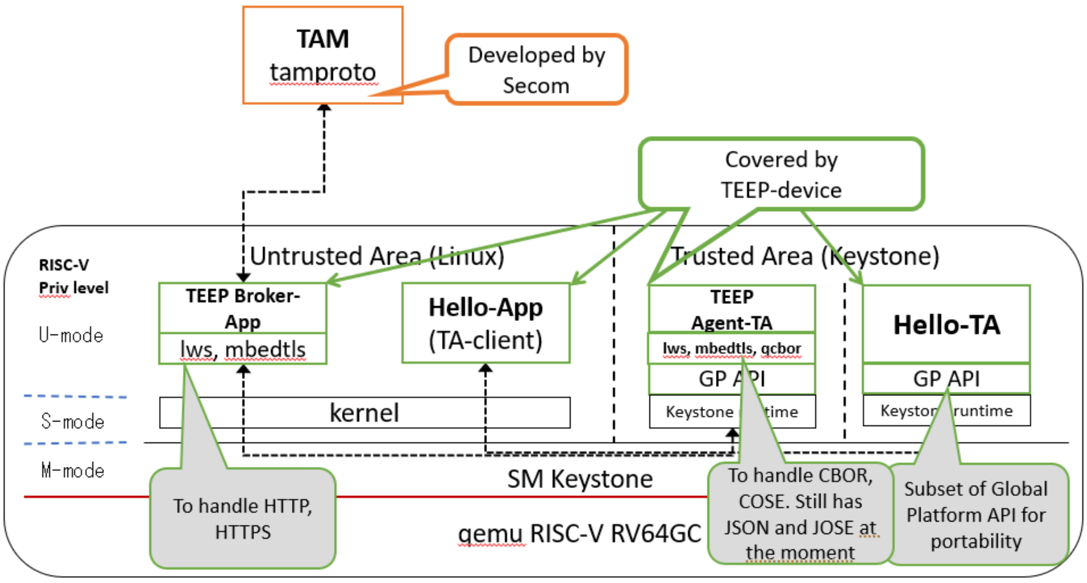
Trusted Application Programming Reference on Portable TEE

The National Institute of Advanced Industrial Science and Technology

2021-12-14

1 Overview of ta-ref



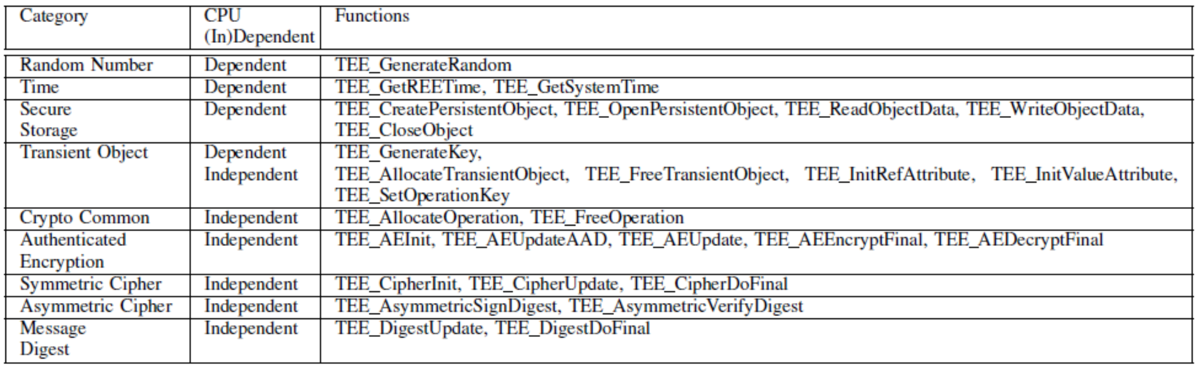
1.1 Features

1.1.1 What we did on RISC-V

- We designed the GP internal API library to be portable.
  - Keystone SDK is utilized because of runtime "Eyrie".
  - The library is ported to Intel SGX as well as RISC-V Keystone.
- Implementation Challenge
  - The combination of GP internal API and cipher suite is big.
    - We pick up some important GP internal APIs.
  - Some APIs depend on CPU architecture.
    - We separate APIs into CPU architecture dependent / independent.
  - Integrate GP TEE Internal API to Keystone SDK.
    - Keystone SDK includes EDL (Enclave Definition Language) named “keedger”.
    - Keedger creates the code for OCALL (request from TEE to REE) to check the pointer and boundary.

1.1.2 Separate GP TEE Internal API

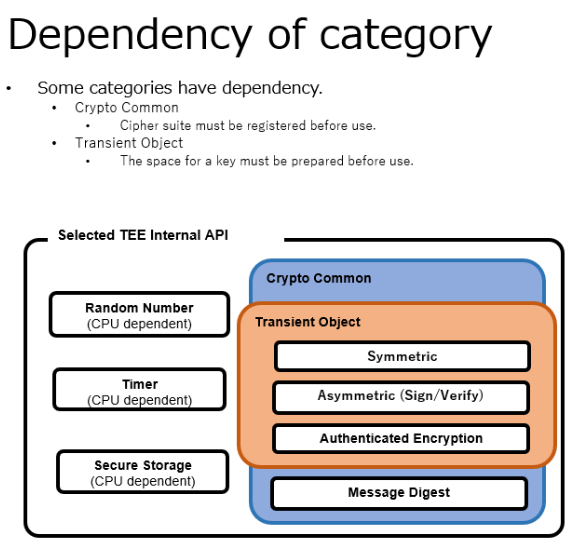
- CPU architecture dependent
  - Random Generator, Time, Secure Storage, Transient Object(TEE_GenerateKey)
- CPU architecture independent(Crypto)
  - Transient Object(exclude TEE_GenerateKey), Crypto Common, Authenticated Encryption, Symmetric/Asymmetric Cipher, Message Digest



Category	CPU (In)Dependent	Functions
Random Number	Dependent	TEE_GenerateRandom
Time	Dependent	TEE_GetREETime, TEE_GetSystemTime
Secure Storage	Dependent	TEE_CreatePersistentObject, TEE_OpenPersistentObject, TEE_ReadObjectData, TEE_WriteObjectData, TEE_CloseObject
Transient Object	Dependent Independent	TEE_GenerateKey, TEE_AllocateTransientObject, TEE_FreeTransientObject, TEE_InitRefAttribute, TEE_InitValueAttribute, TEE_SetOperationKey
Crypto Common	Independent	TEE_AllocateOperation, TEE_FreeOperation
Authenticated Encryption	Independent	TEE_AEInit, TEE_AEUpdateAAD, TEE_AEUpdate, TEE_AEEncryptFinal, TEE_AEDecryptFinal
Symmetric Cipher	Independent	TEE_CipherInit, TEE_CipherUpdate, TEE_CipherDoFinal
Asymmetric Cipher	Independent	TEE_AsymmetricSignDigest, TEE_AsymmetricVerifyDigest
Message Digest	Independent	TEE_DigestUpdate, TEE_DigestDoFinal

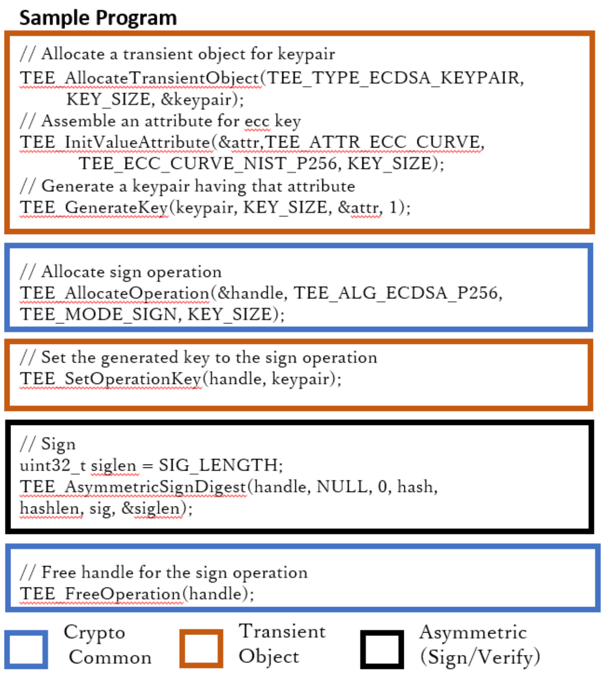
1.2 Diagram

1.2.1 Dependency of category



Dependency of category

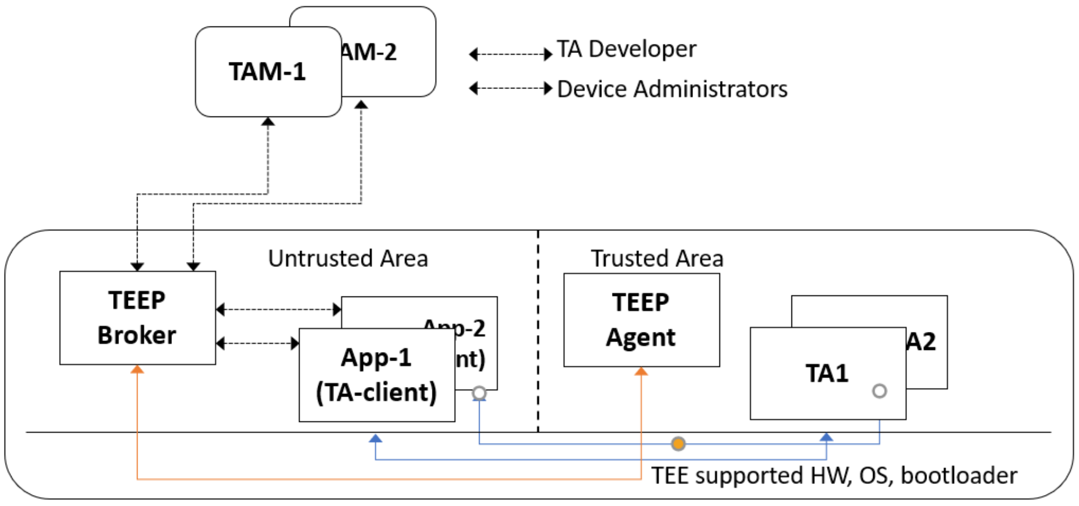
- Some categories have dependency.
  - Crypto Common
    - Cipher suite must be registered before use.
  - Transient Object
    - The space for a key must be prepared before use.



Sample Program

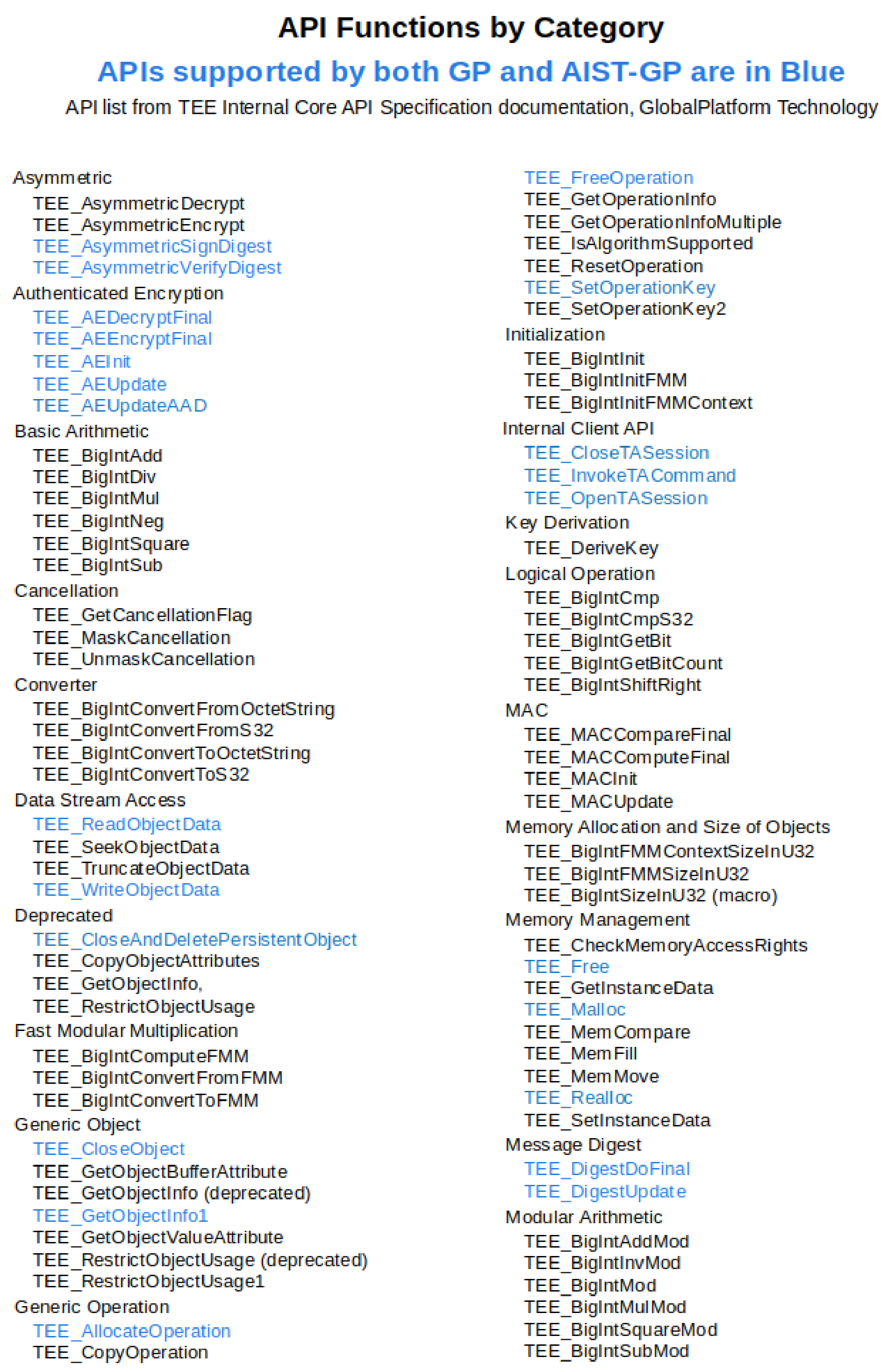
```
// Allocate a transient object for keypair
TEE_AllocateTransientObject(TEE_TYPE_ECDSA_KEYPAIR,
      KEY_SIZE, &keypair);
// Assemble an attribute for ecc key
TEE_InitValueAttribute(&attr,TEE_ATTR_ECC_CURVE,
        TEE_ECC_CURVE_NIST_P256, KEY_SIZE);
// Generate a keypair having that attribute
TEE_GenerateKey(keypair, KEY_SIZE, &attr, 1);

// Allocate sign operation
TEE_AllocateOperation(&handle, TEE_ALG_ECDSA_P256,
TEE_MODE_SIGN, KEY_SIZE);

// Set the generated key to the sign operation
TEE_SetOperationKey(handle, keypair);

// Sign
uint32_t siglen = SIG_LENGTH;
TEE_AsymmetricSignDigest(handle, NULL, 0, hash,
hashlen, sig, &siglen);

// Free handle for the sign operation
TEE_FreeOperation(handle);
```

1.2.2 TEEP Architechture



2 API comparison with full set of GP API

2.1 GP API



API Functions by Category

APIs supported by both GP and AIST-GP are in Blue

API list from TEE Internal Core API Specification documentation, GlobalPlatform Technology

- Asymmetric
  - TEE_AsymmetricDecrypt
  - TEE_AsymmetricEncrypt
  - TEE_AsymmetricSignDigest
  - TEE_AsymmetricVerifyDigest
- Authenticated Encryption
  - TEE_AEDecryptFinal
  - TEE_AEEncryptFinal
  - TEE_AEInit
  - TEE_AEUpdate
  - TEE_AEUpdateAAD
- Basic Arithmetic
  - TEE_BigIntAdd
  - TEE_BigIntDiv
  - TEE_BigIntMul
  - TEE_BigIntNeg
  - TEE_BigIntSquare
  - TEE_BigIntSub
- Cancellation
  - TEE_GetCancellationFlag
  - TEE_MaskCancellation
  - TEE_UnmaskCancellation
- Converter
  - TEE_BigIntConvertFromOctetString
  - TEE_BigIntConvertFromS32
  - TEE_BigIntConvertToOctetString
  - TEE_BigIntConvertToS32
- Data Stream Access
  - TEE_ReadObjectData
  - TEE_SeekObjectData
  - TEE_TruncateObjectData
  - TEE_WriteObjectData
- Deprecated
  - TEE_CloseAndDeletePersistentObject
  - TEE_CopyObjectAttributes
  - TEE_GetObjectInfo,
  - TEE_RestrictObjectUsage
- Fast Modular Multiplication
  - TEE_BigIntComputeFMM
  - TEE_BigIntConvertFromFMM
  - TEE_BigIntConvertToFMM
- Generic Object
  - TEE_CloseObject
  - TEE_GetObjectBufferAttribute
  - TEE_GetObjectInfo (deprecated)
  - TEE_GetObjectInfo1
  - TEE_GetObjectValueAttribute
  - TEE_RestrictObjectUsage (deprecated)
  - TEE_RestrictObjectUsage1
- Generic Operation
  - TEE_AllocateOperation
  - TEE_CopyOperation
  - TEE_FreeOperation
  - TEE_GetOperationInfo
  - TEE_GetOperationInfoMultiple
  - TEE_IsAlgorithmSupported
  - TEE_ResetOperation
  - TEE_SetOperationKey
  - TEE_SetOperationKey2
- Initialization
  - TEE_BigIntInit
  - TEE_BigIntInitFMM
  - TEE_BigIntInitFMMContext
- Internal Client API
  - TEE_CloseTASession
  - TEE_InvokeTACommand
  - TEE_OpenTASession
- Key Derivation
  - TEE_DeriveKey
- Logical Operation
  - TEE_BigIntCmp
  - TEE_BigIntCmpS32
  - TEE_BigIntGetBit
  - TEE_BigIntGetBitCount
  - TEE_BigIntShiftRight
- MAC
  - TEE_MACCompareFinal
  - TEE_MACComputeFinal
  - TEE_MACInit
  - TEE_MACUpdate
- Memory Allocation and Size of Objects
  - TEE_BigIntFMMContextSizeInU32
  - TEE_BigIntFMMSizeInU32
  - TEE_BigIntSizeInU32 (macro)
- Memory Management
  - TEE_CheckMemoryAccessRights
  - TEE_Free
  - TEE_GetInstanceData
  - TEE_Malloc
  - TEE_MemCompare
  - TEE_MemFill
  - TEE_MemMove
  - TEE_Realloc
  - TEE_SetInstanceData
- Message Digest
  - TEE_DigestDoFinal
  - TEE_DigestUpdate
- Modular Arithmetic
  - TEE_BigIntAddMod
  - TEE_BigIntInvMod
  - TEE_BigIntMod
  - TEE_BigIntMulMod
  - TEE_BigIntSquareMod
  - TEE_BigIntSubMod

Other Arithmetic
- TEE_BigIntComputeExtendedGcd
- TEE_BigIntIsProbablePrime
- TEE_BigIntRelativePrime

Panic Function
- TEE_Panic

Persistent Object
- TEE_CloseAndDeletePersistentObject (deprecated)
- TEE_CloseAndDeletePersistentObject1
- TEE_CreatePersistentObject
- TEE_OpenPersistentObject
- TEE_RenamePersistentObject

Persistent Object Enumeration *
- TEE_AllocatePersistentObjectEnumerator
- TEE_FreePersistentObjectEnumerator
- TEE_GetNextPersistentObject
- TEE_ResetPersistentObjectEnumerator
- TEE_StartPersistentObjectEnumerator

Property Access
- TEE_AllocatePropertyEnumerator
- TEE_FreePropertyEnumerator
- TEE_GetNextProperty
- TEE_GetPropertyAsBinaryBlock
- TEE_GetPropertyAsBool
- TEE_GetPropertyAsIdentity
- TEE_GetPropertyAsString
- TEE_GetPropertyAsU32
- TEE_GetPropertyAsU64
- TEE_GetPropertyAsUUID
- TEE_GetPropertyName
- TEE_ResetPropertyEnumerator
- TEE_StartPropertyEnumerator

Random Data Generation
- TEE_GenerateRandom

Symmetric Cipher
- TEE_CipherDoFinal
- TEE_CipherInit
- TEE_CipherUpdate

TA Interface
- TA_CloseSessionEntryPoint
- TA_CreateEntryPoint
- TA_DestroyEntryPoint
- TA_InvokeCommandEntryPoint
- TA_OpenSessionEntryPoint

Time
- TEE_GetREETime
- TEE_GetSystemTime
- TEE_GetTAPersistentTime
- TEE_SetTAPersistentTime
- TEE_Wait

Transient Object
- TEE_AllocateTransientObject
- TEE_CopyObjectAttributes (deprecated)
- TEE_CopyObjectAttributes1
- TEE_FreeTransientObject
- TEE_GenerateKey
- TEE_InitRefAttribute
- TEE_InitValueAttribute
- TEE_PopulateTransientObject
- TEE_ResetTransientObject

3 How to Program on ta-ref

3.1 Time Functions

This function retrieves the current time as seen from the point of view of the REE, which expressed in the number of seconds and prints the "GP REE second and millisecond".

```
--- start Ree time ---
void gp_ree_time_test(void)
{
    TEE_Time time;

    /* REE time */
    TEE_GetREETime(&time);

    tee_printf ("@GP REE time %u sec %u millis\n", time.seconds, time.millis);
}
--- end Ree Time ---
```

This function retrieves the current system time as seen from the point of view of the TA, which expressed in the number of seconds and print the "GP System time second and millisecond".

```
--- start System time ---
void gp_trusted_time_test(void)
{
    TEE_Time time;

    /* System time */
    TEE_GetSystemTime(&time);

    tee_printf ("@GP System time %u sec %u millis\n", time.seconds, time.millis);
}
--- end System time ---
```

3.2 Random Functions

This function generates the random data by invoking TEE_GenerateRandom function and it prints the generated random data.

```
--- start Random ---
 void gp_random_test(void)
{
    unsigned char rbuf[16];

    // Generate Random
    TEE_GenerateRandom(rbuf, sizeof(rbuf));

    tee_printf("@random: ");
    for (int i = 0; i < sizeof(rbuf); i++) {
        tee_printf ("%02x", rbuf[i]);
    }
    tee_printf("\n");
}
--- end Random ---
```

3.3 Hash Functions

Pseudo code of how to use Message Digest Functions. Keystone uses sha3.c which is almost identical. The function performs many operations to achieve message data hash techniques to allocate the handle for a new cryptographic operation. And then finalize the message digest operation to produce the message hash. It prints the hash message.

```
--- start Message Digest ---
void gp_message_digest_test(void)
{
    static unsigned char data[256] = {
     #include "test.dat"
    };
    unsigned char hash[SHA_LENGTH];
    uint32_t hashlen = SHA_LENGTH;
    TEE_OperationHandle handle;
    TEE_Result rv;

    // Take hash of test data
    /* sha3_init() in sha3.c */
    rv = TEE_AllocateOperation(&handle, TEE_ALG_SHA256, TEE_MODE_DIGEST, SHA_LENGTH);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    /* sha3_update() in sha3.c */
    TEE_DigestUpdate(handle, data, sizeof(data));

    /* sha3_final() in sha3.c */
    rv = TEE_DigestDoFinal(handle, NULL, 0, hash, &hashlen);
    GP_ASSERT(rv, "TEE_DigestDoFinal fails");

    TEE_FreeOperation(handle);
    /* hash value is ready */
    // Dump hashed data
    tee_printf("hash: ");
    for (int i = 0; i < hashlen; i++) {
      tee_printf ("%02x", hash[i]);
    }
    tee_printf("\n");
}
--- end Message Digest ---
```

3.4 Symmetric Crypto Functions

Crypto, Authenticated Encryption with Symmetric Key Verification Functions. This function allocates an uninitialized transient object, i.e. a container for attributes. Transient objects are used to hold a cryptographic object (key or key-pair). With the generation of a key, a new cryptographic operation for encrypt and decrypt data is initiated with a symmetric cipher operation. The original data is compared with decrypted data by checking the data and its length.

```
--- start Symmetric Key Encryption ---
 void gp_symmetric_key_enc_verify_test(void)
{
    TEE_OperationHandle handle;

    static unsigned char data[CIPHER_LENGTH] = {
        // 0x00,0x01,...,0xff
        #include "test.dat"
    };
    uint8_t iv[16];
    unsigned char out[CIPHER_LENGTH];
    uint32_t outlen;

    TEE_ObjectHandle key;
    TEE_Result rv;

    // Generate key
    rv = TEE_AllocateTransientObject(TEE_TYPE_AES, 32*8, &key);
    GP_ASSERT(rv, "TEE_AllocateTransientObject fails");

    rv = TEE_GenerateKey(key, 256, NULL, 0);
    GP_ASSERT(rv, "TEE_GenerateKey fails");

    // Encrypt test data
    rv = TEE_AllocateOperation(&handle, TEE_ALG_AES_CBC_NOPAD, TEE_MODE_ENCRYPT, 256);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    rv = TEE_SetOperationKey(handle, key);
    GP_ASSERT(rv, "TEE_SetOperationKey fails");

    TEE_GenerateRandom(iv, sizeof(iv));
    TEE_CipherInit(handle, iv, sizeof(iv));
    //GP_ASSERT(rv, "TEE_AEInit fails");

    outlen = CIPHER_LENGTH;
    rv = TEE_CipherUpdate(handle, data, CIPHER_LENGTH, out, &outlen);
    GP_ASSERT(rv, "TEE_CipherUpdate fails");
    TEE_FreeOperation(handle);

    // Dump encrypted data
    tee_printf("@cipher: ");
    for (int i = 0; i < CIPHER_LENGTH; i++) {
        tee_printf ("%02x", out[i]);
    }
    tee_printf("\n");

    // Decrypt it
    rv= TEE_AllocateOperation(&handle, TEE_ALG_AES_CBC_NOPAD, TEE_MODE_DECRYPT, 256);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    rv = TEE_SetOperationKey(handle, key);
    GP_ASSERT(rv, "TEE_SetOperationKey fails");

    TEE_CipherInit(handle, iv, sizeof(iv));
    //GP_ASSERT(rv, "TEE_AEInit fails");

    outlen = CIPHER_LENGTH;
    rv = TEE_CipherUpdate(handle, out, CIPHER_LENGTH, out, &outlen);
    GP_ASSERT(rv, "TEE_CipherUpdate fails");

    TEE_FreeOperation(handle);
    TEE_FreeTransientObject(key);

    // Dump data
    tee_printf("decrypted to: ");
    for (int i = 0; i < CIPHER_LENGTH; i++) {
        tee_printf ("%02x", out[i]);
    }
    tee_printf("\n");

    // Verify decrypted data against original one
    int verify_ok;
    verify_ok = !memcmp(out, data, CIPHER_LENGTH);
    if (verify_ok) {
        tee_printf("verify ok\n");
    } else {
        tee_printf("verify fails\n");
    }
}
--- end Symmetric Key Encryption ---
```

3.5 Symmetric Crypto AES-GCM Functions

This function encrypt and decrypt the test data. The function allocates an uninitialized transient object, i.e. a container for attributes. Transient objects are used to hold a cryptographic object (key or key-pair).With the generation of a key, a new cryptographic operation for encrypt and decrypt data is initiated with a symmetric cipher operation. The data is also checked whether it is completely encrypted or decrypted. The original data is compared with decrypted data by checking the data and cipher length.

```
--- start Symmetric Key GCM  ---
void gp_symmetric_key_gcm_verify_test(void)
{
    TEE_OperationHandle handle;

    static unsigned char data[CIPHER_LENGTH] = {
        // 0x00,0x01,...,0xff
        #include "test.dat"
    };

    uint8_t iv[16];
    unsigned char out[CIPHER_LENGTH];
    uint32_t outlen;
    unsigned char tag[16];

    TEE_ObjectHandle key;
    TEE_Result rv;

    // Generate key
    rv = TEE_AllocateTransientObject(TEE_TYPE_AES, 256, &key);
    GP_ASSERT(rv, "TEE_AllocateTransientObject fails");

    rv = TEE_GenerateKey(key, 256, NULL, 0);
    GP_ASSERT(rv, "TEE_GenerateKey fails");
    // Encrypt test data
    rv = TEE_AllocateOperation(&handle, TEE_ALG_AES_GCM, TEE_MODE_ENCRYPT, 256);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    rv = TEE_SetOperationKey(handle, key);
    GP_ASSERT(rv, "TEE_SetOperationKey fails");

    TEE_GenerateRandom(iv, sizeof(iv));

    /* Equivalent in openssl is EVP_EncryptInit_ex() */
    rv = TEE_AEInit(handle, iv, sizeof(iv), 16*8, 16, 16);
    GP_ASSERT(rv, "TEE_AEInit fails");

    /* Equivalent in openssl is EVP_EncryptUpdate() */
    //  rv = TEE_AEUpdateAAD(handle, aad, 16);
    //  GP_ASSERT(rv, "TEE_AEUpdateAAD fails");

    unsigned int taglen = 16;
    memset(tag, 0, 16);

    outlen = CIPHER_LENGTH;

    /* Equivalent in openssl is EVP_EncryptFinal() */
    rv = TEE_AEEncryptFinal(handle, data, 256, out, &outlen, tag, &taglen);

    TEE_FreeOperation(handle);

    /* Get the auth_tag */
    // Dump encrypted data and tag
    tee_printf("@cipher: ");
    for (int i = 0; i < CIPHER_LENGTH; i++) {
      tee_printf ("%02x", out[i]);
    }
    tee_printf("\n");
    tee_printf("@tag: ");
    for (int i = 0; i < 16; i++) {
      tee_printf ("%02x", tag[i]);
    }
    tee_printf("\n");

    // Decrypt it
    rv = TEE_AllocateOperation(&handle, TEE_ALG_AES_GCM, TEE_MODE_DECRYPT, 256);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    rv = TEE_SetOperationKey(handle, key);
    GP_ASSERT(rv, "TEE_SetOperationKey fails");

    /* Equivalent in openssl is EVP_DecryptInit_ex() */
    rv = TEE_AEInit(handle, iv, sizeof(iv), 16*8, 16, 16);
    GP_ASSERT(rv, "TEE_AEInit fails");

    //  rv = TEE_AEUpdateAAD(handle, aad, 16);
    //  GP_ASSERT(rv, "TEE_AEUpdateAAD fails");

    unsigned char decode[CIPHER_LENGTH];
    outlen = 256;
    /* Equivalent in openssl require two functions
       EVP_CIPHER_CTX_ctrl(tag) and EVP_DecryptFinal(others) */
    rv = TEE_AEDecryptFinal(handle, out, 256, decode, &outlen, tag, 16);
    GP_ASSERT(rv, "TEE_AEDecryptFinal fails");

    TEE_FreeOperation(handle);
    TEE_FreeTransientObject(key);

    // Dump data and tag
    tee_printf("decrypted to: ");
    for (int i = 0; i < CIPHER_LENGTH; i++) {
      tee_printf ("%02x", decode[i]);
    }
    tee_printf("\n");

    // Verify decrypted data against original one
    /* Check verify_ok for success of decrypting and authentication */
    int verify_ok;
    verify_ok = !memcmp(decode, data, CIPHER_LENGTH);
    if (verify_ok) {
      tee_printf("verify ok\n");
    } else {
      tee_printf("verify fails\n");
    }

}
--- end Symmetric Key GCM ---
```

3.6 Asymmetric Crypto Functions

Crypto, Sign and Verify with Asymmetric Key Verification Functions. Cryptographic Operations for API Message Digest Functions. The function performs cryptographic operation for API Message. To achieve this, the function allocates a handle for a new cryptographic operation, to finalize the message digest operation and to produce the message hash. The Hashed data is signed with signature key within an asymmetric operation. The original Hashed Data and Signed hashed data is compared for ok status.

```
--- start Asymmetric Key Signed ---
void gp_asymmetric_key_sign_test(void)
{
    static unsigned char data[256] = {
        // 0x00,0x01,...,0xff
        #include "test.dat"
    };
    unsigned char hash[SHA_LENGTH];
    unsigned char sig[SIG_LENGTH];
    uint32_t hashlen = SHA_LENGTH;
    TEE_OperationHandle handle;
    TEE_Result rv;

    // Take hash of test data
    /* Calculate hash */
    /* sha3_init() in sha3.c */
    rv = TEE_AllocateOperation(&handle, TEE_ALG_SHA256, TEE_MODE_DIGEST, SHA_LENGTH);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    /* sha3_update() in sha3.c */
    TEE_DigestUpdate(handle, data, sizeof(data));

    /* sha3_final() in sha3.c */
    rv = TEE_DigestDoFinal(handle, NULL, 0, hash, &hashlen);
    GP_ASSERT(rv, "TEE_DigestDoFinal fails");

    /* free up */
    TEE_FreeOperation(handle);
    /* Get the signature */

    // Dump hashed data
    tee_printf("@digest: ");
    for (int i = 0; i < SHA_LENGTH; i++) {
      tee_printf ("%02x", hash[i]);
    }
    tee_printf("\n");

    uint32_t siglen = SIG_LENGTH;
    TEE_ObjectHandle keypair;

    // Sign hashed data with the generated keys
    /* set ecdsa_p256 key */
    rv = TEE_AllocateOperation(&handle, TEE_ALG_ECDSA_P256, TEE_MODE_SIGN, 256);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    // Generate keypair
    rv = TEE_AllocateTransientObject(TEE_TYPE_ECDSA_KEYPAIR, 256, &keypair);
    GP_ASSERT(rv, "TEE_AllocateTransientObject fails");

    TEE_Attribute attr;
    TEE_InitValueAttribute(&attr,
                TEE_ATTR_ECC_CURVE,
                TEE_ECC_CURVE_NIST_P256,
                256);
    rv = TEE_GenerateKey(keypair, 256, &attr, 1);
    GP_ASSERT(rv, "TEE_GenerateKey fails");

    rv = TEE_SetOperationKey(handle, keypair);
    GP_ASSERT(rv, "TEE_SetOperationKey fails");

    /* Keystone has ecdsa_p256_sign() Equivalent in openssl is EVP_DigestSign() */
    rv = TEE_AsymmetricSignDigest(handle, NULL, 0, hash, hashlen, sig, &siglen);
    GP_ASSERT(rv, "TEE_AsymmetricSignDigest fails");

    /* free up */
    TEE_FreeOperation(handle);

    /* Get the signature */
    // Dump signature
    tee_printf("@signature: ");
    for (uint32_t i = 0; i < siglen; i++) {
      tee_printf ("%02x", sig[i]);
    }
    tee_printf("\n");
    // Verify signature against hashed data
    /* set ecdsa_p256 key */
    rv = TEE_AllocateOperation(&handle, TEE_ALG_ECDSA_P256, TEE_MODE_VERIFY, 256);
    GP_ASSERT(rv, "TEE_AllocateOperation fails");

    rv = TEE_SetOperationKey(handle, keypair);
    GP_ASSERT(rv, "TEE_SetOperationKey fails");

    /* Keystone has ecdsa_p256_verify() Equivalent in openssl is EVP_DigestVerify() */
    TEE_Result verify_ok;
    verify_ok = TEE_AsymmetricVerifyDigest(handle, NULL, 0, hash, hashlen, sig, siglen);

    /* free up */
    TEE_FreeOperation(handle);
    tee_printf("@@TEE_FreeOperation: \n");

    TEE_FreeTransientObject(keypair);

    if (verify_ok == TEE_SUCCESS) {
      tee_printf("verify ok\n");
    } else {
      tee_printf("verify fails\n");
    }

}
/* Check verify_ok for success of verification */
--- end Asymmetric Key Signed ---
```

3.7 Open, Read, Write, Close On Secure Storage

Core Functions, Secure Storage Functions. Pseudo code of how to use Secure Storage. These could be implemented using ocall on Keystone. Almost identical to open(), clone(), read(), write() in POSIX API. The function creates a persistent object for reading and writing the data. The created data individually for read and write are compared for data length. If the length of both the objects are same, the function prints "verify ok" and prints "verify fails" if it is not the same.

```
--- start Secure storage ---
void gp_secure_storage_test(void)
{
    static unsigned char data[] = {
        // 0x00,0x01,...,0xff
        #include "test.dat"
    };
    static unsigned char buf[DATA_LENGTH];

    TEE_Result rv;

    /* write */
    TEE_ObjectHandle object;
    rv = TEE_CreatePersistentObject(TEE_STORAGE_PRIVATE,
                    "FileOne", strlen("FileOne"),
                    (TEE_DATA_FLAG_ACCESS_WRITE
                     | TEE_DATA_FLAG_OVERWRITE),
                    TEE_HANDLE_NULL,
                    NULL, 0,
                    &object);
    GP_ASSERT(rv, "TEE_CreatePersistentObject fails");

    memcpy(buf, data, DATA_LENGTH);

    /* fill the date in buffer */
    rv = TEE_WriteObjectData(object, (const char *)data, DATA_LENGTH);
    GP_ASSERT(rv, "TEE_WriteObjectData fails");

    TEE_CloseObject(object);
    --- write file end ---

    /* clear buf */
    memset(buf, 0, DATA_LENGTH);

    --- read file start ---
    /* read */
    rv = TEE_OpenPersistentObject(TEE_STORAGE_PRIVATE,
                  "FileOne", strlen("FileOne"),
                  TEE_DATA_FLAG_ACCESS_READ,
                  &object);
    GP_ASSERT(rv, "TEE_OpenPersistentObject fails");
    uint32_t count;
    rv = TEE_ReadObjectData(object, (char *)buf, DATA_LENGTH, &count);

    GP_ASSERT(rv, "TEE_ReadObjectData fails");
    TEE_CloseObject(object);

    /* use the date in buffer */
    tee_printf("%d bytes read: ", count);
    for (uint32_t i = 0; i < count; i++) {
      tee_printf ("%02x", buf[i]);
    }
    tee_printf("\n");

    /* Compare read data with written data */
    int verify_ok;
    verify_ok = !memcmp(buf, data, DATA_LENGTH);
    if (verify_ok) {
      tee_printf("verify ok\n");
    } else {
      tee_printf("verify fails\n");
    }

}
--- end Secure storage ---
```

4 Preparation before building ta-ref

4.1 Keystone(RISC-V Unleased)

Keystone is an open-source TEE framework for RISC-V processors. For more details check,

- http://docs.keystone-enclave.org/en/latest

4.1.1 Required Packages

Install following Packages

```
$ sudo apt-get update
$ sudo apt-get install -y autoconf automake autotools-dev bc bison
  build-essential curl expat libexpat1-dev flex gawk gcc git gperf libgmp-dev
  libmpc-dev libmpfr-dev libtool texinfo tmux patchutils zlib1g-dev wget
  bzip2 patch vim-common lbzip2 python pkg-config libglib2.0-dev libpixman-1-dev
  libssl-dev screen device-tree-compiler expect makeself unzip cpio rsync cmake
```

4.1.2 Build Keystone

Download the keystone sources

```
$ git clone https://github.com/keystone-enclave/keystone.git
$ cd keystone
$ git checkout v0.3
$ ./fast-setup.sh
$ make
$ source source.sh
./sdk/scripts/init.sh
./sdk/examples/hello/vault.sh
./sdk/examples/hello-native/vault.sh
./tests/tests/vault.sh
$ make image
```

RISC-V Toolchain:

- When you execute `./fast-setup.sh`, the toolchain for RISC-V has been installed at `$KEYSTONE_↩ DIR/riscv/bin` and it adds to your PATH.

4.1.3 Run Keystone examples

Launch QEMU console

```
$ ./scripts/run-qemu.sh
Welcome to Buildroot
```

Login to console with user=root, passwd=sifive

```
buildroot login: root
Password:
$
```

Run hello example

```
$ insmod keystone-driver.ko
[  365.354299] keystone_driver: loading out-of-tree module taints kernel.
[  365.364279] keystone_enclave: keystone enclave v0.2
$ ./hello/hello.ke
Verifying archive integrity...  100%   All good.
Uncompressing Keystone vault archive  100%
hello, world!
```

Poweroff the console incase, if you want to exit.

```
$ poweroff
```

4.2 OP-TEE (ARM64 Raspberry Pi 3 Model B)

OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm. Lets build OP-TEE for QEMU and Raspberry Pi3 Model B development board. For more details check,

- https://optee.readthedocs.io/en/latest/

4.2.1 Required Packages

Install following packages on Ubuntu 18.04

```
$ sudo dpkg --add-architecture i386
$ sudo apt-get update -y
$ sudo apt-get install -y android-tools-adb android-tools-fastboot autoconf \
        automake bc bison build-essential ccache cscope curl device-tree-compiler \
        expect flex ftp-upload gdisk iasl libattr1-dev libc6:i386 libcap-dev \
        libfdt-dev libftdi-dev libglib2.0-dev libhidapi-dev libncurses5-dev \
        libpixman-1-dev libssl-dev libstdc++6:i386 libtool libz1:i386 make \
        mtools netcat python python-crypto python3-crypto python-pyelftools \
        python3-pycryptodome python3-pyelftools python3-serial vim-common \
        rsync unzip uuid-dev xdg-utils xterm xz-utils zlib1g-dev \
        git python3-pip wget cpio \
        texlive texinfo \
$ sudo pip3 install pycryptodomex
```

4.2.2 Build OP-TEE v3.9.0

Configure git

```
$ git config --global user.name "dummy"
$ git config --global user.email "dummy@gmail.com"
$ git config --global color.ui false
$ mkdir ~/bin
$ curl https://storage.googleapis.com/git-repo-downloads/repo > ~/bin/repo && \
$ chmod a+x ~/bin/repo
```

4.2.2.1 Download Toolchains

```
$ export TOOLCHAIN_DIR=${HOME}/toolchains
$ sudo apt-get install -y wget xz-utils
$ mkdir -p ${TOOLCHAIN_DIR}/aarch64 ${TOOLCHAIN_DIR}/aarch32
$ wget http://192.168.100.100:2000/gcc-arm-8.3-2019.03-x86_64-arm-linux-gnueabihf.tar.xz -o
       /dev/null -O aarch32.tar.xz && \
  tar xf aarch32.tar.xz --strip-components=1 -C ${TOOLCHAIN_DIR}/aarch32
$ wget http://192.168.100.100:2000/gcc-arm-8.3-2019.03-x86_64-aarch64-linux-gnu.tar.xz -o /dev/null
       -O aarch64.tar.xz && \
  tar xf aarch64.tar.xz --strip-components=1 -C ${TOOLCHAIN_DIR}/aarch64
$ export PATH=${TOOLCHAIN_DIR}/aarch64/bin:${TOOLCHAIN_DIR}/aarch32/bin:${PATH}
```

4.2.2.2 Clone and Build OP-TEE v3.9.0 for QEMU

Clone optee version 3.9.0 for QEMU

```
$ mkdir optee_3.9.0_qemu
$ cd optee_3.9.0_qemu
$ ~/bin/repo init -u https://github.com/knknkn1162/manifest.git -m qemu_v8.xml -b 3.9.0
$ ~/bin/repo sync -j4 --no-clone-bundle
$ ln -s ~/toolchains toolchains
$ cd build
$ make
```

If build is successfull, the rootfs can be found as follows

```
$ ls -l ../out-br/images/rootfs.cpio.gz
```

4.2.2.3 Clone and Build OP-TEE v3.9.0 for RPI3

Copy the following lines into "optee-rpi3.sh" script

```
#!/bin/bash -u
export OPTEE_VER=$1
export OPTEE_DIR=${PWD}/optee_${OPTEE_VER}_rpi3
mkdir ${OPTEE_DIR} || true
cd ${OPTEE_DIR}
~/bin/repo init -u https://github.com/knknkn1162/manifest.git -m rpi3.xml -b ${OPTEE_VER}
~/bin/repo sync -j4 --no-clone-bundle
ln -s ~/toolchains ${OPTEE_DIR}/. || true
echo 'CONFIG_CMDLINE="console=ttyAMA0,115200 kgdboc=ttyAMA0,115200 root=/dev/mmcblk0p2
       rootfstype=ext4 noinitrd rw rootwait init=/lib/systemd/systemd"' > build/defconfig-cmdline.txt
cd build
make OPTEE_CLIENT_BIN_ARCH_EXCLUDE=/boot
    LINUX_DEFCONFIG_COMMON_FILES="${OPTEE_DIR}/linux/arch/arm64/configs/bcmrpi3_defconfig
    ${OPTEE_DIR}/build/kconfigs/rpi3.conf ${OPTEE_DIR}/build/defconfig-cmdline.txt"
       BR2_PACKAGE_OPTEE_OS_EXT=n BR2_PACKAGE_OPTEE_TEST_EXT=n
    BR2_PACKAGE_OPTEE_EXAMPLES_EXT=n BR2_TOOLCHAIN_EXTERNAL_GCC_8=y BR2_TOOLCHAIN_EXTERNAL_HEADERS_4_19=y
       BR2_HOST_GCC_AT_LEAST_8=y
    BR2_TOOLCHAIN_HEADERS_AT_LEAST="4.19" -j'nproc'
```

Run the script as follows

```
$ chmod +x optee-rpi3.sh
$ ./optee-rpi3.sh 3.9.0
```

If build is successfull, the rootfs can be found as follows

```
$ ls -l ../out-br/images/rootfs.cpio.gz
```

4.2.3 Run OP-TEE Examples

4.2.3.1 Launching QEMU Console

Run following commands from OP-TEE build directory

```
$ cd $OPTEE_DIR/build
$ make run
```

Once above command is success, QEMU is ready

```
* QEMU is now waiting to start the execution
* Start execution with either a 'c' followed by <enter> in the QEMU console or
* attach a debugger and continue from there.
*
* To run OP-TEE tests, use the xtest command in the 'Normal World' terminal
* Enter 'xtest -h' for help.
cd /TEE/demo/rpi3/optee_3.9.0_qemu/build/../out/bin
     && /TEE/demo/rpi3/optee_3.9.0_qemu/build/../qemu/aarch64-softmmu/qemu-system-aarch64 \
    -nographic \
    -serial tcp:localhost:54320 -serial tcp:localhost:54321 \
    -smp 2 \
    -s -S -machine virt,secure=on -cpu cortex-a57 \
    -d unimp -semihosting-config enable,target=native \
    -m 1057 \
    -bios bl1.bin \
    -initrd rootfs.cpio.gz \
    -kernel Image -no-acpi \
    -append 'console=ttyAMA0,38400 keep_bootcon root=/dev/vda2' \
    -object rng-random,filename=/dev/urandom,id=rng0 -device virtio-rng-pci,rng=rng0,max-bytes=1024,
        period=1000 -netdev user,id=vmnic -device virtio-net-device,netdev=vmnic
QEMU 3.0.93 monitor - type 'help' for more information
(qemu) c
Now Optee started to boot from another tab on the Terminal
```

4.2.3.2 Run hello world example

Once boot completed it displays following message, then enter "root" to login to the shell

```
Welcome to Buildroot, type root or test to login
buildroot login: root
$
$ optee_example_hello_world
Invoking TA to increment 42
TA incremented value to 43
```

Poweroff the console in case, if you want to exit.

```
$ poweroff
```

4.3 SGX (Intel NUC)

Intel(R) Software Guard Extensions (Intel(R) SGX) is an Intel technology for application developers who is seeking to protect selected code and data from disclosure or modification. For more details check,

- https://github.com/intel/linux-sgx/blob/master/README.md

4.3.1 List of machines which are confirmed to work

1. Intel NUC7PJYH - Intel(R) Celeron(R) J4005 CPU @ 2.00GHz
2. Intel NUC7PJYH - Intel(R) Pentium(R) Silver J5005 CPU @ 1.50GHz
3. Intel NUC9VXQNX - Intel(R) Xeon(R) E-2286M CPU @ 2.40GHz (Partially working)

4.3.2 BIOS Versions which are failed or scucceeded in IAS Test

1. BIOS Version JYGLKCPX.86A.0050.2019.0418.1441 - IAS Test was Failed
2. BIOS Version JYGLKCPX.86A.0053.2019.1015.1510 - IAS Test was Failed
3. BIOS Version JYGLKCPX.86A.0057.2020.1020.1637 - IAS Test was Success
4. BIOS Version QNCFLX70.0034.2019.1125.1424 - IAS Test was Failed
5. BIOS Version QNCFLX70.0059.2020.1130.2122 - IAS Test was Success

Update BIOS from:

- `https://downloadcenter.intel.com/download/29987/BIOS-Update-JYGLKCPX-`
- `https://downloadcenter.intel.com/download/30069/BIOS-Update-QNCFLX70-`

4.3.3 BIOS Settings

1. Make sure you are running with latest version BIOS
2. Make sure you enabled SGX support in BIOS
3. Make sure `Secure Boot` disabled in BIOS

Refer: `https://github.com/intel/sgx-software-enable/blob/master/README.md`

4.3.4 Required Packages

Intall following packages on Ubuntu 18.04

```
$ sudo apt-get install build-essential ocaml ocamlbuild automake autoconf libtool wget python
      libssl-dev git cmake perl libssl-dev libcurl4-openssl-dev protobuf-compiler libprotobuf-dev
      debhelper cmake reprepro expect unzip sshpass
```

4.3.5 Build SGX

There are 3 components which need to be build for SGX

1. linux-sgx
2. linux-sgx-driver
3. sgx-ra-sample

4.3.5.1 SGX SDK

Clone and build

```
$ git clone https://github.com/intel/linux-sgx.git -b sgx_2.10
$ cd linux-sgx
$ git checkout sgx_2.10
$ ./download_prebuilt.sh
$ sudo cp external/toolset/ubuntu18.04/{as,ld,ld.gold,objdump} /usr/local/bin/
$ make -j`nproc` sdk_install_pkg DEBUG=1
```

Install SGX SDK

```
$ sudo ./linux/installer/bin//sgx_linux_x64_sdk_${version}.bin
```

where ${version} is a string something similar to 2.10.100.2.
Answer the question with `no` and input the install dir as `/opt/intel`

Build and Install SGX PSW packages
See here: https://github.com/intel/linux-sgx#install-the-intelr-sgx-psw

```
$ source /opt/intel/sgxsdk/environment
$ make deb_psw_pkg DEBUG=1
$ rm ./linux/installer/deb/*/*sgx-dcap-pccs*.deb
$ sudo dpkg -i ./linux/installer/deb/*/*.deb
```

Install SGX PSW packages from Intel Repository

See here: https://github.com/intel/linux-sgx#install-the-intelr-sgx-psw-1
Using the local repo is recommended, since the system will resolve the dependencies automatically.
Check at page no.7, https://download.01.org/intel-sgx/sgx-linux/2.9/docs/Intel_↩
SGX_Installation_Guide_Linux_2.9_Open_Source.pdf

```
$ sudo apt install libsgx-enclave-common libsgx-epid libsgx-launch libsgx-urts libsgx-uae-service
     libsgx-quote-ex
```

If you see below error,

```
Errors were encountered while processing:
 /tmp/apt-dpkg-install-pCB0cR/04-libsgx-headers_2.12.100.3-bionic1_amd64.deb
```

Here is the fix

```
$ sudo apt -o Dpkg::Options::="--force-overwrite" --fix-broken install
```

4.3.5.2 Build and Install SGX Driver

See linux-sgx-driver.

