AES_KEY_WRAP_PARAMS** structure.

The mechanism can wrap and unwrap a target asymmetric key of any length and type using an RSA key.

- A temporary AES key is used for wrapping the target key using CKM_AES_WRAP mechanism.
- The temporary AES key is wrapped with the wrapping RSA key using CKM_RSA_PKCS_OAEP mechanism.

For wrapping, the mechanism -

- Generates temporary random AES key of *ulAESKeyBits* length. This key is not accessible to the user - no handle is returned.
- Wraps the AES key with the wrapping RSA key using **CKM_RSA_PKCS_OAEP** with parameters of *OAEPParams*.
- Wraps the target key with the temporary AES key using **CKM_AES_KEY_WRAP_PAD** (RFC5649) .
- Zeroizes the temporary AES key
- Concatenates two wrapped keys and outputs the concatenated blob.

The recommended format for an asymmetric target key being wrapped is as a PKCS8 PrivateKeyInfo

The use of Attributes in the PrivateKeyInfo structure is OPTIONAL. In case of conflicts between the object attribute template, and Attributes in the PrivateKeyInfo structure, an error should be thrown

For unwrapping, the mechanism -

- Splits the input into two parts. The first is the wrapped AES key, and the second is the wrapped target key. The length of the first part is equal to the length of the unwrapping RSA key.
- Un-wraps the temporary AES key from the first part with the private RSA key using **CKM_RSA_PKCS_OAEP** with parameters of *OAEPParams*.
- Un-wraps the target key from the second part with the temporary AES key using **CKM_AES_KEY_WRAP_PAD**_(RFC5649) .
- Zeroizes the temporary AES key.
- Returns the handle to the newly unwrapped target key.

	Functions						
Mechanism	**Encrypt & Decrypt**	**Sign & Verify**	**SR & VR** [1]	**Digest**	**Gen. Key/ Key Pair**	**Wrap & Unwrap**	**Derive**
CKM_RSA_AES_KEY_WRAP						✓	

[1] SR = SignRecover, VR = VerifyRecover