Caveat: Whenever updating kernel, don't forget rebuilding this driver with new version of the kernel header. (There are a few linux-sgx-driver-dkms repo, though I've experianced troubles with them.)

Clone and build

```
$ git clone https://github.com/intel/linux-sgx-driver.git
$ cd linux-sgx-driver
$ make
```

Install SGX driver

```
$ sudo mkdir -p "/lib/modules/"`uname -r`"/kernel/drivers/intel/sgx"
$ sudo cp isgx.ko "/lib/modules/"`uname -r`"/kernel/drivers/intel/sgx"
$ sudo sh -c "cat /etc/modules | grep -Fxq isgx || echo isgx » /etc/modules"
$ sudo /sbin/depmod
$ sudo /sbin/modprobe isgx
```

When modprove fails with "Operation is not permitted", disable `secure boot` in BIOS. So that the unsigned kernel driver can be installed. If it is success, reboot your machine and verify `sudo lsmod | grep isgx` if it shows `isgx.ko`

4.3.6 Run sgx-ra-sample

4.3.6.1 Build sgx-ra-sample

Clone and build OpenSSL 1.1.c

```
$ wget https://www.openssl.org/source/openssl-1.1.1c.tar.gz
$ tar xf openssl-1.1.1c.tar.gz
$ cd openssl-1.1.1c/
$ ./config --prefix=/opt/openssl/1.1.1c --openssldir=/opt/openssl/1.1.1c
$ make
$ sudo make install
$ cd ..
```

Clone and build sgx-ra-sample

```
$ git clone https://github.com/intel/sgx-ra-sample.git
$ cd sgx-ra-sample/
$ ./bootstrap
$ ./configure --with-openssldir=/opt/openssl/1.1.1c
$ make
```

4.3.6.2 Prepare for IAS Test

1. Obtain a subscription key for the Intel SGX Attestation Service Utilizing Enhanced Privacy ID (EPID). See here: `https://api.portal.trustedservices.intel.com/EPID-attestation`
2. Download Intel_SGX_Attestation_RootCA.pem form above portal.
3. Edit `settings` file and update the file with your own values obtained from portal.

```
@@ -15,14 +15,14 @@ QUERY_IAS_PRODUCTION=0
 # Your Service Provider ID. This should be a 32-character hex string.
 # [REQUIRED]

-SPID=0123456789ABCDEF0123456789ABCDEF
+SPID=EF9AE4A8635825B88751C8698CB370B4


 # Set to a non-zero value if this SPID is associated with linkable
 # quotes. If you change this, you'll need to change SPID,
 # IAS_PRIMARY_SUBSCRIPTION_KEY and IAS_SECONDARY_SUBSCRIPTION_KEY too.

-LINKABLE=0
+LINKABLE=1

 #======================================================================
@@ -50,18 +50,18 @@ USE_PLATFORM_SERVICES=0
 # More Info: https://api.portal.trustedservices.intel.com/EPID-attestation
 # Associated SPID above is required

-IAS_PRIMARY_SUBSCRIPTION_KEY=
+IAS_PRIMARY_SUBSCRIPTION_KEY=b6da4c9c41464924a14954ad8c03e8cf

 # Intel Attestation Service  Secondary Subscription Key
 # This will be used in case the primary subscription key does not work

-IAS_SECONDARY_SUBSCRIPTION_KEY=
+IAS_SECONDARY_SUBSCRIPTION_KEY=188d91f86c064deb97e7472175ae1e79

 # The Intel IAS SGX Report Signing CA file. You are sent this certificate
 # when you apply for access to SGX Developer Services at
 # http://software.intel.com/sgx [REQUIRED]

-IAS_REPORT_SIGNING_CA_FILE=
+IAS_REPORT_SIGNING_CA_FILE=./Intel_SGX_Attestation_RootCA.pem

 # Debugging options
@@ -82,7 +82,7 @@ IAS_REPORT_SIGNING_CA_FILE=

 # Set to non-zero for verbose output

-VERBOSE=0
+VERBOSE=1
```

4.3.6.3 Run IAS Test

Run "run-server"

```
$ ./run-server
Listening for connections on port 7777
Waiting for a client to connect...
Connection from 127.0.0.1
Waiting for msg0||msg1
---- Copy/Paste Msg2 Below to Client ---------------------------------------
44f2e22125f052e0118018febceefd469f1f4b73de22b34ebdf27003605963946bb862980be691a2f532d8e66abb2ce4eaad
f778593b1ce7a14b2759f133beceef9ae4a8635825b88751c8698cb370b401000100fbb75d7ce414edc45510aa87a7547ffb
a65415fca10e83c0936729c2abfb6c2687ee6dde5c6540a835fae6032bbfaf9f8eaefbcfafcf606e94ece103d82ecc82a457
a16692d4023dad4e4fee38fb20d00000000
----------------------------------------------------------------------------
Waiting for msg3
+++ POST data written to /tmp/wgetpostwnMRxU
---- Copy/Paste Msg4 Below to Client ---------------------------------------
0300000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000
----------------------------------------------------------------------------
Waiting for a client to connect...
```

Open another terminal and run "run-client"

```
$ ./run-client
---- Copy/Paste Msg0||Msg1 Below to SP -------------------------------------
00000000a7fa6ed63bec97891885abc2e2e80bd4bb2bd5bb32a7e142337f486bb9f6e76a9db59aa9
aaac50cd24c3625451a79bce7c51e24447981444cf51666f3b61cd0cfb0b0000
----------------------------------------------------------------------------
Waiting for msg2
---- Copy/Paste Msg3 Below to SP --------------------------------------------
787d992031b5ed7d57f149aec7f04912a7fa6ed63bec97891885abc2e2e80bd4bb2bd5bb32a7e142337f486bb9f6e76a9db5
9aa9aaac50cd24c3625451a79bce7c51e24447981444cf51666f3b61cd0c0000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000002000100fb0b00000b000a000000
0000ef9ae4a8635825b88751c8698cb370b4000000000000000000000000000000000303000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000070000000000000030000000000000000188d
d04a51cc90bf27ca2e733a3a97557dcaabff3e2d037d11a1d0680c8f22c10000000000000000000000000000000000000000
00000000000000000000000bd71c6380ef77c5417e8b2d1ce2d4b6504b9f418e5049342440cfff2443d95bd0000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000001000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000ab2e17de92aadea169f418e9266ea4e79b393f0028754ed46c6e538d3aed1e5a00000000000000000000000000000
00000000000000000000000000000000000a80200007657efd8ff80410670f40aba48cc5a0c61aa70a3c656f021c28104503
9ea3c16f5831825fd3405eb6090d70a6e87853374eefb690285367ac35f471df09571fda8f96de9e2067f6f7c12fa97a4f06
5311e71d01cd97a89c93c9ba9b0d02d56723f67a51ee742974c46d05e313db18826f6b4183a83a421b0df4b6c3a059b814a3
7d6b905f28422076e41d23016b22d1ec2ea5712c6bc470070313d8d50f6968b97e1ca65524ec677191b5ccb5c14e9629efc1
e1e1cc6e87388143712c1f15593ec5fdea02ce426139c461cfd6cc63025124ed5ea5c0160fdb59ea65e97449d44d78355018
c54f11290930d8464096723fc0e25421fb0849a156ce0af973af0324a86bdb583501f0779e86d108afef02faa6c73c6d6035
e8d4c8ba3478ca58779dd26f015d31dff046e8d74fe680100004af4eed5e48babde1db56dc88ab96a689de24c33ad955ca33
86d9bf9fb842d2ef2f09883e9dead7e5c58c841181e987599532e769b3e1445a570c7b7fc5d866906d5064770919001a47b3
f4dde0635451047a0d1fc8a3971525866fa07da59e3cce44e71eba19a8a00e265ecc04dc5529a942afe6dd222045e746411c
```

```
d4c89541a432de0c7464ba8d54e775f1530098a3fc4876c140028e12edcd0e3df1b176271f74207b54b0bd76a9d4b3549f8b
b950a492a64a4949eeaa8192432d99eabebd46eb56507a675c184de8ee6c53461753cf123bb9e26ddfb8422e4c130efe7c5d
f3f328cb02945bfa575f79e376d9aac40da397e9cdcb449f223842bec9e07e4b2c736409ed964799ac9cf51a71f0cbdf91f9
4bd362e761ae35ed27d2872112caf2476846e397141106d9898b96295fa969dbd9b48c7dd8f27c5ba1bb1d6bb202aad86346
695c8f18efe073e9424382f3f73757ee99e95c30da5dd47d94185eda2b97613b0872a622c58f4f2dd91d1e4d876ac8e40a18
60a
----------------------------------------------------------------------------
---- Enclave Trust Status from Service Provider ----------------------------
Enclave TRUSTED
```

4.3.6.4 Possible wget Error

Server may invoke wget command to get some files from intel servers. If the server side fails with following error

```
Connecting to api.trustedservices.intel.com (api.trustedservices.intel.com)|40.87.90.88|:443...
       connected.
ERROR: cannot verify api.trustedservices.intel.com's certificate, issued by 'CN=COMODO RSA
       Organization Validation Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater
       Manchester,C=GB':
  Unable to locally verify the issuer's authority.
To connect to api.trustedservices.intel.com insecurely, use `--no-check-certificate'.
```

then add a line `ca-certificate = /etc/ssl/certs/ca-certificates.crt` to /etc/wgetrc file as super user, then test again.

4.3.6.5 BIOS Updating

If BIOS version is outdated, IAS may not succeed. So when you are done with BIOS update, the sgx driver would be reqired to make and install again.

Update BIOS from:

- https://downloadcenter.intel.com/download/29987/BIOS-Update-JYGLKCPX-
- https://downloadcenter.intel.com/download/30069/BIOS-Update-QNCFLX70-

4.3.6.6 Run LocalAttestation

Running SDK code samples in simulation mode

```
$ source /opt/intel/sgxsdk/environment
$ cd linux-sgx/SampleCode/LocalAttestation
$ make SGX_MODE=SIM
$ cd bin
$ ./app
succeed to load enclaves.
succeed to establish secure channel.
Succeed to exchange secure message...
Succeed to close Session...
```

Running in hardware mode (It works when you have latest BIOS and SGX support is enabled in BIOS)

```
$ source /opt/intel/sgxsdk/environment
$ cd linux-sgx/SampleCode/LocalAttestation
$ make SGX_MODE=HW
$ cd bin
$ ./app
succeed to load enclaves.
succeed to establish secure channel.
Succeed to exchange secure message...
Succeed to close Session...
```

4.4 Customizing MbedTLS Configuration file

MbedTLS is a C library that implements cryptographic primitives, X.509 certificate manipulation and the SSL/TLS and DTLS protocols. MbedTLS has a configuration file `config.h` where we can select platform-specific settings, customize the features that will be build, select the modules and its configurations.

In our case, we customize mbedtls config file to add/remove crypto algorithms when building the mbedtls. The mbedtls default config supports many cryto algorithms which might be unneccessary and also increases the built binary size.

It is advisable to reduce the size of the binaries, by selecting only the required crypto algorithms for the embedded systems.

4.4.1 What can be customized?

1. how many hash algorithms to be supported
   For ex: md5, sha1, sha256, sha3 or etc
2. how many symmetric algorithms to be supported
   For ex: des, aes-cbc, aes-gcm or etc
3. how many asymmetric algorithms to be supported
   For ex: dsa, rsa, ecdsa, eddsa or etc and their key length

4.4.2 mbedtls configuration file (config.h)

The mbedtls official way is customizing config file is by editing the `include/mbedtls/config.h` file. But in optee's build system, it require modifying
`optee_os/lib/libmbedtls/include/mbedtls_config_kernel.h`

Below are the different environments mbedtls config file locations, reference file and sample config.h configurations.

4.4.2.1 Optee mbetls config file

Location of the config file in optee environment
`optee/mbedtls/include/mbedtls/config.h`

Have a look at the source which uses config.h file for reference.
Example source:
`optee/mbedtls/include/mbedtls/library/ssl_ciphersuites.c`

Some sample configurations can be found in `configs/` directory. In Optee, the contents of configs directory is listed below.

```
$ ls -l optee/mbedtls/configs
total 24
-rw-r--r-- 1 akirat akirat 2852 Feb 17  2021 config-ccm-psk-tls1_2.h
-rw-r--r-- 1 akirat akirat 2102 Feb 17  2021 config-mini-tls1_1.h
-rw-r--r-- 1 akirat akirat 2628 Feb 17  2021 config-no-entropy.h
-rw-r--r-- 1 akirat akirat 3573 Feb 17  2021 config-suite-b.h
-rw-r--r-- 1 akirat akirat 2680 Feb 17  2021 config-thread.h
-rw-r--r-- 1 akirat akirat 1050 Feb 17  2021 README.txt
```

4.4.2.2 ta-ref mbetls config file

Location of the config file in ta-ref environment
`ta-ref/teep-device/libteep/mbedtls/include/mbedtls/config.h`

Have a look at the source which uses config.h file for reference.
Example source:
`ta-ref/teep-device/libteep/mbedtls/include/mbedtls/library/ssl_↩ ciphersuites.c`

Some sample configurations can be found in `configs/` directory. In ta-ref, the contents of configs directory is listed below.

```
$ ls -l ta-ref/teep-device/libteep/mbedtls/configs
total 24
-rw-r--r-- 1 akirat akirat 2852 Feb 18  2021 config-ccm-psk-tls1_2.h
-rw-r--r-- 1 akirat akirat 2102 Feb 18  2021 config-mini-tls1_1.h
-rw-r--r-- 1 akirat akirat 2628 Feb 18  2021 config-no-entropy.h
-rw-r--r-- 1 akirat akirat 3573 Feb 18  2021 config-suite-b.h
-rw-r--r-- 1 akirat akirat 2680 Feb 18  2021 config-thread.h
-rw-r--r-- 1 akirat akirat 1050 Feb 18  2021 README.txt
```

4.4.2.3 teep-device mbetls config file

Location of the config file in teep-device environment
`teep-device/libteep/mbedtls/include/mbedtls/config.h`

Have a look at the source which uses config.h file for reference.
Example source:
`teep-device/libteep/mbedtls/include/mbedtls/library/ssl_ciphersuites.c`

Some sample configurations can be found in `configs/` directory. In teep-device, the contents of configs directory is listed below.

```
$ ls -l teep-device/libteep/mbedtls/configs
total 24
-rw-r--r-- 1 akirat akirat 2852 Feb 18  2021 config-ccm-psk-tls1_2.h
-rw-r--r-- 1 akirat akirat 2102 Feb 18  2021 config-mini-tls1_1.h
-rw-r--r-- 1 akirat akirat 2628 Feb 18  2021 config-no-entropy.h
-rw-r--r-- 1 akirat akirat 3573 Feb 18  2021 config-suite-b.h
-rw-r--r-- 1 akirat akirat 2680 Feb 18  2021 config-thread.h
-rw-r--r-- 1 akirat akirat 1050 Feb 18  2021 README.txt
```

4.4.3 Supplement Investigation information

It is necessary to edit the following file to select the cryptographic algorithm when using mbedtls in optee.

In optee, AES-GCM is not included by default. So we need to modify the mbedtls config file to enable AES-GCM algorithm. Below is the path of the file in optee kernal where we will select the crypto algorithms.
`optee/optee_os/lib/libmbedtls/include/mbedtls_config_kernel.h`

Below is the path of file in TA SDK where we will select the crypto algorithms. In TA sdk, the AES-GCM is enabled by default. So any TA which uses AES-GCM should build successfully without any modification to the mbedtls config file.
`optee/optee_os/lib/libmbedtls/include/mbedtls_config_uta.h`

5 Building

5.1 Install Doxygen-1.9.2

This PDF was generated using Doxygen version 1.9.2. To install `doxygen-1.9.2` following procedure is necessary.

5.2 Install Required Packages

Install following packages on Ubuntu 18.04

```
$ sudo apt install doxygen-latex graphviz texlive-full texlive-latex-base latex-cjk-all
```

Above packages required to generate PDF using doxygen.

5.3 Build and Install

```
$ git clone https://github.com/doxygen/doxygen.git
$ cd doxygen
$ mkdir build
$ cd build
$ cmake -G "Unix Makefiles" ..
$ make
$ sudo make install
```

5.4 ta-ref with Keystone

Make sure Keystone and other dependant sources have been built

5.4.1 Cloning source and building

Install required packages

```
$ sudo apt-get update
$ sudo apt-get install -y clang-tools-6.0 libclang-6.0-dev cmake ocaml expect screen sshpass
```

Setup Env

```
$ export KEYSTONE_DIR=<path to your keystone directory>
$ export PATH=$PATH:$KEYSTONE_DIR/riscv/bin
```

Clone and Build KEYEDGE

```
$ GIT_SSL_NO_VERIFY=1 git clone --recursive https://192.168.100.100/rinkai/keyedge.git
$ cd keyedge
$ git checkout f9406aba2117147cc54462ede4766e26f028ced9
$ make
```

Clone and Build KEEDGER8R

```
$ GIT_SSL_NO_VERIFY=1 git clone --recursive https://192.168.100.100/rinkai/keedger8r.git
$ cd keedger8r
$ make
$ sed -i ’s/MAX_EDGE_CALL 10$/MAX_EDGE_CALL 1000/’ ${KEYSTONE_DIR}/sdk/lib/edge/include/edge_common.h
$ make -C ${KEYSTONE_DIR}/sdk/lib clean all
```

Clone the source

```
$ git clone https://192.168.100.100/rinkai/ta-ref.git
$ cd ta-ref
$ git checkout teep-device-tb-slim
$ git submodule sync --recursive
git submodule update --init --recursive
```

Build

```
$ export KEYSTONE_DIR=<path to keystone directory>
$ export KEYSTONE_SDK_DIR=$KEYSTONE_DIR/sdk
$ export KEYEDGE_DIR=<path to keyedge directory>
$ export KEEDGER8R_DIR=<path to keedger8r directory>
$ source env/keystone.sh
$ make build test-bin MACHINE=HIFIVE TEST_DIR=test_hello
$ make build test-bin MACHINE=HIFIVE TEST_DIR=test_gp
```

5.4.2 Check ta-ref by running test_gp, test_hello, on QEMU

Copy the test_hello and test_gp programs to QEMU.

5.4.2.1 Launch QEMU Console

```
$ cd $KEYSTONE_DIR
$ ./scripts/run-qemu.sh
Welcome to Buildroot
```

5.4.2.2 test_hello

Run test_hello

```
$ cp test_hello/keystone/Enclave/Enclave.eapp_riscv $KEYSTONE_DIR/buildroot_overlay/root/test_hello/
$ cp test_hello/keystone/Enclave/App.client $KEYSTONE_DIR/buildroot_overlay/root/test_hello/
$ cp $KEYSTONE_SDK_DIR/rts/eyrie/eyrie-rt $KEYSTONE_DIR/buildroot_overlay/root/test_hello/

$ insmod keystone-driver.ko
./App.client Enclave.eapp_riscv eyrie-rt
hello world!
```

5.4.2.3 test_gp

Run test_gp

```
$ cp test_gp/keystone/Enclave/Enclave.eapp_riscv $KEYSTONE_DIR/buildroot_overlay/root/test_gp/
$ cp test_gp/keystone/Enclave/App.client $KEYSTONE_DIR/buildroot_overlay/root/test_gp/
$ cp $KEYSTONE_SDK_DIR/rts/eyrie/eyrie-rt $KEYSTONE_DIR/buildroot_overlay/root/test_gp/
$ insmod keystone-driver.ko
$ ./App.client Enclave.eapp_riscv eyrie-rt
main start
TEE_GenerateRandom(0x000000003FFFFEE0, 16): start
```

```
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@random: 5ea8741bd8a3b298cf53d214eca693fb
TEE_GetREETime(): start
@[SE] gettimeofday 77 sec 865873 usec -> 0
@GP REE time 77 sec 865 millis
TEE_GetSystemTime(): start
@GP System time 100063195 sec 609 millis
TEE_CreatePersistentObject(): start
@[SE] open file FileOne flags 241 -> 3 (0)
TEE_WriteObjectData(): start
@[SE] write desc 3 buf 480d0 len 256-> 256
TEE_CloseObject(): start
@[SE] close desc 3 -> 0
TEE_OpenPersistentObject(): start
@[SE] open file FileOne flags 0 -> 3 (0)
TEE_ReadObjectData(): start
@[SE] read desc 3 buf fff41664 len 256-> 256
TEE_CloseObject(): start
@[SE] close desc 3 -> 0
256 bytes read: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f303132333435363738393a3b3c3d3f
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
hash: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateTransientObject(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(0x000000003FFFFD88, 32): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AllocateOperation(): start
TEE_GenerateRandom(0x000000003FFFFED0, 16): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_CipherInit(): start
TEE_CipherUpdate(): start
TEE_FreeOperation(): start
@cipher: e94431cd22a6029185d0dbb1a17b5d62843bfeef25591583d2d668ec6fed1c692f88ce4754d690c346c8d9f2726
630e0386abf4e45699a2ca2b34b344eaa454bc489c
TEE_AllocateOperation(): start
TEE_CipherInit(): start
TEE_CipherUpdate(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f
verify ok
TEE_AllocateTransientObject(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(0x000000003FFFFC68, 32): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AllocateOperation(): start
TEE_GenerateRandom(0x000000003FFFFEC8, 16): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AEInit(): start
TEE_AEEncryptFinal(): start
TEE_FreeOperation(): start
@cipher: c23e9ce04589e80a66debe23a788ae5393bdcd8e875e87e1bcf2b2d998f6418ccc6ee4ab112fdbfc5175868691e
fb40781a318ff439d30b49cc9f726886ad42d5be15
@tag: a551f999317b3fbd1eea7b622ce2caee
TEE_AllocateOperation(): start
TEE_AEInit(): start
TEE_AEDecryptFinal(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
@digest: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateOperation(): start
TEE_AllocateTransientObject(): start
TEE_InitValueAttribute(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(0x000000003FFFFE28, 32): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AsymmetricSignDigest(): start
TEE_FreeOperation(): start
@signature: d6e6b6e54db8b6a62fc1927886938bead27f4813f19ce77182e3016b5426bcad067ca98cd75f9dfddafe9eb0
```

```
655c48df992d3ad674db69d831f26ae63caf1405
TEE_AllocateOperation(): start
TEE_AsymmetricVerifyDigest(): start
TEE_FreeOperation(): start
@@TEE_FreeOperation:
TEE_FreeTransientObject(): start
verify ok
main end
```

5.5 ta-ref with OP-TEE

Make sure optee_3.9.0_rpi3 has been built already.

5.5.1 Cloning source and building

Clone the source

```
$ git clone https://192.168.100.100/rinkai/ta-ref.git
$ cd ta-ref
$ git checkout teep-device-tb-slim
$ git submodule sync --recursive
$ git submodule update --init --recursive
```

Build

```
$ export OPTEE_DIR=<path to optee_3.9.0_rpi3>
$ source env/optee_rpi3.sh
$ make build test-bin MACHINE=RPI3 TEST_DIR=test_hello
$ make build test-bin MACHINE=RPI3 TEST_DIR=test_gp
```

5.5.2 Check ta-ref by running test_gp, test_hello, on QEMU

Copy the test_hello and test_gp programs to QEMU buildroot directory

```
$ mkdir -p optee_3.9.0_qemu/out-br/target/home/gitlab/out/{test_hello,test_gp}
$ cp ta-ref/test_hello/optee/App/optee_ref_ta optee_3.9.0_qemu/out-br/target/home/gitlab/out/test_hello/
$ cp ta-ref/test_hello/optee/Enclave/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
     optee_3.9.0_qemu/out-br/target/home/gitlab/out/test_hello/
$ cp ta-ref/test_gp/optee/App/optee_ref_ta
     optee_3.9.0_qemu/out-br/target/home/gitlab/out/test_gp/
$ cp ta-ref/test_gp/optee/Enclave/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
     optee_3.9.0_qemu/out-br/target/home/gitlab/out/test_gp/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
$ cp ./test_gp/optee/Enclave/Enclave.nm
    /TEE/demo/rpi3/optee_3.9.0_qemu/out-br/target/home/gitlab/out/test_gp/
```

5.5.2.1 test_hello

Run test_hello

```
$ cd /home/gitlab/out/test_hello/
$ cp a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta /home/gitlab/out/
$ ln -s /home/gitlab/out/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
     /lib64/optee_armtz/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
$ ./optee_ref_ta
--- enclave log start---
ecall_ta_main() start
hello world!
```

```
ecall_ta_main() end
--- enclave log end---
```

If executed successfully, you see above messages

5.5.2.2 test_gp

Run test_gp

```
$ cd /home/gitlab/out/test_gp/
$ cp a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta /home/gitlab/out/
$ ln -s /home/gitlab/out/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
     /lib64/optee_armtz/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
$ ./optee_ref_ta
start TEEC_InvokeCommand
--- enclave log start---
ecall_ta_main() start
@random: fe0c7d3eefb9bd5e63b8a0cce29af7eb
@GP REE time 1612156259 sec 390 millis
@GP System time 249187 sec 954 millis
256 bytes read: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292
2a2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b
5c5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d
8e8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebf
c0c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1
f2f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
hash: 40aff2e9d2d8922e47afd4648e6967497158785fbd1da870e7110266bf944880
@cipher: 30a558176172c53be4a2ac320776de105da79c29726879fe67d06b629f065731285f8a90f8a521ce34eceea51e1
5e928d157ea10d149bb687dd78be79469c28696506283edcda527fcd86f6a47e852bbc3488df3fc651b46b034faf4ab5f12f
51a285478ea01e58d40e8177d415be243df93b23cdf889feb91fa3be8906fe190d836fe61168aed0473406be1054dd88a381
ef25381d920ea3780ba74fb1cfe1434cbd168de8386dcc2e2b92eee0fc432f3c0514f462cbeaf96753b174a4a673f323e671
61272fe932ead4bc95770fcc130dd5877b521d6a79f961eeadd1680042f69257ccf9368927aa170176af8ac211dd22161997
7224837232dad970220f4
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
@cipher: ff409d8fe203bf0d81de36832b86c702f07edd343f408d3a2fb5ab347b4f72b10031efff0c17b7e0bc56c3f2f95
f53c0d731ed87eb3e1187b6714a25cfc65082284682b44450941654e7edc99af0f7b037c3ba9ea731036070aa9496e34cfeb
db6845e8aa9955416ba227970d3dd1f8207b5743e1490a7f5fd78d81fce0a24576de06a2f528d49c5b11e79a5cab015806ba
d73f118e205a3645a95b2b330ffd9da12e00c693e7ee8cfd04eb0f08c3c657c4fa0ae384ed2d5ab1e15ffc835c3e4cc116cd
1049611f896cf445ab36dc8b393a6fe75d20d45b2273a5d8c2d3b935e3f22bc82b24c952812d66a902155d288d5f26ac6722
fe72498bd72ea523c914c
@tag: 9b357baf76d2632fa7d16231640d6324
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
@digest: 40aff2e9d2d8922e47afd4648e6967497158785fbd1da870e7110266bf944880
@signature: 719fa9898f3423b754675b835268f9b2368b77a429eeabf7369d60d135dee08158c3902fd2ed3c1bf17cb34e
76f2ba25da915fa3970c757962f7533c8d8bad7d
@@TEE_FreeOperation:
verify ok
ecall_ta_main() end
--- enclave log end---
res = TEEC_SUCCESS; TEEC_InvokeCommand succeeded!
```

If executed successfully, you see above messages

5.6 ta-ref with SGX

Build ta-ref for Intel SGX platforms

5.6.1 Cloning source and building

Clone the source

```
$ git clone https://192.168.100.100/rinkai/ta-ref.git
$ cd ta-ref
$ git checkout teep-device-tb-slim
$ git submodule sync --recursive
$ git submodule update --init --recursive
```

Build

```
$ source /opt/intel/sgxsdk/environment
$ source env/sgx_x64.sh
$ make build test-bin MACHINE=NUC TEST_DIR=test_hello
$ make build test-bin MACHINE=NUC TEST_DIR=test_gp
```

5.6.2 Check ta-ref by running test_gp, test_hello, simulation mode on any pc

Copy the ta-ref's test_hello & test_gp executables to test directory

5.6.2.1 test_hello

Run test_hello

```
$ cp test_hello/sgx/Enclave/enclave.signed.so <test directory>
$ cp test_hello/sgx/App/sgx_app <test directory>
$ <test directory>/sgx_app
hello world!
Info: Enclave successfully returned.
```

5.6.2.2 test_gp

Run test_gp

```
$ cp test_gp/sgx/Enclave/enclave.signed.so <test directory>
$ cp test_gp/sgx/App/sgx_app <test directory>
$ <test directory>/sgx_app
main start
TEE_GenerateRandom(): start
@random: f35c1d1e4bbf6641c5511c9dc5aaf638
TEE_GetREETime(): start
request to get unix time 1612257364, 199
@GP REE time 1612257364 sec 199 millis
TEE_GetSystemTime(): start
@GP System time 727941859 sec 984 millis
TEE_CreatePersistentObject(): start
request to open FileOne flags 241 -> 3
TEE_WriteObjectData(): start
request to write 256 bytes to descriptor 3
TEE_CloseObject(): start
request to close descriptor 3
TEE_OpenPersistentObject(): start
request to open FileOne flags 0 -> 3
TEE_ReadObjectData(): start
request to read 256 bytes from descriptor 3
TEE_CloseObject(): start
request to close descriptor 3
256 bytes read: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728 29
2a2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b
5c5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d
8e8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebf
c0c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1
f2f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
```

```
hash: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateTransientObject(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(): start
TEE_AllocateOperation(): start
TEE_GenerateRandom(): start
TEE_CipherInit(): start
TEE_CipherUpdate(): start
TEE_FreeOperation(): start
@cipher: 7427bff21e729a824a239e25332ebd455d18fa6aec1ec6618b77c252f768e0a9345608b0135727568867ce5b0fa
c872f6647787861b88220840281f3944eea456a2769081e6598079b52edc541e2201ffd2e96a6c3e485be25a0ce4f5c07544
aa0c67b3e34bd069b293843daf66db51b751b3c09f2a9c6912c22a6062c8ecbd0effd4698081660e218f6f0c1249e3691a33
e91836953953513040eb29ce709efe50f96e67f07d6a1b00f08beacebc5950f9744b0049cb76ec5ba17a49d7270b60034c47
23bb79dc61d465062b0394e8d93f98c2391ee2b02b7b537b375e0e1cc5eeb8eb2e62df839048db0f1fdbdd1b7f5c6ef2faa1
a5b305ef045936c9146f8
TEE_AllocateOperation(): start
TEE_CipherInit(): start
TEE_CipherUpdate(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
TEE_AllocateTransientObject(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(): start
TEE_AllocateOperation(): start
TEE_GenerateRandom(): start
TEE_AEInit(): start
TEE_AEEncryptFinal(): start
TEE_FreeOperation(): start
@cipher: e33f34122c80b9a10002725e4e21542256da7c7cd3f6dd1b62b71cf8308f9e4a0daa50b29880a8f76707c4ed432
549c4da9e68e7930189d2127fdd7aa2379106090814b5deed9a9e161ef0886da03a2a94c3fb9e0faadfd1ce8bb09fb5388bb
23a042944fbe269d486aa4f21a91a41968184122520dfc308850059efce660a52adb17361bd52f570bfba05cccad32ffa9ea
c94914725ded073355f28eb3dc30d60f00cfd2de76c3a05df8bef32f302bb4d14b493a3a90b1dee4eba64e625695c4d58ec4
febf8436d62e4cac82fcbd00e60c8138af7176995a742b08a572f64e539e9f9850a9f6f33907a829108ca6540332aab53f3f
6a4fd2c3de35c5556a427
@tag: 4c920ce2aef079e468ab24e25730d9d2
TEE_AllocateOperation(): start
TEE_AEInit(): start
TEE_AEDecryptFinal(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
@digest: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateOperation(): start
TEE_AllocateTransientObject(): start
TEE_InitValueAttribute(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(): start
TEE_AsymmetricSignDigest(): start
TEE_FreeOperation(): start
@signature: 100b392ce043e9b8dc703088f505dd3083ec47bfcb8d59d968a66b54e80464d684d56dc9c44336f08fd96309
79863a2d8fb7cd672a819ef609357e9ac6a3d80e
TEE_AllocateOperation(): start
TEE_AsymmetricVerifyDigest(): start
TEE_FreeOperation(): start
@@TEE_FreeOperation:
TEE_FreeTransientObject(): start
verify ok
main end
Info: Enclave successfully returned.
```

6 Running on Development Boards

6.1 Keystone, Unleased

Make sure Keystone and other dependant sources have been built

6.1.1 Preparation of rootfs on SD Card

Build a modified gdisk which can handle the sifive specific partition types.

Prerequisites: libncursesw5-dev, libpopt-dev

```
$ cd ..
$ sudo apt install libncursesw5-dev lib64ncurses5-dev uuid-dev libpopt-dev build-essential
$ git clone https://192.168.100.100/rinkai/gptfdisk.git
$ cd gptfdisk
$ git checkout -b risc-v-sd 3d6a15873f582803aa8ad3288b3e32d3daff9fde
$ make
```

6.1.1.1 Create SD-card partition manually

```
$ sudo ./gdisk /dev/mmcblk0
GPT fdisk (gdisk) version 1.0.4
Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present
Found valid GPT with protective MBR; using GPT.
Command (? for help): n
Partition number (1-128, default 1): 1
First sector (34-15523806, default = 2048) or {+-}size{KMGTP}:
Last sector (2048-15523806, default = 15523806) or {+-}size{KMGTP}: 67583
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): 5202
Changed type of partition to 'SiFive bare-metal (or stage 2 loader)'
Command (? for help): n
Partition number (2-128, default 2): 4
First sector (34-15523806, default = 67584) or {+-}size{KMGTP}:
Last sector (67584-15523806, default = 15523806) or {+-}size{KMGTP}: 67839
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): 5201
Changed type of partition to 'SiFive FSBL (first-stage bootloader)'
Command (? for help): n
Partition number (2-128, default 2):
First sector (34-15523806, default = 69632) or {+-}size{KMGTP}: 264192
Last sector (264192-15523806, default = 15523806) or {+-}size{KMGTP}:
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): 8300
Changed type of partition to 'Linux filesystem'
Command (? for help): p
Disk /dev/mmcblk0: 15523840 sectors, 7.4 GiB
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): 11A0F8F6-D5DE-4993-8C0D-D543DFBA17AD
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 15523806
Partitions will be aligned on 2048-sector boundaries
Total free space is 198366 sectors (96.9 MiB)
Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048           67583   32.0 MiB    5202  SiFive bare-metal (...
   2          264192        15523806   7.3 GiB     8300  Linux filesystem
   4           67584           67839   128.0 KiB   5201  SiFive FSBL (first-...
Command (? for help): i
Partition number (1-4): 4
Partition GUID code: 5B193300-FC78-40CD-8002-E86C45580B47 (SiFive FSBL (first-stage bootloader))
Partition unique GUID: FC1FBC7C-EC94-4B0A-9DAF-0ED85452B885
First sector: 67584 (at 33.0 MiB)
```

```
Last sector: 67839 (at 33.1 MiB)
Partition size: 256 sectors (128.0 KiB)
Attribute flags: 0000000000000000
Partition name: 'SiFive FSBL (first-stage bootloader)'
Command (? for help): i
Partition number (1-4): 1
Partition GUID code: 2E54B353-1271-4842-806F-E436D6AF6985 (SiFive bare-metal (or stage 2 loader))
Partition unique GUID: 2FFF07EF-E44A-4278-A16D-C29697C6653D
First sector: 2048 (at 1024.0 KiB)
Last sector: 67583 (at 33.0 MiB)
Partition size: 65536 sectors (32.0 MiB)
Attribute flags: 0000000000000000
Partition name: 'SiFive bare-metal (or stage 2 loader'
Command (? for help): wq
Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!
Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/mmcblk1.
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
```

6.1.1.2 Write boot and rootfs files into SD-card

Build FSBL for hifive-Unleased board

```
$ git clone https://github.com/keystone-enclave/freedom-u540-c000-bootloader.git
$ cd freedom-u540-c000-bootloader
$ git checkout -b dev-unleashed bbfcc288fb438312af51adef420aa444a0833452
$ # Make sure riscv64 compiler set to PATH (export PATH=$KEYSTONE_DIR/riscv/bin:$PATH)
$ make
```

Writing fsbl.bin and bbl.bin

```
$ sudo dd if=freedom-u540-c000-bootloader/fsbl.bin of=/dev/mmcblk0p4 bs=4096 conv=fsync
$ sudo dd if=$KEYSTONE_DIR/hifive-work/bbl.bin of=/dev/mmcblk0p1 bs=4096 conv=fsync
```

Once files written, insert the SD-card into unleased

6.1.2 Copying binaries of test_hello and test_gp

```
$ sudo mount /dev/mmcblk0p1 /media/rootfs/
$ sudo mkdir /media/rootfs/root/{test_hello,test_gp}
```

Copy test_hello

```
$ sudo cp ta-ref/test_hello/keystone/Enclave/Enclave.eapp_riscv /media/rootfs/root/test_hello/
$ sudo cp ta-ref/test_hello/keystone/Enclave/App.client /media/rootfs/root/test_hello/
$ sudo cp $KEYSTONE_SDK_DIR/rts/eyrie/eyrie-rt /media/rootfs/root/test_hello/
```

Copy test_gp

```
$ sudo cp ta-ref/test_gp/keystone/Enclave/Enclave.eapp_riscv /media/rootfs/root/test_gp/
$ sudo cp ta-ref/test_gp/keystone/Enclave/App.client /media/rootfs/root/test_gp/
$ sudo cp $KEYSTONE_SDK_DIR/rts/eyrie/eyrie-rt /media/rootfs/root/test_gp/
```

Now, we are ready to test on unleased board.

6.1.3 Check test_hello and test_gp on Unleased

1. Insert SD-card into unleased board
2. Boot Hifive-Unleased board
3. Connect Unleased board with your development machine over USB-Serial cable (/dev/ttyUSB1)
4. Checking on Unleased
   Login to serial console with user=root, passwd=sifive

```
buildroot login: root
Password:
$
```

test_hello:

```
$ insmod keystone-driver.ko
./App.client Enclave.eapp_riscv eyrie-rt
hello world!
```

test_gp:

```
$ insmod keystone-driver.ko
./App.client Enclave.eapp_riscv eyrie-rt
main start
TEE_GenerateRandom(0x000000003FFFFEE0, 16): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@random: 5ea8741bd8a3b298cf53d214eca693fb
TEE_GetREETime(): start
@[SE] gettimeofday 77 sec 865873 usec -> 0
@GP REE time 77 sec 865 millis
TEE_GetSystemTime(): start
@GP System time 100063195 sec 609 millis
TEE_CreatePersistentObject(): start
@[SE] open file FileOne flags 241 -> 3 (0)
TEE_WriteObjectData(): start
@[SE] write desc 3 buf 480d0 len 256-> 256
TEE_CloseObject(): start
@[SE] close desc 3 -> 0
TEE_OpenPersistentObject(): start
@[SE] open file FileOne flags 0 -> 3 (0)
TEE_ReadObjectData(): start
@[SE] read desc 3 buf fff41664 len 256-> 256
TEE_CloseObject(): start
@[SE] close desc 3 -> 0
256 bytes read: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292
2a2b2c2d2e2f303132333435363738393a3b3c3d3f
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
hash: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateTransientObject(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(0x000000003FFFFD88, 32): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AllocateOperation(): start
TEE_GenerateRandom(0x000000003FFFFED0, 16): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_CipherInit(): start
TEE_CipherUpdate(): start
TEE_FreeOperation(): start
@cipher: e94431cd22a6029185d0dbb1a17b5d62843bfeef25591583d2d668ec6fed1c692f88ce4754d690c346c8d9f2726
630e0386abf4e45699a2ca2b34b344eaa454bc489c
TEE_AllocateOperation(): start
TEE_CipherInit(): start
TEE_CipherUpdate(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f
verify ok
TEE_AllocateTransientObject(): start
```

```
TEE_GenerateKey(): start
TEE_GenerateRandom(0x000000003FFFFC68, 32): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AllocateOperation(): start
TEE_GenerateRandom(0x000000003FFFFEC8, 16): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AEInit(): start
TEE_AEEncryptFinal(): start
TEE_FreeOperation(): start
@cipher: c23e9ce04589e80a66debe23a788ae5393bdcd8e875e87e1bcf2b2d998f6418ccc6ee4ab112fdbfc5175868691e
fb40781a318ff439d30b49cc9f726886ad42d5be15
@tag: a551f999317b3fbd1eea7b622ce2caee
TEE_AllocateOperation(): start
TEE_AEInit(): start
TEE_AEDecryptFinal(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
@digest: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateOperation(): start
TEE_AllocateTransientObject(): start
TEE_InitValueAttribute(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(0x000000003FFFFE28, 32): start
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
@[SE] getrandom buf fff41844 len 16 flags 0 -> 16
TEE_AsymmetricSignDigest(): start
TEE_FreeOperation(): start
@signature: d6e6b6e54db8b6a62fc1927886938bead27f4813f19ce77182e3016b5426bcad067ca98cd75f9dfddafe9eb0
655c48df992d3ad674db69d831f26ae63caf1405
TEE_AllocateOperation(): start
TEE_AsymmetricVerifyDigest(): start
TEE_FreeOperation(): start
@@TEE_FreeOperation:
TEE_FreeTransientObject(): start
verify ok
main end
```

Test is successful.

6.2 OP-TEE, RPI3

Make sure OP-TEE v3.9.0 and other dependant sources have been built

6.2.1 Preparation of rootfs on SD Card

Use following examples to create partitions of boot and roots on SD-card

```
$ make img-help
$ fdisk /dev/sdx   # where sdx is the name of your sd-card
   > p             # prints partition table
   > d             # repeat until all partitions are deleted
   > n             # create a new partition
   > p             # create primary
   > 1             # make it the first partition
   > <enter>       # use the default sector
   > +32M          # create a boot partition with 32MB of space
   > n             # create rootfs partition
   > p
   > 2
   > <enter>
   > <enter>       # fill the remaining disk, adjust size to fit your needs
   > t             # change partition type
   > 1             # select first partition
   > e             # use type 'e' (FAT16)
   > a             # make partition bootable
```

```
    > 1             # select first partition
    > p             # double check everything looks right
    > w             # write partition table to disk.
```

Usually your SD-card detected as `/dev/mmcblk0`. After partition it looks like below BOOT partition = /dev/mmcblk0p1 rootfs partition = /dev/mmcblk0p2

Write boot file

```
$ mkfs.vfat -F16 -n BOOT /dev/mmcblk0p1
$ mkdir -p /media/boot
$ sudo mount /dev/mmcblk0p1 /media/boot
$ cd /media
$ gunzip -cd optee_3.9.0_rpi3/out-br/images/rootfs.cpio.gz | sudo cpio -idmv "boot/*"
$ umount boot
```

Write rootfs

```
$ mkfs.ext4 -L rootfs /dev/mmcblk0p2
$ mkdir -p /media/rootfs
$ sudo mount /dev/mmcblk0p2 /media/rootfs
$ cd rootfs
$ gunzip -cd <your-base-dir>/optee_3.9.0_rpi3/build/../out-br/images/rootfs.cpio.gz | sudo cpio
      -idmv
$ rm -rf /media/rootfs/boot/*
$ cd .. && sudo umount rootfs
```

If you use CI from AIST, download rpi3_sdimage as follows

```
$ wget http://192.168.100.100:2000/optee_rpi3_sdimage.tar.xz
$ tar xf optee_rpi3_sdimage.tar.xz
$ dd if=rpi3_sdimage.bin of=/dev/mmcblk0p2 conv=fsync bs=4096
```

Now SD-card is ready to boot RPI3.

6.2.2 Copying binaries of test_hello and test_gp to rootfs partition

Copying test_hello & test_gp

```
$ sudo mount /dev/mmcblk0p2 /media/rootfs
$ sudo mkdir -p /media/rootfs/home/gitlab/out/{test_hello,test_gp}
$ sudo cp ta-ref/test_hello/optee/App/optee_ref_ta /media/rootfs/home/gitlab/out/test_hello/
$ sudo cp ta-ref/test_hello/optee/Enclave/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
   /media/rootfs/home/gitlab/out/test_hello/
$ sudo cp ta-ref/test_gp/optee/App/optee_ref_ta /media/rootfs/home/gitlab/out/test_gp/
$ sudo cp ta-ref/test_gp/optee/Enclave/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
   /media/rootfs/home/gitlab/out/test_gp/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
$ sudo cp ta-ref/test_gp/optee/Enclave/Enclave.nm /media/rootfs/home/gitlab/out/test_gp/
```

6.2.3 Check test_hello and test_gp

1. Insert SD-card into RPI3 board, then power-on
2. Connect RPI3 board Serial console to your laptop (/dev/ttyUSB0 over minicom)
3. Checking on RPI3

Login to Serial console and enter "root" as username

```
buildroot login: root
Password:
$
```

test_hello:

```
$ cp /home/gitlab/out/test_hello/
$ cp a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta /home/gitlab/out/
$ ln -s /home/gitlab/out/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
    /lib64/optee_armtz/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
$ ./optee_ref_ta
--- enclave log start---
ecall_ta_main() start
hello world!
ecall_ta_main() end
--- enclave log end---
```

If executed successfully, you see above messages

test_gp:

```
$ cd /home/gitlab/out/test_gp/
$ cp a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta /home/gitlab/out/
$ ln -s /home/gitlab/out/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
  /lib64/optee_armtz/a6f77c1e-96fe-4a0e-9e74-262582a4c8f1.ta
$ ./optee_ref_ta
start TEEC_InvokeCommand
--- enclave log start---
ecall_ta_main() start
@random: fe0c7d3eefb9bd5e63b8a0cce29af7eb
@GP REE time 1612156259 sec 390 millis
@GP System time 249187 sec 954 millis
256 bytes read: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292
2a2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b
5c5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d
8e8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebf
c0c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1
f2f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
hash: 40aff2e9d2d8922e47afd4648e6967497158785fbd1da870e7110266bf944880
@cipher: 30a558176172c53be4a2ac320776de105da79c29726879fe67d06b629f065731285f8a90f8a521ce34eceea51e1
5e928d157ea10d149bb687dd78be79469c28696506283edcda527fcd86f6a47e852bbc3488df3fc651b46b034faf4ab5f12f
51a285478ea01e58d40e8177d415be243df93b23cdf889feb91fa3be8906fe190d836fe61168aed0473406be1054dd88a381
ef25381d920ea3780ba74fb1cfe1434cbd168de8386dcc2e2b92eee0fc432f3c0514f462cbeaf96753b174a4a673f323e671
61272fe932ead4bc95770fcc130dd5877b521d6a79f961eeadd1680042f69257ccf9368927aa170176af8ac211dd22161997
7224837232dad970220f4
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
@cipher: ff409d8fe203bf0d81de36832b86c702f07edd343f408d3a2fb5ab347b4f72b10031efff0c17b7e0bc56c3f2f95
f53c0d731ed87eb3e1187b6714a25cfc65082284682b44450941654e7edc99af0f7b037c3ba9ea731036070aa9496e34cfeb
db6845e8aa9955416ba227970d3dd1f8207b5743e1490a7f5fd78d81fce0a24576de06a2f528d49c5b11e79a5cab015806ba
d73f118e205a3645a95b2b330ffd9da12e00c693e7ee8cfd04eb0f08c3c657c4fa0ae384ed2d5ab1e15ffc835c3e4cc116cd
1049611f896cf445ab36dc8b393a6fe75d20d45b2273a5d8c2d3b935e3f22bc82b24c952812d66a902155d288d5f26ac6722
fe72498bd72ea523c914c
@tag: 9b357baf76d2632fa7d16231640d6324
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
@digest: 40aff2e9d2d8922e47afd4648e6967497158785fbd1da870e7110266bf944880
@signature: 719fa9898f3423b754675b835268f9b2368b77a429eeabf7369d60d135dee08158c3902fd2ed3c1bf17cb34e
76f2ba25da915fa3970c757962f7533c8d8bad7d
@@TEE_FreeOperation:
verify ok
ecall_ta_main() end
--- enclave log end---
res = TEEC_SUCCESS; TEEC_InvokeCommand succeeded!
```

If executed successfully, you see above messages

6.3 SGX, NUC

Make sure SGX SDK, sgx driver and other dependant sources have been built and installed on NUC machine

6.3.1 Copying binaries of test_hello and test_gp to NUC machine

Login to NUC machine over SSH (Assuming that SSH enabled on NIC machine). Assuming that `ta-ref` was natively built on NUC machine at `~/ta-ref`

```
$ ssh <ssh-user>@<IP-Address> 'mkdir -p ~/{test_hello,test_gp}'
$ scp ta-ref/test_hello/sgx/Enclave/enclave.signed.so <ssh-user>@<IP-Address>:~/test_hello
$ scp ta-ref/test_hello/sgx/App/sgx_app <ssh-user>@<IP-Address>:~/test_hello
$ scp ta-ref/test_gp/sgx/Enclave/enclave.signed.so <ssh-user>@<IP-Address>:~/test_gp
$ scp ta-ref/test_gp/sgx/App/sgx_app <ssh-user>@<IP-Address>:~/test_gp
```

Now can login to NUC machine for further testing.

6.3.2 Check test_hello and test_gp

Checking test_hello

```
$ cd ~/test_hello
$ ./sgx_app
hello world!
Info: Enclave successfully returned.
```

Checking test_gp

```
$ cd ~/test_gp
$ ./sgx_app
main start
TEE_GenerateRandom(): start
@random: f35c1d1e4bbf6641c5511c9dc5aaf638
TEE_GetREETime(): start
request to get unix time 1612257364, 199
@GP REE time 1612257364 sec 199 millis
TEE_GetSystemTime(): start
@GP System time 727941859 sec 984 millis
TEE_CreatePersistentObject(): start
request to open FileOne flags 241 -> 3
TEE_WriteObjectData(): start
request to write 256 bytes to descriptor 3
TEE_CloseObject(): start
request to close descriptor 3
TEE_OpenPersistentObject(): start
request to open FileOne flags 0 -> 3
TEE_ReadObjectData(): start
request to read 256 bytes from descriptor 3
TEE_CloseObject(): start
request to close descriptor 3
256 bytes read: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728 29
2a2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b
5c5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d
8e8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebf
c0c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1
f2f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
hash: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateTransientObject(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(): start
TEE_AllocateOperation(): start
TEE_GenerateRandom(): start
TEE_CipherInit(): start
TEE_CipherUpdate(): start
```

```
TEE_FreeOperation(): start
@cipher: 7427bff21e729a824a239e25332ebd455d18fa6aec1ec6618b77c252f768e0a9345608b0135727568867ce5b0fa
c872f6647787861b88220840281f3944eea456a2769081e6598079b52edc541e2201ffd2e96a6c3e485be25a0ce4f5c07544
aa0c67b3e34bd069b293843daf66db51b751b3c09f2a9c6912c22a6062c8ecbd0effd4698081660e218f6f0c1249e3691a33
e91836953953513040eb29ce709efe50f96e67f07d6a1b00f08beacebc5950f9744b0049cb76ec5ba17a49d7270b60034c47
23bb79dc61d465062b0394e8d93f98c2391ee2b02b7b537b375e0e1cc5eeb8eb2e62df839048db0f1fdbdd1b7f5c6ef2faa1
a5b305ef045936c9146f8
TEE_AllocateOperation(): start
TEE_CipherInit(): start
TEE_CipherUpdate(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
TEE_AllocateTransientObject(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(): start
TEE_AllocateOperation(): start
TEE_GenerateRandom(): start
TEE_AEInit(): start
TEE_AEEncryptFinal(): start
TEE_FreeOperation(): start
@cipher: e33f34122c80b9a10002725e4e21542256da7c7cd3f6dd1b62b71cf8308f9e4a0daa50b29880a8f76707c4ed432
549c4da9e68e7930189d2127fdd7aa2379106090814b5deed9a9e161ef0886da03a2a94c3fb9e0faadfd1ce8bb09fb5388bb
23a042944fbe269d486aa4f21a91a41968184122520dfc308850059efce660a52adb17361bd52f570bfba05cccad32ffa9ea
c94914725ded073355f28eb3dc30d60f00cfd2de76c3a05df8bef32f302bb4d14b493a3a90b1dee4eba64e625695c4d58ec4
febf8436d62e4cac82fcbd00e60c8138af7176995a742b08a572f64e539e9f9850a9f6f33907a829108ca6540332aab53f3f
6a4fd2c3de35c5556a427
@tag: 4c920ce2aef079e468ab24e25730d9d2
TEE_AllocateOperation(): start
TEE_AEInit(): start
TEE_AEDecryptFinal(): start
TEE_FreeOperation(): start
TEE_FreeTransientObject(): start
decrypted to: 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a
2b2c2d2e2f303132333435363738393a3b3c3d3e3f404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c
5d5e5f606162636465666768696a6b6c6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e
8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0
c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4e5e6e7e8e9eaebecedeeeff0f1f2
f3f4f5f6f7f8f9fafbfcfdfeff
verify ok
TEE_AllocateOperation(): start
TEE_FreeOperation(): start
TEE_DigestDoFinal(): start
TEE_FreeOperation(): start
@digest: 9b04c091da96b997afb8f2585d608aebe9c4a904f7d52c8f28c7e4d2dd9fba5f
TEE_AllocateOperation(): start
TEE_AllocateTransientObject(): start
TEE_InitValueAttribute(): start
TEE_GenerateKey(): start
TEE_GenerateRandom(): start
TEE_AsymmetricSignDigest(): start
TEE_FreeOperation(): start
@signature: 100b392ce043e9b8dc703088f505dd3083ec47bfcb8d59d968a66b54e80464d684d56dc9c44336f08fd96309
79863a2d8fb7cd672a819ef609357e9ac6a3d80e
TEE_AllocateOperation(): start
TEE_AsymmetricVerifyDigest(): start
TEE_FreeOperation(): start
@@TEE_FreeOperation:
TEE_FreeTransientObject(): start
verify ok
main end
Info: Enclave successfully returned.
```

7 Class Index

7.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

8 File Index

8.1 File List

Here is a list of all files with brief descriptions:

9 Class Documentation

9.1 __TEE_ObjectHandle Struct Reference

```
#include <tee_api_tee_types.h>
```

Public Attributes

- unsigned int type
- int flags
- int desc
- mbedtls_aes_context persist_ctx
- unsigned char persist_iv [TEE_OBJECT_NONCE_SIZE]
- unsigned char public_key [TEE_OBJECT_KEY_SIZE]
- unsigned char private_key [TEE_OBJECT_SKEY_SIZE]

9.1.1 Member Data Documentation

9.1.1.1 desc `int __TEE_ObjectHandle::desc`

9.1.1.2 flags `int __TEE_ObjectHandle::flags`

9.1.1.3 persist_ctx `mbedtls_aes_context __TEE_ObjectHandle::persist_ctx`

9.1.1.4 persist_iv `unsigned char __TEE_ObjectHandle::persist_iv`

9.1.1.5 private_key `unsigned char __TEE_ObjectHandle::private_key`

9.1.1.6 public_key `unsigned char __TEE_ObjectHandle::public_key`

9.1.1.7 type `unsigned int __TEE_ObjectHandle::type`

The documentation for this struct was generated from the following files:

- ta-ref/api/keystone/tee_api_tee_types.h
- ta-ref/api/sgx/tee_api_tee_types.h

9.2 __TEE_OperationHandle Struct Reference

```
#include <tee_api_tee_types.h>
```

Public Attributes

- int mode
- int flags
- int alg
- sha3_ctx_t ctx
- mbedtls_aes_context aectx
- mbedtls_gcm_context aegcmctx
- int aegcm_state
- unsigned char aeiv [TEE_OBJECT_NONCE_SIZE]
- unsigned char aekey [32]
- unsigned char pubkey [TEE_OBJECT_KEY_SIZE]
- unsigned char prikey [TEE_OBJECT_SKEY_SIZE]

9.2.1 Member Data Documentation

9.2.1.1 aectx `mbedtls_aes_context __TEE_OperationHandle::aectx`

9.2.1.2 aegcm_state `int __TEE_OperationHandle::aegcm_state`

9.2.1.3 aegcmctx `mbedtls_gcm_context __TEE_OperationHandle::aegcmctx`

9.2.1.4 aeiv `unsigned char __TEE_OperationHandle::aeiv`

9.2.1.5 aekey `unsigned char __TEE_OperationHandle::aekey`

9.2.1.6 alg `int __TEE_OperationHandle::alg`

9.2.1.7 ctx `sha3_ctx_t __TEE_OperationHandle::ctx`

9.2.1.8 flags `int __TEE_OperationHandle::flags`

9.2.1.9 mode `int __TEE_OperationHandle::mode`

9.2.1.10 prikey `unsigned char __TEE_OperationHandle::prikey`

9.2.1.11 pubkey `unsigned char __TEE_OperationHandle::pubkey`

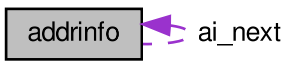
The documentation for this struct was generated from the following files:

- ta-ref/api/keystone/tee_api_tee_types.h
- ta-ref/api/sgx/tee_api_tee_types.h

9.3 addrinfo Struct Reference

```
#include <tee_api_types.h>
```

Collaboration diagram for addrinfo:



Public Attributes

- int ai_flags
- int ai_family
- int ai_socktype
- int ai_protocol
- socklen_t ai_addrlen
- struct sockaddr ∗ ai_addr
- char ∗ ai_canonname
- struct addrinfo ∗ ai_next

9.3.1 Member Data Documentation

9.3.1.1 ai_addr `struct sockaddr* addrinfo::ai_addr`

9.3.1.2 ai_addrlen `socklen_t addrinfo::ai_addrlen`

9.3.1.3 ai_canonname `char* addrinfo::ai_canonname`

9.3.1.4 ai_family `int addrinfo::ai_family`

9.3.1.5 ai_flags `int addrinfo::ai_flags`

9.3.1.6 ai_next `struct addrinfo* addrinfo::ai_next`

9.3.1.7 ai_protocol `int addrinfo::ai_protocol`

9.3.1.8 ai_socktype `int addrinfo::ai_socktype`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.4 enclave_report Struct Reference

```
#include <report.h>
```

Public Attributes

- uint8_t hash [MDSIZE]
- uint64_t data_len
- uint8_t data [ATTEST_DATA_MAXLEN]
- uint8_t signature [SIGNATURE_SIZE]

9.4.1 Member Data Documentation

9.4.1.1 data `uint8_t enclave_report::data[ATTEST_DATA_MAXLEN]`

9.4.1.2 data_len `uint64_t enclave_report::data_len`

9.4.1.3 hash `uint8_t enclave_report::hash[MDSIZE]`

9.4.1.4 signature `uint8_t enclave_report::signature[SIGNATURE_SIZE]`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/report.h

9.5 out_fct_wrap_type Struct Reference

Public Attributes

- void(∗ fct)(char character, void ∗arg)
- void ∗ arg

9.5.1 Member Data Documentation

9.5.1.1 arg `void* out_fct_wrap_type::arg`

9.5.1.2 fct `void(* out_fct_wrap_type::fct) (char character, void *arg)`

The documentation for this struct was generated from the following file:

- ta-ref/api/keystone/vsnprintf.c

9.6 pollfd Struct Reference

`#include <tee_api_types.h>`

Public Attributes

- int fd
- short int events
- short int revents

9.6.1 Member Data Documentation

9.6.1.1 events `short int pollfd::events`

9.6.1.2 fd `int pollfd::fd`

9.6.1.3 revents `short int pollfd::revents`

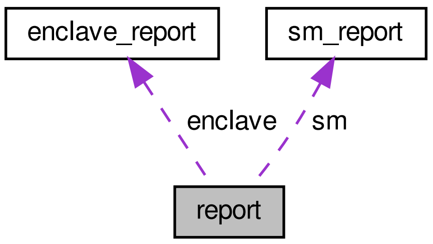
The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.7 report Struct Reference

`#include <report.h>`

Collaboration diagram for report:



Public Attributes

- struct enclave_report enclave
- struct sm_report sm
- uint8_t dev_public_key [PUBLIC_KEY_SIZE]

9.7.1 Member Data Documentation

9.7.1.1 dev_public_key `uint8_t report::dev_public_key[PUBLIC_KEY_SIZE]`

9.7.1.2 enclave `struct enclave_report report::enclave`

9.7.1.3 sm `struct sm_report report::sm`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/report.h

9.8 sm_report Struct Reference

`#include <report.h>`

Public Attributes

- uint8_t hash [MDSIZE]
- uint8_t public_key [PUBLIC_KEY_SIZE]
- uint8_t signature [SIGNATURE_SIZE]

9.8.1 Member Data Documentation

9.8.1.1 hash `uint8_t sm_report::hash[MDSIZE]`

9.8.1.2 public_key `uint8_t sm_report::public_key[PUBLIC_KEY_SIZE]`

9.8.1.3 signature `uint8_t sm_report::signature[SIGNATURE_SIZE]`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/report.h

9.9 TEE_Attribute Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- uint32_t attributeID
- union {
  struct {
  void ∗ buffer
  uint32_t length
  } ref
  struct {
  uint32_t a
  uint32_t b
  } value
  } content

9.9.1 Member Data Documentation

9.9.1.1 a `uint32_t TEE_Attribute::a`

9.9.1.2 attributeID `uint32_t TEE_Attribute::attributeID`

9.9.1.3 b `uint32_t TEE_Attribute::b`

9.9.1.4 buffer `void* TEE_Attribute::buffer`

9.9.1.5 `union { ... } TEE_Attribute::content`

9.9.1.6 length `uint32_t TEE_Attribute::length`

9.9.1.7 `struct { ... } TEE_Attribute::ref`

9.9.1.8 `struct { ... } TEE_Attribute::value`

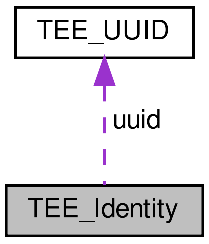
The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.10 TEE_Identity Struct Reference

```
#include <tee_api_types.h>
```

Collaboration diagram for TEE_Identity:



Public Attributes

- uint32_t login
- TEE_UUID uuid

9.10.1 Member Data Documentation

9.10.1.1 login `uint32_t TEE_Identity::login`

9.10.1.2 uuid `TEE_UUID TEE_Identity::uuid`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.11 TEE_ObjectInfo Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- uint32_t objectType
- union {
    uint32_t keySize
    uint32_t objectSize
  };
- union {
    uint32_t maxKeySize
    uint32_t maxObjectSize
  };
- uint32_t objectUsage
- uint32_t dataSize
- uint32_t dataPosition
- uint32_t handleFlags

9.11.1 Member Data Documentation

9.11.1.1 `__extension__ union { ... } TEE_ObjectInfo::@3`

9.11.1.2 `__extension__ union { ... } TEE_ObjectInfo::@5`

9.11.1.3 dataPosition `uint32_t TEE_ObjectInfo::dataPosition`

9.11.1.4 dataSize `uint32_t TEE_ObjectInfo::dataSize`

9.11.1.5 handleFlags `uint32_t TEE_ObjectInfo::handleFlags`

9.11.1.6 keySize `uint32_t TEE_ObjectInfo::keySize`

9.11.1.7 maxKeySize `uint32_t TEE_ObjectInfo::maxKeySize`

9.11.1.8 maxObjectSize `uint32_t TEE_ObjectInfo::maxObjectSize`

9.11.1.9 objectSize `uint32_t TEE_ObjectInfo::objectSize`

9.11.1.10 objectType `uint32_t TEE_ObjectInfo::objectType`

9.11.1.11 objectUsage `uint32_t TEE_ObjectInfo::objectUsage`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.12 TEE_OperationInfo Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- uint32_t algorithm
- uint32_t operationClass
- uint32_t mode
- uint32_t digestLength
- uint32_t maxKeySize
- uint32_t keySize
- uint32_t requiredKeyUsage
- uint32_t handleState

9.12.1 Member Data Documentation

9.12.1.1 algorithm `uint32_t TEE_OperationInfo::algorithm`

9.12.1.2 digestLength `uint32_t TEE_OperationInfo::digestLength`

9.12.1.3 handleState `uint32_t TEE_OperationInfo::handleState`

9.12.1.4 keySize `uint32_t TEE_OperationInfo::keySize`

9.12.1.5 maxKeySize `uint32_t TEE_OperationInfo::maxKeySize`

9.12.1.6 mode `uint32_t TEE_OperationInfo::mode`

9.12.1.7 operationClass `uint32_t TEE_OperationInfo::operationClass`

9.12.1.8 requiredKeyUsage `uint32_t TEE_OperationInfo::requiredKeyUsage`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.13 TEE_OperationInfoKey Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- uint32_t keySize
- uint32_t requiredKeyUsage

9.13.1 Member Data Documentation

9.13.1.1 keySize `uint32_t TEE_OperationInfoKey::keySize`

9.13.1.2 requiredKeyUsage `uint32_t TEE_OperationInfoKey::requiredKeyUsage`

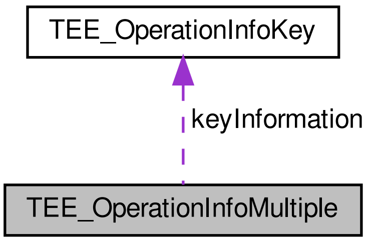
The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.14 TEE_OperationInfoMultiple Struct Reference

`#include <tee_api_types.h>`

Collaboration diagram for TEE_OperationInfoMultiple:



Public Attributes

- uint32_t algorithm
- uint32_t operationClass
- uint32_t mode
- uint32_t digestLength
- uint32_t maxKeySize
- uint32_t handleState
- uint32_t operationState
- uint32_t numberOfKeys
- TEE_OperationInfoKey keyInformation [ ]

9.14.1 Member Data Documentation

9.14.1.1 algorithm `uint32_t TEE_OperationInfoMultiple::algorithm`

9.14.1.2 digestLength `uint32_t TEE_OperationInfoMultiple::digestLength`

9.14.1.3 handleState `uint32_t TEE_OperationInfoMultiple::handleState`

9.14.1.4 keyInformation `TEE_OperationInfoKey TEE_OperationInfoMultiple::keyInformation[ ]`

9.14.1.5 maxKeySize `uint32_t TEE_OperationInfoMultiple::maxKeySize`

9.14.1.6 mode `uint32_t TEE_OperationInfoMultiple::mode`

9.14.1.7 numberOfKeys `uint32_t TEE_OperationInfoMultiple::numberOfKeys`

9.14.1.8 operationClass `uint32_t TEE_OperationInfoMultiple::operationClass`

9.14.1.9 operationState `uint32_t TEE_OperationInfoMultiple::operationState`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.15 TEE_Param Union Reference

```
#include <tee_api_types.h>
```

Public Attributes

- struct {
  void ∗ buffer
  uint32_t size
  } memref
- struct {
  uint32_t a
  uint32_t b
  } value

9.15.1 Member Data Documentation

9.15.1.1 a `uint32_t TEE_Param::a`

9.15.1.2 b `uint32_t TEE_Param::b`

9.15.1.3 buffer `void* TEE_Param::buffer`

9.15.1.4 `struct { ... } TEE_Param::memref`

9.15.1.5 size `uint32_t TEE_Param::size`

9.15.1.6 `struct { ... } TEE_Param::value`

The documentation for this union was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.16 TEE_SEAID Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- uint8_t ∗ buffer
- size_t bufferLen

9.16.1 Member Data Documentation

9.16.1.1 buffer `uint8_t* TEE_SEAID::buffer`

9.16.1.2 bufferLen `size_t TEE_SEAID::bufferLen`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.17 TEE_SEReaderProperties Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- bool sePresent
- bool teeOnly
- bool selectResponseEnable

9.17.1 Member Data Documentation

9.17.1.1 selectResponseEnable `bool TEE_SEReaderProperties::selectResponseEnable`

9.17.1.2 sePresent `bool TEE_SEReaderProperties::sePresent`

9.17.1.3 teeOnly `bool TEE_SEReaderProperties::teeOnly`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.18 TEE_Time Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- uint32_t seconds
- uint32_t millis

9.18.1 Member Data Documentation

9.18.1.1 millis `uint32_t TEE_Time::millis`

9.18.1.2 seconds `uint32_t TEE_Time::seconds`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.19 TEE_UUID Struct Reference

```
#include <tee_api_types.h>
```

Public Attributes

- uint32_t timeLow
- uint16_t timeMid
- uint16_t timeHiAndVersion
- uint8_t clockSeqAndNode [8]

9.19.1 Member Data Documentation

9.19.1.1 clockSeqAndNode `uint8_t TEE_UUID::clockSeqAndNode[8]`

9.19.1.2 timeHiAndVersion `uint16_t TEE_UUID::timeHiAndVersion`

9.19.1.3 timeLow `uint32_t TEE_UUID::timeLow`

9.19.1.4 timeMid `uint16_t TEE_UUID::timeMid`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_api_types.h

9.20 TEEC_Context Struct Reference

```
#include <tee_client_api.h>
```

Public Attributes

- int fd
- bool reg_mem

9.20.1 Detailed Description

struct TEEC_Context - Represents a connection between a client application and a TEE.

9.20.2 Member Data Documentation

9.20.2.1 fd `int TEEC_Context::fd`

9.20.2.2 reg_mem `bool TEEC_Context::reg_mem`

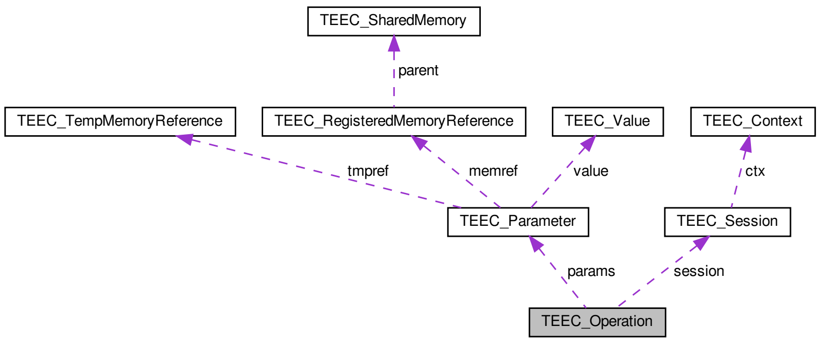
The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.21 TEEC_Operation Struct Reference

```
#include <tee_client_api.h>
```

Collaboration diagram for TEEC_Operation:



Public Attributes

- uint32_t started
- uint32_t paramTypes
- TEEC_Parameter params [TEEC_CONFIG_PAYLOAD_REF_COUNT]
- TEEC_Session ∗ session

9.21.1 Detailed Description

struct TEEC_Operation - Holds information and memory references used in TEEC_InvokeCommand().

Parameters

started	Client must initialize to zero if it needs to cancel an operation about to be performed.
paramTypes	Type of data passed. Use TEEC_PARAMS_TYPE macro to create the correct flags. 0 means TEEC_NONE is passed for all params.
params	Array of parameters of type TEEC_Parameter.
session	Internal pointer to the last session used by TEEC_InvokeCommand with this operation.

9.21.2 Member Data Documentation

9.21.2.1 params `TEEC_Parameter TEEC_Operation::params[TEEC_CONFIG_PAYLOAD_REF_COUNT]`

9.21.2.2 paramTypes `uint32_t TEEC_Operation::paramTypes`

9.21.2.3 session `TEEC_Session* TEEC_Operation::session`

9.21.2.4 started `uint32_t TEEC_Operation::started`

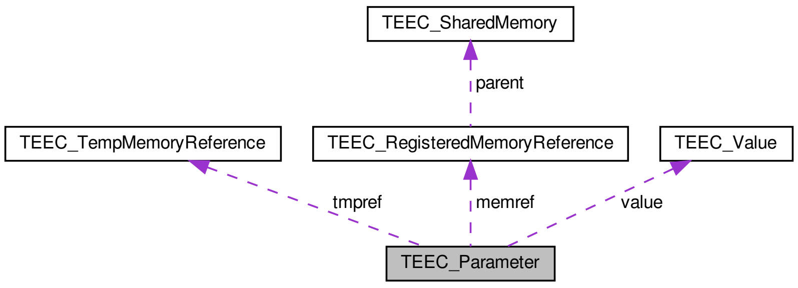
The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.22 TEEC_Parameter Union Reference

`#include <tee_client_api.h>`

Collaboration diagram for TEEC_Parameter:



Public Attributes

- TEEC_TempMemoryReference tmpref
- TEEC_RegisteredMemoryReference memref
- TEEC_Value value

9.22.1 Detailed Description

union TEEC_Parameter - Memory container to be used when passing data between client application and trusted code.

Either the client uses a shared memory reference, parts of it or a small raw data container.

Parameters

tmpref	A temporary memory reference only valid for the duration of the operation.
memref	The entire shared memory or parts of it.
value	The small raw data container to use

9.22.2 Member Data Documentation

9.22.2.1 memref `TEEC_RegisteredMemoryReference TEEC_Parameter::memref`

9.22.2.2 tmpref `TEEC_TempMemoryReference TEEC_Parameter::tmpref`

9.22.2.3 value `TEEC_Value TEEC_Parameter::value`

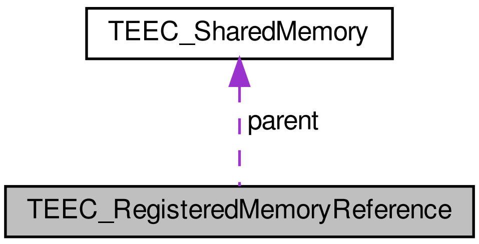
The documentation for this union was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.23 TEEC_RegisteredMemoryReference Struct Reference

```
#include <tee_client_api.h>
```

Collaboration diagram for TEEC_RegisteredMemoryReference:



Public Attributes

- TEEC_SharedMemory ∗ parent
- size_t size
- size_t offset

9.23.1 Detailed Description

struct TEEC_RegisteredMemoryReference - use a pre-registered or pre-allocated shared memory block of memory to transfer data between a client application and trusted code.

Parameters

parent	Points to a shared memory structure. The memory reference may utilize the whole shared memory or only a part of it. Must not be NULL
size	The size, in bytes, of the memory buffer.
offset	The offset, in bytes, of the referenced memory region from the start of the shared memory block.

9.23.2 Member Data Documentation

9.23.2.1 offset `size_t TEEC_RegisteredMemoryReference::offset`

9.23.2.2 parent `TEEC_SharedMemory* TEEC_RegisteredMemoryReference::parent`

9.23.2.3 size `size_t TEEC_RegisteredMemoryReference::size`

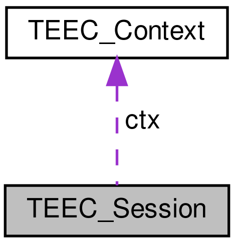
The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.24 TEEC_Session Struct Reference

```
#include <tee_client_api.h>
```

Collaboration diagram for TEEC_Session:



Public Attributes

- TEEC_Context * ctx
- uint32_t session_id

9.24.1 Detailed Description

struct TEEC_Session - Represents a connection between a client application and a trusted application.

9.24.2 Member Data Documentation

9.24.2.1 ctx `TEEC_Context* TEEC_Session::ctx`

9.24.2.2 session_id `uint32_t TEEC_Session::session_id`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.25 TEEC_SharedMemory Struct Reference

```
#include <tee_client_api.h>
```

Public Attributes

- void ∗ buffer
- size_t size
- uint32_t flags
- int id
- size_t alloced_size
- void ∗ shadow_buffer
- int registered_fd
- bool buffer_allocated

9.25.1 Detailed Description

struct TEEC_SharedMemory - Memory to transfer data between a client application and trusted code.

Parameters

buffer	The memory buffer which is to be, or has been, shared with the TEE.
size	The size, in bytes, of the memory buffer.
flags	Bit-vector which holds properties of buffer. The bit-vector can contain either or both of the TEEC_MEM_INPUT and TEEC_MEM_OUTPUT flags.

A shared memory block is a region of memory allocated in the context of the client application memory space that can be used to transfer data between that client application and a trusted application. The user of this struct is responsible to populate the buffer pointer.

9.25.2 Member Data Documentation

9.25.2.1 alloced_size `size_t TEEC_SharedMemory::alloced_size`

9.25.2.2 buffer `void* TEEC_SharedMemory::buffer`

9.25.2.3 buffer_allocated `bool TEEC_SharedMemory::buffer_allocated`

9.25.2.4 flags `uint32_t TEEC_SharedMemory::flags`

9.25.2.5 id `int TEEC_SharedMemory::id`

9.25.2.6 registered_fd `int TEEC_SharedMemory::registered_fd`

9.25.2.7 shadow_buffer `void* TEEC_SharedMemory::shadow_buffer`

9.25.2.8 size `size_t TEEC_SharedMemory::size`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.26 TEEC_TempMemoryReference Struct Reference

```
#include <tee_client_api.h>
```

Public Attributes

- void ∗ buffer
- size_t size

9.26.1 Detailed Description

struct TEEC_TempMemoryReference - Temporary memory to transfer data between a client application and trusted code, only used for the duration of the operation.

Parameters

buffer	The memory buffer which is to be, or has been shared with the TEE.
size	The size, in bytes, of the memory buffer.

A memory buffer that is registered temporarily for the duration of the operation to be called.

9.26.2 Member Data Documentation

9.26.2.1 buffer `void* TEEC_TempMemoryReference::buffer`

9.26.2.2 size `size_t TEEC_TempMemoryReference::size`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.27 TEEC_UUID Struct Reference

```
#include <tee_client_api.h>
```

Public Attributes

- uint32_t timeLow
- uint16_t timeMid
- uint16_t timeHiAndVersion
- uint8_t clockSeqAndNode [8]

9.27.1 Detailed Description

This type contains a Universally Unique Resource Identifier (UUID) type as defined in RFC4122. These UUID values are used to identify Trusted Applications.

9.27.2 Member Data Documentation

9.27.2.1 clockSeqAndNode `uint8_t TEEC_UUID::clockSeqAndNode[8]`

9.27.2.2 timeHiAndVersion `uint16_t TEEC_UUID::timeHiAndVersion`

9.27.2.3 timeLow `uint32_t TEEC_UUID::timeLow`

9.27.2.4 timeMid `uint16_t TEEC_UUID::timeMid`

The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

9.28 TEEC_Value Struct Reference

```
#include <tee_client_api.h>
```

Public Attributes

- uint32_t a
- uint32_t b

9.28.1 Detailed Description

struct TEEC_Value - Small raw data container

Instead of allocating a shared memory buffer this structure can be used to pass small raw data between a client application and trusted code.

Parameters

a	The first integer value.
b	The second second value.

9.28.2 Member Data Documentation

9.28.2.1 a `uint32_t TEEC_Value::a`

9.28.2.2 b `uint32_t TEEC_Value::b`

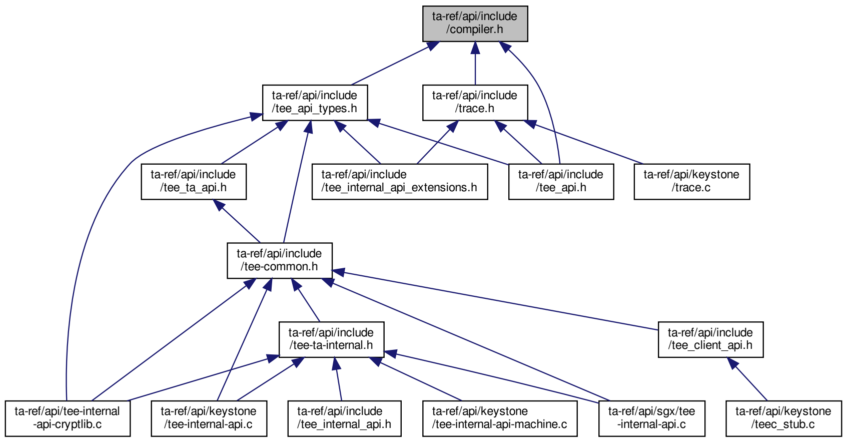
The documentation for this struct was generated from the following file:

- ta-ref/api/include/tee_client_api.h

10 File Documentation

10.1 ta-ref/api/include/compiler.h File Reference

This graph shows which files directly or indirectly include this file:


ta-ref/api/include/compiler.h
ta-ref/api/include/tee_api_types.h
ta-ref/api/include/trace.h
ta-ref/api/include/tee_ta_api.h
ta-ref/api/include/tee_internal_api_extensions.h
ta-ref/api/include/tee_api.h
ta-ref/api/keystone/trace.c
ta-ref/api/include/tee-common.h
ta-ref/api/include/tee-ta-internal.h
ta-ref/api/include/tee_client_api.h
ta-ref/api/tee-internal-api-cryptlib.c
ta-ref/api/keystone/tee-internal-api.c
ta-ref/api/include/tee_internal_api.h
ta-ref/api/keystone/tee-internal-api-machine.c
ta-ref/api/sgx/tee-internal-api.c
ta-ref/api/keystone/teec_stub.c

10.2 compiler.h

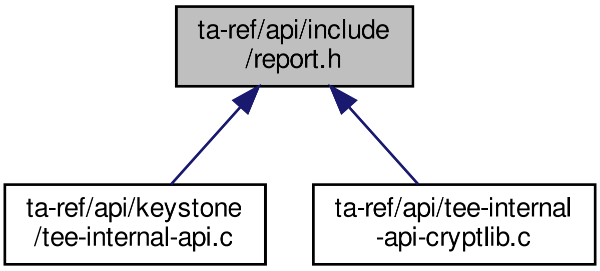
Go to the documentation of this file.

```c
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */

#ifndef COMPILER_H
#define COMPILER_H

#ifndef DOXYGEN_SHOULD_SKIP_THIS
/*
 * Macros that should be used instead of using __attribute__ directly to
 * ease portability and make the code easier to read.
 */

#define __deprecated    __attribute__((deprecated))
#define __packed    __attribute__((packed))
#define __weak      __attribute__((weak))
```

```
#define __noreturn  __attribute__((noreturn))
#define __pure      __attribute__((pure))
#define __aligned(x)    __attribute__((aligned(x)))
#define __printf(a, b)  __attribute__((format(printf, a, b)))
#define __noinline  __attribute__((noinline))
#define __attr_const    __attribute__((__const__))
#define __unused    __attribute__((unused))
#define __maybe_unused  __attribute__((unused))
#define __used      __attribute__((__used__))
#define __must_check    __attribute__((warn_unused_result))
#define __cold      __attribute__((__cold__))
#define __section(x)    __attribute__((section(x)))
#define __data      __section(".data")
#define __bss       __section(".bss")
#define __rodata    __section(".rodata")
#define __rodata_unpaged __section(".rodata.__unpaged")
#define __early_ta  __section(".rodata.early_ta")
#define __noprof    __attribute__((no_instrument_function))

#define __compiler_bswap64(x)   __builtin_bswap64((x))
#define __compiler_bswap32(x)   __builtin_bswap32((x))
#define __compiler_bswap16(x)   __builtin_bswap16((x))

#define __GCC_VERSION (__GNUC__ * 10000 + __GNUC_MINOR__ * 100 + \
               __GNUC_PATCHLEVEL__)

#if __GCC_VERSION >= 50100 && !defined(__CHECKER__)
#define __HAVE_BUILTIN_OVERFLOW 1
#endif

#ifdef __HAVE_BUILTIN_OVERFLOW
#define __compiler_add_overflow(a, b, res) \
    __builtin_add_overflow((a), (b), (res))

#define __compiler_sub_overflow(a, b, res) \
    __builtin_sub_overflow((a), (b), (res))

#define __compiler_mul_overflow(a, b, res) \
    __builtin_mul_overflow((a), (b), (res))
#else
/*
 * Copied/inspired from https://www.fefe.de/intof.html
 */
#define __INTOF_HALF_MAX_SIGNED(type) ((type)1 « (sizeof(type)*8-2))
#define __INTOF_MAX_SIGNED(type) (__INTOF_HALF_MAX_SIGNED(type) - 1 + \
                __INTOF_HALF_MAX_SIGNED(type))
#define __INTOF_MIN_SIGNED(type) (-1 - __INTOF_MAX_SIGNED(type))

#define __INTOF_MIN(type) ((type)-1 < 1?__INTOF_MIN_SIGNED(type):(type)0)
#define __INTOF_MAX(type) ((type)~__INTOF_MIN(type))

#define __INTOF_ASSIGN(dest, src) (__extension__({ \
    typeof(src) __intof_x = (src); \
    typeof(dest) __intof_y = __intof_x; \
    (((uintmax_t)__intof_x == (uintmax_t)__intof_y) && \
     ((__intof_x < 1) == (__intof_y < 1)) ? \
        (void)((dest) = __intof_y) , 0 : 1); \
}))

#define __INTOF_ADD(c, a, b) (__extension__({ \
    typeof(a) __intofa_a = (a); \
    typeof(b) __intofa_b = (b); \
    \
    __intofa_b < 1 ? \
        ((__INTOF_MIN(typeof(c)) - __intofa_b <= __intofa_a) ? \
            __INTOF_ASSIGN((c), __intofa_a + __intofa_b) : 1) : \
        ((__INTOF_MAX(typeof(c)) - __intofa_b >= __intofa_a) ? \
            __INTOF_ASSIGN((c), __intofa_a + __intofa_b) : 1); \
}))

#define __INTOF_SUB(c, a, b) (__extension__({ \
    typeof(a) __intofs_a = a; \
    typeof(b) __intofs_b = b; \
    \
    __intofs_b < 1 ? \
        ((__INTOF_MAX(typeof(c)) + __intofs_b >= __intofs_a) ? \
            __INTOF_ASSIGN((c), __intofs_a - __intofs_b) : 1) : \
        ((__INTOF_MIN(typeof(c)) + __intofs_b <= __intofs_a) ? \
            __INTOF_ASSIGN((c), __intofs_a - __intofs_b) : 1); \
}))

/*
 * Dealing with detecting overflow in multiplication of integers.
 *
 * First step is to remove two corner cases with the minum signed integer
 * which can't be represented as a positive integer + sign.
 * Multiply with 0 or 1 can't overflow, no checking needed of the operation,
 * only if it can be assigned to the result.
 *
 * After the corner cases are eliminated we convert the two factors to
 * positive unsigned values, keeping track of the original in another
 * variable which is used at the end to determine the sign of the product.
 *
 * The two terms (a and b) are divided into upper and lower half (x1 upper
 * and x0 lower), so the product is:
 * ((a1 « hshift) + a0) * ((b1 « hshift) + b0)
 * which also is:
 * ((a1 * b1) « (hshift * 2)) +                (T1)
 * ((a1 * b0 + a0 * b1) « hshift) +                (T2)
 * (a0 * b0)                            (T3)
 *
 * From this we can tell and (a1 * b1) has to be 0 or we'll overflow, that
 * is, at least one of a1 or b1 has to be 0. Once this has been checked the
 * addition: ((a1 * b0) « hshift) + ((a0 * b1) « hshift)
 * isn't an addition as one of the terms will be 0.
 *
 * Since each factor in: (a0 * b0)
 * only uses half the capicity of the underlaying type it can't overflow
 *
 * The addition of T2 and T3 can overflow so we use __INTOF_ADD() to
 * perform that addition. If the addition succeeds without overflow the
 * result is assigned the required sign and checked for overflow again.
 */

#define __intof_mul_negate  ((__intof_oa < 1) != (__intof_ob < 1))
#define __intof_mul_hshift  (sizeof(uintmax_t) * 8 / 2)
#define __intof_mul_hmask   (UINTMAX_MAX » __intof_mul_hshift)
#define __intof_mul_a0      ((uintmax_t)(__intof_a) » __intof_mul_hshift)
#define __intof_mul_b0      ((uintmax_t)(__intof_b) » __intof_mul_hshift)
#define __intof_mul_a1      ((uintmax_t)(__intof_a) & __intof_mul_hmask)
#define __intof_mul_b1      ((uintmax_t)(__intof_b) & __intof_mul_hmask)
#define __intof_mul_t       (__intof_mul_a1 * __intof_mul_b0 + \
                 __intof_mul_a0 * __intof_mul_b1)

#define __INTOF_MUL(c, a, b) (__extension__({ \
    typeof(a) __intof_oa = (a); \
    typeof(a) __intof_a = __intof_oa < 1 ? -__intof_oa : __intof_oa; \
    typeof(b) __intof_ob = (b); \
    typeof(b) __intof_b = __intof_ob < 1 ? -__intof_ob : __intof_ob; \
    typeof(c) __intof_c; \
    \
    __intof_oa == 0 || __intof_ob == 0 || \
    __intof_oa == 1 || __intof_ob == 1 ? \
        __INTOF_ASSIGN((c), __intof_oa * __intof_ob) : \
    (__intof_mul_a0 && __intof_mul_b0) || \
     __intof_mul_t > __intof_mul_hmask ?  1 : \
    __INTOF_ADD((__intof_c), __intof_mul_t « __intof_mul_hshift, \
                 __intof_mul_a1 * __intof_mul_b1) ? 1 : \
    __intof_mul_negate ? __INTOF_ASSIGN((c), -__intof_c) : \
                 __INTOF_ASSIGN((c), __intof_c); \
}))

#define __compiler_add_overflow(a, b, res) __INTOF_ADD(*(res), (a), (b))
#define __compiler_sub_overflow(a, b, res) __INTOF_SUB(*(res), (a), (b))
#define __compiler_mul_overflow(a, b, res) __INTOF_MUL(*(res), (a), (b))

#endif
#define __compiler_compare_and_swap(p, oval, nval) \
    __atomic_compare_exchange_n((p), (oval), (nval), true, \
                    __ATOMIC_ACQUIRE, __ATOMIC_RELAXED) \

#define __compiler_atomic_load(p) __atomic_load_n((p), __ATOMIC_RELAXED)
#define __compiler_atomic_store(p, val) \
    __atomic_store_n((p), (val), __ATOMIC_RELAXED)

#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
#endif /*COMPILER_H*/
```

10.3 ta-ref/api/include/report.h File Reference

This graph shows which files directly or indirectly include this file:



Classes

- struct enclave_report
- struct sm_report
- struct report

10.4 report.h

Go to the documentation of this file.

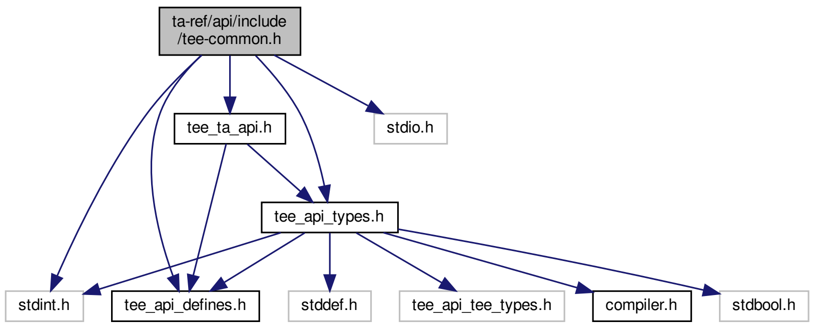
```

#ifndef _REPORT_H
#define _REPORT_H

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define MDSIZE  64
#define SIGNATURE_SIZE  64
#define PUBLIC_KEY_SIZE 32
#define ATTEST_DATA_MAXLEN  1024
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

/* attestation reports */
struct enclave_report
{
  uint8_t hash[MDSIZE];
  uint64_t data_len;
  uint8_t data[ATTEST_DATA_MAXLEN];
  uint8_t signature[SIGNATURE_SIZE];
};

struct sm_report
{
  uint8_t hash[MDSIZE];
  uint8_t public_key[PUBLIC_KEY_SIZE];
  uint8_t signature[SIGNATURE_SIZE];
};

struct report
{
  struct enclave_report enclave;
  struct sm_report sm;
  uint8_t dev_public_key[PUBLIC_KEY_SIZE];
};

#endif // _REPORT_H
```

10.5 ta-ref/api/include/tee-common.h File Reference

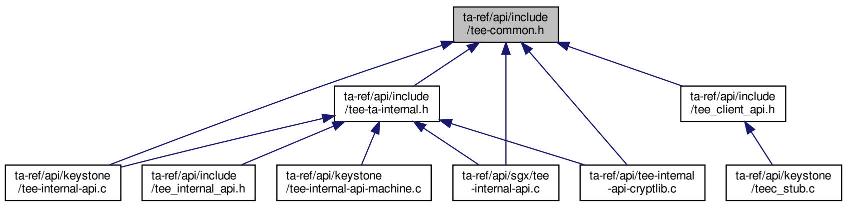
Common type and definitions of RISC-V TEE.

```
#include <stdint.h>
#include <stdio.h>
#include <tee_api_defines.h>
#include <tee_api_types.h>
#include <tee_ta_api.h>
```

Include dependency graph for tee-common.h:



This graph shows which files directly or indirectly include this file:



10.5.1 Detailed Description

Common type and definitions of RISC-V TEE.

draft RISC-V Internal TEE API

Author

Akira Tsukamoto, AIST

Date

2019/09/25

10.6 tee-common.h

Go to the documentation of this file.

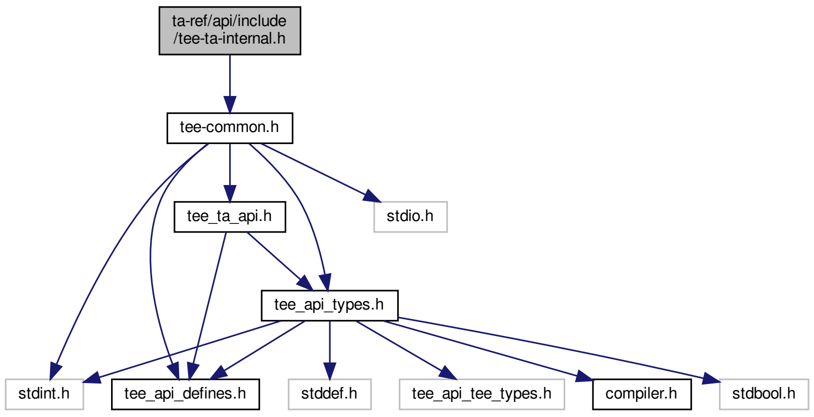
```
/*
 * SPDX-License-Identifier: BSD-2-Clause
 *
 * Copyright (C) 2019 National Institute of Advanced Industrial Science
 *                           and Technology (AIST)
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
  *
  * 1. Redistributions of source code must retain the above copyright notice,
  * this list of conditions and the following disclaimer.
  *
  * 2. Redistributions in binary form must reproduce the above copyright notice,
  * this list of conditions and the following disclaimer in the documentation
  * and/or other materials provided with the distribution.
  *
  * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
  * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
  * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
  * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
  * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
  * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
  * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
  * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
  * POSSIBILITY OF SUCH DAMAGE.
  */
#ifndef TEE_COMMON_H
#define TEE_COMMON_H

#include <stdint.h>
#include <stdio.h>

#ifdef __cplusplus
extern "C" {
#endif

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#ifdef DEBUG
#define pr_deb(...)       do { printf(__VA_ARGS__); } while (0)
#else
#define pr_deb(...)       do { } while (0)
#endif /* DEBUG */
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

//#include <tee_api.h>
#include <tee_api_defines.h>
#include <tee_api_types.h>
#include <tee_ta_api.h>

//typedef uint32_t TEE_Result;

#ifdef __cplusplus
}
#endif

#endif /* TEE_COMMON_H */
```

10.7 ta-ref/api/include/tee-ta-internal.h File Reference

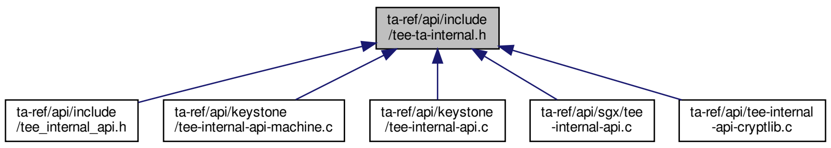
Candidate API list for Global Platform like RISC-V TEE.

```
#include "tee-common.h"
```

Include dependency graph for tee-ta-internal.h:



This graph shows which files directly or indirectly include this file:



Functions

- void __attribute__ ((noreturn)) TEE_Panic(unsigned long code)
- void TEE_GetREETime (TEE_Time ∗time)

  Core Functions, Time Functions.
- void TEE_GetSystemTime (TEE_Time ∗time)

  Core Functions, Time Functions.
- TEE_Result GetRelTimeStart (uint64_t start)

  Core Functions, Time Functions.
- TEE_Result GetRelTimeEnd (uint64_t end)

  Core Functions, Time Functions.
- TEE_Result TEE_CreatePersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle attributes, const void ∗initialData, uint32_t initialDataLen, TEE_ObjectHandle ∗object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_OpenPersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle ∗object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_GetObjectInfo1 (TEE_ObjectHandle object, TEE_ObjectInfo ∗objectInfo)

  Core Functions, Secure Storage Functions (data is isolated for each TA)

- TEE_Result TEE_WriteObjectData (TEE_ObjectHandle object, const void ∗buffer, uint32_t size)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_ReadObjectData (TEE_ObjectHandle object, void ∗buffer, uint32_t size, uint32_t ∗count)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- void TEE_CloseObject (TEE_ObjectHandle object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- void TEE_GenerateRandom (void ∗randomBuffer, uint32_t randomBufferLen)

  Crypto, common.
- TEE_Result TEE_AllocateOperation (TEE_OperationHandle ∗operation, uint32_t algorithm, uint32_t mode, uint32_t maxKeySize)

  Crypto, for all Crypto Functions.
- void TEE_FreeOperation (TEE_OperationHandle operation)

  Crypto, for all Crypto Functions.
- void TEE_DigestUpdate (TEE_OperationHandle operation, const void ∗chunk, uint32_t chunkSize)

  Crypto, Message Digest Functions.
- TEE_Result TEE_DigestDoFinal (TEE_OperationHandle operation, const void ∗chunk, uint32_t chunkLen, void ∗hash, uint32_t ∗hashLen)
- TEE_Result TEE_SetOperationKey (TEE_OperationHandle operation, TEE_ObjectHandle key)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEInit (TEE_OperationHandle operation, const void ∗nonce, uint32_t nonceLen, uint32_t tagLen, uint32_t AADLen, uint32_t payloadLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEUpdate (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- void TEE_AEUpdateAAD (TEE_OperationHandle operation, const void ∗AADdata, uint32_t AADdataLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEEncryptFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen, void ∗tag, uint32_t ∗tagLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEDecryptFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen, void ∗tag, uint32_t tagLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- void TEE_CipherInit (TEE_OperationHandle operation, const void ∗nonce, uint32_t nonceLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_CipherUpdate (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_GenerateKey (TEE_ObjectHandle object, uint32_t keySize, const TEE_Attribute ∗params, uint32_t paramCount)

  Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_AllocateTransientObject (TEE_ObjectType objectType, uint32_t maxKeySize, TEE_ObjectHandle ∗object)

  Crypto, Asymmetric key Verification Functions.
- void TEE_InitRefAttribute (TEE_Attribute ∗attr, uint32_t attributeID, const void ∗buffer, uint32_t length)

  Crypto, Asymmetric key Verification Functions.
- void TEE_InitValueAttribute (TEE_Attribute ∗attr, uint32_t attributeID, uint32_t a, uint32_t b)

  Crypto, Asymmetric key Verification Functions.
- void TEE_FreeTransientObject (TEE_ObjectHandle object)

  Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_AsymmetricSignDigest (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗digest, uint32_t digestLen, void ∗signature, uint32_t ∗signatureLen)

  Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_AsymmetricVerifyDigest (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗digest, uint32_t digestLen, const void ∗signature, uint32_t signatureLen)

  Crypto, Asymmetric key Verification Functions.

10.7.1 Detailed Description

Candidate API list for Global Platform like RISC-V TEE.

draft RISC-V Internal TEE API

Author

Akira Tsukamoto, AIST

Date

2019/09/25

10.7.2 Function Documentation

10.7.2.1 __attribute__() `void __attribute__ ( (noreturn) )`

TEE_Panic() - Raises a panic in the Trusted Application instance.

When a Trusted Application calls the TEE_Panic function, the current instance shall be destroyed and all the resources opened by the instance shall be reclaimed. All sessions opened from the panicking instance on another TA shall be gracefully closed and all cryptographic objects and operations shall be closed properly.

Parameters

code	An informative panic code defined by the TA.

Returns

panic code will be returned.

TEE_Panic() - Raises a Panic in the Trusted Application instance

When a Trusted Application calls the TEE_Panic function, the current instance shall be destroyed and all the resources opened by the instance shall be reclaimed.

Parameters

ec	An informative panic code defined by the TA. May be displayed in traces if traces are available.

10.7.2.2 GetRelTimeEnd()

```
TEE_Result GetRelTimeEnd (
        uint64_t end )
```

Core Functions, Time Functions.

Return the elapsed.

GetRelTimeEnd() - finds the real time of the end timing.

This function prints the ending time.

Parameters

end	End timing

Returns

0 If success

GetRelTimeStart() - find the real time of the end timing.

This function prints the End timing.

Parameters

end	End timing

Returns

0 if success else error occured

10.7.2.3 GetRelTimeStart()

```
TEE_Result GetRelTimeStart (
        uint64_t start )
```

Core Functions, Time Functions.

Fast relative Time function which guarantees no hart switch or context switch between Trusted and Untrusted sides.

Most of the time ending up writing similar functions when only measuring the relative time in usec resolution which do not require the quality of the time itself but the distance of the two points.
For the usage above, the function does not have to return wall clock time.
Not prepared in both Keystone and GP.

GetRelTimeStart() - Gets the real time of the start timing.

This function prints the starting time.

Parameters

start	Start timing

Returns

0 on success

GetRelTimeStart() - Gets the real time of the start timing.

Ths function prints the start timing.

Parameters

start	start timing

Returns

0 if success else error occured.

10.7.2.4 TEE_AEDecryptFinal()

```
TEE_Result TEE_AEDecryptFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen,
        void * tag,
        uint32_t tagLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Supports TEE_ALG_AES_CCM, TEE_ALG_AES_GCM.

TEE_AEDecryptFinal() - Processes data that has not been processed by previous calls to TEE_AEUpdate as well as data supplied in srcData.

This function completes the AE operation and compares the computed tag with the tag supplied in the parameter tag .The operation handle can be reused or newly initialized.The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation may be in either initial or active state and enters initial state afterwards.

Parameters

operation	Handle of a running AE operation
srcData	Reference to final chunk of input data to be encrypted
srcLen	length of the input data
destData	Output buffer. Can be omitted if the output is to be discarded.
destLen	length of the buffer.
tag	Output buffer filled with the computed tag
tagLen	length of the tag.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output

TEE_ERROR_MAC_INVALID If the computed tag does not match the supplied tag

10.7.2.5 TEE_AEEncryptFinal()

```
TEE_Result TEE_AEEncryptFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen,
        void * tag,
        uint32_t * tagLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Supports TEE_ALG_AES_CCM, TEE_ALG_AES_GCM.

TEE_AEEncryptFinal() - processes data that has not been processed by previous calls to TEE_AEUpdate as well as data supplied in srcData .

TEE_AEEncryptFinal completes the AE operation and computes the tag. The operation handle can be reused or newly initialized. The buffers srcData and destData SHALL be either completely disjoint or equal in their starting positions.The operation may be in either initial or active state and enters initial state afterwards.

Parameters

operation	Handle of a running AE operation
srcData	Reference to final chunk of input data to be encrypted
srcLen	length of the input data
destData	Output buffer. Can be omitted if the output is to be discarded.
destLen	length of the buffer.
tag	Output buffer filled with the computed tag
tagLen	length of the tag.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER If the output or tag buffer is not large enoughto contain the output.

10.7.2.6 TEE_AEInit()

```
TEE_Result TEE_AEInit (
        TEE_OperationHandle operation,
        const void * nonce,
        uint32_t nonceLen,
        uint32_t tagLen,
        uint32_t AADLen,
        uint32_t payloadLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Supports TEE_ALG_AES_CCM, TEE_ALG_AES_GCM.

TEE_AEInit() - Initializes an Authentication Encryption operation.

The operation must be in initial state and remains in the initial state afterwards.

Parameters

operation	A handle on the operation.
nonce	The operation nonce or IV
nonceLen	length of nonce
tagLen	Size in bits of the tag
AADLen	Length in bytes of the AAD
payloadLen	Length in bytes of the payload.

Returns

0 on success.

TEE_ERROR_NOT_SUPPORTED If the tag length is not supported by the algorithm.

10.7.2.7 TEE_AEUpdate()

```
TEE_Result TEE_AEUpdate (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Supports TEE_ALG_AES_CCM, TEE_ALG_AES_GCM.

TEE_AEUpdate() - Accumulates data for an Authentication Encryption operation

This function describes Input data does not have to be a multiple of block size. Subsequent calls to this function are possible. Unless one or more calls of this function have supplied sufficient input data,no output is generated. when using this routine to decrypt the returned data may be corrupt since the integrity check is not performed until all the data has been processed. If this is a concern then only use the TEE_AEDecryptFinal routine.

Parameters

operation	Handle of a running AE operation.
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of the input buffer.
destData	Output buffer
destLen	length of the out put buffer.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER if the output buffer is not large enough to contain the output.

10.7.2.8 TEE_AEUpdateAAD()

```
void TEE_AEUpdateAAD (
    TEE_OperationHandle operation,
    const void * AADdata,
    uint32_t AADdataLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Supports TEE_ALG_AES_CCM, TEE_ALG_AES_GCM.

TEE_AEUpdateAAD() - Feeds a new chunk of Additional Authentication Data (AAD) to the AE operation. Subsequent calls to this function are possible.

The TEE_AEUpdateAAD function feeds a new chunk of Additional Authentication Data (AAD) to the AE operation. Subsequent calls to this function are possible.The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation SHALL be in initial state and remains in initial state afterwards.

Parameters

operation	Handle on the AE operation
AADdata	Input buffer containing the chunk of AAD
AADdataLen	length of the chunk of AAD.

10.7.2.9 TEE_AllocateOperation()

```
TEE_Result TEE_AllocateOperation (
    TEE_OperationHandle * operation,
    uint32_t algorithm,
    uint32_t mode,
    uint32_t maxKeySize )
```

Crypto, for all Crypto Functions.

All Crypto Functions use TEE_OperationHandle∗ operation instances.
Create Crypto instance.

TEE_AllocateOperation() - Allocates a handle for a new cryptographic operation and sets the mode and algorithm type.

If this function does not return with TEE_SUCCESS then there is no valid handle value.Once a cryptographic operation has been created, the implementation shall guarantee that all resources necessary for the operation are allocated and that any operation with a key of at most maxKeySize bits can be performed. For algorithms that take multiple keys, for example the AES XTS algorithm, the maxKeySize parameter specifies the size of the largest key. It is up to the implementation to properly allocate space for multiple keys if the algorithm so requires.

Parameters

operation	reference to generated operation handle.
algorithm	One of the cipher algorithms.
mode	The operation mode.
maxKeySize	Maximum key size in bits for the operation.

Returns

0 in case of success

TEE_ERROR_OUT_OF_MEMORY If there are not enough resources to allocate the operation.

TEE_ERROR_NOT_SUPPORTED If the mode is not compatible with the algorithm or key size or if the algorithm is not one of the listed algorithms or if maxKeySize is not appropriate for the algorithm.

10.7.2.10 TEE_AllocateTransientObject()

```
TEE_Result TEE_AllocateTransientObject (
        TEE_ObjectType objectType,
        uint32_t maxKeySize,
        TEE_ObjectHandle * object )
```

Crypto, Asymmetric key Verification Functions.

Create object storing asymmetric key.

TEE_AllocateTransientObject() - Allocates an uninitialized transient object. Transient objects are used to hold a cryptographic object (key or key-pair).

The value TEE_KEYSIZE_NO_KEY should be used for maxObjectSize for object types that do not require a key so that all the container resources can be pre-allocated. As allocated, the container is uninitialized. It can be initialized by subsequently importing the object material,generating an object, deriving an object, or loading an object from the Trusted Storage.

Parameters

objectType	Type of uninitialized object container to be created
maxKeySize	Key Size of the object.
object	Filled with a handle on the newly created key container.

Returns

0 on success

TEE_ERROR_OUT_OF_MEMORY If not enough resources are available to allocate the object handle.

TEE_ERROR_NOT_SUPPORTED If the key size is not supported or the object type is not supported.

10.7.2.11 TEE_AsymmetricSignDigest()

```
TEE_Result TEE_AsymmetricSignDigest (
        TEE_OperationHandle operation,
        const TEE_Attribute * params,
        uint32_t paramCount,
        const void * digest,
        uint32_t digestLen,
        void * signature,
        uint32_t * signatureLen )
```

Crypto, Asymmetric key Verification Functions.

Sign a message digest within an asymmetric key operation.
Keystone has ed25519_sign().
Equivalent in openssl is EVP_DigestSign().

TEE_AsymmetricSignDigest() - Signs a message digest within an asymmetric operation.

Parameters

operation	Handle on the operation, which SHALL have been suitably set up with an operation key.
params	Optional operation parameters
paramCount	size of param
digest	Input buffer containing the input message digest
digestLen	length of input buffer.
signature	Output buffer written with the signature of the digest
signatureLen	length of output buffer.

Returns

0 on sccess

TEE_ERROR_SHORT_BUFFER If the signature buffer is not large enough to hold the result

10.7.2.12 TEE_AsymmetricVerifyDigest()

```
TEE_Result TEE_AsymmetricVerifyDigest (
        TEE_OperationHandle operation,
        const TEE_Attribute * params,
        uint32_t paramCount,
        const void * digest,
        uint32_t digestLen,
        const void * signature,
        uint32_t signatureLen )
```

Crypto, Asymmetric key Verification Functions.

Verifies a message digest signature within an asymmetric key operation.
Keystone has ed25519_verify().
Equivalent in openssl is EVP_DigestVerify().

TEE_AsymmetricVerifyDigest() - verifies a message digest signature within an asymmetric operation.

This function describes the message digest signature verify by calling ed25519_verify().

Parameters

operation	Handle on the operation, which SHALL have been suitably set up with an operation key.
params	Optional operation parameters
paramCount	size of param.
digest	Input buffer containing the input message digest
digestLen	length of input buffer.
signature	Output buffer written with the signature of the digest
signatureLen	length of output buffer.

Returns

TEE_SUCCESS on success

TEE_ERROR_SIGNATURE_INVALID if the signature is invalid.

10.7.2.13 TEE_CipherInit()

```
void TEE_CipherInit (
TEE_OperationHandle operation,
const void * nonce,
uint32_t nonceLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Supports TEE_ALG_AES_CBC.

TEE_CipherInit() - starts the symmetric cipher operation.

The operation shall have been associated with a key. If the operation is in active state, it is reset and then initialized. If the operation is in initial state, it is moved to active state.

Parameters

operation	A handle on an opened cipher operation setup with a key
nonce	Buffer containing the operation Initialization Vector as appropriate.
nonceLen	length of the buffer

10.7.2.14 TEE_CipherUpdate()

```
TEE_Result TEE_CipherUpdate (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Supports TEE_ALG_AES_CBC.

TEE_CipherUpdate() - encrypts or decrypts input data.

Input data does not have to be a multiple of block size. Subsequent calls to this function are possible. Unless one or more calls of this function have supplied sufficient input data, no output is generated. The cipher operation is finalized with a call to TEE_CipherDoFinal .The buffers srcData and destData SHALL be either completely disjoint or equal in their starting positions.The operation SHALL be in active state.

Parameters

operation	Handle of a running Cipher operation
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of input buffer
destData	output buffer
destLen	ouput buffer length.

Returns

0 on success else

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output. In this case, the input is not fed into the algorithm.

10.7.2.15 TEE_CloseObject()

```
void TEE_CloseObject (
        TEE_ObjectHandle object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

Destroy object (key, key-pair or Data).

TEE_CloseObject() - Closes an opened object handle.

The object can be persistent or transient.For transient objects, TEE_CloseObject is equivalent to TEE_Free↩
TransientObject.

Parameters

object	Handle of the object.

Returns

TEE_SUCCESS if success else error occured.

TEE_CloseObject() - Function closes an opened object handle.

The object can be persistent or transient.For transient objects, TEE_CloseObject is equivalent to TEE_Free↩ TransientObject.

Parameters

object	Handle of the object

Returns

TEE_SUCCESS if success else error occured.

10.7.2.16 TEE_CreatePersistentObject()

```
TEE_Result TEE_CreatePersistentObject (
        uint32_t storageID,
        const void * objectID,
        uint32_t objectIDLen,
        uint32_t flags,
        TEE_ObjectHandle attributes,
        const void * initialData,
        uint32_t initialDataLen,
        TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

Create persistent object (key, key-pair or Data).
For the people who have not written code on GP then probably do not need to care the meaning of what is Persistent Object is, since the following are enough to use secure storage feature.

TEE_CreatePersistentObject() - Creates a persistent object with initial attributes.

In this function an initial data stream content returns either a handle on the created object or TEE_HANDLE_NULL upon failure.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier

Paramter list continued on next page

flags	The flags which determine the settings under which the object is opened.
attributes	A handle on a persistent object or an initialized transient object from which to take the persistent object attributes
initialData	The initial data content of the persistent object
initialDataLen	The initial data content of the persistent object
object	A pointer to the handle which contains the opened handle upon successful completion

Returns

0 if success else error occured.

TEE_CreatePersistentObject() - Creates a persistent object with initial attributes.

An initial data stream content, and optionally returns either a handle on the created object, or TEE_HANDLE_NULL upon failure.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
attributes	A handle on a persistent object or an initialized transient object from which to take the persistent object attributes
initialData	The initial data content of the persistent object
initialDataLen	The initial data content of the persistent object
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success, else error occured.

10.7.2.17 TEE_DigestDoFinal()

```
TEE_Result TEE_DigestDoFinal (
        TEE_OperationHandle operation,
        const void * chunk,
        uint32_t chunkLen,
        void * hash,
        uint32_t * hashLen )
```

Function accumulates message data for hashing.

TEE_DigestDoFinal() - Finalizes the message digest operation and produces the message hash.

This function finalizes the message digest operation and produces the message hash. Afterwards the Message Digest operation is reset to initial state and can be reused.

Parameters

operation	Handle of a running Message Digest operation.
chunk	Chunk of data to be hashed.
chunkLen	size of the chunk.
hash	Output buffer filled with the message hash.
hashLen	lenth of the mesaage hash.

Returns

0 on success

TEE_ERROR_SHORT_BUFFER If the output buffer is too small. In this case, the operation is not finalized.

10.7.2.18 TEE_DigestUpdate()

```
void TEE_DigestUpdate (
        TEE_OperationHandle operation,
        const void * chunk,
        uint32_t chunkSize )
```

Crypto, Message Digest Functions.

Function accumulates message data for hashing.

TEE_DigestUpdate()- Accumulates message data for hashing.

This function describes the message does not have to be block aligned. Subsequent calls to this function are possible.The operation may be in either initial or active state and becomes active.

Parameters

operation	Handle of a running Message Digest operation.
chunk	Chunk of data to be hashed
chunkSize	size of the chunk.

10.7.2.19 TEE_FreeOperation()

```
void TEE_FreeOperation (
        TEE_OperationHandle operation )
```

Crypto, for all Crypto Functions.

All Crypto Functions use TEE_OperationHandle∗ operation instances.
Destroy Crypto instance.

TEE_FreeOperation() - Deallocates all resources associated with an operation handle.

This function deallocates all resources associated with an operation handle. After this function is called, the operation handle is no longer valid. All cryptographic material in the operation is destroyed. The function does nothing if operation is TEE_HANDLE_NULL.

Parameters

operation	Reference to operation handle.

Returns

nothing after the operation free.

10.7.2.20 TEE_FreeTransientObject()

```
void TEE_FreeTransientObject (
        TEE_ObjectHandle object )
```

Crypto, Asymmetric key Verification Functions.

Destroy object storing asymmetric key.

TEE_FreeTransientObject() - Deallocates a transient object previously allocated with TEE_AllocateTransientObject .

this function describes the object handle is no longer valid and all resources associated with the transient object shall have been reclaimed after the TEE_AllocateTransientObject() call.

Parameters

object	Handle on the object to free.

10.7.2.21 TEE_GenerateKey()

```
TEE_Result TEE_GenerateKey (
        TEE_ObjectHandle object,
        uint32_t keySize,
        const TEE_Attribute * params,
        uint32_t paramCount )
```

Crypto, Asymmetric key Verification Functions.

Generate asymmetric keypair.

TEE_GenerateKey () - Generates a random key or a key-pair and populates a transient key object with the generated key material.

The size of the desired key is passed in the keySize parameter and shall be less than or equal to the maximum key size specified when the transient object was created.

Parameters

object	Handle on an uninitialized transient key to populate with the generated key.
keySize	Requested key size shall be less than or equal to the maximum key size specified when the object container was created
params	Parameters for the key generation.
paramCount	The values of all parameters are copied nto the object so that the params array and all the memory buffers it points to may be freed after this routine returns without affecting the object.

Returns

0 on succes

TEE_ERROR_BAD_PARAMETERS If an incorrect or inconsistent attribute is detected. The checks that are performed depend on the implementation.

10.7.2.22 TEE_GenerateRandom()

```
void TEE_GenerateRandom (
            void * randomBuffer,
            uint32_t randomBufferLen )
```

Crypto, common.

Random Data Generation Function. The quality of the random is implementation dependent.
I am not sure this should be in Keystone or not, but it is very handy.
Good to have adding a way to check the quality of the random implementation.

TEE_GenerateRandom() - Generates random data.

This function generates random data of random buffer length and is stored in to random Buffer by calling wc_←
RNG_GenerateBlock().If ret is not equal
to 0 then TEE_Panic is called.

Parameters

randomBuffer	Reference to generated random data
randomBufferLen	Byte length of requested random data

Returns

random data random data will be returned.

TEE_GenerateRandom() - Generates random data.

This function generates random data of random bufferlength and is stored in to randomBuffer by calling sgx_read←
_rand().

Parameters

randomBuffer	Reference to generated random data
randomBufferLen	Byte length of requested random data

10.7.2.23 TEE_GetObjectInfo1()

```
TEE_Result TEE_GetObjectInfo1 (
    TEE_ObjectHandle object,
    TEE_ObjectInfo * objectInfo )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

Get length of object required before reading the object.

TEE_GetObjectInfo1() - Returns the characteristics of an object.

This function returns a handle which can be used to access the object's attributes and data stream.

Parameters

objectInfo	Pointer to a structure filled with the object information
object	Handle of the object

Returns

0 if success else error occured.

TEE_GetObjectInfo1() - Function returns the characteristics of an object.

It returns a handle that can be used to access the object's attributes and data stream.

Parameters

objectInfo	Pointer to a structure filled with the object information
object	Handle of the object

Returns

0 if success else error occured.

10.7.2.24 TEE_GetREETime()

```
void TEE_GetREETime (
    TEE_Time * time )
```

Core Functions, Time Functions.

Wall clock time of host OS, expressed in the number of seconds since 1970-01-01 UTC.
This could be implemented on Keystone using ocall.

TEE_GetREETime() - Retrieves the current REE system time.

This function retrieves the current time as seen from the point of view of
the REE.

Parameters

time	Filled with the number of seconds and milliseconds

TEE_GetREETime() - Function retrieves the current REE system time.

This function retrieves the current time as seen from the point of view of the REE.

Parameters

time	Filled with the number of seconds and milliseconds.

10.7.2.25 TEE_GetSystemTime()

```
void TEE_GetSystemTime (
        TEE_Time * time )
```

Core Functions, Time Functions.

Time of TEE-controlled secure timer or Host OS time, implementation dependent.

TEE_GetSystemTime() - Retrieves the current system time.

This function describes the system time has an arbitrary implementation
defined origin that can vary across TA instances. The minimum guarantee
is that the system time shall be monotonic for a given TA instance.

Parameters

time	Filled with the number of seconds and milliseconds

TEE_GetSystemTime() - Retrieves the current system time.

The system time has an arbitrary implementation-defined origin that can vary across TA instances

Parameters

time	Filled with the number of seconds and milliseconds.

10.7.2.26 TEE_InitRefAttribute()

```
void TEE_InitRefAttribute (
        TEE_Attribute * attr,
        uint32_t attributeID,
        const void * buffer,
        uint32_t length )
```

Crypto, Asymmetric key Verification Functions.

Storing asymmetric key.

TEE_InitRefAttribute() - The helper function can be used to populate a single attribute either with a reference to a buffer or with integer values.

In TEE_InitRefAttribute () only the buffer pointer is copied, not the content of the buffer. This means that the attribute structure maintains a pointer back to the supplied buffer. It is the responsibility of the TA author to ensure that the contents of the buffer maintain their value until the attributes array is no longer in use.

Parameters

attr	attribute structure to initialize.
attributeID	Identifier of the attribute to populate.
buffer	input buffer that holds the content of the attribute.
length	buffer length.

10.7.2.27 TEE_InitValueAttribute()

```
void TEE_InitValueAttribute (
        TEE_Attribute * attr,
        uint32_t attributeID,
        uint32_t a,
        uint32_t b )
```

Crypto, Asymmetric key Verification Functions.

Storing asymmetric key.

TEE_InitValueAttribute() - The helper function can be used to populate a single attribute either with a reference to a buffer or with integer values.

Parameters

attr	attribute structure to initialize.
attributeID	Identifier of the attribute to populate.
a	unsigned integer value to assign to the a member of the attribute structure.
b	unsigned integer value to assign to the b member of the attribute structure

10.7.2.28 TEE_OpenPersistentObject()

```
TEE_Result TEE_OpenPersistentObject (
            uint32_t storageID,
            const void * objectID,
            uint32_t objectIDLen,
            uint32_t flags,
            TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

Open persistent object.

TEE_OpenPersistentObject() - Opens a handle on an existing persistent object.

This function returns a handle which can be used to access the object's attributes and data stream.

Parameters

storageID	The storage to use
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success else error occured.

TEE_OpenPersistentObject() - Opens a handle on an existing persistent object.

This function returns a handle that can be used to access the object's attributes and data stream.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success, else error occured.

10.7.2.29 TEE_ReadObjectData()

```
TEE_Result TEE_ReadObjectData (
        TEE_ObjectHandle object,
        void * buffer,
        uint32_t size,
        uint32_t * count )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

Read object.

TEE_ReadObjectData() - Attempts to read size bytes from the data stream associated with the object into the buffer pointed to by buffer.

The bytes are read starting at the position in the data stream currently stored in the object handle. The handle's position is incremented by the number of bytes actually read. On completion of TEE_ReadObjectData sets the number of bytes actually read in the "uint32_t" pointed to by count. The value written to ∗count may be less than size if the number of bytes until the end-of3067 stream is less than size. It is set to 0 if the position at the start of the read operation is at or beyond the end-of-stream. These are the only cases where ∗count may be less than size.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write
count	size of the buffer.

Returns

TEE_SUCCESS if success else error occured.

TEE_ReadObjectData() - Attempts to read size bytes from the data stream associated with the object object into the buffer pointed to by buffer.

The bytes are read starting at the position in the data stream currently stored in the object handle. The handle's position is incremented by the number of bytes actually read. On completion TEE_ReadObjectData sets the number of bytes actually read in the uint32_t pointed to by count. The value written to ∗count may be less than size if the number of bytes until the end-of3067 stream is less than size. It is set to 0 if the position at the start of the read operation is at or beyond the end-of-stream. These are the only cases where ∗count may be less than size.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write
count	size of the buffer.

Returns

TEE_SUCCESS if success, else error occured.

10.7.2.30 TEE_SetOperationKey()

```
TEE_Result TEE_SetOperationKey (
        TEE_OperationHandle operation,
        TEE_ObjectHandle key )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

Set symmetric key used in operation.

TEE_SetOperationKey() - Programs the key of an operation; that is, it associates an operation with a key.

The key material is copied from the key object handle into the operation. After the key has been set, there is no longer any link between the operation and the key object. The object handle can be closed or reset and this will not affect the operation. This copied material exists until the operation is freed using TEE_FreeOperation or another key is set into the operation.

Parameters

operation	Operation handle.
key	A handle on a key object.

Returns

0 on success return

TEE_ERROR_CORRUPT_OBJECT If the object is corrupt. The object handle is closed.

TEE_ERROR_STORAGE_NOT_AVAILABLE If the persistent object is stored in a storage area which is currently inaccessible.

10.7.2.31 TEE_WriteObjectData()

```
TEE_Result TEE_WriteObjectData (
        TEE_ObjectHandle object,
        const void * buffer,
        uint32_t size )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

Write object.

TEE_WriteObjectData() - Writes the buffer data in to persistent objects.

In this function it checks if object is present or not, the encryption/ decryption buffer is taken by calling mbedtls_aes↩_crypt_cbc() then that buffer data is encrypted and mapped to object.On the base of object creation TEE_SUCCESS appears else TEE_ERROR_GENERIC appears.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write

Returns

TEE_SUCCESS if success else error occured.

TEE_WriteObjectData() - writes size bytes from the buffer pointed to by buffer to the data stream associated with the open object handle object.

If the current data position points before the end-of-stream, then size bytes are written to the data stream, overwriting bytes starting at the current data position. If the current data position points beyond the stream's end, then the data stream is first extended with zero bytes until the length indicated by the data position indicator is reached, and then size bytes are written to the stream.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write

Returns

TEE_SUCCESS if success else error occured.

10.8 tee-ta-internal.h

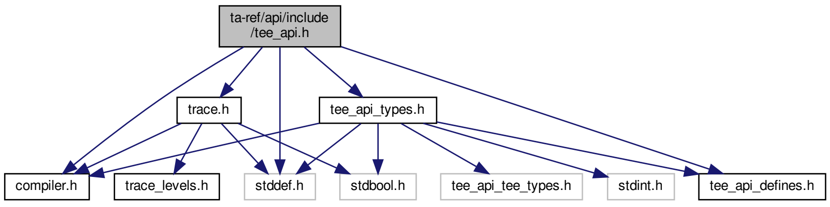
Go to the documentation of this file.

```
/*
 * SPDX-License-Identifier: BSD-2-Clause
 *
 * Copyright (C) 2019 National Institute of Advanced Industrial Science
 *                            and Technology (AIST)
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */
#ifndef TA_INTERNAL_TEE_H
#define TA_INTERNAL_TEE_H

#include "tee-common.h"

#ifdef __cplusplus
extern "C" {
#endif

void __attribute__((noreturn)) TEE_Panic(unsigned long code);


void TEE_GetREETime(TEE_Time *time);



/* Wall clock time is important for verifying certificates. */
void TEE_GetSystemTime(TEE_Time *time);



/* Start timer */
TEE_Result GetRelTimeStart(uint64_t start);



TEE_Result GetRelTimeEnd(uint64_t end);



TEE_Result TEE_CreatePersistentObject(uint32_t storageID, const void *objectID,
                                      uint32_t objectIDLen, uint32_t flags,
                                      TEE_ObjectHandle attributes,
                                      const void *initialData,
                                      uint32_t initialDataLen,
                                      TEE_ObjectHandle *object);

TEE_Result TEE_OpenPersistentObject(uint32_t storageID, const void *objectID,
                                    uint32_t objectIDLen, uint32_t flags,
                                    TEE_ObjectHandle *object);

TEE_Result TEE_GetObjectInfo1(TEE_ObjectHandle object, TEE_ObjectInfo *objectInfo);

TEE_Result TEE_WriteObjectData(TEE_ObjectHandle object, const void *buffer,
                               uint32_t size);
TEE_Result TEE_ReadObjectData(TEE_ObjectHandle object, void *buffer,
                              uint32_t size, uint32_t *count);

void TEE_CloseObject(TEE_ObjectHandle object);




void TEE_GenerateRandom(void *randomBuffer, uint32_t randomBufferLen);



TEE_Result TEE_AllocateOperation(TEE_OperationHandle *operation,
                                 uint32_t algorithm, uint32_t mode,
                                 uint32_t maxKeySize);

void TEE_FreeOperation(TEE_OperationHandle operation);




void TEE_DigestUpdate(TEE_OperationHandle operation,
                      const void *chunk, uint32_t chunkSize);
TEE_Result TEE_DigestDoFinal(TEE_OperationHandle operation, const void *chunk,
                             uint32_t chunkLen, void *hash, uint32_t *hashLen);



TEE_Result TEE_SetOperationKey(TEE_OperationHandle operation,
                   TEE_ObjectHandle key);

TEE_Result TEE_AEInit(TEE_OperationHandle operation, const void *nonce,
                      uint32_t nonceLen, uint32_t tagLen, uint32_t AADLen,
                      uint32_t payloadLen);

TEE_Result TEE_AEUpdate(TEE_OperationHandle operation, const void *srcData,
                        uint32_t srcLen, void *destData, uint32_t *destLen);

void TEE_AEUpdateAAD(TEE_OperationHandle operation, const void *AADdata,
             uint32_t AADdataLen);

TEE_Result TEE_AEEncryptFinal(TEE_OperationHandle operation,
                              const void *srcData, uint32_t srcLen,
                              void *destData, uint32_t *destLen, void *tag,
                              uint32_t *tagLen);

TEE_Result TEE_AEDecryptFinal(TEE_OperationHandle operation,
                              const void *srcData, uint32_t srcLen,
                              void *destData, uint32_t *destLen, void *tag,
                              uint32_t tagLen);



void TEE_CipherInit(TEE_OperationHandle operation, const void *nonce,
           uint32_t nonceLen);

TEE_Result TEE_CipherUpdate(TEE_OperationHandle operation, const void *srcData,
                uint32_t srcLen, void *destData, uint32_t *destLen);



TEE_Result TEE_GenerateKey(TEE_ObjectHandle object, uint32_t keySize,
                    const TEE_Attribute *params, uint32_t paramCount);

TEE_Result TEE_AllocateTransientObject(TEE_ObjectType objectType,
                                       uint32_t maxKeySize,
                                       TEE_ObjectHandle *object);

void TEE_InitRefAttribute(TEE_Attribute *attr, uint32_t attributeID,
                          const void *buffer, uint32_t length);

void TEE_InitValueAttribute(TEE_Attribute *attr, uint32_t attributeID,
                uint32_t a, uint32_t b);

void TEE_FreeTransientObject(TEE_ObjectHandle object);


TEE_Result TEE_AsymmetricSignDigest(TEE_OperationHandle operation,
                                    const TEE_Attribute *params,
                                    uint32_t paramCount, const void *digest,
                                    uint32_t digestLen, void *signature,
                                    uint32_t *signatureLen);

TEE_Result TEE_AsymmetricVerifyDigest(TEE_OperationHandle operation,
                                      const TEE_Attribute *params,
                                      uint32_t paramCount, const void *digest,
                                      uint32_t digestLen, const void *signature,
                                      uint32_t signatureLen);

#ifdef __cplusplus
}
#endif

#endif /* TA_INTERNAL_TEE_H */
```

10.9 ta-ref/api/include/tee_api.h File Reference

```
#include <stddef.h>
#include <compiler.h>
#include <tee_api_defines.h>
#include <tee_api_types.h>
#include <trace.h>
```

Include dependency graph for tee_api.h:



Functions

- TEE_Result TEE_GetPropertyAsString (TEE_PropSetHandle propsetOrEnumerator, const char ∗name, char ∗valueBuffer, uint32_t ∗valueBufferLen)
- TEE_Result TEE_GetPropertyAsBool (TEE_PropSetHandle propsetOrEnumerator, const char ∗name, bool ∗value)
- TEE_Result TEE_GetPropertyAsU32 (TEE_PropSetHandle propsetOrEnumerator, const char ∗name, uint32_t ∗value)
- TEE_Result TEE_GetPropertyAsBinaryBlock (TEE_PropSetHandle propsetOrEnumerator, const char ∗name, void ∗valueBuffer, uint32_t ∗valueBufferLen)

- TEE_Result TEE_GetPropertyAsUUID (TEE_PropSetHandle propsetOrEnumerator, const char ∗name, TEE_UUID ∗value)
- TEE_Result TEE_GetPropertyAsIdentity (TEE_PropSetHandle propsetOrEnumerator, const char ∗name, TEE_Identity ∗value)
- TEE_Result TEE_AllocatePropertyEnumerator (TEE_PropSetHandle ∗enumerator)
- void TEE_FreePropertyEnumerator (TEE_PropSetHandle enumerator)
- void TEE_StartPropertyEnumerator (TEE_PropSetHandle enumerator, TEE_PropSetHandle propSet)
- void TEE_ResetPropertyEnumerator (TEE_PropSetHandle enumerator)
- TEE_Result TEE_GetPropertyName (TEE_PropSetHandle enumerator, void ∗nameBuffer, uint32_t ∗name←↩ BufferLen)
- TEE_Result TEE_GetNextProperty (TEE_PropSetHandle enumerator)
- void TEE_Panic (TEE_Result panicCode)
- TEE_Result TEE_OpenTASession (const TEE_UUID ∗destination, uint32_t cancellationRequestTimeout, uint32_t paramTypes, TEE_Param params[TEE_NUM_PARAMS], TEE_TASessionHandle ∗session, uint32_t ∗returnOrigin)
- void TEE_CloseTASession (TEE_TASessionHandle session)
- TEE_Result TEE_InvokeTACommand (TEE_TASessionHandle session, uint32_t cancellationRequestTimeout, uint32_t commandID, uint32_t paramTypes, TEE_Param params[TEE_NUM_PARAMS], uint32_t ∗returnOrigin)
- bool TEE_GetCancellationFlag (void)
- bool TEE_UnmaskCancellation (void)
- bool TEE_MaskCancellation (void)
- TEE_Result TEE_CheckMemoryAccessRights (uint32_t accessFlags, void ∗buffer, uint32_t size)
- void TEE_SetInstanceData (const void ∗instanceData)
- const void ∗ TEE_GetInstanceData (void)
- void ∗ TEE_Malloc (uint32_t size, uint32_t hint)
- void ∗ TEE_Realloc (void ∗buffer, uint32_t newSize)
- void TEE_Free (void ∗buffer)
- void ∗ TEE_MemMove (void ∗dest, const void ∗src, uint32_t size)
- int32_t TEE_MemCompare (const void ∗buffer1, const void ∗buffer2, uint32_t size)
- void ∗ TEE_MemFill (void ∗buff, uint32_t x, uint32_t size)
- void TEE_GetObjectInfo (TEE_ObjectHandle object, TEE_ObjectInfo ∗objectInfo)
- TEE_Result TEE_GetObjectInfo1 (TEE_ObjectHandle object, TEE_ObjectInfo ∗objectInfo)

    Core Functions, Secure Storage Functions (data is isolated for each TA)
- void TEE_RestrictObjectUsage (TEE_ObjectHandle object, uint32_t objectUsage)
- TEE_Result TEE_RestrictObjectUsage1 (TEE_ObjectHandle object, uint32_t objectUsage)
- TEE_Result TEE_GetObjectBufferAttribute (TEE_ObjectHandle object, uint32_t attributeID, void ∗buffer, uint32_t ∗size)
- TEE_Result TEE_GetObjectValueAttribute (TEE_ObjectHandle object, uint32_t attributeID, uint32_t ∗a, uint32_t ∗b)
- void TEE_CloseObject (TEE_ObjectHandle object)

    Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_AllocateTransientObject (TEE_ObjectType objectType, uint32_t maxKeySize, TEE_ObjectHandle ∗object)

    Crypto, Asymmetric key Verification Functions.
- void TEE_FreeTransientObject (TEE_ObjectHandle object)

    Crypto, Asymmetric key Verification Functions.
- void TEE_ResetTransientObject (TEE_ObjectHandle object)
- TEE_Result TEE_PopulateTransientObject (TEE_ObjectHandle object, const TEE_Attribute ∗attrs, uint32_t attrCount)
- void TEE_InitRefAttribute (TEE_Attribute ∗attr, uint32_t attributeID, const void ∗buffer, uint32_t length)

    Crypto, Asymmetric key Verification Functions.
- void TEE_InitValueAttribute (TEE_Attribute ∗attr, uint32_t attributeID, uint32_t a, uint32_t b)

    Crypto, Asymmetric key Verification Functions.

- void TEE_CopyObjectAttributes (TEE_ObjectHandle destObject, TEE_ObjectHandle srcObject)
- TEE_Result TEE_CopyObjectAttributes1 (TEE_ObjectHandle destObject, TEE_ObjectHandle srcObject)
- TEE_Result TEE_GenerateKey (TEE_ObjectHandle object, uint32_t keySize, const TEE_Attribute ∗params, uint32_t paramCount)

  Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_OpenPersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle ∗object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_CreatePersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle attributes, const void ∗initialData, uint32_t initialDataLen, TEE_ObjectHandle ∗object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- void TEE_CloseAndDeletePersistentObject (TEE_ObjectHandle object)
- TEE_Result TEE_CloseAndDeletePersistentObject1 (TEE_ObjectHandle object)
- TEE_Result TEE_RenamePersistentObject (TEE_ObjectHandle object, const void ∗newObjectID, uint32_t newObjectIDLen)
- TEE_Result TEE_AllocatePersistentObjectEnumerator (TEE_ObjectEnumHandle ∗objectEnumerator)
- void TEE_FreePersistentObjectEnumerator (TEE_ObjectEnumHandle objectEnumerator)
- void TEE_ResetPersistentObjectEnumerator (TEE_ObjectEnumHandle objectEnumerator)
- TEE_Result TEE_StartPersistentObjectEnumerator (TEE_ObjectEnumHandle objectEnumerator, uint32_↩
t storageID)
- TEE_Result TEE_GetNextPersistentObject (TEE_ObjectEnumHandle objectEnumerator, TEE_ObjectInfo ∗objectInfo, void ∗objectID, uint32_t ∗objectIDLen)
- TEE_Result TEE_ReadObjectData (TEE_ObjectHandle object, void ∗buffer, uint32_t size, uint32_t ∗count)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_WriteObjectData (TEE_ObjectHandle object, const void ∗buffer, uint32_t size)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_TruncateObjectData (TEE_ObjectHandle object, uint32_t size)
- TEE_Result TEE_SeekObjectData (TEE_ObjectHandle object, int32_t offset, TEE_Whence whence)
- TEE_Result TEE_AllocateOperation (TEE_OperationHandle ∗operation, uint32_t algorithm, uint32_t mode, uint32_t maxKeySize)

  Crypto, for all Crypto Functions.
- void TEE_FreeOperation (TEE_OperationHandle operation)

  Crypto, for all Crypto Functions.
- void TEE_GetOperationInfo (TEE_OperationHandle operation, TEE_OperationInfo ∗operationInfo)
- TEE_Result TEE_GetOperationInfoMultiple (TEE_OperationHandle operation, TEE_OperationInfoMultiple ∗operationInfoMultiple, uint32_t ∗operationSize)
- void TEE_ResetOperation (TEE_OperationHandle operation)
- TEE_Result TEE_SetOperationKey (TEE_OperationHandle operation, TEE_ObjectHandle key)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_SetOperationKey2 (TEE_OperationHandle operation, TEE_ObjectHandle key1, TEE_ObjectHandle key2)
- void TEE_CopyOperation (TEE_OperationHandle dstOperation, TEE_OperationHandle srcOperation)
- TEE_Result TEE_IsAlgorithmSupported (uint32_t algId, uint32_t element)
- void TEE_DigestUpdate (TEE_OperationHandle operation, const void ∗chunk, uint32_t chunkSize)

  Crypto, Message Digest Functions.
- TEE_Result TEE_DigestDoFinal (TEE_OperationHandle operation, const void ∗chunk, uint32_t chunkLen, void ∗hash, uint32_t ∗hashLen)
- void TEE_CipherInit (TEE_OperationHandle operation, const void ∗IV, uint32_t IVLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_CipherUpdate (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)

  Crypto, Authenticated Encryption with Symmetric key Verification Functions.

- TEE_Result TEE_CipherDoFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)
- void TEE_MACInit (TEE_OperationHandle operation, const void ∗IV, uint32_t IVLen)
- void TEE_MACUpdate (TEE_OperationHandle operation, const void ∗chunk, uint32_t chunkSize)
- TEE_Result TEE_MACComputeFinal (TEE_OperationHandle operation, const void ∗message, uint32_←
t messageLen, void ∗mac, uint32_t ∗macLen)
- TEE_Result TEE_MACCompareFinal (TEE_OperationHandle operation, const void ∗message, uint32_←
t messageLen, const void ∗mac, uint32_t macLen)
- TEE_Result TEE_AEInit (TEE_OperationHandle operation, const void ∗nonce, uint32_t nonceLen, uint32_t tagLen, uint32_t AADLen, uint32_t payloadLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- void TEE_AEUpdateAAD (TEE_OperationHandle operation, const void ∗AADdata, uint32_t AADdataLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEUpdate (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEEncryptFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen, void ∗tag, uint32_t ∗tagLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEDecryptFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen, void ∗tag, uint32_t tagLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AsymmetricEncrypt (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)
- TEE_Result TEE_AsymmetricDecrypt (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)
- TEE_Result TEE_AsymmetricSignDigest (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗digest, uint32_t digestLen, void ∗signature, uint32_t ∗signatureLen)

    Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_AsymmetricVerifyDigest (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗digest, uint32_t digestLen, const void ∗signature, uint32_t signatureLen)

    Crypto, Asymmetric key Verification Functions.
- void TEE_DeriveKey (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, TEE_ObjectHandle derivedKey)
- void TEE_GenerateRandom (void ∗randomBuffer, uint32_t randomBufferLen)

    Crypto, common.
- void TEE_GetSystemTime (TEE_Time ∗time)

    Core Functions, Time Functions.
- TEE_Result TEE_Wait (uint32_t timeout)
- TEE_Result TEE_GetTAPersistentTime (TEE_Time ∗time)
- TEE_Result TEE_SetTAPersistentTime (const TEE_Time ∗time)
- void TEE_GetREETime (TEE_Time ∗time)

    Core Functions, Time Functions.
- uint32_t TEE_BigIntFMMSizeInU32 (uint32_t modulusSizeInBits)
- uint32_t TEE_BigIntFMMContextSizeInU32 (uint32_t modulusSizeInBits)
- void TEE_BigIntInit (TEE_BigInt ∗bigInt, uint32_t len)
- void TEE_BigIntInitFMMContext (TEE_BigIntFMMContext ∗context, uint32_t len, const TEE_BigInt ∗modulus)
- void TEE_BigIntInitFMM (TEE_BigIntFMM ∗bigIntFMM, uint32_t len)
- TEE_Result TEE_BigIntConvertFromOctetString (TEE_BigInt ∗dest, const uint8_t ∗buffer, uint32_t bufferLen, int32_t sign)
- TEE_Result TEE_BigIntConvertToOctetString (uint8_t ∗buffer, uint32_t ∗bufferLen, const TEE_BigInt ∗bigInt)
- void TEE_BigIntConvertFromS32 (TEE_BigInt ∗dest, int32_t shortVal)
- TEE_Result TEE_BigIntConvertToS32 (int32_t ∗dest, const TEE_BigInt ∗src)

- int32_t TEE_BigIntCmp (const TEE_BigInt ∗op1, const TEE_BigInt ∗op2)
- int32_t TEE_BigIntCmpS32 (const TEE_BigInt ∗op, int32_t shortVal)
- void TEE_BigIntShiftRight (TEE_BigInt ∗dest, const TEE_BigInt ∗op, size_t bits)
- bool TEE_BigIntGetBit (const TEE_BigInt ∗src, uint32_t bitIndex)
- uint32_t TEE_BigIntGetBitCount (const TEE_BigInt ∗src)
- void TEE_BigIntAdd (TEE_BigInt ∗dest, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2)
- void TEE_BigIntSub (TEE_BigInt ∗dest, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2)
- void TEE_BigIntNeg (TEE_BigInt ∗dest, const TEE_BigInt ∗op)
- void TEE_BigIntMul (TEE_BigInt ∗dest, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2)
- void TEE_BigIntSquare (TEE_BigInt ∗dest, const TEE_BigInt ∗op)
- void TEE_BigIntDiv (TEE_BigInt ∗dest_q, TEE_BigInt ∗dest_r, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2)
- void TEE_BigIntMod (TEE_BigInt ∗dest, const TEE_BigInt ∗op, const TEE_BigInt ∗n)
- void TEE_BigIntAddMod (TEE_BigInt ∗dest, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2, const TEE_BigInt ∗n)
- void TEE_BigIntSubMod (TEE_BigInt ∗dest, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2, const TEE_BigInt ∗n)
- void TEE_BigIntMulMod (TEE_BigInt ∗dest, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2, const TEE_BigInt ∗n)
- void TEE_BigIntSquareMod (TEE_BigInt ∗dest, const TEE_BigInt ∗op, const TEE_BigInt ∗n)
- void TEE_BigIntInvMod (TEE_BigInt ∗dest, const TEE_BigInt ∗op, const TEE_BigInt ∗n)
- bool TEE_BigIntRelativePrime (const TEE_BigInt ∗op1, const TEE_BigInt ∗op2)
- void TEE_BigIntComputeExtendedGcd (TEE_BigInt ∗gcd, TEE_BigInt ∗u, TEE_BigInt ∗v, const TEE_BigInt ∗op1, const TEE_BigInt ∗op2)
- int32_t TEE_BigIntIsProbablePrime (const TEE_BigInt ∗op, uint32_t confidenceLevel)
- void TEE_BigIntConvertToFMM (TEE_BigIntFMM ∗dest, const TEE_BigInt ∗src, const TEE_BigInt ∗n, const TEE_BigIntFMMContext ∗context)
- void TEE_BigIntConvertFromFMM (TEE_BigInt ∗dest, const TEE_BigIntFMM ∗src, const TEE_BigInt ∗n, const TEE_BigIntFMMContext ∗context)
- void TEE_BigIntFMMConvertToBigInt (TEE_BigInt ∗dest, const TEE_BigIntFMM ∗src, const TEE_BigInt ∗n, const TEE_BigIntFMMContext ∗context)
- void TEE_BigIntComputeFMM (TEE_BigIntFMM ∗dest, const TEE_BigIntFMM ∗op1, const TEE_BigIntFMM ∗op2, const TEE_BigInt ∗n, const TEE_BigIntFMMContext ∗context)

10.9.1 Function Documentation

10.9.1.1 TEE_AEDecryptFinal()

```
TEE_Result TEE_AEDecryptFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen,
        void * tag,
        uint32_t tagLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEDecryptFinal() - Processes data that has not been processed by previous calls to TEE_AEUpdate as well as data supplied in srcData.

This function completes the AE operation and compares the computed tag with the tag supplied in the parameter tag .The operation handle can be reused or newly initialized.The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation may be in either initial or active state and enters initial state afterwards.

Parameters

operation	Handle of a running AE operation
srcData	Reference to final chunk of input data to be encrypted
srcLen	length of the input data
destData	Output buffer. Can be omitted if the output is to be discarded.
destLen	length of the buffer.
tag	Output buffer filled with the computed tag
tagLen	length of the tag.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output

TEE_ERROR_MAC_INVALID If the computed tag does not match the supplied tag

10.9.1.2 TEE_AEEncryptFinal()

```
TEE_Result TEE_AEEncryptFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen,
        void * tag,
        uint32_t * tagLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEEncryptFinal() - processes data that has not been processed by previous calls to TEE_AEUpdate as well as data supplied in srcData .

TEE_AEEncryptFinal completes the AE operation and computes the tag. The operation handle can be reused or newly initialized. The buffers srcData and destData SHALL be either completely disjoint or equal in their starting positions.The operation may be in either initial or active state and enters initial state afterwards.

Parameters

operation	Handle of a running AE operation
srcData	Reference to final chunk of input data to be encrypted
srcLen	length of the input data
destData	Output buffer. Can be omitted if the output is to be discarded.
destLen	length of the buffer.
tag	Output buffer filled with the computed tag
tagLen	length of the tag.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER If the output or tag buffer is not large enoughto contain the output.

10.9.1.3 TEE_AEInit()

```
TEE_Result TEE_AEInit (
        TEE_OperationHandle operation,
        const void * nonce,
        uint32_t nonceLen,
        uint32_t tagLen,
        uint32_t AADLen,
        uint32_t payloadLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEInit() - Initializes an Authentication Encryption operation.

The operation must be in initial state and remains in the initial state afterwards.

Parameters

operation	A handle on the operation.
nonce	The operation nonce or IV
nonceLen	length of nonce
tagLen	Size in bits of the tag
AADLen	Length in bytes of the AAD
payloadLen	Length in bytes of the payload.

Returns

0 on success.

TEE_ERROR_NOT_SUPPORTED If the tag length is not supported by the algorithm.

10.9.1.4 TEE_AEUpdate()

```
TEE_Result TEE_AEUpdate (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEUpdate() - Accumulates data for an Authentication Encryption operation

This function describes Input data does not have to be a multiple of block size. Subsequent calls to this function are possible. Unless one or more calls of this function have supplied sufficient input data,no output is generated. when using this routine to decrypt the returned data may be corrupt since the integrity check is not performed until all the data has been processed. If this is a concern then only use the TEE_AEDecryptFinal routine.

Parameters

operation	Handle of a running AE operation.
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of the input buffer.
destData	Output buffer
destLen	length of the out put buffer.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER if the output buffer is not large enough to contain the output.

10.9.1.5 TEE_AEUpdateAAD()

```
void TEE_AEUpdateAAD (
        TEE_OperationHandle operation,
        const void * AADdata,
        uint32_t AADdataLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEUpdateAAD() - Feeds a new chunk of Additional Authentication Data (AAD) to the AE operation. Subsequent calls to this function are possible.

The TEE_AEUpdateAAD function feeds a new chunk of Additional Authentication Data (AAD) to the AE operation. Subsequent calls to this function are possible.The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation SHALL be in initial state and remains in initial state afterwards.

Parameters

operation	Handle on the AE operation
AADdata	Input buffer containing the chunk of AAD
AADdataLen	length of the chunk of AAD.

10.9.1.6 TEE_AllocateOperation()

```
TEE_Result TEE_AllocateOperation (
        TEE_OperationHandle * operation,
        uint32_t algorithm,
        uint32_t mode,
        uint32_t maxKeySize )
```

Crypto, for all Crypto Functions.

TEE_AllocateOperation() - Allocates a handle for a new cryptographic operation and sets the mode and algorithm type.

If this function does not return with TEE_SUCCESS then there is no valid handle value.Once a cryptographic operation has been created, the implementation shall guarantee that all resources necessary for the operation are allocated and that any operation with a key of at most maxKeySize bits can be performed. For algorithms that take multiple keys, for example the AES XTS algorithm, the maxKeySize parameter specifies the size of the largest key. It is up to the implementation to properly allocate space for multiple keys if the algorithm so requires.

Parameters

operation	reference to generated operation handle.
algorithm	One of the cipher algorithms.
mode	The operation mode.
maxKeySize	Maximum key size in bits for the operation.

Returns

0 in case of success

TEE_ERROR_OUT_OF_MEMORY If there are not enough resources to allocate the operation.

TEE_ERROR_NOT_SUPPORTED If the mode is not compatible with the algorithm or key size or if the algorithm is not one of the listed algorithms or if maxKeySize is not appropriate for the algorithm.

10.9.1.7 TEE_AllocatePersistentObjectEnumerator()

```
TEE_Result
TEE_AllocatePersistentObjectEnumerator (
            TEE_ObjectEnumHandle * objectEnumerator )
```

10.9.1.8 TEE_AllocatePropertyEnumerator()

```
TEE_Result TEE_AllocatePropertyEnumerator (
            TEE_PropSetHandle * enumerator )
```

10.9.1.9 TEE_AllocateTransientObject()

```
TEE_Result TEE_AllocateTransientObject (
            TEE_ObjectType objectType,
            uint32_t maxKeySize,
            TEE_ObjectHandle * object )
```

Crypto, Asymmetric key Verification Functions.

TEE_AllocateTransientObject() - Allocates an uninitialized transient object. Transient objects are used to hold a cryptographic object (key or key-pair).

The value TEE_KEYSIZE_NO_KEY should be used for maxObjectSize for object types that do not require a key so that all the container resources can be pre-allocated. As allocated, the container is uninitialized. It can be initialized by subsequently importing the object material,generating an object, deriving an object, or loading an object from the Trusted Storage.

Parameters

objectType	Type of uninitialized object container to be created
maxKeySize	Key Size of the object.
object	Filled with a handle on the newly created key container.

Returns

0 on success

TEE_ERROR_OUT_OF_MEMORY If not enough resources are available to allocate the object handle.

TEE_ERROR_NOT_SUPPORTED If the key size is not supported or the object
type is not supported.

10.9.1.10 TEE_AsymmetricDecrypt()

```
TEE_Result TEE_AsymmetricDecrypt (
    TEE_OperationHandle operation,
    const TEE_Attribute * params,
    uint32_t paramCount,
    const void * srcData,
    uint32_t srcLen,
    void * destData,
    uint32_t * destLen )
```

10.9.1.11 TEE_AsymmetricEncrypt()

```
TEE_Result TEE_AsymmetricEncrypt (
    TEE_OperationHandle operation,
    const TEE_Attribute * params,
    uint32_t paramCount,
    const void * srcData,
    uint32_t srcLen,
    void * destData,
    uint32_t * destLen )
```

10.9.1.12 TEE_AsymmetricSignDigest()

```
TEE_Result TEE_AsymmetricSignDigest (
    TEE_OperationHandle operation,
    const TEE_Attribute * params,
    uint32_t paramCount,
    const void * digest,
    uint32_t digestLen,
    void * signature,
    uint32_t * signatureLen )
```

Crypto, Asymmetric key Verification Functions.

TEE_AsymmetricSignDigest() - Signs a message digest within an asymmetric operation.

Parameters

operation	Handle on the operation, which SHALL have been suitably set up with an operation key.
params	Optional operation parameters
paramCount	size of param
digest	Input buffer containing the input message digest
digestLen	length of input buffer.
signature	Output buffer written with the signature of the digest
signatureLen	length of output buffer.

Returns

0 on sccess

TEE_ERROR_SHORT_BUFFER If the signature buffer is not large enough to hold the result

10.9.1.13 TEE_AsymmetricVerifyDigest()

```
TEE_Result TEE_AsymmetricVerifyDigest (
        TEE_OperationHandle operation,
        const TEE_Attribute * params,
        uint32_t paramCount,
        const void * digest,
        uint32_t digestLen,
        const void * signature,
        uint32_t signatureLen )
```

Crypto, Asymmetric key Verification Functions.

TEE_AsymmetricVerifyDigest() - verifies a message digest signature within an asymmetric operation.

This function describes the message digest signature verify by calling ed25519_verify().

Parameters

operation	Handle on the operation, which SHALL have been suitably set up with an operation key.
params	Optional operation parameters
paramCount	size of param.
digest	Input buffer containing the input message digest
digestLen	length of input buffer.
signature	Output buffer written with the signature of the digest
signatureLen	length of output buffer.

Returns

TEE_SUCCESS on success

TEE_ERROR_SIGNATURE_INVALID if the signature is invalid.

10.9.1.14 TEE_BigIntAdd() `void TEE_BigIntAdd (`

```
TEE_BigInt * dest,
const TEE_BigInt * op1,
const TEE_BigInt * op2 )
```

10.9.1.15 TEE_BigIntAddMod() `void TEE_BigIntAddMod (`

```
TEE_BigInt * dest,
const TEE_BigInt * op1,
const TEE_BigInt * op2,
const TEE_BigInt * n )
```

10.9.1.16 TEE_BigIntCmp() `int32_t TEE_BigIntCmp (`

```
const TEE_BigInt * op1,
const TEE_BigInt * op2 )
```

10.9.1.17 TEE_BigIntCmpS32() `int32_t TEE_BigIntCmpS32 (`

```
const TEE_BigInt * op,
int32_t shortVal )
```

10.9.1.18 TEE_BigIntComputeExtendedGcd() `void TEE_BigIntComputeExtendedGcd (`

```
TEE_BigInt * gcd,
TEE_BigInt * u,
TEE_BigInt * v,
const TEE_BigInt * op1,
const TEE_BigInt * op2 )
```

10.9.1.19 TEE_BigIntComputeFMM() `void TEE_BigIntComputeFMM (`

```
TEE_BigIntFMM * dest,
const TEE_BigIntFMM * op1,
const TEE_BigIntFMM * op2,
const TEE_BigInt * n,
const TEE_BigIntFMMContext * context )
```

10.9.1.20 TEE_BigIntConvertFromFMM() `void TEE_BigIntConvertFromFMM (`

```
TEE_BigInt * dest,
const TEE_BigIntFMM * src,
const TEE_BigInt * n,
const TEE_BigIntFMMContext * context )
```

10.9.1.21 TEE_BigIntConvertFromOctetString()

```
TEE_Result TEE_BigIntConvertFromOctetString (
        TEE_BigInt * dest,
        const uint8_t * buffer,
        uint32_t bufferLen,
        int32_t sign )
```

10.9.1.22 TEE_BigIntConvertFromS32()

```
void TEE_BigIntConvertFromS32 (
        TEE_BigInt * dest,
        int32_t shortVal )
```

10.9.1.23 TEE_BigIntConvertToFMM()

```
void TEE_BigIntConvertToFMM (
        TEE_BigIntFMM * dest,
        const TEE_BigInt * src,
        const TEE_BigInt * n,
        const TEE_BigIntFMMContext * context )
```

10.9.1.24 TEE_BigIntConvertToOctetString()

```
TEE_Result TEE_BigIntConvertToOctetString (
        uint8_t * buffer,
        uint32_t * bufferLen,
        const TEE_BigInt * bigInt )
```

10.9.1.25 TEE_BigIntConvertToS32()

```
TEE_Result TEE_BigIntConvertToS32 (
        int32_t * dest,
        const TEE_BigInt * src )
```

10.9.1.26 TEE_BigIntDiv()

```
void TEE_BigIntDiv (
        TEE_BigInt * dest_q,
        TEE_BigInt * dest_r,
        const TEE_BigInt * op1,
        const TEE_BigInt * op2 )
```

10.9.1.27 TEE_BigIntFMMContextSizeInU32()

```
uint32_t TEE_BigIntFMMContextSizeInU32 (
        uint32_t modulusSizeInBits )
```

10.9.1.28 TEE_BigIntFMMConvertToBigInt()

```
void TEE_BigIntFMMConvertToBigInt (
    TEE_BigInt * dest,
    const TEE_BigIntFMM * src,
    const TEE_BigInt * n,
    const TEE_BigIntFMMContext * context )
```

10.9.1.29 TEE_BigIntFMMSizeInU32()

```
uint32_t TEE_BigIntFMMSizeInU32 (
    uint32_t modulusSizeInBits )
```

10.9.1.30 TEE_BigIntGetBit()

```
bool TEE_BigIntGetBit (
    const TEE_BigInt * src,
    uint32_t bitIndex )
```

10.9.1.31 TEE_BigIntGetBitCount()

```
uint32_t TEE_BigIntGetBitCount (
    const TEE_BigInt * src )
```

10.9.1.32 TEE_BigIntInit()

```
void TEE_BigIntInit (
    TEE_BigInt * bigInt,
    uint32_t len )
```

10.9.1.33 TEE_BigIntInitFMM()

```
void TEE_BigIntInitFMM (
    TEE_BigIntFMM * bigIntFMM,
    uint32_t len )
```

10.9.1.34 TEE_BigIntInitFMMContext()

```
void TEE_BigIntInitFMMContext (
    TEE_BigIntFMMContext * context,
    uint32_t len,
    const TEE_BigInt * modulus )
```

10.9.1.35 TEE_BigIntInvMod()

```
void TEE_BigIntInvMod (
    TEE_BigInt * dest,
    const TEE_BigInt * op,
    const TEE_BigInt * n )
```

10.9.1.36 TEE_BigIntIsProbablePrime()

```
int32_t TEE_BigIntIsProbablePrime (
        const TEE_BigInt * op,
        uint32_t confidenceLevel )
```

10.9.1.37 TEE_BigIntMod()

```
void TEE_BigIntMod (
        TEE_BigInt * dest,
        const TEE_BigInt * op,
        const TEE_BigInt * n )
```

10.9.1.38 TEE_BigIntMul()

```
void TEE_BigIntMul (
        TEE_BigInt * dest,
        const TEE_BigInt * op1,
        const TEE_BigInt * op2 )
```

10.9.1.39 TEE_BigIntMulMod()

```
void TEE_BigIntMulMod (
        TEE_BigInt * dest,
        const TEE_BigInt * op1,
        const TEE_BigInt * op2,
        const TEE_BigInt * n )
```

10.9.1.40 TEE_BigIntNeg()

```
void TEE_BigIntNeg (
        TEE_BigInt * dest,
        const TEE_BigInt * op )
```

10.9.1.41 TEE_BigIntRelativePrime()

```
bool TEE_BigIntRelativePrime (
        const TEE_BigInt * op1,
        const TEE_BigInt * op2 )
```

10.9.1.42 TEE_BigIntShiftRight()

```
void TEE_BigIntShiftRight (
        TEE_BigInt * dest,
        const TEE_BigInt * op,
        size_t bits )
```

10.9.1.43 TEE_BigIntSquare()

```
void TEE_BigIntSquare (
        TEE_BigInt * dest,
        const TEE_BigInt * op )
```

10.9.1.44 TEE_BigIntSquareMod()

```
void TEE_BigIntSquareMod (
        TEE_BigInt * dest,
        const TEE_BigInt * op,
        const TEE_BigInt * n )
```

10.9.1.45 TEE_BigIntSub()

```
void TEE_BigIntSub (
        TEE_BigInt * dest,
        const TEE_BigInt * op1,
        const TEE_BigInt * op2 )
```

10.9.1.46 TEE_BigIntSubMod()

```
void TEE_BigIntSubMod (
        TEE_BigInt * dest,
        const TEE_BigInt * op1,
        const TEE_BigInt * op2,
        const TEE_BigInt * n )
```

10.9.1.47 TEE_CheckMemoryAccessRights()

```
TEE_Result TEE_CheckMemoryAccessRights (
        uint32_t accessFlags,
        void * buffer,
        uint32_t size )
```

10.9.1.48 TEE_CipherDoFinal()

```
TEE_Result TEE_CipherDoFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen )
```

TEE_CipherDoFinal() - Finalizes the cipher operation, processing data that has not been processed by previous calls to TEE_CipherUpdate as well as data supplied in srcData .

This function describes The operation handle can be reused or re-initialized. The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation SHALL be in active state and is set to initial state afterwards.

Parameters

operation	Handle of a running Cipher operation
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of input buffer
destData	output buffer
destLen	ouput buffer length.

Returns

0 on success

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output

10.9.1.49 TEE_CipherInit()

```
void TEE_CipherInit (
    TEE_OperationHandle operation,
    const void * nonce,
    uint32_t nonceLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_CipherInit() - starts the symmetric cipher operation.

The operation shall have been associated with a key. If the operation is in active state, it is reset and then initialized. If the operation is in initial state, it is moved to active state.

Parameters

operation	A handle on an opened cipher operation setup with a key
nonce	Buffer containing the operation Initialization Vector as appropriate.
nonceLen	length of the buffer

10.9.1.50 TEE_CipherUpdate()

```
TEE_Result TEE_CipherUpdate (
    TEE_OperationHandle operation,
    const void * srcData,
    uint32_t srcLen,
    void * destData,
    uint32_t * destLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_CipherUpdate() - encrypts or decrypts input data.

Input data does not have to be a multiple of block size. Subsequent calls to this function are possible. Unless one or more calls of this function have supplied sufficient input data, no output is generated. The cipher operation is finalized with a call to TEE_CipherDoFinal .The buffers srcData and destData SHALL be either completely disjoint or equal in their starting positions.The operation SHALL be in active state.

Parameters

operation	Handle of a running Cipher operation
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of input buffer
destData	output buffer
destLen	ouput buffer length.

Returns

0 on success else

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output. In this case, the input is not fed into the algorithm.

10.9.1.51 TEE_CloseAndDeletePersistentObject()

```
void TEE_CloseAndDeletePersistentObject (
        TEE_ObjectHandle object )
```

10.9.1.52 TEE_CloseAndDeletePersistentObject1()

```
TEE_Result TEE_CloseAndDeletePersistentObject1 (
        TEE_ObjectHandle object )
```

10.9.1.53 TEE_CloseObject()

```
void TEE_CloseObject (
        TEE_ObjectHandle object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_CloseObject() - Closes an opened object handle.

The object can be persistent or transient.For transient objects, TEE_CloseObject is equivalent to TEE_Free↵TransientObject.

Parameters

object	Handle of the object.

Returns

TEE_SUCCESS if success else error occured.

TEE_CloseObject() - Function closes an opened object handle.

The object can be persistent or transient.For transient objects, TEE_CloseObject is equivalent to TEE_Free↵TransientObject.

Parameters

object	Handle of the object

Returns

TEE_SUCCESS if success else error occured.

10.9.1.54 TEE_CloseTASession()

```
void TEE_CloseTASession (
        TEE_TASessionHandle session )
```

10.9.1.55 TEE_CopyObjectAttributes()

```
void TEE_CopyObjectAttributes (
        TEE_ObjectHandle destObject,
        TEE_ObjectHandle srcObject )
```

10.9.1.56 TEE_CopyObjectAttributes1()

```
TEE_Result TEE_CopyObjectAttributes1 (
        TEE_ObjectHandle destObject,
        TEE_ObjectHandle srcObject )
```

10.9.1.57 TEE_CopyOperation()

```
void TEE_CopyOperation (
        TEE_OperationHandle dstOperation,
        TEE_OperationHandle srcOperation )
```

10.9.1.58 TEE_CreatePersistentObject()

```
TEE_Result TEE_CreatePersistentObject (
        uint32_t storageID,
        const void * objectID,
        uint32_t objectIDLen,
        uint32_t flags,
        TEE_ObjectHandle attributes,
        const void * initialData,
        uint32_t initialDataLen,
        TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_CreatePersistentObject() - Creates a persistent object with initial attributes.

In this function an initial data stream content returns either a handle on the created object or TEE_HANDLE_NULL upon failure.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
attributes	A handle on a persistent object or an initialized transient object from which to take the persistent object attributes
initialData	The initial data content of the persistent object
initialDataLen	The initial data content of the persistent object

Returns

0 if success else error occured.

TEE_CreatePersistentObject() - Creates a persistent object with initial attributes.

An initial data stream content, and optionally returns either a handle on the created object, or TEE_HANDLE_NULL upon failure.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
attributes	A handle on a persistent object or an initialized transient object from which to take the persistent object attributes
initialData	The initial data content of the persistent object
initialDataLen	The initial data content of the persistent object
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success, else error occured.

10.9.1.59 TEE_DeriveKey()

```
void TEE_DeriveKey (
        TEE_OperationHandle operation,
        const TEE_Attribute * params,
        uint32_t paramCount,
        TEE_ObjectHandle derivedKey )
```

10.9.1.60 TEE_DigestDoFinal()

```
TEE_Result TEE_DigestDoFinal (
        TEE_OperationHandle operation,
        const void * chunk,
        uint32_t chunkLen,
        void * hash,
        uint32_t * hashLen )
```

TEE_DigestDoFinal() - Finalizes the message digest operation and produces the message hash.

This function finalizes the message digest operation and produces the message hash. Afterwards the Message Digest operation is reset to initial state and can be reused.

Parameters

operation	Handle of a running Message Digest operation.
chunk	Chunk of data to be hashed.
chunkLen	size of the chunk.
hash	Output buffer filled with the message hash.
hashLen	lenth of the mesaage hash.

Returns

0 on success

TEE_ERROR_SHORT_BUFFER If the output buffer is too small. In this case, the operation is not finalized.

10.9.1.61 TEE_DigestUpdate()

```
void TEE_DigestUpdate (
        TEE_OperationHandle operation,
        const void * chunk,
        uint32_t chunkSize )
```

Crypto, Message Digest Functions.

TEE_DigestUpdate()- Accumulates message data for hashing.

This function describes the message does not have to be block aligned. Subsequent calls to this function are possible.The operation may be in either initial or active state and becomes active.

Parameters

operation	Handle of a running Message Digest operation.
chunk	Chunk of data to be hashed
chunkSize	size of the chunk.

10.9.1.62 TEE_Free()

```
void TEE_Free (
        void * buffer )
```

TEE_Free() - causes the space pointed to by buffer to be deallocated;that is made available for further allocation.

This function describes if buffer is a NULL pointer, TEE_Free does nothing. Otherwise, it is a Programmer Error if the argument does not match a pointer previously returned by the TEE_Malloc or TEE_Realloc if the space has been deallocated by a call to TEE_Free or TEE_Realloc.

Parameters

buffer	The pointer to the memory block to be freed.

10.9.1.63 TEE_FreeOperation()

```
void TEE_FreeOperation (
        TEE_OperationHandle operation )
```

Crypto, for all Crypto Functions.

TEE_FreeOperation() - Deallocates all resources associated with an operation handle.

This function deallocates all resources associated with an operation handle. After this function is called, the operation handle is no longer valid. All cryptographic material in the operation is destroyed. The function does nothing if operation is TEE_HANDLE_NULL.

Parameters

operation	Reference to operation handle.

Returns

nothing after the operation free.

10.9.1.64 TEE_FreePersistentObjectEnumerator()

```
void TEE_FreePersistentObjectEnumerator (
        TEE_ObjectEnumHandle objectEnumerator )
```

10.9.1.65 TEE_FreePropertyEnumerator()

```
void TEE_FreePropertyEnumerator (
        TEE_PropSetHandle enumerator )
```

10.9.1.66 TEE_FreeTransientObject()

```
void TEE_FreeTransientObject (
        TEE_ObjectHandle object )
```

Crypto, Asymmetric key Verification Functions.

TEE_FreeTransientObject() - Deallocates a transient object previously allocated with TEE_AllocateTransientObject .

this function describes the object handle is no longer valid and all resources associated with the transient object shall have been reclaimed after the TEE_AllocateTransientObject() call.

Parameters

object	Handle on the object to free.

10.9.1.67 TEE_GenerateKey()

```
TEE_Result TEE_GenerateKey (
        TEE_ObjectHandle object,
        uint32_t keySize,
        const TEE_Attribute * params,
        uint32_t paramCount )
```

Crypto, Asymmetric key Verification Functions.

TEE_GenerateKey () - Generates a random key or a key-pair and populates a transient key object with the generated key material.

The size of the desired key is passed in the keySize parameter and shall be less than or equal to the maximum key size specified when the transient object was created.

Parameters

object	Handle on an uninitialized transient key to populate with the generated key.
keySize	Requested key size shall be less than or equal to the maximum key size specified when the object container was created
params	Parameters for the key generation.
paramCount	The values of all parameters are copied nto the object so that the params array and all the memory buffers it points to may be freed after this routine returns without affecting the object.

Returns

0 on succes

TEE_ERROR_BAD_PARAMETERS If an incorrect or inconsistent attribute is detected. The checks that are performed depend on the implementation.

10.9.1.68 TEE_GenerateRandom()

```
void TEE_GenerateRandom (
        void * randomBuffer,
        uint32_t randomBufferLen )
```

Crypto, common.

TEE_GenerateRandom() - Generates random data.

This function generates random data of random buffer length and is stored in to random Buffer by calling wc_↩
RNG_GenerateBlock().If ret is not equal
to 0 then TEE_Panic is called.

Parameters

randomBuffer	Reference to generated random data
randomBufferLen	Byte length of requested random data

Returns

random data random data will be returned.

TEE_GenerateRandom() - Generates random data.

This function generates random data of random bufferlength and is stored in to randomBuffer by calling sgx_read↩
_rand().

Parameters

randomBuffer	Reference to generated random data
randomBufferLen	Byte length of requested random data

10.9.1.69 TEE_GetCancellationFlag()

```
bool TEE_GetCancellationFlag (
    void )
```

10.9.1.70 TEE_GetInstanceData()

```
const void * TEE_GetInstanceData (
    void )
```

10.9.1.71 TEE_GetNextPersistentObject()

```
TEE_Result TEE_GetNextPersistentObject (
    TEE_ObjectEnumHandle objectEnumerator,
    TEE_ObjectInfo * objectInfo,
    void * objectID,
    uint32_t * objectIDLen )
```

10.9.1.72 TEE_GetNextProperty()

```
TEE_Result TEE_GetNextProperty (
    TEE_PropSetHandle enumerator )
```

10.9.1.73 TEE_GetObjectBufferAttribute()

```
TEE_Result TEE_GetObjectBufferAttribute (
    TEE_ObjectHandle object,
    uint32_t attributeID,
    void * buffer,
    uint32_t * size )
```

10.9.1.74 TEE_GetObjectInfo()

```
void TEE_GetObjectInfo (
    TEE_ObjectHandle object,
    TEE_ObjectInfo * objectInfo )
```

10.9.1.75 TEE_GetObjectInfo1()

```
TEE_Result TEE_GetObjectInfo1 (
    TEE_ObjectHandle object,
    TEE_ObjectInfo * objectInfo )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_GetObjectInfo1() - Returns the characteristics of an object.

This function returns a handle which can be used to access the object's attributes and data stream.

Parameters

objectInfo	Pointer to a structure filled with the object information
object	Handle of the object

Returns

0 if success else error occured.

TEE_GetObjectInfo1() - Function returns the characteristics of an object.

It returns a handle that can be used to access the object's attributes and data stream.

Parameters

objectInfo	Pointer to a structure filled with the object information
object	Handle of the object

Returns

0 if success else error occured.

10.9.1.76 TEE_GetObjectValueAttribute()

```
TEE_Result TEE_GetObjectValueAttribute (
        TEE_ObjectHandle object,
        uint32_t attributeID,
        uint32_t * a,
        uint32_t * b )
```

10.9.1.77 TEE_GetOperationInfo()

```
void TEE_GetOperationInfo (
        TEE_OperationHandle operation,
        TEE_OperationInfo * operationInfo )
```

10.9.1.78 TEE_GetOperationInfoMultiple()

```
TEE_Result TEE_GetOperationInfoMultiple (
        TEE_OperationHandle operation,
        TEE_OperationInfoMultiple * operationInfoMultiple,
        uint32_t * operationSize )
```

10.9.1.79 TEE_GetPropertyAsBinaryBlock()

```
TEE_Result TEE_GetPropertyAsBinaryBlock (
    TEE_PropSetHandle propsetOrEnumerator,
    const char * name,
    void * valueBuffer,
    uint32_t * valueBufferLen )
```

10.9.1.80 TEE_GetPropertyAsBool()

```
TEE_Result TEE_GetPropertyAsBool (
    TEE_PropSetHandle propsetOrEnumerator,
    const char * name,
    bool * value )
```

10.9.1.81 TEE_GetPropertyAsIdentity()

```
TEE_Result TEE_GetPropertyAsIdentity (
    TEE_PropSetHandle propsetOrEnumerator,
    const char * name,
    TEE_Identity * value )
```

10.9.1.82 TEE_GetPropertyAsString()

```
TEE_Result TEE_GetPropertyAsString (
    TEE_PropSetHandle propsetOrEnumerator,
    const char * name,
    char * valueBuffer,
    uint32_t * valueBufferLen )
```

10.9.1.83 TEE_GetPropertyAsU32()

```
TEE_Result TEE_GetPropertyAsU32 (
    TEE_PropSetHandle propsetOrEnumerator,
    const char * name,
    uint32_t * value )
```

10.9.1.84 TEE_GetPropertyAsUUID()

```
TEE_Result TEE_GetPropertyAsUUID (
    TEE_PropSetHandle propsetOrEnumerator,
    const char * name,
    TEE_UUID * value )
```

10.9.1.85 TEE_GetPropertyName()

```
TEE_Result TEE_GetPropertyName (
    TEE_PropSetHandle enumerator,
    void * nameBuffer,
    uint32_t * nameBufferLen )
```

10.9.1.86 TEE_GetREETime()

```
void TEE_GetREETime (
    TEE_Time * time )
```

Core Functions, Time Functions.

TEE_GetREETime() - Retrieves the current REE system time.

This function retrieves the current time as seen from the point of view of the REE.

Parameters

time	Filled with the number of seconds and milliseconds

TEE_GetREETime() - Function retrieves the current REE system time.

This function retrieves the current time as seen from the point of view of the REE.

Parameters

time	Filled with the number of seconds and milliseconds.

10.9.1.87 TEE_GetSystemTime() `void TEE_GetSystemTime ( TEE_Time * time )`

Core Functions, Time Functions.

TEE_GetSystemTime() - Retrieves the current system time.

This function describes the system time has an arbitrary implementation
defined origin that can vary across TA instances. The minimum guarantee
is that the system time shall be monotonic for a given TA instance.

Parameters

time	Filled with the number of seconds and milliseconds

TEE_GetSystemTime() - Retrieves the current system time.

The system time has an arbitrary implementation-defined origin that can vary across TA instances

Parameters

time	Filled with the number of seconds and milliseconds.

10.9.1.88 TEE_GetTAPersistentTime() `TEE_Result TEE_GetTAPersistentTime ( TEE_Time * time )`

10.9.1.89 TEE_InitRefAttribute()

```
void TEE_InitRefAttribute (
        TEE_Attribute * attr,
        uint32_t attributeID,
        const void * buffer,
        uint32_t length )
```

Crypto, Asymmetric key Verification Functions.

TEE_InitRefAttribute() - The helper function can be used to populate a single attribute either with a reference to a buffer or with integer values.

In TEE_InitRefAttribute () only the buffer pointer is copied, not the content of the buffer. This means that the attribute structure maintains a pointer back to the supplied buffer. It is the responsibility of the TA author to ensure that the contents of the buffer maintain their value until the attributes array is no longer in use.

Parameters

attr	attribute structure to initialize.
attributeID	Identifier of the attribute to populate.
buffer	input buffer that holds the content of the attribute.
length	buffer length.

10.9.1.90 TEE_InitValueAttribute()

```
void TEE_InitValueAttribute (
        TEE_Attribute * attr,
        uint32_t attributeID,
        uint32_t a,
        uint32_t b )
```

Crypto, Asymmetric key Verification Functions.

TEE_InitValueAttribute() - The helper function can be used to populate a single attribute either with a reference to a buffer or with integer values.

Parameters

attr	attribute structure to initialize.
attributeID	Identifier of the attribute to populate.
a	unsigned integer value to assign to the a member of the attribute structure.
b	unsigned integer value to assign to the b member of the attribute structure

10.9.1.91 TEE_InvokeTACommand()

```
TEE_Result TEE_InvokeTACommand (
        TEE_TASessionHandle session,
        uint32_t cancellationRequestTimeout,
        uint32_t commandID,
        uint32_t paramTypes,
        TEE_Param params[TEE_NUM_PARAMS],
        uint32_t * returnOrigin )
```

10.9.1.92 TEE_IsAlgorithmSupported()

```
TEE_Result TEE_IsAlgorithmSupported (
    uint32_t algId,
    uint32_t element )
```

10.9.1.93 TEE_MACCompareFinal()

```
TEE_Result TEE_MACCompareFinal (
    TEE_OperationHandle operation,
    const void * message,
    uint32_t messageLen,
    const void * mac,
    uint32_t macLen )
```

10.9.1.94 TEE_MACComputeFinal()

```
TEE_Result TEE_MACComputeFinal (
    TEE_OperationHandle operation,
    const void * message,
    uint32_t messageLen,
    void * mac,
    uint32_t * macLen )
```

10.9.1.95 TEE_MACInit()

```
void TEE_MACInit (
    TEE_OperationHandle operation,
    const void * IV,
    uint32_t IVLen )
```

10.9.1.96 TEE_MACUpdate()

```
void TEE_MACUpdate (
    TEE_OperationHandle operation,
    const void * chunk,
    uint32_t chunkSize )
```

10.9.1.97 TEE_Malloc()

```
void * TEE_Malloc (
    uint32_t size,
    uint32_t hint )
```

TEE_Malloc() - Allocates space for an object whose size in bytes is specified in the parameter size.

This function describes the pointer returned is guaranteed to be aligned
such that it may be assigned as a pointer to any basic C type.The valid hint values are a bitmask and can be independently set. This parameter allows Trusted Applications to refer to various pools of memory or to
request special characteristics for the allocated memory by using an
implementation-defined hint. Future versions of this specification may introduce additional standard hints.

Parameters

size	The size of the buffer to be allocated.
hint	A hint to the allocator.

Returns

Upon successful completion, with size not equal to zero, the function returns a pointer to the allocated space.

10.9.1.98 TEE_MaskCancellation()

```
bool TEE_MaskCancellation (
    void )
```

10.9.1.99 TEE_MemCompare()

```
int32_t TEE_MemCompare (
    const void * buffer1,
    const void * buffer2,
    uint32_t size )
```

10.9.1.100 TEE_MemFill()

```
void * TEE_MemFill (
    void * buff,
    uint32_t x,
    uint32_t size )
```

10.9.1.101 TEE_MemMove()

```
void * TEE_MemMove (
    void * dest,
    const void * src,
    uint32_t size )
```

10.9.1.102 TEE_OpenPersistentObject()

```
TEE_Result TEE_OpenPersistentObject (
    uint32_t storageID,
    const void * objectID,
    uint32_t objectIDLen,
    uint32_t flags,
    TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_OpenPersistentObject() - Opens a handle on an existing persistent object.

This function returns a handle which can be used to access the object's attributes and data stream.

Parameters

storageID	The storage to use
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success else error occured.

TEE_OpenPersistentObject() - Opens a handle on an existing persistent object.

This function returns a handle that can be used to access the object's attributes and data stream.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success, else error occured.

10.9.1.103 TEE_OpenTASession()

```
TEE_Result TEE_OpenTASession (
        const TEE_UUID * destination,
        uint32_t cancellationRequestTimeout,
        uint32_t paramTypes,
        TEE_Param params[TEE_NUM_PARAMS],
        TEE_TASessionHandle * session,
        uint32_t * returnOrigin )
```

10.9.1.104 TEE_Panic()

```
void TEE_Panic (
        TEE_Result panicCode )
```

10.9.1.105 TEE_PopulateTransientObject()

```
TEE_Result TEE_PopulateTransientObject (
        TEE_ObjectHandle object,
        const TEE_Attribute * attrs,
        uint32_t attrCount )
```

10.9.1.106 TEE_ReadObjectData()

```
TEE_Result TEE_ReadObjectData (
        TEE_ObjectHandle object,
        void * buffer,
        uint32_t size,
        uint32_t * count )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_ReadObjectData() - Attempts to read size bytes from the data stream associated with the object into the buffer pointed to by buffer.

The bytes are read starting at the position in the data stream currently stored in the object handle. The handle's position is incremented by the number of bytes actually read. On completion of TEE_ReadObjectData sets the number of bytes actually read in the "uint32_t" pointed to by count. The value written to ∗count may be less than size if the number of bytes until the end-of3067 stream is less than size. It is set to 0 if the position at the start of the read operation is at or beyond the end-of-stream. These are the only cases where ∗count may be less than size.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write
count	size of the buffer.

Returns

TEE_SUCCESS if success else error occured.

TEE_ReadObjectData() - Attempts to read size bytes from the data stream associated with the object object into the buffer pointed to by buffer.

The bytes are read starting at the position in the data stream currently stored in the object handle. The handle's position is incremented by the number of bytes actually read. On completion TEE_ReadObjectData sets the number of bytes actually read in the uint32_t pointed to by count. The value written to ∗count may be less than size if the number of bytes until the end-of3067 stream is less than size. It is set to 0 if the position at the start of the read operation is at or beyond the end-of-stream. These are the only cases where ∗count may be less than size.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write
count	size of the buffer.

Returns

TEE_SUCCESS if success, else error occured.

10.9.1.107 TEE_Realloc()

```
void * TEE_Realloc (
    void * buffer,
    uint32_t newSize )
```

TEE_Realloc() - Changes the size of the memory object pointed to by buffer to the size specified by new size.

This function describes the content of the object remains unchanged up to the lesser of the new and old sizes. Space in excess of the old size contains unspecified content. If the new size of the memory object requires movement of the object, the space for the previous instantiation of the object is deallocated. If the space cannot be allocated, the original object remains allocated, and this function returns a NULL pointer.

Parameters

buffer	The pointer to the object to be reallocated.
newSize	The new size required for the object

Returns

Upon successful completion, TEE_Realloc returns a pointer to the (possibly moved) allocated space. If there is not enough available memory, TEE_Realloc returns a NULL pointer and the original buffer is still allocated and unchanged.

10.9.1.108 TEE_RenamePersistentObject()

```
TEE_Result TEE_RenamePersistentObject (
    TEE_ObjectHandle object,
    const void * newObjectID,
    uint32_t newObjectIDLen )
```

10.9.1.109 TEE_ResetOperation()

```
void TEE_ResetOperation (
    TEE_OperationHandle operation )
```

10.9.1.110 TEE_ResetPersistentObjectEnumerator()

```
void TEE_ResetPersistentObjectEnumerator (
    TEE_ObjectEnumHandle objectEnumerator )
```

10.9.1.111 TEE_ResetPropertyEnumerator()

```
void TEE_ResetPropertyEnumerator (
        TEE_PropSetHandle enumerator )
```

10.9.1.112 TEE_ResetTransientObject()

```
void TEE_ResetTransientObject (
        TEE_ObjectHandle object )
```

10.9.1.113 TEE_RestrictObjectUsage()

```
void TEE_RestrictObjectUsage (
        TEE_ObjectHandle object,
        uint32_t objectUsage )
```

10.9.1.114 TEE_RestrictObjectUsage1()

```
TEE_Result TEE_RestrictObjectUsage1 (
        TEE_ObjectHandle object,
        uint32_t objectUsage )
```

10.9.1.115 TEE_SeekObjectData()

```
TEE_Result TEE_SeekObjectData (
        TEE_ObjectHandle object,
        int32_t offset,
        TEE_Whence whence )
```

10.9.1.116 TEE_SetInstanceData()

```
void TEE_SetInstanceData (
        const void * instanceData )
```

10.9.1.117 TEE_SetOperationKey()

```
TEE_Result TEE_SetOperationKey (
        TEE_OperationHandle operation,
        TEE_ObjectHandle key )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_SetOperationKey() - Programs the key of an operation; that is, it associates an operation with a key.

The key material is copied from the key object handle into the operation. After the key has been set, there is no longer any link between the operation and the key object. The object handle can be closed or reset and this will not affect the operation. This copied material exists until the operation is freed using TEE_FreeOperation or another key is set into the operation.

Parameters

operation	Operation handle.
key	A handle on a key object.

Returns

0 on success return

TEE_ERROR_CORRUPT_OBJECT If the object is corrupt. The object handle is closed.

TEE_ERROR_STORAGE_NOT_AVAILABLE If the persistent object is stored in a storage area which is currently inaccessible.

10.9.1.118 TEE_SetOperationKey2()

```
TEE_Result TEE_SetOperationKey2 (
        TEE_OperationHandle operation,
        TEE_ObjectHandle key1,
        TEE_ObjectHandle key2 )
```

10.9.1.119 TEE_SetTAPersistentTime()

```
TEE_Result TEE_SetTAPersistentTime (
        const TEE_Time * time )
```

10.9.1.120 TEE_StartPersistentObjectEnumerator()

```
TEE_Result TEE_StartPersistentObjectEnumerator
(
        TEE_ObjectEnumHandle objectEnumerator,
        uint32_t storageID )
```

10.9.1.121 TEE_StartPropertyEnumerator()

```
void TEE_StartPropertyEnumerator (
        TEE_PropSetHandle enumerator,
        TEE_PropSetHandle propSet )
```

10.9.1.122 TEE_TruncateObjectData()

```
TEE_Result TEE_TruncateObjectData (
        TEE_ObjectHandle object,
        uint32_t size )
```

10.9.1.123 TEE_UnmaskCancellation()

```
bool TEE_UnmaskCancellation (
        void )
```

10.9.1.124 TEE_Wait()
```
TEE_Result TEE_Wait (
    uint32_t timeout )
```

10.9.1.125 TEE_WriteObjectData()
```
TEE_Result TEE_WriteObjectData (
    TEE_ObjectHandle object,
    const void * buffer,
    uint32_t size )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_WriteObjectData() - Writes the buffer data in to persistent objects.

In this function it checks if object is present or not, the encryption/ decryption buffer is taken by calling mbedtls_aes↩_crypt_cbc() then that buffer data is encrypted and mapped to object.On the base of object creation TEE_SUCCESS appears else TEE_ERROR_GENERIC appears.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write

Returns

TEE_SUCCESS if success else error occured.

TEE_WriteObjectData() - writes size bytes from the buffer pointed to by buffer to the data stream associated with the open object handle object.

If the current data position points before the end-of-stream, then size bytes are written to the data stream, overwriting bytes starting at the current data position. If the current data position points beyond the stream's end, then the data stream is first extended with zero bytes until the length indicated by the data position indicator is reached, and then size bytes are written to the stream.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write

Returns

TEE_SUCCESS if success else error occured.

10.10 tee_api.h

Go to the documentation of this file.

```
/* SPDX-License-Identifier: BSD-2-Clause */
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 */

/* Based on GP TEE Internal API Specification Version 1.1 */
#ifndef TEE_API_H
#define TEE_API_H

#include <stddef.h>
#include <compiler.h>
#include <tee_api_defines.h>
#include <tee_api_types.h>
#include <trace.h>

/* Property access functions */

TEE_Result TEE_GetPropertyAsString(TEE_PropSetHandle propsetOrEnumerator,
                   const char *name, char *valueBuffer,
                   uint32_t *valueBufferLen);

TEE_Result TEE_GetPropertyAsBool(TEE_PropSetHandle propsetOrEnumerator,
                 const char *name, bool *value);

TEE_Result TEE_GetPropertyAsU32(TEE_PropSetHandle propsetOrEnumerator,
                const char *name, uint32_t *value);

TEE_Result TEE_GetPropertyAsBinaryBlock(TEE_PropSetHandle propsetOrEnumerator,
                    const char *name, void *valueBuffer,
                    uint32_t *valueBufferLen);

TEE_Result TEE_GetPropertyAsUUID(TEE_PropSetHandle propsetOrEnumerator,
                 const char *name, TEE_UUID *value);

TEE_Result TEE_GetPropertyAsIdentity(TEE_PropSetHandle propsetOrEnumerator,
                     const char *name, TEE_Identity *value);

TEE_Result TEE_AllocatePropertyEnumerator(TEE_PropSetHandle *enumerator);

void TEE_FreePropertyEnumerator(TEE_PropSetHandle enumerator);

void TEE_StartPropertyEnumerator(TEE_PropSetHandle enumerator,
                 TEE_PropSetHandle propSet);

void TEE_ResetPropertyEnumerator(TEE_PropSetHandle enumerator);

TEE_Result TEE_GetPropertyName(TEE_PropSetHandle enumerator,
                   void *nameBuffer, uint32_t *nameBufferLen);

TEE_Result TEE_GetNextProperty(TEE_PropSetHandle enumerator);

/* System API - Misc */

void TEE_Panic(TEE_Result panicCode);

/* System API - Internal Client API */

TEE_Result TEE_OpenTASession(const TEE_UUID *destination,
                uint32_t cancellationRequestTimeout,
                uint32_t paramTypes,
                TEE_Param params[TEE_NUM_PARAMS],
                TEE_TASessionHandle *session,
                uint32_t *returnOrigin);

void TEE_CloseTASession(TEE_TASessionHandle session);

TEE_Result TEE_InvokeTACommand(TEE_TASessionHandle session,
                uint32_t cancellationRequestTimeout,
                uint32_t commandID, uint32_t paramTypes,
                TEE_Param params[TEE_NUM_PARAMS],
                uint32_t *returnOrigin);

/* System API - Cancellations */

bool TEE_GetCancellationFlag(void);

bool TEE_UnmaskCancellation(void);

bool TEE_MaskCancellation(void);

/* System API - Memory Management */

TEE_Result TEE_CheckMemoryAccessRights(uint32_t accessFlags, void *buffer,
                       uint32_t size);

```

```c
void TEE_SetInstanceData(const void *instanceData);

const void *TEE_GetInstanceData(void);

void *TEE_Malloc(uint32_t size, uint32_t hint);

void *TEE_Realloc(void *buffer, uint32_t newSize);

void TEE_Free(void *buffer);

void *TEE_MemMove(void *dest, const void *src, uint32_t size);

/*
 * Note: TEE_MemCompare() has a constant-time implementation (execution time
 * does not depend on buffer content but only on buffer size). It is the main
 * difference with memcmp().
 */
int32_t TEE_MemCompare(const void *buffer1, const void *buffer2, uint32_t size);

void *TEE_MemFill(void *buff, uint32_t x, uint32_t size);

/* Data and Key Storage API  - Generic Object Functions */

void TEE_GetObjectInfo(TEE_ObjectHandle object, TEE_ObjectInfo *objectInfo);
TEE_Result TEE_GetObjectInfo1(TEE_ObjectHandle object, TEE_ObjectInfo *objectInfo);

void TEE_RestrictObjectUsage(TEE_ObjectHandle object, uint32_t objectUsage);
TEE_Result TEE_RestrictObjectUsage1(TEE_ObjectHandle object, uint32_t objectUsage);

TEE_Result TEE_GetObjectBufferAttribute(TEE_ObjectHandle object,
                    uint32_t attributeID, void *buffer,
                    uint32_t *size);

TEE_Result TEE_GetObjectValueAttribute(TEE_ObjectHandle object,
                       uint32_t attributeID, uint32_t *a,
                       uint32_t *b);

void TEE_CloseObject(TEE_ObjectHandle object);

/* Data and Key Storage API  - Transient Object Functions */

TEE_Result TEE_AllocateTransientObject(TEE_ObjectType objectType,
                       uint32_t maxKeySize,
                       TEE_ObjectHandle *object);

void TEE_FreeTransientObject(TEE_ObjectHandle object);

void TEE_ResetTransientObject(TEE_ObjectHandle object);

TEE_Result TEE_PopulateTransientObject(TEE_ObjectHandle object,
                       const TEE_Attribute *attrs,
                       uint32_t attrCount);

void TEE_InitRefAttribute(TEE_Attribute *attr, uint32_t attributeID,
              const void *buffer, uint32_t length);

void TEE_InitValueAttribute(TEE_Attribute *attr, uint32_t attributeID,
                uint32_t a, uint32_t b);

void TEE_CopyObjectAttributes(TEE_ObjectHandle destObject,
                  TEE_ObjectHandle srcObject);

TEE_Result TEE_CopyObjectAttributes1(TEE_ObjectHandle destObject,
                  TEE_ObjectHandle srcObject);

TEE_Result TEE_GenerateKey(TEE_ObjectHandle object, uint32_t keySize,
               const TEE_Attribute *params, uint32_t paramCount);

/* Data and Key Storage API  - Persistent Object Functions */

TEE_Result TEE_OpenPersistentObject(uint32_t storageID, const void *objectID,
                    uint32_t objectIDLen, uint32_t flags,
                    TEE_ObjectHandle *object);

TEE_Result TEE_CreatePersistentObject(uint32_t storageID, const void *objectID,
                      uint32_t objectIDLen, uint32_t flags,
                      TEE_ObjectHandle attributes,
                      const void *initialData,
                      uint32_t initialDataLen,
                      TEE_ObjectHandle *object);

void TEE_CloseAndDeletePersistentObject(TEE_ObjectHandle object);

TEE_Result TEE_CloseAndDeletePersistentObject1(TEE_ObjectHandle object);

TEE_Result TEE_RenamePersistentObject(TEE_ObjectHandle object,
                      const void *newObjectID,
                      uint32_t newObjectIDLen);

TEE_Result TEE_AllocatePersistentObjectEnumerator(TEE_ObjectEnumHandle *
                          objectEnumerator);

void TEE_FreePersistentObjectEnumerator(TEE_ObjectEnumHandle objectEnumerator);

void TEE_ResetPersistentObjectEnumerator(TEE_ObjectEnumHandle objectEnumerator);

TEE_Result TEE_StartPersistentObjectEnumerator(TEE_ObjectEnumHandle
                           objectEnumerator,
                           uint32_t storageID);

TEE_Result TEE_GetNextPersistentObject(TEE_ObjectEnumHandle objectEnumerator,
                       TEE_ObjectInfo *objectInfo,
                       void *objectID, uint32_t *objectIDLen);

/* Data and Key Storage API  - Data Stream Access Functions */

TEE_Result TEE_ReadObjectData(TEE_ObjectHandle object, void *buffer,
                  uint32_t size, uint32_t *count);

TEE_Result TEE_WriteObjectData(TEE_ObjectHandle object, const void *buffer,
                   uint32_t size);

TEE_Result TEE_TruncateObjectData(TEE_ObjectHandle object, uint32_t size);

TEE_Result TEE_SeekObjectData(TEE_ObjectHandle object, int32_t offset,
                  TEE_Whence whence);

/* Cryptographic Operations API - Generic Operation Functions */

TEE_Result TEE_AllocateOperation(TEE_OperationHandle *operation,
                 uint32_t algorithm, uint32_t mode,
                 uint32_t maxKeySize);

void TEE_FreeOperation(TEE_OperationHandle operation);

void TEE_GetOperationInfo(TEE_OperationHandle operation,
              TEE_OperationInfo *operationInfo);

TEE_Result TEE_GetOperationInfoMultiple(TEE_OperationHandle operation,
              TEE_OperationInfoMultiple *operationInfoMultiple,
              uint32_t *operationSize);

void TEE_ResetOperation(TEE_OperationHandle operation);

TEE_Result TEE_SetOperationKey(TEE_OperationHandle operation,
                   TEE_ObjectHandle key);

TEE_Result TEE_SetOperationKey2(TEE_OperationHandle operation,
                TEE_ObjectHandle key1, TEE_ObjectHandle key2);

void TEE_CopyOperation(TEE_OperationHandle dstOperation,
               TEE_OperationHandle srcOperation);

TEE_Result TEE_IsAlgorithmSupported(uint32_t algId, uint32_t element);

/* Cryptographic Operations API - Message Digest Functions */

void TEE_DigestUpdate(TEE_OperationHandle operation,
              const void *chunk, uint32_t chunkSize);

TEE_Result TEE_DigestDoFinal(TEE_OperationHandle operation, const void *chunk,
                 uint32_t chunkLen, void *hash, uint32_t *hashLen);

/* Cryptographic Operations API - Symmetric Cipher Functions */

void TEE_CipherInit(TEE_OperationHandle operation, const void *IV,
            uint32_t IVLen);

TEE_Result TEE_CipherUpdate(TEE_OperationHandle operation, const void *srcData,
                uint32_t srcLen, void *destData, uint32_t *destLen);

TEE_Result TEE_CipherDoFinal(TEE_OperationHandle operation,
                 const void *srcData, uint32_t srcLen,
                 void *destData, uint32_t *destLen);

/* Cryptographic Operations API - MAC Functions */

void TEE_MACInit(TEE_OperationHandle operation, const void *IV,
         uint32_t IVLen);

```

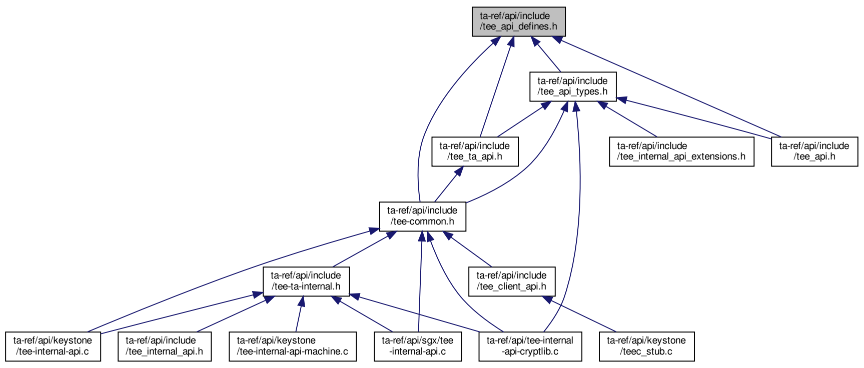
```c
void TEE_MACUpdate(TEE_OperationHandle operation, const void *chunk,
           uint32_t chunkSize);

TEE_Result TEE_MACComputeFinal(TEE_OperationHandle operation,
                   const void *message, uint32_t messageLen,
                   void *mac, uint32_t *macLen);

TEE_Result TEE_MACCompareFinal(TEE_OperationHandle operation,
                   const void *message, uint32_t messageLen,
                   const void *mac, uint32_t macLen);

/* Cryptographic Operations API - Authenticated Encryption Functions */

TEE_Result TEE_AEInit(TEE_OperationHandle operation, const void *nonce,
              uint32_t nonceLen, uint32_t tagLen, uint32_t AADLen,
              uint32_t payloadLen);

void TEE_AEUpdateAAD(TEE_OperationHandle operation, const void *AADdata,
             uint32_t AADdataLen);

TEE_Result TEE_AEUpdate(TEE_OperationHandle operation, const void *srcData,
            uint32_t srcLen, void *destData, uint32_t *destLen);

TEE_Result TEE_AEEncryptFinal(TEE_OperationHandle operation,
                  const void *srcData, uint32_t srcLen,
                  void *destData, uint32_t *destLen, void *tag,
                  uint32_t *tagLen);

TEE_Result TEE_AEDecryptFinal(TEE_OperationHandle operation,
                  const void *srcData, uint32_t srcLen,
                  void *destData, uint32_t *destLen, void *tag,
                  uint32_t tagLen);

/* Cryptographic Operations API - Asymmetric Functions */

TEE_Result TEE_AsymmetricEncrypt(TEE_OperationHandle operation,
                 const TEE_Attribute *params,
                 uint32_t paramCount, const void *srcData,
                 uint32_t srcLen, void *destData,
                 uint32_t *destLen);

TEE_Result TEE_AsymmetricDecrypt(TEE_OperationHandle operation,
                 const TEE_Attribute *params,
                 uint32_t paramCount, const void *srcData,
                 uint32_t srcLen, void *destData,
                 uint32_t *destLen);

TEE_Result TEE_AsymmetricSignDigest(TEE_OperationHandle operation,
                    const TEE_Attribute *params,
                    uint32_t paramCount, const void *digest,
                    uint32_t digestLen, void *signature,
                    uint32_t *signatureLen);

TEE_Result TEE_AsymmetricVerifyDigest(TEE_OperationHandle operation,
                      const TEE_Attribute *params,
                      uint32_t paramCount, const void *digest,
                      uint32_t digestLen, const void *signature,
                      uint32_t signatureLen);

/* Cryptographic Operations API - Key Derivation Functions */

void TEE_DeriveKey(TEE_OperationHandle operation,
           const TEE_Attribute *params, uint32_t paramCount,
           TEE_ObjectHandle derivedKey);

/* Cryptographic Operations API - Random Number Generation Functions */

void TEE_GenerateRandom(void *randomBuffer, uint32_t randomBufferLen);

/* Date & Time API */

void TEE_GetSystemTime(TEE_Time *time);

TEE_Result TEE_Wait(uint32_t timeout);

TEE_Result TEE_GetTAPersistentTime(TEE_Time *time);

TEE_Result TEE_SetTAPersistentTime(const TEE_Time *time);

void TEE_GetREETime(TEE_Time *time);

/* TEE Arithmetical API - Memory allocation and size of objects */

uint32_t TEE_BigIntFMMSizeInU32(uint32_t modulusSizeInBits);

```

```
uint32_t TEE_BigIntFMMContextSizeInU32(uint32_t modulusSizeInBits);

/* TEE Arithmetical API - Initialization functions */

void TEE_BigIntInit(TEE_BigInt *bigInt, uint32_t len);

void TEE_BigIntInitFMMContext(TEE_BigIntFMMContext *context, uint32_t len,
                  const TEE_BigInt *modulus);

void TEE_BigIntInitFMM(TEE_BigIntFMM *bigIntFMM, uint32_t len);

/* TEE Arithmetical API - Converter functions */

TEE_Result TEE_BigIntConvertFromOctetString(TEE_BigInt *dest,
                        const uint8_t *buffer,
                        uint32_t bufferLen,
                        int32_t sign);

TEE_Result TEE_BigIntConvertToOctetString(uint8_t *buffer, uint32_t *bufferLen,
                      const TEE_BigInt *bigInt);

void TEE_BigIntConvertFromS32(TEE_BigInt *dest, int32_t shortVal);

TEE_Result TEE_BigIntConvertToS32(int32_t *dest, const TEE_BigInt *src);

/* TEE Arithmetical API - Logical operations */

int32_t TEE_BigIntCmp(const TEE_BigInt *op1, const TEE_BigInt *op2);

int32_t TEE_BigIntCmpS32(const TEE_BigInt *op, int32_t shortVal);

void TEE_BigIntShiftRight(TEE_BigInt *dest, const TEE_BigInt *op,
              size_t bits);

bool TEE_BigIntGetBit(const TEE_BigInt *src, uint32_t bitIndex);

uint32_t TEE_BigIntGetBitCount(const TEE_BigInt *src);

void TEE_BigIntAdd(TEE_BigInt *dest, const TEE_BigInt *op1,
           const TEE_BigInt *op2);

void TEE_BigIntSub(TEE_BigInt *dest, const TEE_BigInt *op1,
           const TEE_BigInt *op2);

void TEE_BigIntNeg(TEE_BigInt *dest, const TEE_BigInt *op);

void TEE_BigIntMul(TEE_BigInt *dest, const TEE_BigInt *op1,
           const TEE_BigInt *op2);

void TEE_BigIntSquare(TEE_BigInt *dest, const TEE_BigInt *op);

void TEE_BigIntDiv(TEE_BigInt *dest_q, TEE_BigInt *dest_r,
           const TEE_BigInt *op1, const TEE_BigInt *op2);

/* TEE Arithmetical API - Modular arithmetic operations */

void TEE_BigIntMod(TEE_BigInt *dest, const TEE_BigInt *op,
           const TEE_BigInt *n);

void TEE_BigIntAddMod(TEE_BigInt *dest, const TEE_BigInt *op1,
              const TEE_BigInt *op2, const TEE_BigInt *n);

void TEE_BigIntSubMod(TEE_BigInt *dest, const TEE_BigInt *op1,
              const TEE_BigInt *op2, const TEE_BigInt *n);

void TEE_BigIntMulMod(TEE_BigInt *dest, const  TEE_BigInt *op1,
              const TEE_BigInt *op2, const TEE_BigInt *n);

void TEE_BigIntSquareMod(TEE_BigInt *dest, const TEE_BigInt *op,
             const TEE_BigInt *n);

void TEE_BigIntInvMod(TEE_BigInt *dest, const TEE_BigInt *op,
              const TEE_BigInt *n);

/* TEE Arithmetical API - Other arithmetic operations */

bool TEE_BigIntRelativePrime(const TEE_BigInt *op1, const TEE_BigInt *op2);

void TEE_BigIntComputeExtendedGcd(TEE_BigInt *gcd, TEE_BigInt *u,
                  TEE_BigInt *v, const TEE_BigInt *op1,
                  const TEE_BigInt *op2);

int32_t TEE_BigIntIsProbablePrime(const TEE_BigInt *op,
                  uint32_t confidenceLevel);

```

```
/* TEE Arithmetical API - Fast modular multiplication operations */

void TEE_BigIntConvertToFMM(TEE_BigIntFMM *dest, const TEE_BigInt *src,
                const TEE_BigInt *n,
                const TEE_BigIntFMMContext *context);

void TEE_BigIntConvertFromFMM(TEE_BigInt *dest, const TEE_BigIntFMM *src,
                  const TEE_BigInt *n,
                  const TEE_BigIntFMMContext *context);

void TEE_BigIntFMMConvertToBigInt(TEE_BigInt *dest, const TEE_BigIntFMM *src,
                  const TEE_BigInt *n,
                  const TEE_BigIntFMMContext *context);

void TEE_BigIntComputeFMM(TEE_BigIntFMM *dest, const TEE_BigIntFMM *op1,
              const TEE_BigIntFMM *op2, const TEE_BigInt *n,
              const TEE_BigIntFMMContext *context);

#endif /* TEE_API_H */
```

10.11 ta-ref/api/include/tee_api_defines.h File Reference

This graph shows which files directly or indirectly include this file:



10.12 tee_api_defines.h

Go to the documentation of this file.

```
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
  *
  * 2. Redistributions in binary form must reproduce the above copyright notice,
  * this list of conditions and the following disclaimer in the documentation
  * and/or other materials provided with the distribution.
  *
  * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
  * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
  * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
  * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
  * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
  * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
  * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
  * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
  * POSSIBILITY OF SUCH DAMAGE.
  */

 /* Based on GP TEE Internal Core API Specification Version 1.1 */

 #ifndef TEE_API_DEFINES_H
 #define TEE_API_DEFINES_H

 #ifndef DOXYGEN_SHOULD_SKIP_THIS
 #define TEE_INT_CORE_API_SPEC_VERSION     0x0000000A

 #define TEE_HANDLE_NULL                   0

 #define TEE_TIMEOUT_INFINITE              0xFFFFFFFF

 /* API Error Codes */
 #define TEE_SUCCESS                       0x00000000
 #define TEE_ERROR_CORRUPT_OBJECT          0xF0100001
 #define TEE_ERROR_CORRUPT_OBJECT_2        0xF0100002
 #define TEE_ERROR_STORAGE_NOT_AVAILABLE   0xF0100003
 #define TEE_ERROR_STORAGE_NOT_AVAILABLE_2 0xF0100004
 #define TEE_ERROR_GENERIC                 0xFFFF0000
 #define TEE_ERROR_ACCESS_DENIED           0xFFFF0001
 #define TEE_ERROR_CANCEL                  0xFFFF0002
 #define TEE_ERROR_ACCESS_CONFLICT         0xFFFF0003
 #define TEE_ERROR_EXCESS_DATA             0xFFFF0004
 #define TEE_ERROR_BAD_FORMAT              0xFFFF0005
 #define TEE_ERROR_BAD_PARAMETERS          0xFFFF0006
 #define TEE_ERROR_BAD_STATE               0xFFFF0007
 #define TEE_ERROR_ITEM_NOT_FOUND          0xFFFF0008
 #define TEE_ERROR_NOT_IMPLEMENTED         0xFFFF0009
 #define TEE_ERROR_NOT_SUPPORTED           0xFFFF000A
 #define TEE_ERROR_NO_DATA                 0xFFFF000B
 #define TEE_ERROR_OUT_OF_MEMORY           0xFFFF000C
 #define TEE_ERROR_BUSY                    0xFFFF000D
 #define TEE_ERROR_COMMUNICATION           0xFFFF000E
 #define TEE_ERROR_SECURITY                0xFFFF000F
 #define TEE_ERROR_SHORT_BUFFER            0xFFFF0010
 #define TEE_ERROR_EXTERNAL_CANCEL         0xFFFF0011
 #define TEE_ERROR_OVERFLOW                0xFFFF300F
 #define TEE_ERROR_TARGET_DEAD             0xFFFF3024
 #define TEE_ERROR_STORAGE_NO_SPACE        0xFFFF3041
 #define TEE_ERROR_MAC_INVALID             0xFFFF3071
 #define TEE_ERROR_SIGNATURE_INVALID       0xFFFF3072
 #define TEE_ERROR_TIME_NOT_SET            0xFFFF5000
 #define TEE_ERROR_TIME_NEEDS_RESET        0xFFFF5001

 /* Parameter Type Constants */
 #define TEE_PARAM_TYPE_NONE             0
 #define TEE_PARAM_TYPE_VALUE_INPUT      1
 #define TEE_PARAM_TYPE_VALUE_OUTPUT     2
 #define TEE_PARAM_TYPE_VALUE_INOUT      3
 #define TEE_PARAM_TYPE_MEMREF_INPUT     5
 #define TEE_PARAM_TYPE_MEMREF_OUTPUT    6
 #define TEE_PARAM_TYPE_MEMREF_INOUT     7

 /* Login Type Constants */
 #define TEE_LOGIN_PUBLIC                0x00000000
 #define TEE_LOGIN_USER                  0x00000001
 #define TEE_LOGIN_GROUP                 0x00000002
 #define TEE_LOGIN_APPLICATION           0x00000004
 #define TEE_LOGIN_APPLICATION_USER      0x00000005
 #define TEE_LOGIN_APPLICATION_GROUP     0x00000006
 #define TEE_LOGIN_TRUSTED_APP           0xF0000000

 /* Origin Code Constants */
 #define TEE_ORIGIN_API                  0x00000001
 #define TEE_ORIGIN_COMMS                0x00000002
 #define TEE_ORIGIN_TEE                  0x00000003
 #define TEE_ORIGIN_TRUSTED_APP          0x00000004

 /* Property Sets pseudo handles */
 #define TEE_PROPSET_TEE_IMPLEMENTATION  (TEE_PropSetHandle)0xFFFFFFFD
 #define TEE_PROPSET_CURRENT_CLIENT      (TEE_PropSetHandle)0xFFFFFFFE
 #define TEE_PROPSET_CURRENT_TA          (TEE_PropSetHandle)0xFFFFFFFF

  /* Memory Access Rights Constants */
  #define TEE_MEMORY_ACCESS_READ              0x00000001
  #define TEE_MEMORY_ACCESS_WRITE             0x00000002
  #define TEE_MEMORY_ACCESS_ANY_OWNER         0x00000004

  /* Memory Management Constant */
  #define TEE_MALLOC_FILL_ZERO                0x00000000

```

```
/* Other constants */
#define TEE_STORAGE_PRIVATE                0x00000001

#define TEE_DATA_FLAG_ACCESS_READ          0x00000001
#define TEE_DATA_FLAG_ACCESS_WRITE         0x00000002
#define TEE_DATA_FLAG_ACCESS_WRITE_META    0x00000004
#define TEE_DATA_FLAG_SHARE_READ           0x00000010
#define TEE_DATA_FLAG_SHARE_WRITE          0x00000020
#define TEE_DATA_FLAG_OVERWRITE            0x00000400
#define TEE_DATA_MAX_POSITION              0xFFFFFFFF
#define TEE_OBJECT_ID_MAX_LEN              64
#define TEE_USAGE_EXTRACTABLE              0x00000001
#define TEE_USAGE_ENCRYPT                  0x00000002
#define TEE_USAGE_DECRYPT                  0x00000004
#define TEE_USAGE_MAC                      0x00000008
#define TEE_USAGE_SIGN                     0x00000010
#define TEE_USAGE_VERIFY                   0x00000020
#define TEE_USAGE_DERIVE                   0x00000040
#define TEE_HANDLE_FLAG_PERSISTENT         0x00010000
#define TEE_HANDLE_FLAG_INITIALIZED        0x00020000
#define TEE_HANDLE_FLAG_KEY_SET            0x00040000
#define TEE_HANDLE_FLAG_EXPECT_TWO_KEYS    0x00080000
#define TEE_OPERATION_CIPHER               1
#define TEE_OPERATION_MAC                  3
#define TEE_OPERATION_AE                   4
#define TEE_OPERATION_DIGEST               5
#define TEE_OPERATION_ASYMMETRIC_CIPHER    6
#define TEE_OPERATION_ASYMMETRIC_SIGNATURE 7
#define TEE_OPERATION_KEY_DERIVATION       8
#define TEE_OPERATION_STATE_INITIAL        0x00000000
#define TEE_OPERATION_STATE_ACTIVE         0x00000001

/* Algorithm Identifiers */
#define TEE_ALG_AES_ECB_NOPAD                      0x10000010
#define TEE_ALG_AES_CBC_NOPAD                      0x10000110
#define TEE_ALG_AES_CTR                            0x10000210
#define TEE_ALG_AES_CTS                            0x10000310
#define TEE_ALG_AES_XTS                            0x10000410
#define TEE_ALG_AES_CBC_MAC_NOPAD                  0x30000110
#define TEE_ALG_AES_CBC_MAC_PKCS5                  0x30000510
#define TEE_ALG_AES_CMAC                           0x30000610
#define TEE_ALG_AES_CCM                            0x40000710
#define TEE_ALG_AES_GCM                            0x40000810
#define TEE_ALG_DES_ECB_NOPAD                      0x10000011
#define TEE_ALG_DES_CBC_NOPAD                      0x10000111
#define TEE_ALG_DES_CBC_MAC_NOPAD                  0x30000111
#define TEE_ALG_DES_CBC_MAC_PKCS5                  0x30000511
#define TEE_ALG_DES3_ECB_NOPAD                     0x10000013
#define TEE_ALG_DES3_CBC_NOPAD                     0x10000113
#define TEE_ALG_DES3_CBC_MAC_NOPAD                 0x30000113
#define TEE_ALG_DES3_CBC_MAC_PKCS5                 0x30000513
#define TEE_ALG_RSASSA_PKCS1_V1_5_MD5              0x70001830
#define TEE_ALG_RSASSA_PKCS1_V1_5_SHA1             0x70002830
#define TEE_ALG_RSASSA_PKCS1_V1_5_SHA224           0x70003830
#define TEE_ALG_RSASSA_PKCS1_V1_5_SHA256           0x70004830
#define TEE_ALG_RSASSA_PKCS1_V1_5_SHA384           0x70005830
#define TEE_ALG_RSASSA_PKCS1_V1_5_SHA512           0x70006830
#define TEE_ALG_RSASSA_PKCS1_V1_5_MD5SHA1          0x7000F830
#define TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA1         0x70212930
#define TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA224       0x70313930
#define TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA256       0x70414930
#define TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA384       0x70515930
#define TEE_ALG_RSASSA_PKCS1_PSS_MGF1_SHA512       0x70616930
#define TEE_ALG_RSAES_PKCS1_V1_5                   0x60000130
#define TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA1         0x60210230
#define TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA224       0x60310230
#define TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA256       0x60410230
#define TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA384       0x60510230
#define TEE_ALG_RSAES_PKCS1_OAEP_MGF1_SHA512       0x60610230
#define TEE_ALG_RSA_NOPAD                          0x60000030
#define TEE_ALG_DSA_SHA1                           0x70002131
#define TEE_ALG_DSA_SHA224                         0x70003131
#define TEE_ALG_DSA_SHA256                         0x70004131
#define TEE_ALG_DH_DERIVE_SHARED_SECRET            0x80000032
#define TEE_ALG_MD5                                0x50000001
#define TEE_ALG_SHA1                               0x50000002
#define TEE_ALG_SHA224                             0x50000003
#define TEE_ALG_SHA256                             0x50000004
#define TEE_ALG_SHA384                             0x50000005
#define TEE_ALG_SHA512                             0x50000006
#define TEE_ALG_MD5SHA1                            0x5000000F
#define TEE_ALG_HMAC_MD5                           0x30000001
#define TEE_ALG_HMAC_SHA1                          0x30000002
#define TEE_ALG_HMAC_SHA224                        0x30000003
#define TEE_ALG_HMAC_SHA256                        0x30000004
```

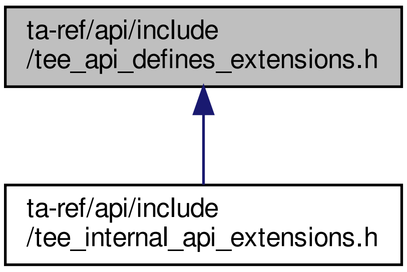
```
#define TEE_ALG_HMAC_SHA384                     0x30000005
#define TEE_ALG_HMAC_SHA512                     0x30000006
/*
 * Fix GP Internal Core API v1.1
 *     "Table 6-12:  Structure of Algorithm Identifier"
 *     indicates ECDSA have the algorithm "0x41" and ECDH "0x42"
 * whereas
 *     "Table 6-11:  List of Algorithm Identifiers" defines
 *     TEE_ALG_ECDSA_P192 as 0x70001042
 *
 * We chose to define TEE_ALG_ECDSA_P192 as 0x70001041 (conform to table 6-12)
 */
#define TEE_ALG_ECDSA_P192                      0x70001041
#define TEE_ALG_ECDSA_P224                      0x70002041
#define TEE_ALG_ECDSA_P256                      0x70003041
#define TEE_ALG_ECDSA_P384                      0x70004041
#define TEE_ALG_ECDSA_P521                      0x70005041
#define TEE_ALG_ECDH_P192                       0x80001042
#define TEE_ALG_ECDH_P224                       0x80002042
#define TEE_ALG_ECDH_P256                       0x80003042
#define TEE_ALG_ECDH_P384                       0x80004042
#define TEE_ALG_ECDH_P521                       0x80005042

/* Object Types */

#define TEE_TYPE_AES                        0xA0000010
#define TEE_TYPE_DES                        0xA0000011
#define TEE_TYPE_DES3                       0xA0000013
#define TEE_TYPE_HMAC_MD5                   0xA0000001
#define TEE_TYPE_HMAC_SHA1                  0xA0000002
#define TEE_TYPE_HMAC_SHA224                0xA0000003
#define TEE_TYPE_HMAC_SHA256                0xA0000004
#define TEE_TYPE_HMAC_SHA384                0xA0000005
#define TEE_TYPE_HMAC_SHA512                0xA0000006
#define TEE_TYPE_RSA_PUBLIC_KEY             0xA0000030
#define TEE_TYPE_RSA_KEYPAIR                0xA1000030
#define TEE_TYPE_DSA_PUBLIC_KEY             0xA0000031
#define TEE_TYPE_DSA_KEYPAIR                0xA1000031
#define TEE_TYPE_DH_KEYPAIR                 0xA1000032
#define TEE_TYPE_ECDSA_PUBLIC_KEY           0xA0000041
#define TEE_TYPE_ECDSA_KEYPAIR              0xA1000041
#define TEE_TYPE_ECDH_PUBLIC_KEY            0xA0000042
#define TEE_TYPE_ECDH_KEYPAIR               0xA1000042
#define TEE_TYPE_GENERIC_SECRET             0xA0000000
#define TEE_TYPE_CORRUPTED_OBJECT           0xA00000BE
#define TEE_TYPE_DATA                       0xA00000BF

/* List of Object or Operation Attributes */

#define TEE_ATTR_SECRET_VALUE               0xC0000000
#define TEE_ATTR_RSA_MODULUS                0xD0000130
#define TEE_ATTR_RSA_PUBLIC_EXPONENT        0xD0000230
#define TEE_ATTR_RSA_PRIVATE_EXPONENT       0xC0000330
#define TEE_ATTR_RSA_PRIME1                 0xC0000430
#define TEE_ATTR_RSA_PRIME2                 0xC0000530
#define TEE_ATTR_RSA_EXPONENT1              0xC0000630
#define TEE_ATTR_RSA_EXPONENT2              0xC0000730
#define TEE_ATTR_RSA_COEFFICIENT            0xC0000830
#define TEE_ATTR_DSA_PRIME                  0xD0001031
#define TEE_ATTR_DSA_SUBPRIME               0xD0001131
#define TEE_ATTR_DSA_BASE                   0xD0001231
#define TEE_ATTR_DSA_PUBLIC_VALUE           0xD0000131
#define TEE_ATTR_DSA_PRIVATE_VALUE          0xC0000231
#define TEE_ATTR_DH_PRIME                   0xD0001032
#define TEE_ATTR_DH_SUBPRIME                0xD0001132
#define TEE_ATTR_DH_BASE                    0xD0001232
#define TEE_ATTR_DH_X_BITS                  0xF0001332
#define TEE_ATTR_DH_PUBLIC_VALUE            0xD0000132
#define TEE_ATTR_DH_PRIVATE_VALUE           0xC0000232
#define TEE_ATTR_RSA_OAEP_LABEL             0xD0000930
#define TEE_ATTR_RSA_PSS_SALT_LENGTH        0xF0000A30
#define TEE_ATTR_ECC_PUBLIC_VALUE_X         0xD0000141
#define TEE_ATTR_ECC_PUBLIC_VALUE_Y         0xD0000241
#define TEE_ATTR_ECC_PRIVATE_VALUE          0xC0000341
#define TEE_ATTR_ECC_CURVE                  0xF0000441

#define TEE_ATTR_BIT_PROTECTED      (1 « 28)
#define TEE_ATTR_BIT_VALUE      (1 « 29)

/* List of Supported ECC Curves */
#define TEE_ECC_CURVE_NIST_P192             0x00000001
#define TEE_ECC_CURVE_NIST_P224             0x00000002
#define TEE_ECC_CURVE_NIST_P256             0x00000003
#define TEE_ECC_CURVE_NIST_P384             0x00000004
#define TEE_ECC_CURVE_NIST_P521             0x00000005
```

```


/* Panicked Functions Identification */
/* TA Interface */
#define TEE_PANIC_ID_TA_CLOSESESSIONENTRYPOINT      0x00000101
#define TEE_PANIC_ID_TA_CREATEENTRYPOINT            0x00000102
#define TEE_PANIC_ID_TA_DESTROYENTRYPOINT           0x00000103
#define TEE_PANIC_ID_TA_INVOKECOMMANDENTRYPOINT     0x00000104
#define TEE_PANIC_ID_TA_OPENSESSIONENTRYPOINT       0x00000105
/* Property Access */
#define TEE_PANIC_ID_TEE_ALLOCATEPROPERTYENUMERATOR 0x00000201
#define TEE_PANIC_ID_TEE_FREEPROPERTYENUMERATOR     0x00000202
#define TEE_PANIC_ID_TEE_GETNEXTPROPERTY            0x00000203
#define TEE_PANIC_ID_TEE_GETPROPERTYASBINARYBLOCK   0x00000204
#define TEE_PANIC_ID_TEE_GETPROPERTYASBOOL          0x00000205
#define TEE_PANIC_ID_TEE_GETPROPERTYASIDENTITY      0x00000206
#define TEE_PANIC_ID_TEE_GETPROPERTYASSTRING        0x00000207
#define TEE_PANIC_ID_TEE_GETPROPERTYASU32           0x00000208
#define TEE_PANIC_ID_TEE_GETPROPERTYASUUID          0x00000209
#define TEE_PANIC_ID_TEE_GETPROPERTYNAME            0x0000020A
#define TEE_PANIC_ID_TEE_RESETPROPERTYENUMERATOR    0x0000020B
#define TEE_PANIC_ID_TEE_STARTPROPERTYENUMERATOR    0x0000020C
/* Panic Function */
#define TEE_PANIC_ID_TEE_PANIC                      0x00000301
/* Internal Client API */
#define TEE_PANIC_ID_TEE_CLOSETASESSION             0x00000401
#define TEE_PANIC_ID_TEE_INVOKETACOMMAND            0x00000402
#define TEE_PANIC_ID_TEE_OPENTASESSION              0x00000403
/* Cancellation */
#define TEE_PANIC_ID_TEE_GETCANCELLATIONFLAG        0x00000501
#define TEE_PANIC_ID_TEE_MASKCANCELLATION           0x00000502
#define TEE_PANIC_ID_TEE_UNMASKCANCELLATION         0x00000503
/* Memory Management */
#define TEE_PANIC_ID_TEE_CHECKMEMORYACCESSRIGHTS    0x00000601
#define TEE_PANIC_ID_TEE_FREE                       0x00000602
#define TEE_PANIC_ID_TEE_GETINSTANCEDATA            0x00000603
#define TEE_PANIC_ID_TEE_MALLOC                     0x00000604
#define TEE_PANIC_ID_TEE_MEMCOMPARE                 0x00000605
#define TEE_PANIC_ID_TEE_MEMFILL                    0x00000606
#define TEE_PANIC_ID_TEE_MEMMOVE                    0x00000607
#define TEE_PANIC_ID_TEE_REALLOC                    0x00000608
#define TEE_PANIC_ID_TEE_SETINSTANCEDATA            0x00000609
/* Generic Object */
#define TEE_PANIC_ID_TEE_CLOSEOBJECT                0x00000701
#define TEE_PANIC_ID_TEE_GETOBJECTBUFFERATTRIBUTE   0x00000702
/* deprecated */
#define TEE_PANIC_ID_TEE_GETOBJECTINFO              0x00000703
#define TEE_PANIC_ID_TEE_GETOBJECTVALUEATTRIBUTE    0x00000704
/* deprecated */
#define TEE_PANIC_ID_TEE_RESTRICTOBJECTUSAGE        0x00000705
#define TEE_PANIC_ID_TEE_GETOBJECTINFO1             0x00000706
#define TEE_PANIC_ID_TEE_RESTRICTOBJECTUSAGE1       0x00000707
/* Transient Object */
#define TEE_PANIC_ID_TEE_ALLOCATETRANSIENTOBJECT    0x00000801
/* deprecated */
#define TEE_PANIC_ID_TEE_COPYOBJECTATTRIBUTES       0x00000802
#define TEE_PANIC_ID_TEE_FREETRANSIENTOBJECT        0x00000803
#define TEE_PANIC_ID_TEE_GENERATEKEY                0x00000804
#define TEE_PANIC_ID_TEE_INITREFATTRIBUTE           0x00000805
#define TEE_PANIC_ID_TEE_INITVALUEATTRIBUTE         0x00000806
#define TEE_PANIC_ID_TEE_POPULATETRANSIENTOBJECT    0x00000807
#define TEE_PANIC_ID_TEE_RESETTRANSIENTOBJECT       0x00000808
#define TEE_PANIC_ID_TEE_COPYOBJECTATTRIBUTES1      0x00000809
/* Persistent Object */
/* deprecated */
#define TEE_PANIC_ID_TEE_CLOSEANDDELETEPERSISTENTOBJECT  0x00000901
#define TEE_PANIC_ID_TEE_CREATEPERSISTENTOBJECT          0x00000902
#define TEE_PANIC_ID_TEE_OPENPERSISTENTOBJECT            0x00000903
#define TEE_PANIC_ID_TEE_RENAMEPERSISTENTOBJECT          0x00000904
#define TEE_PANIC_ID_TEE_CLOSEANDDELETEPERSISTENTOBJECT1 0x00000905
/* Persistent Object Enumeration */
#define TEE_PANIC_ID_TEE_ALLOCATEPERSISTENTOBJECTENUMERATOR 0x00000A01
#define TEE_PANIC_ID_TEE_FREEPERSISTENTOBJECTENUMERATOR     0x00000A02
#define TEE_PANIC_ID_TEE_GETNEXTPERSISTENTOBJECT            0x00000A03
#define TEE_PANIC_ID_TEE_RESETPERSISTENTOBJECTENUMERATOR    0x00000A04
#define TEE_PANIC_ID_TEE_STARTPERSISTENTOBJECTENUMERATOR    0x00000A05
/* Data Stream Access */
#define TEE_PANIC_ID_TEE_READOBJECTDATA             0x00000B01
#define TEE_PANIC_ID_TEE_SEEKOBJECTDATA             0x00000B02
#define TEE_PANIC_ID_TEE_TRUNCATEOBJECTDATA         0x00000B03
#define TEE_PANIC_ID_TEE_WRITEOBJECTDATA            0x00000B04
/* Generic Operation */
#define TEE_PANIC_ID_TEE_ALLOCATEOPERATION          0x00000C01
#define TEE_PANIC_ID_TEE_COPYOPERATION              0x00000C02
#define TEE_PANIC_ID_TEE_FREEOPERATION              0x00000C03
```

```
#define TEE_PANIC_ID_TEE_GETOPERATIONINFO           0x00000C04
#define TEE_PANIC_ID_TEE_RESETOPERATION             0x00000C05
#define TEE_PANIC_ID_TEE_SETOPERATIONKEY            0x00000C06
#define TEE_PANIC_ID_TEE_SETOPERATIONKEY2           0x00000C07
#define TEE_PANIC_ID_TEE_GETOPERATIONINFOMULTIPLE   0x00000C08
/* Message Digest */
#define TEE_PANIC_ID_TEE_DIGESTDOFINAL              0x00000D01
#define TEE_PANIC_ID_TEE_DIGESTUPDATE               0x00000D02
/* Symmetric Cipher */
#define TEE_PANIC_ID_TEE_CIPHERDOFINAL              0x00000E01
#define TEE_PANIC_ID_TEE_CIPHERINIT                 0x00000E02
#define TEE_PANIC_ID_TEE_CIPHERUPDATE               0x00000E03
/* MAC */
#define TEE_PANIC_ID_TEE_MACCOMPAREFINAL            0x00000F01
#define TEE_PANIC_ID_TEE_MACCOMPUTEFINAL            0x00000F02
#define TEE_PANIC_ID_TEE_MACINIT                    0x00000F03
#define TEE_PANIC_ID_TEE_MACUPDATE                  0x00000F04
/* Authenticated Encryption */
#define TEE_PANIC_ID_TEE_AEDECRYPTFINAL             0x00001001
#define TEE_PANIC_ID_TEE_AEENCRYPTFINAL             0x00001002
#define TEE_PANIC_ID_TEE_AEINIT                     0x00001003
#define TEE_PANIC_ID_TEE_AEUPDATE                   0x00001004
#define TEE_PANIC_ID_TEE_AEUPDATEAAD                0x00001005
/* Asymmetric */
#define TEE_PANIC_ID_TEE_ASYMMETRICDECRYPT          0x00001101
#define TEE_PANIC_ID_TEE_ASYMMETRICENCRYPT          0x00001102
#define TEE_PANIC_ID_TEE_ASYMMETRICSIGNDIGEST       0x00001103
#define TEE_PANIC_ID_TEE_ASYMMETRICVERIFYDIGEST     0x00001104
/* Key Derivation */
#define TEE_PANIC_ID_TEE_DERIVEKEY                  0x00001201
/* Random Data Generation */
#define TEE_PANIC_ID_TEE_GENERATERANDOM             0x00001301
/* Time */
#define TEE_PANIC_ID_TEE_GETREETIME                 0x00001401
#define TEE_PANIC_ID_TEE_GETSYSTEMTIME              0x00001402
#define TEE_PANIC_ID_TEE_GETTAPERSISTENTTIME        0x00001403
#define TEE_PANIC_ID_TEE_SETTAPERSISTENTTIME        0x00001404
#define TEE_PANIC_ID_TEE_WAIT                       0x00001405
/* Memory Allocation and Size of Objects */
#define TEE_PANIC_ID_TEE_BIGINTFMMCONTEXTSIZEINU32  0x00001501
#define TEE_PANIC_ID_TEE_BIGINTFMMSIZEINU32         0x00001502
/* Initialization */
#define TEE_PANIC_ID_TEE_BIGINTINIT                 0x00001601
#define TEE_PANIC_ID_TEE_BIGINTINITFMM              0x00001602
#define TEE_PANIC_ID_TEE_BIGINTINITFMMCONTEXT       0x00001603
/* Converter */
#define TEE_PANIC_ID_TEE_BIGINTCONVERTFROMOCTETSTRING 0x00001701
#define TEE_PANIC_ID_TEE_BIGINTCONVERTFROMS32         0x00001702
#define TEE_PANIC_ID_TEE_BIGINTCONVERTTOOCTETSTRING   0x00001703
#define TEE_PANIC_ID_TEE_BIGINTCONVERTTOS32           0x00001704
/* Logical Operation */
#define TEE_PANIC_ID_TEE_BIGINTCMP                  0x00001801
#define TEE_PANIC_ID_TEE_BIGINTCMPS32               0x00001802
#define TEE_PANIC_ID_TEE_BIGINTGETBIT               0x00001803
#define TEE_PANIC_ID_TEE_BIGINTGETBITCOUNT          0x00001804
#define TEE_PANIC_ID_TEE_BIGINTSHIFTRIGHT           0x00001805
/* Basic Arithmetic */
#define TEE_PANIC_ID_TEE_BIGINTADD                  0x00001901
#define TEE_PANIC_ID_TEE_BIGINTDIV                  0x00001902
#define TEE_PANIC_ID_TEE_BIGINTMUL                  0x00001903
#define TEE_PANIC_ID_TEE_BIGINTNEG                  0x00001904
#define TEE_PANIC_ID_TEE_BIGINTSQUARE               0x00001905
#define TEE_PANIC_ID_TEE_BIGINTSUB                  0x00001906
/* Modular Arithmetic */
#define TEE_PANIC_ID_TEE_BIGINTADDMOD               0x00001A01
#define TEE_PANIC_ID_TEE_BIGINTINVMOD               0x00001A02
#define TEE_PANIC_ID_TEE_BIGINTMOD                  0x00001A03
#define TEE_PANIC_ID_TEE_BIGINTMULMOD               0x00001A04
#define TEE_PANIC_ID_TEE_BIGINTSQUAREMOD            0x00001A05
#define TEE_PANIC_ID_TEE_BIGINTSUBMOD               0x00001A06
/* Other Arithmetic */
#define TEE_PANIC_ID_TEE_BIGINTCOMPUTEEXTENDEDGCD   0x00001B01
#define TEE_PANIC_ID_TEE_BIGINTISPROBABLEPRIME      0x00001B02
#define TEE_PANIC_ID_TEE_BIGINTRELATIVEPRIME        0x00001B03
/* Fast Modular Multiplication */
#define TEE_PANIC_ID_TEE_BIGINTCOMPUTEFMM           0x00001C01
#define TEE_PANIC_ID_TEE_BIGINTCONVERTFROMFMM       0x00001C02
#define TEE_PANIC_ID_TEE_BIGINTCONVERTTOFMM         0x00001C03

/*
 * The macro TEE_PARAM_TYPES can be used to construct a value that you can
 * compare against an incoming paramTypes to check the type of all the
 * parameters in one comparison, like in the following example:
 * if (paramTypes != TEE_PARAM_TYPES(TEE_PARAM_TYPE_MEMREF_INPUT,
 *                                  TEE_PARAM_TYPE_MEMREF_OUPUT,
 *                                    TEE_PARAM_TYPE_NONE, TEE_PARAM_TYPE_NONE)) {
 *      return TEE_ERROR_BAD_PARAMETERS;
 *  }
 */
#define TEE_PARAM_TYPES(t0,t1,t2,t3) \
   ((t0) | ((t1) « 4) | ((t2) « 8) | ((t3) « 12))

/*
 * The macro TEE_PARAM_TYPE_GET can be used to extract the type of a given
 * parameter from paramTypes if you need more fine-grained type checking.
 */
#define TEE_PARAM_TYPE_GET(t, i) ((((uint32_t)t) » ((i)*4)) & 0xF)

/*
 * The macro TEE_PARAM_TYPE_SET can be used to load the type of a given
 * parameter from paramTypes without specifying all types (TEE_PARAM_TYPES)
 */
#define TEE_PARAM_TYPE_SET(t, i) (((uint32_t)(t) & 0xF) « ((i)*4))

/* Not specified in the standard */
#define TEE_NUM_PARAMS  4

/* TEE Arithmetical APIs */

#define TEE_BigIntSizeInU32(n) ((((n)+31)/32)+2)

#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
#endif /* TEE_API_DEFINES_H */
```

10.13 ta-ref/api/include/tee_api_defines_extensions.h File Reference

This graph shows which files directly or indirectly include this file:



10.14 tee_api_defines_extensions.h

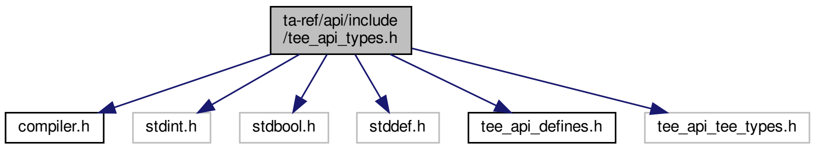
Go to the documentation of this file.

```
/*
 * Copyright (c) 2014, Linaro Limited
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */

#ifndef TEE_API_DEFINES_EXTENSIONS_H
#define TEE_API_DEFINES_EXTENSIONS_H
#ifndef DOXYGEN_SHOULD_SKIP_THIS

/*
 * HMAC-based Extract-and-Expand Key Derivation Function (HKDF)
 */

#define TEE_ALG_HKDF_MD5_DERIVE_KEY     0x800010C0
#define TEE_ALG_HKDF_SHA1_DERIVE_KEY    0x800020C0
#define TEE_ALG_HKDF_SHA224_DERIVE_KEY  0x800030C0
#define TEE_ALG_HKDF_SHA256_DERIVE_KEY  0x800040C0
#define TEE_ALG_HKDF_SHA384_DERIVE_KEY  0x800050C0
#define TEE_ALG_HKDF_SHA512_DERIVE_KEY  0x800060C0

#define TEE_TYPE_HKDF_IKM               0xA10000C0

#define TEE_ATTR_HKDF_IKM               0xC00001C0
#define TEE_ATTR_HKDF_SALT              0xD00002C0
#define TEE_ATTR_HKDF_INFO              0xD00003C0
#define TEE_ATTR_HKDF_OKM_LENGTH        0xF00004C0

/*
 * Concatenation Key Derivation Function (Concat KDF)
 * NIST SP 800-56A section 5.8.1
 */

#define TEE_ALG_CONCAT_KDF_SHA1_DERIVE_KEY    0x800020C1
#define TEE_ALG_CONCAT_KDF_SHA224_DERIVE_KEY  0x800030C1
#define TEE_ALG_CONCAT_KDF_SHA256_DERIVE_KEY  0x800040C1
#define TEE_ALG_CONCAT_KDF_SHA384_DERIVE_KEY  0x800050C1
#define TEE_ALG_CONCAT_KDF_SHA512_DERIVE_KEY  0x800060C1

#define TEE_TYPE_CONCAT_KDF_Z                 0xA10000C1

#define TEE_ATTR_CONCAT_KDF_Z                 0xC00001C1
#define TEE_ATTR_CONCAT_KDF_OTHER_INFO        0xD00002C1
#define TEE_ATTR_CONCAT_KDF_DKM_LENGTH        0xF00003C1

/*
 * PKCS #5 v2.0 Key Derivation Function 2 (PBKDF2)
 * RFC 2898 section 5.2
 * https://www.ietf.org/rfc/rfc2898.txt
 */

#define TEE_ALG_PBKDF2_HMAC_SHA1_DERIVE_KEY 0x800020C2

#define TEE_TYPE_PBKDF2_PASSWORD            0xA10000C2

#define TEE_ATTR_PBKDF2_PASSWORD            0xC00001C2
#define TEE_ATTR_PBKDF2_SALT                0xD00002C2
#define TEE_ATTR_PBKDF2_ITERATION_COUNT     0xF00003C2
#define TEE_ATTR_PBKDF2_DKM_LENGTH          0xF00004C2

/*
 * Implementation-specific object storage constants
 */

/* Storage is provided by the Rich Execution Environment (REE) */
#define TEE_STORAGE_PRIVATE_REE  0x80000000
/* Storage is the Replay Protected Memory Block partition of an eMMC device */
#define TEE_STORAGE_PRIVATE_RPMB 0x80000100
/* Was TEE_STORAGE_PRIVATE_SQL, which isn't supported any longer */
#define TEE_STORAGE_PRIVATE_SQL_RESERVED  0x80000200

/*
 * Extension of "Memory Access Rights Constants"
 * #define TEE_MEMORY_ACCESS_READ             0x00000001
 * #define TEE_MEMORY_ACCESS_WRITE            0x00000002
 * #define TEE_MEMORY_ACCESS_ANY_OWNER        0x00000004
 *
 * TEE_MEMORY_ACCESS_NONSECURE : if set TEE_CheckMemoryAccessRights()
  * successfully returns only if target vmem range is mapped non-secure.
  *
  * TEE_MEMORY_ACCESS_SECURE : if set TEE_CheckMemoryAccessRights()
  * successfully returns only if target vmem range is mapped secure.

  */
 #define TEE_MEMORY_ACCESS_NONSECURE          0x10000000
 #define TEE_MEMORY_ACCESS_SECURE             0x20000000

 #endif /*DOXYGEN_SHOULD_SKIP_THIS*/
 #endif /* TEE_API_DEFINES_EXTENSIONS_H */
```

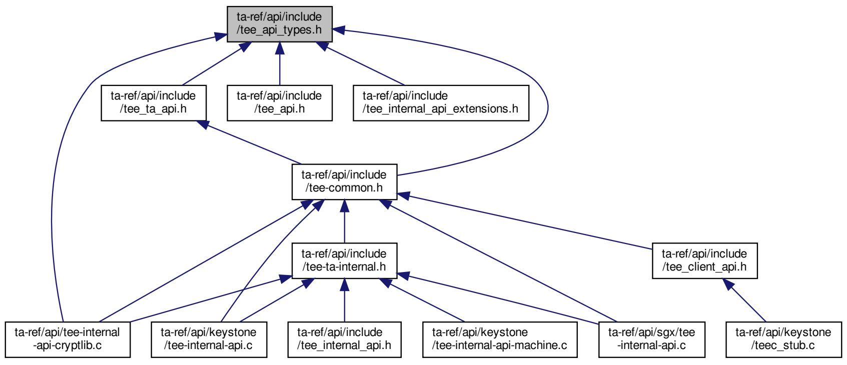
10.15 ta-ref/api/include/tee_api_types.h File Reference

```
#include <compiler.h>
#include <stdint.h>
#include <stdbool.h>
#include <stddef.h>
#include <tee_api_defines.h>
#include "tee_api_tee_types.h"
```

Include dependency graph for tee_api_types.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct TEE_UUID
- struct TEE_Identity

- union TEE_Param
- struct TEE_ObjectInfo
- struct TEE_Attribute
- struct TEE_OperationInfo
- struct TEE_OperationInfoKey
- struct TEE_OperationInfoMultiple
- struct TEE_Time
- struct TEE_SEReaderProperties
- struct TEE_SEAID
- struct pollfd
- struct addrinfo

Typedefs

- typedef uint32_t TEE_Result
- typedef struct __TEE_TASessionHandle ∗ TEE_TASessionHandle
- typedef struct __TEE_PropSetHandle ∗ TEE_PropSetHandle
- typedef struct __TEE_ObjectHandle ∗ TEE_ObjectHandle
- typedef struct __TEE_ObjectEnumHandle ∗ TEE_ObjectEnumHandle
- typedef struct __TEE_OperationHandle ∗ TEE_OperationHandle
- typedef uint32_t TEE_ObjectType
- typedef uint32_t TEE_BigInt
- typedef uint32_t TEE_BigIntFMM
- typedef uint32_t TEE_BigIntFMMContext __aligned(__alignof__(void ∗))
- typedef struct __TEE_SEServiceHandle ∗ TEE_SEServiceHandle
- typedef struct __TEE_SEReaderHandle ∗ TEE_SEReaderHandle
- typedef struct __TEE_SESessionHandle ∗ TEE_SESessionHandle
- typedef struct __TEE_SEChannelHandle ∗ TEE_SEChannelHandle
- typedef uint32_t TEE_ErrorOrigin
- typedef void ∗ TEE_Session
- typedef unsigned long int nfds_t
- typedef uint32_t socklen_t

Enumerations

- enum TEE_Whence { TEE_DATA_SEEK_SET = 0 , TEE_DATA_SEEK_CUR = 1 , TEE_DATA_SEEK_END = 2 }
- enum TEE_OperationMode {
  TEE_MODE_ENCRYPT = 0 , TEE_MODE_DECRYPT = 1 , TEE_MODE_SIGN = 2 , TEE_MODE_VERIFY = 3 ,
  TEE_MODE_MAC = 4 , TEE_MODE_DIGEST = 5 , TEE_MODE_DERIVE = 6 }

10.15.1 Typedef Documentation

10.15.1.1 __aligned `typedef uint32_t TEE_BigIntFMMContext __aligned(__alignof__(void *))`

10.15.1.2 nfds_t

`typedef unsigned long int nfds_t`

10.15.1.3 socklen_t

`typedef uint32_t socklen_t`

10.15.1.4 TEE_BigInt

`typedef uint32_t TEE_BigInt`

10.15.1.5 TEE_BigIntFMM

`typedef uint32_t TEE_BigIntFMM`

10.15.1.6 TEE_ErrorOrigin

`typedef uint32_t TEE_ErrorOrigin`

10.15.1.7 TEE_ObjectEnumHandle

`typedef struct __TEE_ObjectEnumHandle* TEE_ObjectEnumHandle`

10.15.1.8 TEE_ObjectHandle

`typedef struct __TEE_ObjectHandle* TEE_ObjectHandle`

10.15.1.9 TEE_ObjectType

`typedef uint32_t TEE_ObjectType`

10.15.1.10 TEE_OperationHandle

`typedef struct __TEE_OperationHandle* TEE_OperationHandle`

10.15.1.11 TEE_PropSetHandle

`typedef struct __TEE_PropSetHandle* TEE_PropSetHandle`

10.15.1.12 TEE_Result

`typedef uint32_t TEE_Result`

10.15.1.13 TEE_SEChannelHandle `typedef struct __TEE_SEChannelHandle* TEE_SEChannelHandle`

10.15.1.14 TEE_SEReaderHandle `typedef struct __TEE_SEReaderHandle* TEE_SEReaderHandle`

10.15.1.15 TEE_SEServiceHandle `typedef struct __TEE_SEServiceHandle* TEE_SEServiceHandle`

10.15.1.16 TEE_SESessionHandle `typedef struct __TEE_SESessionHandle* TEE_SESessionHandle`

10.15.1.17 TEE_Session `typedef void* TEE_Session`

10.15.1.18 TEE_TASessionHandle `typedef struct __TEE_TASessionHandle* TEE_TASessionHandle`

10.15.2 Enumeration Type Documentation

10.15.2.1 TEE_OperationMode `enum TEE_OperationMode`

Enumerator

TEE_MODE_ENCRYPT	
TEE_MODE_DECRYPT	
TEE_MODE_SIGN	
TEE_MODE_VERIFY	
TEE_MODE_MAC	
TEE_MODE_DIGEST	
TEE_MODE_DERIVE	

10.15.2.2 TEE_Whence `enum TEE_Whence`

Enumerator

TEE_DATA_SEEK_SET	
TEE_DATA_SEEK_CUR	
TEE_DATA_SEEK_END	

10.16 tee_api_types.h

Go to the documentation of this file.

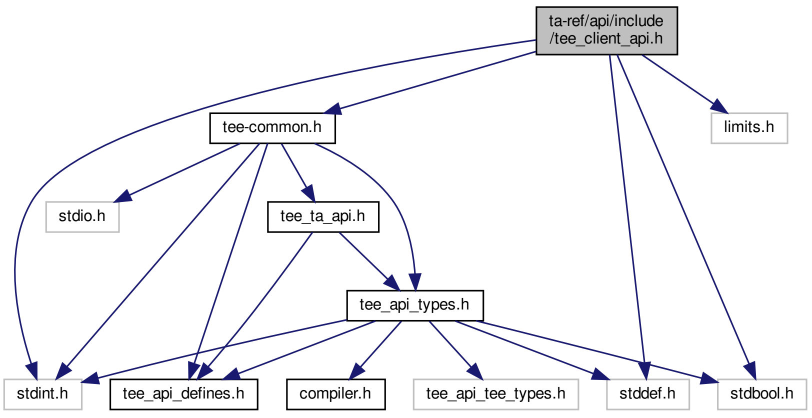
```
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */

/* Based on GP TEE Internal API Specification Version 0.11 */
#ifndef TEE_API_TYPES_H
#define TEE_API_TYPES_H

#include <compiler.h>
#include <stdint.h>
#include <stdbool.h>
#include <stddef.h>
#include <tee_api_defines.h>
#include "tee_api_tee_types.h"

/*
 * Common Definitions
 */

typedef uint32_t TEE_Result;

typedef struct {
    uint32_t timeLow;
    uint16_t timeMid;
    uint16_t timeHiAndVersion;
    uint8_t clockSeqAndNode[8];
} TEE_UUID;

/*
 * The TEE_Identity structure defines the full identity of a Client:
 * - login is one of the TEE_LOGIN_XXX constants
 * - uuid contains the client UUID or Nil if not applicable
 */
typedef struct {
    uint32_t login;
    TEE_UUID uuid;
} TEE_Identity;

/*
 * This union describes one parameter passed by the Trusted Core Framework
 * to the entry points TA_OpenSessionEntryPoint or
 * TA_InvokeCommandEntryPoint or by the TA to the functions
 * TEE_OpenTASession or TEE_InvokeTACommand.
 *
 * Which of the field value or memref to select is determined by the
 * parameter type specified in the argument paramTypes passed to the entry
 * point.
*/
typedef union {
    struct {
        void *buffer;
        uint32_t size;
    } memref;
    struct {
        uint32_t a;
        uint32_t b;
    } value;
} TEE_Param;

/*
 * The type of opaque handles on TA Session. These handles are returned by
 * the function TEE_OpenTASession.
 */
typedef struct __TEE_TASessionHandle *TEE_TASessionHandle;

/*
 * The type of opaque handles on property sets or enumerators. These
 * handles are either one of the pseudo handles TEE_PROPSET_XXX or are
 * returned by the function TEE_AllocatePropertyEnumerator.
*/
typedef struct __TEE_PropSetHandle *TEE_PropSetHandle;

typedef struct __TEE_ObjectHandle *TEE_ObjectHandle;
typedef struct __TEE_ObjectEnumHandle *TEE_ObjectEnumHandle;
typedef struct __TEE_OperationHandle *TEE_OperationHandle;

/*
 * Storage Definitions
 */

typedef uint32_t TEE_ObjectType;

typedef struct {
    uint32_t objectType;
    __extension__ union {
        uint32_t keySize;    /* used in 1.1 spec */
        uint32_t objectSize;  /* used in 1.1.1 spec */
    };
    __extension__ union {
        uint32_t maxKeySize;  /* used in 1.1 spec */
        uint32_t maxObjectSize;    /* used in 1.1.1 spec */
    };
    uint32_t objectUsage;
    uint32_t dataSize;
    uint32_t dataPosition;
    uint32_t handleFlags;
} TEE_ObjectInfo;

typedef enum {
    TEE_DATA_SEEK_SET = 0,
    TEE_DATA_SEEK_CUR = 1,
    TEE_DATA_SEEK_END = 2
} TEE_Whence;

typedef struct {
    uint32_t attributeID;
    union {
        struct {
            void *buffer;
            uint32_t length;
        } ref;
        struct {
            uint32_t a, b;
        } value;
    } content;
} TEE_Attribute;

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define DMREQ_FINISH 0
#define DMREQ_WRITE 1
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

/* Cryptographic Operations API */

typedef enum {
    TEE_MODE_ENCRYPT = 0,
    TEE_MODE_DECRYPT = 1,
    TEE_MODE_SIGN = 2,
    TEE_MODE_VERIFY = 3,
    TEE_MODE_MAC = 4,
    TEE_MODE_DIGEST = 5,
    TEE_MODE_DERIVE = 6
} TEE_OperationMode;

typedef struct {
    uint32_t algorithm;
    uint32_t operationClass;
    uint32_t mode;
    uint32_t digestLength;
    uint32_t maxKeySize;
    uint32_t keySize;
    uint32_t requiredKeyUsage;
    uint32_t handleState;
} TEE_OperationInfo;

typedef struct {
    uint32_t keySize;
    uint32_t requiredKeyUsage;
} TEE_OperationInfoKey;

typedef struct {
    uint32_t algorithm;
    uint32_t operationClass;
    uint32_t mode;
    uint32_t digestLength;
    uint32_t maxKeySize;
    uint32_t handleState;
    uint32_t operationState;
    uint32_t numberOfKeys;
    TEE_OperationInfoKey keyInformation[];
} TEE_OperationInfoMultiple;

/* Time & Date API */

typedef struct {
    uint32_t seconds;
    uint32_t millis;
} TEE_Time;

/* TEE Arithmetical APIs */

typedef uint32_t TEE_BigInt;

typedef uint32_t TEE_BigIntFMM;

typedef uint32_t TEE_BigIntFMMContext __aligned(__alignof__(void *));

/* Tee Secure Element APIs */

typedef struct __TEE_SEServiceHandle *TEE_SEServiceHandle;
typedef struct __TEE_SEReaderHandle *TEE_SEReaderHandle;
typedef struct __TEE_SESessionHandle *TEE_SESessionHandle;
typedef struct __TEE_SEChannelHandle *TEE_SEChannelHandle;

typedef struct {
    bool sePresent;
    bool teeOnly;
    bool selectResponseEnable;
} TEE_SEReaderProperties;

typedef struct {
    uint8_t *buffer;
    size_t bufferLen;
} TEE_SEAID;

/* Other definitions */
typedef uint32_t TEE_ErrorOrigin;
typedef void *TEE_Session;

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define TEE_MEM_INPUT   0x00000001
#define TEE_MEM_OUTPUT  0x00000002

#define TEE_MEMREF_0_USED  0x00000001
#define TEE_MEMREF_1_USED  0x00000002
#define TEE_MEMREF_2_USED  0x00000004
#define TEE_MEMREF_3_USED  0x00000008

#define TEE_SE_READER_NAME_MAX  20
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

#ifndef PLAT_KEYSTONE
// TODO: ???

```

```
typedef unsigned long int nfds_t;

struct pollfd
{
        int fd;                      /* File descriptor to poll.  */
    short int events;            /* Types of events poller cares about.  */
    short int revents;           /* Types of events that actually occurred.  */
};

typedef uint32_t socklen_t;

struct addrinfo {
    int              ai_flags;
    int              ai_family;
    int              ai_socktype;
    int              ai_protocol;
    socklen_t        ai_addrlen;
    struct sockaddr *ai_addr;
    char            *ai_canonname;
    struct addrinfo *ai_next;
};

#endif /* !PLAT_KEYSTONE */

#endif /* TEE_API_TYPES_H */
```

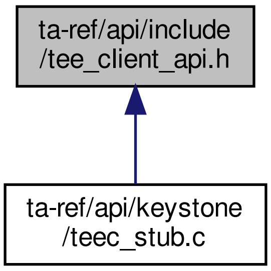
10.17 ta-ref/api/include/tee_client_api.h File Reference

```
#include <stdint.h>
#include <stddef.h>
#include <stdbool.h>
#include <limits.h>
#include "tee-common.h"
```

Include dependency graph for tee_client_api.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct TEEC_Context
- struct TEEC_UUID
- struct TEEC_SharedMemory
- struct TEEC_TempMemoryReference
- struct TEEC_RegisteredMemoryReference
- struct TEEC_Value
- union TEEC_Parameter
- struct TEEC_Session
- struct TEEC_Operation

Typedefs

- typedef uint32_t TEEC_Result

Functions

- TEEC_Result TEEC_InitializeContext (const char ∗name, TEEC_Context ∗context)
- void TEEC_FinalizeContext (TEEC_Context ∗context)
- TEEC_Result TEEC_OpenSession (TEEC_Context ∗context, TEEC_Session ∗session, const TEEC_UUID ∗destination, uint32_t connectionMethod, const void ∗connectionData, TEEC_Operation ∗operation, uint32↩ _t ∗returnOrigin)
- void TEEC_CloseSession (TEEC_Session ∗session)
- TEEC_Result TEEC_InvokeCommand (TEEC_Session ∗session, uint32_t commandID, TEEC_Operation ∗operation, uint32_t ∗returnOrigin)
- TEEC_Result TEEC_RegisterSharedMemory (TEEC_Context ∗context, TEEC_SharedMemory ∗shared↩ Mem)
- TEEC_Result TEEC_AllocateSharedMemory (TEEC_Context ∗context, TEEC_SharedMemory ∗shared↩ Mem)
- void TEEC_ReleaseSharedMemory (TEEC_SharedMemory ∗sharedMemory)
- void TEEC_RequestCancellation (TEEC_Operation ∗operation)

10.17.1 Typedef Documentation

10.17.1.1 TEEC_Result `typedef uint32_t TEEC_Result`

10.17.2 Function Documentation

10.17.2.1 TEEC_AllocateSharedMemory() `TEEC_Result TEEC_AllocateSharedMemory (`

```
TEEC_Context * context,
TEEC_SharedMemory * sharedMem )
```

TEEC_AllocateSharedMemory() - Allocate shared memory for TEE.

Parameters

context	The initialized TEE context structure in which scope to open the session.
sharedMem	Pointer to the allocated shared memory.

Returns

TEEC_SUCCESS The registration was successful.

TEEC_ERROR_OUT_OF_MEMORY Memory exhaustion.

TEEC_Result Something failed.

10.17.2.2 TEEC_CloseSession() `void TEEC_CloseSession (`

```
TEEC_Session * session )
```

TEEC_CloseSession() - Closes the session which has been opened with the specific trusted application.

Parameters

session	The opened session to close.

10.17.2.3 TEEC_FinalizeContext() `void TEEC_FinalizeContext (`

```
TEEC_Context * context )
```

TEEC_FinalizeContext() - Destroys a context holding connection information on the specific TEE.

This function destroys an initialized TEE context, closing the connection between the client application and the TEE. This function must only be called when all sessions related to this TEE context have been closed and all shared memory blocks have been released.

Parameters

context	The context to be destroyed.

TEEC_FinalizeContext() - Destroys a context holding connection information on the specific TEE.

This function finalizes an initialized TEE context, closing the connection between the client application and the TEE. This function must only be called when all sessions related to this TEE context have been closed and all shared memory blocks have been released.

Parameters

context	The context to be finalized.

10.17.2.4 TEEC_InitializeContext()

```
TEEC_Result TEEC_InitializeContext (
        const char * name,
        TEEC_Context * context )
```

TEEC_InitializeContext() - Initializes a context holding connection information on the specific TEE, designated by the name string.

Parameters

name	A zero-terminated string identifying the TEE to connect to. If name is set to NULL, the default TEE is connected to. NULL is the only supported value in this version of the API implementation.
context	The context structure which is to be initialized.

Returns

TEEC_SUCCESS The initialization was successful.

TEEC_Result Something failed.

10.17.2.5 TEEC_InvokeCommand()

```
TEEC_Result TEEC_InvokeCommand (
        TEEC_Session * session,
        uint32_t commandID,
        TEEC_Operation * operation,
        uint32_t * returnOrigin )
```

TEEC_InvokeCommand() - Executes a command in the specified trusted application.

Parameters

session	A handle to an open connection to the trusted application.
commandID	Identifier of the command in the trusted application to invoke.
operation	An operation structure to use in the invoke command. May be set to NULL to signify no operation structure needed.
returnOrigin	A parameter which will hold the error origin if this function returns any value other than TEEC_SUCCESS.

Returns

TEEC_SUCCESS OpenSession successfully opened a new session.

TEEC_Result Something failed.

10.17.2.6 TEEC_OpenSession()

```
TEEC_Result TEEC_OpenSession (
        TEEC_Context * context,
        TEEC_Session * session,
        const TEEC_UUID * destination,
        uint32_t connectionMethod,
        const void * connectionData,
        TEEC_Operation * operation,
        uint32_t * returnOrigin )
```

TEEC_OpenSession() - Opens a new session with the specified trusted application.

Parameters

context	The initialized TEE context structure in which scope to open the session.
session	The session to initialize.
destination	A structure identifying the trusted application with which to open a session.
connectionMethod	The connection method to use.
connectionData	Any data necessary to connect with the chosen connection method. Not supported, should be set to NULL.
operation	An operation structure to use in the session. May be set to NULL to signify no operation structure needed.
returnOrigin	A parameter which will hold the error origin if this function returns any value other than TEEC_SUCCESS.

Returns

TEEC_SUCCESS OpenSession successfully opened a new session.

TEEC_Result Something failed.

10.17.2.7 TEEC_RegisterSharedMemory() TEEC_Result TEEC_RegisterSharedMemory (TEEC_Context * *context*, TEEC_SharedMemory * *sharedMem*)

TEEC_RegisterSharedMemory() - Register a block of existing memory as a shared block within the scope of the specified context.

Parameters

context	The initialized TEE context structure in which scope to open the session.
sharedMem	pointer to the shared memory structure to register.

Returns

TEEC_SUCCESS The registration was successful.

TEEC_ERROR_OUT_OF_MEMORY Memory exhaustion.

TEEC_Result Something failed.

10.17.2.8 TEEC_ReleaseSharedMemory() void TEEC_ReleaseSharedMemory (TEEC_SharedMemory * *sharedMemory*)

TEEC_ReleaseSharedMemory() - Free or deregister the shared memory.

Parameters

sharedMem	Pointer to the shared memory to be freed.

10.17.2.9 TEEC_RequestCancellation() void TEEC_RequestCancellation (TEEC_Operation * *operation*)

TEEC_RequestCancellation() - Request the cancellation of a pending open session or command invocation.

Parameters

operation	Pointer to an operation previously passed to open session or invoke.

10.18 tee_client_api.h

Go to the documentation of this file.

```
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 * All rights reserved.
 * Copyright (c) 2015, Linaro Limited
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
  * 1. Redistributions of source code must retain the above copyright notice,
  * this list of conditions and the following disclaimer.
  *
  * 2. Redistributions in binary form must reproduce the above copyright notice,
  * this list of conditions and the following disclaimer in the documentation
  * and/or other materials provided with the distribution.
  *
  * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
  * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
  * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
  * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
  * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
  * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
  * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
  * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
  * POSSIBILITY OF SUCH DAMAGE.
  */
#ifndef TEE_CLIENT_API_H
#define TEE_CLIENT_API_H

#ifdef __cplusplus
extern "C" {
#endif

#include <stdint.h>
#include <stddef.h>
#include <stdbool.h>
#include <limits.h>
#include "tee-common.h"

#ifndef DOXYGEN_SHOULD_SKIP_THIS
/*
  * Defines the number of available memory references in an open session or
  * invoke command operation payload.
  */
#define TEEC_CONFIG_PAYLOAD_REF_COUNT 4

#define TEEC_CONFIG_SHAREDMEM_MAX_SIZE ULONG_MAX

#define TEEC_NONE                    0x00000000
#define TEEC_VALUE_INPUT             0x00000001
#define TEEC_VALUE_OUTPUT            0x00000002
#define TEEC_VALUE_INOUT             0x00000003
#define TEEC_MEMREF_TEMP_INPUT       0x00000005
#define TEEC_MEMREF_TEMP_OUTPUT      0x00000006
#define TEEC_MEMREF_TEMP_INOUT       0x00000007
#define TEEC_MEMREF_WHOLE            0x0000000C
#define TEEC_MEMREF_PARTIAL_INPUT    0x0000000D
#define TEEC_MEMREF_PARTIAL_OUTPUT   0x0000000E
#define TEEC_MEMREF_PARTIAL_INOUT    0x0000000F

#define TEEC_MEM_INPUT   0x00000001
#define TEEC_MEM_OUTPUT  0x00000002

#define TEEC_SUCCESS                 0x00000000
#define TEEC_ERROR_GENERIC           0xFFFF0000
#define TEEC_ERROR_ACCESS_DENIED     0xFFFF0001
#define TEEC_ERROR_CANCEL            0xFFFF0002
#define TEEC_ERROR_ACCESS_CONFLICT   0xFFFF0003
#define TEEC_ERROR_EXCESS_DATA       0xFFFF0004
#define TEEC_ERROR_BAD_FORMAT        0xFFFF0005
#define TEEC_ERROR_BAD_PARAMETERS    0xFFFF0006
#define TEEC_ERROR_BAD_STATE         0xFFFF0007
#define TEEC_ERROR_ITEM_NOT_FOUND    0xFFFF0008
#define TEEC_ERROR_NOT_IMPLEMENTED   0xFFFF0009
#define TEEC_ERROR_NOT_SUPPORTED     0xFFFF000A
#define TEEC_ERROR_NO_DATA           0xFFFF000B
#define TEEC_ERROR_OUT_OF_MEMORY     0xFFFF000C
#define TEEC_ERROR_BUSY              0xFFFF000D
#define TEEC_ERROR_COMMUNICATION     0xFFFF000E
#define TEEC_ERROR_SECURITY          0xFFFF000F
#define TEEC_ERROR_SHORT_BUFFER      0xFFFF0010
#define TEEC_ERROR_EXTERNAL_CANCEL   0xFFFF0011
#define TEEC_ERROR_TARGET_DEAD       0xFFFF3024
```

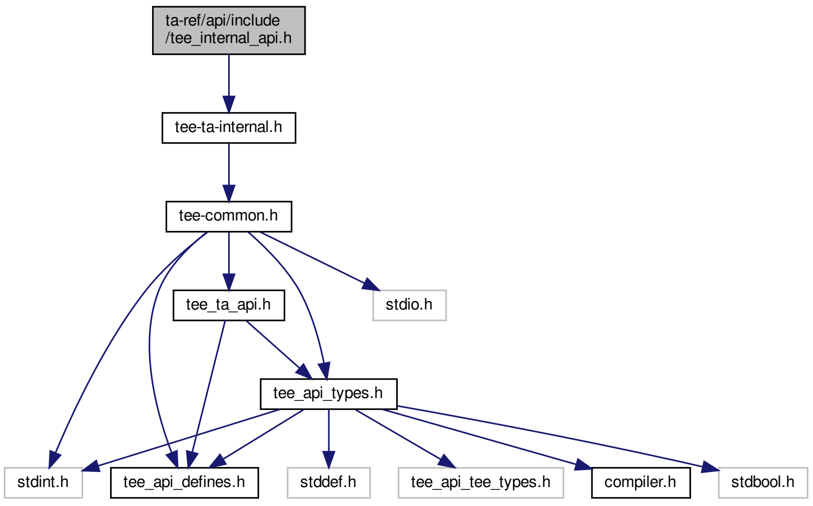
```

#define TEEC_ORIGIN_API          0x00000001
#define TEEC_ORIGIN_COMMS        0x00000002
#define TEEC_ORIGIN_TEE          0x00000003
#define TEEC_ORIGIN_TRUSTED_APP  0x00000004

#define TEEC_LOGIN_PUBLIC       0x00000000
#define TEEC_LOGIN_USER         0x00000001
#define TEEC_LOGIN_GROUP        0x00000002
#define TEEC_LOGIN_APPLICATION  0x00000004
#define TEEC_LOGIN_USER_APPLICATION  0x00000005
#define TEEC_LOGIN_GROUP_APPLICATION  0x00000006

#define TEEC_PARAM_TYPES(p0, p1, p2, p3) \
    ((p0) | ((p1) « 4) | ((p2) « 8) | ((p3) « 12))

#define TEEC_PARAM_TYPE_GET(p, i) (((p) » (i * 4)) & 0xF)
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

typedef uint32_t TEEC_Result;

typedef struct {
    /* Implementation defined */
    int fd;
    bool reg_mem;
} TEEC_Context;

typedef struct {
    uint32_t timeLow;
    uint16_t timeMid;
    uint16_t timeHiAndVersion;
    uint8_t clockSeqAndNode[8];
} TEEC_UUID;

typedef struct {
    void *buffer;
    size_t size;
    uint32_t flags;
    /*
     * Implementation-Defined
     */
    int id;
    size_t alloced_size;
    void *shadow_buffer;
    int registered_fd;
    bool buffer_allocated;
} TEEC_SharedMemory;

typedef struct {
    void *buffer;
    size_t size;
} TEEC_TempMemoryReference;

typedef struct {
    TEEC_SharedMemory *parent;
    size_t size;
    size_t offset;
} TEEC_RegisteredMemoryReference;

typedef struct {
    uint32_t a;
    uint32_t b;
} TEEC_Value;

typedef union {
    TEEC_TempMemoryReference tmpref;
    TEEC_RegisteredMemoryReference memref;
    TEEC_Value value;
} TEEC_Parameter;

typedef struct {
    /* Implementation defined */
    TEEC_Context *ctx;
    uint32_t session_id;
} TEEC_Session;

typedef struct {
    uint32_t started;
    uint32_t paramTypes;
    TEEC_Parameter params[TEEC_CONFIG_PAYLOAD_REF_COUNT];
    /* Implementation-Defined */
    TEEC_Session *session;
} TEEC_Operation;

TEEC_Result TEEC_InitializeContext(const char *name, TEEC_Context *context);
```

```
void TEEC_FinalizeContext(TEEC_Context *context);

TEEC_Result TEEC_OpenSession(TEEC_Context *context,
                 TEEC_Session *session,
                 const TEEC_UUID *destination,
                 uint32_t connectionMethod,
                 const void *connectionData,
                 TEEC_Operation *operation,
                 uint32_t *returnOrigin);

void TEEC_CloseSession(TEEC_Session *session);

TEEC_Result TEEC_InvokeCommand(TEEC_Session *session,
                   uint32_t commandID,
                   TEEC_Operation *operation,
                   uint32_t *returnOrigin);

TEEC_Result TEEC_RegisterSharedMemory(TEEC_Context *context,
                      TEEC_SharedMemory *sharedMem);

TEEC_Result TEEC_AllocateSharedMemory(TEEC_Context *context,
                      TEEC_SharedMemory *sharedMem);

void TEEC_ReleaseSharedMemory(TEEC_SharedMemory *sharedMemory);

void TEEC_RequestCancellation(TEEC_Operation *operation);

#ifdef __cplusplus
}
#endif

#endif
```

10.19 ta-ref/api/include/tee_internal_api.h File Reference

`#include "tee-ta-internal.h"`

Include dependency graph for tee_internal_api.h:



10.20 tee_internal_api.h

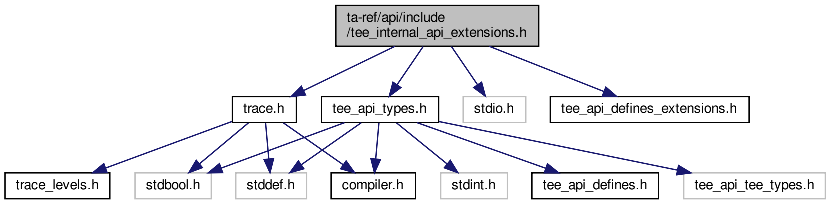
Go to the documentation of this file.

```
#include "tee-ta-internal.h"
```

10.21 ta-ref/api/include/tee_internal_api_extensions.h File Reference

```
#include <trace.h>
#include <stdio.h>
#include <tee_api_defines_extensions.h>
#include <tee_api_types.h>
```

Include dependency graph for tee_internal_api_extensions.h:



Functions

- void tee_user_mem_mark_heap (void)
- size_t tee_user_mem_check_heap (void)
- TEE_Result TEE_CacheClean (char ∗buf, size_t len)
- TEE_Result TEE_CacheFlush (char ∗buf, size_t len)
- TEE_Result TEE_CacheInvalidate (char ∗buf, size_t len)
- void ∗ tee_map_zi (size_t len, uint32_t flags)
- TEE_Result tee_unmap (void ∗buf, size_t len)
- TEE_Result tee_uuid_from_str (TEE_UUID ∗uuid, const char ∗s)

10.21.1 Function Documentation

10.21.1.1 TEE_CacheClean()

```
TEE_Result TEE_CacheClean (
        char * buf,
        size_t len )
```

10.21.1.2 TEE_CacheFlush()

```
TEE_Result TEE_CacheFlush (
        char * buf,
        size_t len )
```

10.21.1.3 TEE_CacheInvalidate()

```
TEE_Result TEE_CacheInvalidate (
        char * buf,
        size_t len )
```

10.21.1.4 tee_map_zi()

```
void * tee_map_zi (
        size_t len,
        uint32_t flags )
```

10.21.1.5 tee_unmap()

```
TEE_Result tee_unmap (
        void * buf,
        size_t len )
```

10.21.1.6 tee_user_mem_check_heap()

```
size_t tee_user_mem_check_heap (
        void )
```

10.21.1.7 tee_user_mem_mark_heap()

```
void tee_user_mem_mark_heap (
        void )
```

10.21.1.8 tee_uuid_from_str()

```
TEE_Result tee_uuid_from_str (
        TEE_UUID * uuid,
        const char * s )
```

10.22 tee_internal_api_extensions.h

Go to the documentation of this file.

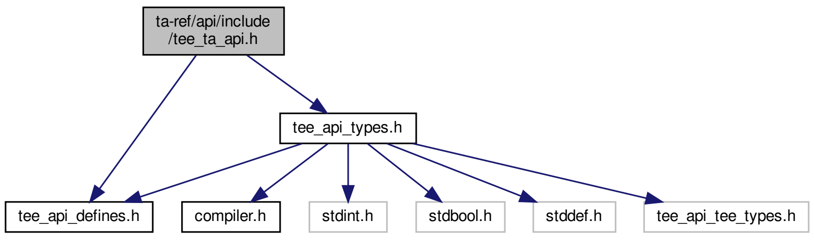
```
/* SPDX-License-Identifier: BSD-2-Clause */
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 */

#ifndef TEE_INTERNAL_API_EXTENSIONS_H
#define TEE_INTERNAL_API_EXTENSIONS_H

/* trace support */
#include <trace.h>
#include <stdio.h>
#include <tee_api_defines_extensions.h>
#include <tee_api_types.h>

void tee_user_mem_mark_heap(void);
size_t tee_user_mem_check_heap(void);
/* Hint implementation defines */

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define TEE_USER_MEM_HINT_NO_FILL_ZERO       0x80000000
```

```
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

/*
 * Cache maintenance support (TA requires the CACHE_MAINTENANCE property)
 *
 * TEE_CacheClean() Write back to memory any dirty data cache lines. The line
 *                  is marked as not dirty. The valid bit is unchanged.
 *
 * TEE_CacheFlush() Purges any valid data cache lines. Any dirty cache lines
 *                  are first written back to memory, then the cache line is
 *                  invalidated.
 *
 * TEE_CacheInvalidate() Invalidate any valid data cache lines. Any dirty line
 *                       are not written back to memory.
 */
TEE_Result TEE_CacheClean(char *buf, size_t len);
TEE_Result TEE_CacheFlush(char *buf, size_t len);
TEE_Result TEE_CacheInvalidate(char *buf, size_t len);

/*
 * tee_map_zi() - Map zero initialized memory
 * @len:     Number of bytes
 * @flags:   0 or TEE_MEMORY_ACCESS_ANY_OWNER to allow sharing with other TAs
 *
 * Returns valid pointer on success or NULL on error.
 */
void *tee_map_zi(size_t len, uint32_t flags);

/*
 * tee_unmap() - Unmap previously mapped memory
 * @buf:     Buffer
 * @len:     Number of bytes
 *
 * Note that supplied @buf and @len has to match exactly what has
 * previously been returned by tee_map_zi().
 *
 * Return TEE_SUCCESS on success or TEE_ERRROR_* on failure.
 */
TEE_Result tee_unmap(void *buf, size_t len);

/*
 * Convert a UUID string @s into a TEE_UUID @uuid
 * Expected format for @s is: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
 * 'x' being any hexadecimal digit (0-9a-fA-F)
 */
TEE_Result tee_uuid_from_str(TEE_UUID *uuid, const char *s);

#endif
```

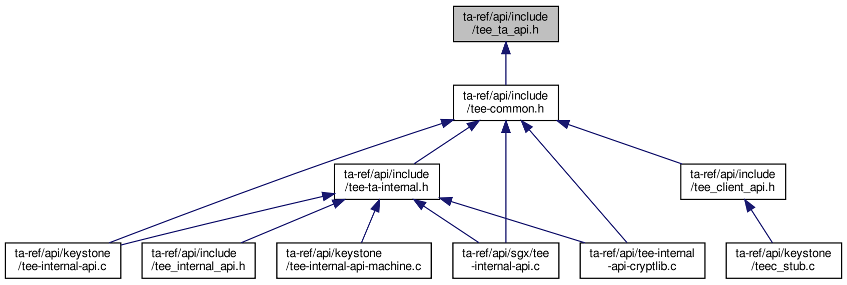
10.23 ta-ref/api/include/tee_ta_api.h File Reference

```
#include <tee_api_defines.h>
#include <tee_api_types.h>
```

Include dependency graph for tee_ta_api.h:



This graph shows which files directly or indirectly include this file:


ta-ref/api/include /tee_ta_api.h
ta-ref/api/include /tee-common.h
ta-ref/api/include /tee-ta-internal.h
ta-ref/api/include /tee_client_api.h
ta-ref/api/keystone /tee-internal-api.c
ta-ref/api/include /tee_internal_api.h
ta-ref/api/keystone /tee-internal-api-machine.c
ta-ref/api/sgx/tee -internal-api.c
ta-ref/api/tee-internal -api-cryptlib.c
ta-ref/api/keystone /teec_stub.c

Functions

- TEE_Result TA_EXPORT TA_CreateEntryPoint (void)
- void TA_EXPORT TA_DestroyEntryPoint (void)
- TEE_Result TA_EXPORT TA_OpenSessionEntryPoint (uint32_t paramTypes, TEE_Param params[TEE_↩ NUM_PARAMS], void ∗∗sessionContext)
- void TA_EXPORT TA_CloseSessionEntryPoint (void ∗sessionContext)
- TEE_Result TA_EXPORT TA_InvokeCommandEntryPoint (void ∗sessionContext, uint32_t commandID, uint32_t paramTypes, TEE_Param params[TEE_NUM_PARAMS])

10.23.1 Function Documentation

10.23.1.1 TA_CloseSessionEntryPoint()

```
void TA_EXPORT TA_CloseSessionEntryPoint (
        void * sessionContext )
```

10.23.1.2 TA_CreateEntryPoint()

```
TEE_Result TA_EXPORT TA_CreateEntryPoint (
        void )
```

10.23.1.3 TA_DestroyEntryPoint()

```
void TA_EXPORT TA_DestroyEntryPoint (
        void )
```

10.23.1.4 TA_InvokeCommandEntryPoint()

```
TEE_Result TA_EXPORT TA_InvokeCommandEntryPoint (
        void * sessionContext,
        uint32_t commandID,
        uint32_t paramTypes,
        TEE_Param params[TEE_NUM_PARAMS] )
```

10.23.1.5 TA_OpenSessionEntryPoint()

```
TEE_Result TA_EXPORT TA_OpenSessionEntryPoint (
        uint32_t paramTypes,
        TEE_Param params[TEE_NUM_PARAMS],
        void ** sessionContext )
```

10.24 tee_ta_api.h

Go to the documentation of this file.

```
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */

/* Based on GP TEE Internal API Specification Version 0.22 */
#ifndef TEE_TA_API_H
#define TEE_TA_API_H

#include <tee_api_defines.h>
#include <tee_api_types.h>

#ifndef DOXYGEN_SHOULD_SKIP_THIS
/* This is a null define in STE TEE environment */
#define TA_EXPORT
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

/*
 * TA Interface
 *
 * Each Trusted Application must provide the Implementation with a number
 * of functions, collectively called the “TA interface”. These functions
 * are the entry points called by the Trusted Core Framework to create the
 * instance, notify the instance that a new client is connecting, notify
 * the instance when the client invokes a command, etc.
 *
 * Trusted Application Entry Points:
 */

/*
 * The function TA_CreateEntryPoint is the Trusted Application's
 * constructor, which the Framework calls when it creates a new instance of
 * the Trusted Application. To register instance data, the implementation
 * of this constructor can use either global variables or the function
 * TEE_InstanceSetData.
 *
 * Return Value:
 * - TEE_SUCCESS: if the instance is successfully created, the function
 *   must return TEE_SUCCESS.
 * - Any other value: if any other code is returned the instance is not
 *   created, and no other entry points of this instance will be called.
 *   The Framework MUST reclaim all resources and dereference all objects
 *   related to the creation of the instance.
 *
 *   If this entry point was called as a result of a client opening a
 *   session, the error code is returned to the client and the session is
 *   not opened.
 */
TEE_Result TA_EXPORT TA_CreateEntryPoint(void);
```

```

/*
 * The function TA_DestroyEntryPoint is the Trusted Applications
 * destructor, which the Framework calls when the instance is being
 * destroyed.
 *
 * When the function TA_DestroyEntryPoint is called, the Framework
 * guarantees that no client session is currently open. Once the call to
 * TA_DestroyEntryPoint has been completed, no other entry point of this
 * instance will ever be called.
 *
 * Note that when this function is called, all resources opened by the
 * instance are still available. It is only after the function returns that
 * the Implementation MUST start automatically reclaiming resources left
 * opened.
 *
 * Return Value:
 * This function can return no success or error code. After this function
 * returns the Implementation MUST consider the instance destroyed and
 * reclaims all resources left open by the instance.
 */
void TA_EXPORT TA_DestroyEntryPoint(void);

/*
 * The Framework calls the function TA_OpenSessionEntryPoint when a client
 * requests to open a session with the Trusted Application. The open
 * session request may result in a new Trusted Application instance being
 * created as defined in section 4.5.
 *
 * The client can specify parameters in an open operation which are passed
 * to the Trusted Application instance in the arguments paramTypes and
 * params. These arguments can also be used by the Trusted Application
 * instance to transfer response data back to the client. See section 4.3.6
 * for a specification of how to handle the operation parameters.
 *
 * If this function returns TEE_SUCCESS, the client is connected to a
 * Trusted Application instance and can invoke Trusted Application
 * commands. When the client disconnects, the Framework will eventually
 * call the TA_CloseSessionEntryPoint entry point.
 *
 * If the function returns any error, the Framework rejects the connection
 * and returns the error code and the current content of the parameters the
 * client. The return origin is then set to TEE_ORIGIN_TRUSTED_APP.
 *
 * The Trusted Application instance can register a session data pointer by
 * setting *psessionContext. The value of this pointer is not interpreted
 * by the Framework, and is simply passed back to other TA_ functions
 * within this session. Note that *sessionContext may be set with a pointer
 * to a memory allocated by the Trusted Application instance or with
 * anything else, like an integer, a handle etc. The Framework will not
 * automatically free *sessionContext when the session is closed; the
 * Trusted Application instance is responsible for freeing memory if
 * required.
 *
 * During the call to TA_OpenSessionEntryPoint the client may request to
 * cancel the operation. See section 4.10 for more details on
 * cancellations. If the call to TA_OpenSessionEntryPoint returns
 * TEE_SUCCESS, the client must consider the session as successfully opened
 * and explicitly close it if necessary.
 *
 * Parameters:
 * - paramTypes: the types of the four parameters.
 * - params: a pointer to an array of four parameters.
 * - sessionContext: A pointer to a variable that can be filled by the
 *   Trusted Application instance with an opaque void* data pointer
 *
 * Return Value:
 * - TEE_SUCCESS if the session is successfully opened.
 * - Any other value if the session could not be open.
 *   o The error code may be one of the pre-defined codes, or may be a new
 *     error code defined by the Trusted Application implementation itself.
 */
TEE_Result TA_EXPORT TA_OpenSessionEntryPoint(uint32_t paramTypes,
                 TEE_Param params[TEE_NUM_PARAMS],
                 void **sessionContext);

/*
 * The Framework calls this function to close a client session. During the
 * call to this function the implementation can use any session functions.
 *
 * The Trusted Application implementation is responsible for freeing any
 * resources consumed by the session being closed. Note that the Trusted
 * Application cannot refuse to close a session, but can hold the closing
 * until it returns from TA_CloseSessionEntryPoint. This is why this
 * function cannot return an error code.
 *
 * Parameters:
 * - sessionContext: The value of the void* opaque data pointer set by the
 *   Trusted Application in the function TA_OpenSessionEntryPoint for this
 *   session.
 */
void TA_EXPORT TA_CloseSessionEntryPoint(void *sessionContext);

/*
 * The Framework calls this function when the client invokes a command
 * within the given session.
 *
 * The Trusted Application can access the parameters sent by the client
 * through the paramTypes and params arguments. It can also use these
 * arguments to transfer response data back to the client.
 *
 * During the call to TA_InvokeCommandEntryPoint the client may request to
 * cancel the operation.
 *
 * A command is always invoked within the context of a client session.
 * Thus, any session function  can be called by the command implementation.
 *
 * Parameter:
 * - sessionContext: The value of the void* opaque data pointer set by the
 *   Trusted Application in the function TA_OpenSessionEntryPoint.
 * - commandID: A Trusted Application-specific code that identifies the
 *   command to be invoked.
 * - paramTypes: the types of the four parameters.
 * - params: a pointer to an array of four parameters.
 *
 * Return Value:
 * - TEE_SUCCESS: if the command is successfully executed, the function
 *   must return this value.
 * - Any other value: if the invocation of the command fails for any
 *   reason.
 *   o The error code may be one of the pre-defined codes, or may be a new
 *     error code defined by the Trusted Application implementation itself.
 */

TEE_Result TA_EXPORT TA_InvokeCommandEntryPoint(void *sessionContext,
            uint32_t commandID,
            uint32_t paramTypes,
            TEE_Param params[TEE_NUM_PARAMS]);

/*
 * Correspondance Client Functions <--> TA Functions
 *
 * TEE_OpenSession or TEE_OpenTASession:
 * If a new Trusted Application instance is needed to handle the session,
 * TA_CreateEntryPoint is called.
 * Then, TA_OpenSessionEntryPoint is called.
 *
 *
 * TEE_InvokeCommand or TEE_InvokeTACommand:
 * TA_InvokeCommandEntryPoint is called.
 *
 *
 * TEE_CloseSession or TEE_CloseTASession:
 * TA_CloseSessionEntryPoint is called.
 * For a multi-instance TA or for a single-instance, non keep-alive TA, if
 * the session closed was the last session on the instance, then
 * TA_DestroyEntryPoint is called. Otherwise, the instance is kept until
 * the TEE shuts down.
 *
 */

#endif
```

10.25 ta-ref/api/include/test_dev_key.h File Reference

Variables

- static const unsigned char _sanctum_dev_secret_key [ ]
- static const size_t _sanctum_dev_secret_key_len = 64
- static const unsigned char _sanctum_dev_public_key [ ]
- static const size_t _sanctum_dev_public_key_len = 32

10.25.1 Variable Documentation

10.25.1.1 _sanctum_dev_public_key `const unsigned char _sanctum_dev_public_key[ ] [static]`

Initial value:

```
= {
  0x0f, 0xaa, 0xd4, 0xff, 0x01, 0x17, 0x85, 0x83, 0xba, 0xa5, 0x88, 0x96,
  0x6f, 0x7c, 0x1f, 0xf3, 0x25, 0x64, 0xdd, 0x17, 0xd7, 0xdc, 0x2b, 0x46,
  0xcb, 0x50, 0xa8, 0x4a, 0x69, 0x27, 0x0b, 0x4c
}
```

10.25.1.2 _sanctum_dev_public_key_len `const size_t _sanctum_dev_public_key_len = 32 [static]`

10.25.1.3 _sanctum_dev_secret_key `const unsigned char _sanctum_dev_secret_key[ ] [static]`

Initial value:

```
= {
  0x40, 0xa0, 0x99, 0x47, 0x8c, 0xce, 0xfa, 0x3a, 0x06, 0x63, 0xab, 0xc9,
  0x5e, 0x7a, 0x1e, 0xc9, 0x54, 0xb4, 0xf5, 0xf6, 0x45, 0xba, 0xd8, 0x04,
  0xdb, 0x13, 0xe7, 0xd7, 0x82, 0x6c, 0x70, 0x73, 0x57, 0x6a, 0x9a, 0xb6,
  0x21, 0x60, 0xd9, 0xd1, 0xc6, 0xae, 0xdc, 0x29, 0x85, 0x2f, 0xb9, 0x60,
  0xee, 0x51, 0x32, 0x83, 0x5a, 0x16, 0x89, 0xec, 0x06, 0xa8, 0x72, 0x34,
  0x51, 0xaa, 0x0e, 0x4a
}
```

10.25.1.4 _sanctum_dev_secret_key_len `const size_t _sanctum_dev_secret_key_len = 64 [static]`

10.26 test_dev_key.h

Go to the documentation of this file.

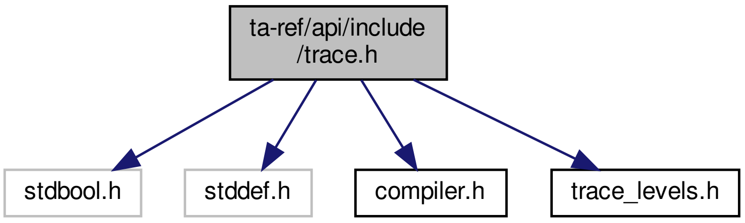
```
/* These are known device TESTING keys, use them for testing on platforms/qemu */

#warning Using TEST device root key. No integrity guarantee.
static const unsigned char _sanctum_dev_secret_key[] = {
  0x40, 0xa0, 0x99, 0x47, 0x8c, 0xce, 0xfa, 0x3a, 0x06, 0x63, 0xab, 0xc9,
  0x5e, 0x7a, 0x1e, 0xc9, 0x54, 0xb4, 0xf5, 0xf6, 0x45, 0xba, 0xd8, 0x04,
  0xdb, 0x13, 0xe7, 0xd7, 0x82, 0x6c, 0x70, 0x73, 0x57, 0x6a, 0x9a, 0xb6,
  0x21, 0x60, 0xd9, 0xd1, 0xc6, 0xae, 0xdc, 0x29, 0x85, 0x2f, 0xb9, 0x60,
  0xee, 0x51, 0x32, 0x83, 0x5a, 0x16, 0x89, 0xec, 0x06, 0xa8, 0x72, 0x34,
  0x51, 0xaa, 0x0e, 0x4a
};
static const size_t _sanctum_dev_secret_key_len = 64;

static const unsigned char _sanctum_dev_public_key[] = {
  0x0f, 0xaa, 0xd4, 0xff, 0x01, 0x17, 0x85, 0x83, 0xba, 0xa5, 0x88, 0x96,
  0x6f, 0x7c, 0x1f, 0xf3, 0x25, 0x64, 0xdd, 0x17, 0xd7, 0xdc, 0x2b, 0x46,
  0xcb, 0x50, 0xa8, 0x4a, 0x69, 0x27, 0x0b, 0x4c
};
```

```
static const size_t _sanctum_dev_public_key_len = 32;
```

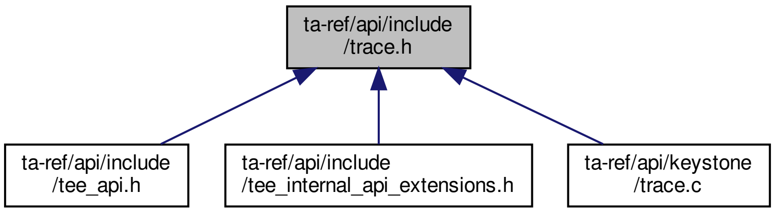
10.27 ta-ref/api/include/trace.h File Reference

```
#include <stdbool.h>
#include <stddef.h>
#include <compiler.h>
#include <trace_levels.h>
```

Include dependency graph for trace.h:



This graph shows which files directly or indirectly include this file:



Functions

- void trace_ext_puts (const char ∗str)
- int trace_ext_get_thread_id (void)
- void trace_set_level (int level)
- int trace_get_level (void)
- void trace_printf (const char ∗func, int line, int level, bool level_ok, const char ∗fmt,...) __printf(5
- void void dhex_dump (const char ∗function, int line, int level, const void ∗buf, int len)

Variables

- int trace_level
- const char trace_ext_prefix [ ]

10.27.1 Function Documentation

10.27.1.1 dhex_dump()

```
void void dhex_dump (
    const char * function,
    int line,
    int level,
    const void * buf,
    int len )
```

10.27.1.2 trace_ext_get_thread_id()

```
int trace_ext_get_thread_id (
    void   )
```

10.27.1.3 trace_ext_puts()

```
void trace_ext_puts (
    const char * str )
```

10.27.1.4 trace_get_level()

```
int trace_get_level (
    void   )
```

10.27.1.5 trace_printf()

```
void trace_printf (
    const char * func,
    int line,
    int level,
    bool level_ok,
    const char * fmt,
     ...   )
```

10.27.1.6 trace_set_level()

```
void trace_set_level (
    int level )
```

10.27.2 Variable Documentation

10.27.2.1 trace_ext_prefix

```
const char trace_ext_prefix[ ]  [extern]
```

10.27.2.2 trace_level

```
int trace_level  [extern]
```

10.28 trace.h

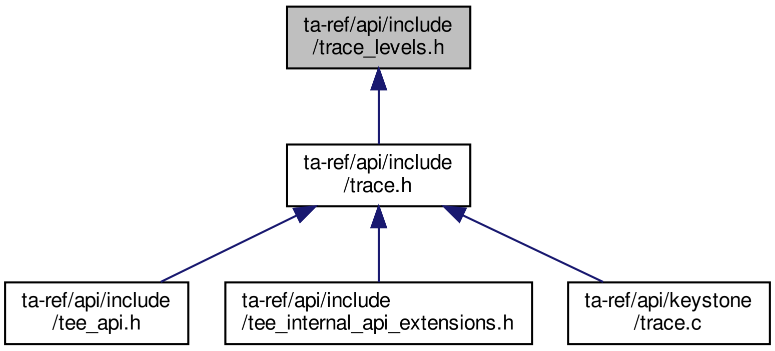
Go to the documentation of this file.

```
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */
#ifndef TRACE_H
#define TRACE_H

#include <stdbool.h>
#include <stddef.h>
#include <compiler.h>
#include <trace_levels.h>

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define MAX_PRINT_SIZE      256
#define MAX_FUNC_PRINT_SIZE 32

#ifndef TRACE_LEVEL
#define TRACE_LEVEL TRACE_MAX
#endif
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

/*
 * Symbols provided by the entity that uses this API.
 */
extern int trace_level;
extern const char trace_ext_prefix[];
void trace_ext_puts(const char *str);
int trace_ext_get_thread_id(void);
void trace_set_level(int level);
int trace_get_level(void);

/* Internal functions used by the macros below */
void trace_printf(const char *func, int line, int level, bool level_ok,
          const char *fmt, ...) __printf(5, 6);

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define trace_printf_helper(level, level_ok, ...) \
    trace_printf(__func__, __LINE__, (level), (level_ok), \
             __VA_ARGS__)

/* Formatted trace tagged with level independent */
#if (TRACE_LEVEL <= 0)
#define MSG(...)   (void)0
#else
#define MSG(...)   trace_printf_helper(0, false, __VA_ARGS__)
#endif

/* Formatted trace tagged with TRACE_ERROR level */
#if (TRACE_LEVEL < TRACE_ERROR)
#define EMSG(...)   (void)0
#else
#define EMSG(...)   trace_printf_helper(TRACE_ERROR, true, __VA_ARGS__)
#endif

/* Formatted trace tagged with TRACE_INFO level */
#if (TRACE_LEVEL < TRACE_INFO)
#define IMSG(...)   (void)0
#else
#define IMSG(...)   trace_printf_helper(TRACE_INFO, true, __VA_ARGS__)
#endif

/* Formatted trace tagged with TRACE_DEBUG level */
#if (TRACE_LEVEL < TRACE_DEBUG)
```

```
#define DMSG(...)   (void)0
#else
#define DMSG(...)   trace_printf_helper(TRACE_DEBUG, true, __VA_ARGS__)
#endif

/* Formatted trace tagged with TRACE_FLOW level */
#if (TRACE_LEVEL < TRACE_FLOW)
#define FMSG(...)   (void)0
#else
#define FMSG(...)   trace_printf_helper(TRACE_FLOW, true, __VA_ARGS__)
#endif

/* Formatted trace tagged with TRACE_FLOW level and prefix with ’> ’ */
#define INMSG(...)     FMSG("> " __VA_ARGS__)
/* Formatted trace tagged with TRACE_FLOW level and prefix with ’< ’ */
#define OUTMSG(...)    FMSG("< " __VA_ARGS__)
/* Formatted trace tagged with TRACE_FLOW level and prefix with ’< ’ and print
 * an error message if r != 0 */
#define OUTRMSG(r)          \
    do {              \
        OUTMSG("r=[%x]", r);    \
        return r;       \
    } while (0)

#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

void dhex_dump(const char *function, int line, int level,
           const void *buf, int len);


#ifndef DOXYGEN_SHOULD_SKIP_THIS
#if (TRACE_LEVEL < TRACE_DEBUG)
#define DHEXDUMP(buf, len) (void)0
#else
#define DHEXDUMP(buf, len) dhex_dump(__func__, __LINE__, TRACE_DEBUG, \
                     buf, len)
#endif


/* Trace api without trace formatting */

#define trace_printf_helper_raw(level, level_ok, ...) \
    trace_printf(NULL, 0, (level), (level_ok), __VA_ARGS__)

/* No formatted trace tagged with level independent */
#if (TRACE_LEVEL <= 0)
#define MSG_RAW(...)   (void)0
#else
#define MSG_RAW(...)   trace_printf_helper_raw(0, false, __VA_ARGS__)
#endif

/* No formatted trace tagged with TRACE_ERROR level */
#if (TRACE_LEVEL < TRACE_ERROR)
#define EMSG_RAW(...)   (void)0
#else
#define EMSG_RAW(...)   trace_printf_helper_raw(TRACE_ERROR, true, __VA_ARGS__)
#endif

/* No formatted trace tagged with TRACE_INFO level */
#if (TRACE_LEVEL < TRACE_INFO)
#define IMSG_RAW(...)   (void)0
#else
#define IMSG_RAW(...)   trace_printf_helper_raw(TRACE_INFO, true, __VA_ARGS__)
#endif

/* No formatted trace tagged with TRACE_DEBUG level */
#if (TRACE_LEVEL < TRACE_DEBUG)
#define DMSG_RAW(...)   (void)0
#else
#define DMSG_RAW(...)   trace_printf_helper_raw(TRACE_DEBUG, true, __VA_ARGS__)
#endif

/* No formatted trace tagged with TRACE_FLOW level */
#if (TRACE_LEVEL < TRACE_FLOW)
#define FMSG_RAW(...)   (void)0
#else
#define FMSG_RAW(...)   trace_printf_helper_raw(TRACE_FLOW, true, __VA_ARGS__)
#endif

#if (TRACE_LEVEL <= 0)
#define SMSG(...)   (void)0
#else
/*
 * Synchronised flushed trace, an Always message straight to HW trace IP.
 * Current only supported inside OP-TEE kernel, will be just like an EMSG()
 * in another context.
 */
#define SMSG(...)   \
    trace_printf(__func__, __LINE__, TRACE_ERROR, true, __VA_ARGS__)

#endif /* TRACE_LEVEL */

#if defined(__KERNEL__) && defined(CFG_UNWIND)
#include <kernel/unwind.h>
#define _PRINT_STACK
#endif

#if defined(_PRINT_STACK) && (TRACE_LEVEL >= TRACE_ERROR)
#define EPRINT_STACK() print_kernel_stack(TRACE_ERROR)
#else
#define EPRINT_STACK() (void)0
#endif

#if defined(_PRINT_STACK) && (TRACE_LEVEL >= TRACE_INFO)
#define IPRINT_STACK() print_kernel_stack(TRACE_INFO)
#else
#define IPRINT_STACK() (void)0
#endif

#if defined(_PRINT_STACK) && (TRACE_LEVEL >= TRACE_DEBUG)
#define DPRINT_STACK() print_kernel_stack(TRACE_DEBUG)
#else
#define DPRINT_STACK() (void)0
#endif

#if defined(_PRINT_STACK) && (TRACE_LEVEL >= TRACE_FLOW)
#define FPRINT_STACK() print_kernel_stack(TRACE_FLOW)
#else
#define FPRINT_STACK() (void)0
#endif

#if defined(__KERNEL__) && defined(CFG_UNWIND)
#undef _PRINT_STACK
#endif

#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
#endif /* TRACE_H */
```

10.29 ta-ref/api/include/trace_levels.h File Reference

This graph shows which files directly or indirectly include this file:


ta-ref/api/include /trace_levels.h
ta-ref/api/include /trace.h
ta-ref/api/include /tee_api.h
ta-ref/api/include /tee_internal_api_extensions.h
ta-ref/api/keystone /trace.c

10.30 trace_levels.h

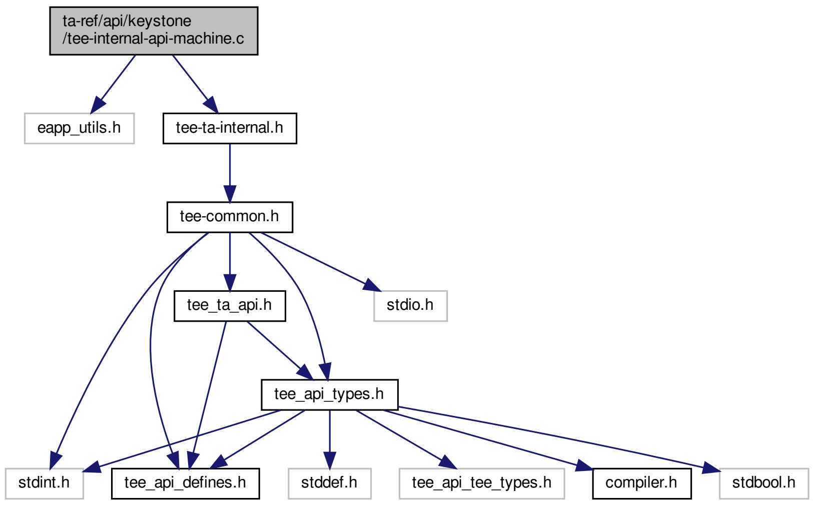
Go to the documentation of this file.

```
/*
 * Copyright (c) 2014, STMicroelectronics International N.V.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
  *
  * 2. Redistributions in binary form must reproduce the above copyright notice,
  * this list of conditions and the following disclaimer in the documentation
  * and/or other materials provided with the distribution.
  *
  * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
  * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
  * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
  * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
  * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
  * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
  * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
  * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
  * POSSIBILITY OF SUCH DAMAGE.
  */
#ifndef TRACE_LEVELS_H
#define TRACE_LEVELS_H

/*
  * Trace levels.
  *
  * ALWAYS is used when you always want a print to be seen, but it is not always
  * an error.
  *
  * ERROR is used when some kind of error has happened, this is most likely the
  * print you will use most of the time when you report some kind of error.
  *
  * INFO is used when you want to print some 'normal' text to the user.
  * This is the default level.
  *
  * DEBUG is used to print extra information to enter deeply in the module.
  *
  * FLOW is used to print the execution flox, typically the in/out of functions.
  *
  */

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define TRACE_MIN       1
#define TRACE_ERROR     TRACE_MIN
#define TRACE_INFO      2
#define TRACE_DEBUG     3
#define TRACE_FLOW      4
#define TRACE_MAX       TRACE_FLOW

/* Trace level of the casual printf */
#define TRACE_PRINTF_LEVEL TRACE_ERROR

#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
#endif /*TRACE_LEVELS_H*/

```

10.31 ta-ref/api/keystone/tee-internal-api-machine.c File Reference

```
#include "eapp_utils.h"
#include "tee-ta-internal.h"
```

Include dependency graph for tee-internal-api-machine.c:



Functions

- void __attribute__ ((noreturn))

10.31.1 Function Documentation

10.31.1.1 __attribute__() `void __attribute__ ( (noreturn) )`

TEE_Panic() - Raises a panic in the Trusted Application instance.

When a Trusted Application calls the TEE_Panic function, the current instance shall be destroyed and all the resources opened by the instance shall be reclaimed. All sessions opened from the panicking instance on another TA shall be gracefully closed and all cryptographic objects and operations shall be closed properly.

Parameters

code	An informative panic code defined by the TA.

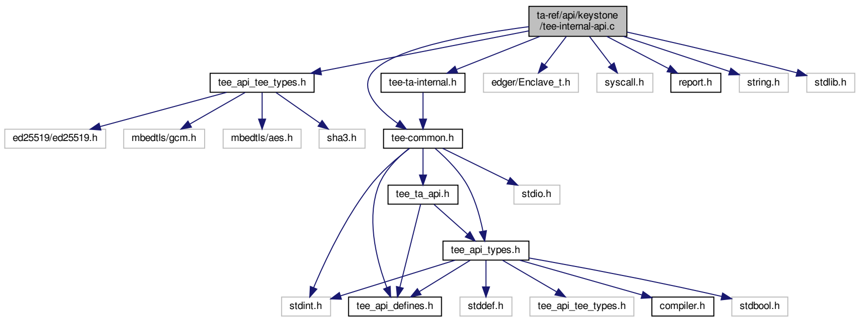
Returns

panic code will be returned.

10.32 ta-ref/api/keystone/tee-internal-api.c File Reference

```
#include "tee_api_tee_types.h"
```

```
#include "tee-common.h"
#include "tee-ta-internal.h"
#include "edger/Enclave_t.h"
#include "syscall.h"
#include "report.h"
#include <string.h>
#include <stdlib.h>
```
Include dependency graph for tee-internal-api.c:



Functions

- void ∗ TEE_Malloc (uint32_t size, uint32_t hint)
- void ∗ TEE_Realloc (void ∗buffer, uint32_t newSize)
- void TEE_Free (void ∗buffer)
- void TEE_GetREETime (TEE_Time ∗time)

  Core Functions, Time Functions.
- void TEE_GetSystemTime (TEE_Time ∗time)

  Core Functions, Time Functions.
- TEE_Result GetRelTimeStart (uint64_t start)

  Core Functions, Time Functions.
- TEE_Result GetRelTimeEnd (uint64_t end)

  Core Functions, Time Functions.
- static int flags2flags (int flags)
- static int set_object_key (void ∗id, unsigned int idlen, TEE_ObjectHandle object)
- static TEE_Result OpenPersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle ∗object, int ocreat)
- TEE_Result TEE_CreatePersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle attributes, const void ∗initialData, uint32_t initialDataLen, TEE_ObjectHandle ∗object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_OpenPersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle ∗object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_GetObjectInfo1 (TEE_ObjectHandle object, TEE_ObjectInfo ∗objectInfo)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_WriteObjectData (TEE_ObjectHandle object, const void ∗buffer, uint32_t size)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_ReadObjectData (TEE_ObjectHandle object, void ∗buffer, uint32_t size, uint32_t ∗count)

  Core Functions, Secure Storage Functions (data is isolated for each TA)
- void TEE_CloseObject (TEE_ObjectHandle object)

Core Functions, Secure Storage Functions (data is isolated for each TA)

- static int ocall_getrandom (char ∗buf, size_t len, unsigned int flags)
- WC_RNG ∗ get_wc_rng (void)
- int wc_ocall_genseed (void ∗nonce, uint32_t len)
- void TEE_GenerateRandom (void ∗randomBuffer, uint32_t randomBufferLen)

  Crypto, common.

Variables

- static int wc_rng_init = 0
- static WC_RNG rngstr

10.32.1 Function Documentation

10.32.1.1 flags2flags()

```
static int flags2flags (
    int flags )  [inline], [static]
```

flags2flags() - Checks the status for reading or writing of the file operational.

This function is used to check the status for reading or writing of the file operational.

Parameters

flags	Flags of the referencing node.

Returns

ret if success.

10.32.1.2 get_wc_rng()

```
WC_RNG * get_wc_rng (
    void  )
```

get_wc_rng() - Gets the seed (from OS) and key cipher for rng (random number genertor).

This function returns the random number or unique number of "rngstr".

Returns

random number if success else error occured.

10.32.1.3 GetRelTimeEnd()

```
TEE_Result GetRelTimeEnd (
    uint64_t end )
```

Core Functions, Time Functions.

GetRelTimeEnd() - finds the real time of the end timing.

This function prints the ending time.

Parameters

end	End timing

Returns

0 If success

10.32.1.4 GetRelTimeStart()

```
TEE_Result GetRelTimeStart (
        uint64_t start )
```

Core Functions, Time Functions.

GetRelTimeStart() - Gets the real time of the start timing.

This function prints the starting time.

Parameters

start	Start timing

Returns

0 on success

10.32.1.5 ocall_getrandom()

```
static int ocall_getrandom (
        char * buf,
        size_t len,
        unsigned int flags )  [static]
```

ocall_getrandom() - For getting random data.

This function describes that the retval is returned based on the size of buffer by calling the functions ocall_↩ getrandom196 and ocall_getrandom16

Parameters

buf	character type buffer
len	size of the buffer
flags	unassigned integer flag

Returns

retval value will be returned based on length of buffer.

10.32.1.6 OpenPersistentObject()

```
static TEE_Result OpenPersistentObject (
        uint32_t storageID,
        const void * objectID,
        uint32_t objectIDLen,
        uint32_t flags,
        TEE_ObjectHandle * object,
        int ocreat ) [static]
```

OpenPersistentObject() - Opens a handle on an existing persistent object.

The flags parameter is a set of flags that controls the access rights and sharing permissions with which the object handle is opened. The value of the flags parameter is constructed by a bitwise-inclusive OR of flags TEE_DATA↩_FLAG_ACCESS_READ, the object is opened with the read access right. This allows the Trusted Application to call the function TEE_ReadObjectData. TEE_DATA_FLAG_ACCESS_WRITE, the object is opened with the write access right. TEE_DATA_FLAG_ACCESS_WRITE_META, the object is opened with the write-meta access right.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	length of the identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion.

Returns

0 if success else error occured.

10.32.1.7 set_object_key()

```
static int set_object_key (
        void * id,
        unsigned int idlen,
        TEE_ObjectHandle object ) [static]
```

set_object_key() - Initialize report and then attest enclave with file.

This function describes the intialization of report, attest the enclave with file id and its length then assigned to ret. Based on "mbedtls" key encryption and decryption position of the object will be copied. Finally ret value returns on success else signature too short error will appear on failure.

Parameters

id	id of the object.
idlen	length of the id.
object	TEE_ObjectHandle type handle.

Returns

ret if success.

10.32.1.8 TEE_CloseObject()

```
void TEE_CloseObject (
    TEE_ObjectHandle object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_CloseObject() - Closes an opened object handle.

The object can be persistent or transient.For transient objects, TEE_CloseObject is equivalent to TEE_Free←TransientObject.

Parameters

object	Handle of the object.

Returns

TEE_SUCCESS if success else error occured.

10.32.1.9 TEE_CreatePersistentObject()

```
TEE_Result TEE_CreatePersistentObject (
    uint32_t storageID,
    const void * objectID,
    uint32_t objectIDLen,
    uint32_t flags,
    TEE_ObjectHandle attributes,
    const void * initialData,
    uint32_t initialDataLen,
    TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_CreatePersistentObject() - Creates a persistent object with initial attributes.

In this function an initial data stream content returns either a handle on the created object or TEE_HANDLE_NULL upon failure.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
attributes	A handle on a persistent object or an initialized transient object from which to take the persistent object attributes
initialData	The initial data content of the persistent object
initialDataLen	The initial data content of the persistent object
object	A pointer to the handle which contains the opened handle upon successful completion

Returns

0 if success else error occured.

10.32.1.10 TEE_Free()

```
void TEE_Free (
        void * buffer )
```

TEE_Free() - causes the space pointed to by buffer to be deallocated;that is made available for further allocation.

This function describes if buffer is a NULL pointer, TEE_Free does nothing. Otherwise, it is a Programmer Error if the argument does not match a pointer previously returned by the TEE_Malloc or TEE_Realloc if the space has been deallocated by a call to TEE_Free or TEE_Realloc.

Parameters

buffer	The pointer to the memory block to be freed.

10.32.1.11 TEE_GenerateRandom()

```
void TEE_GenerateRandom (
        void * randomBuffer,
        uint32_t randomBufferLen )
```

Crypto, common.

TEE_GenerateRandom() - Generates random data.

This function generates random data of random buffer length and is stored in to random Buffer by calling wc_↩
RNG_GenerateBlock().If ret is not equal
to 0 then TEE_Panic is called.

Parameters

randomBuffer	Reference to generated random data
randomBufferLen	Byte length of requested random data

Returns

random data random data will be returned.

10.32.1.12 TEE_GetObjectInfo1()

```
TEE_Result TEE_GetObjectInfo1 (
        TEE_ObjectHandle object,
        TEE_ObjectInfo * objectInfo )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_GetObjectInfo1() - Returns the characteristics of an object.

This function returns a handle which can be used to access the object's attributes and data stream.

Parameters

objectInfo	Pointer to a structure filled with the object information
object	Handle of the object

Returns

0 if success else error occured.

10.32.1.13 TEE_GetREETime()

```
void TEE_GetREETime (
        TEE_Time * time )
```

Core Functions, Time Functions.

TEE_GetREETime() - Retrieves the current REE system time.

This function retrieves the current time as seen from the point of view of the REE.

Parameters

time	Filled with the number of seconds and milliseconds

10.32.1.14 TEE_GetSystemTime()

```
void TEE_GetSystemTime (
        TEE_Time * time )
```

Core Functions, Time Functions.

TEE_GetSystemTime() - Retrieves the current system time.

This function describes the system time has an arbitrary implementation defined origin that can vary across TA instances. The minimum guarantee is that the system time shall be monotonic for a given TA instance.

Parameters

time	Filled with the number of seconds and milliseconds

10.32.1.15 TEE_Malloc()

```
void * TEE_Malloc (
        uint32_t size,
        uint32_t hint )
```

TEE_Malloc() - Allocates space for an object whose size in bytes is specified in the parameter size.

This function describes the pointer returned is guaranteed to be aligned
such that it may be assigned as a pointer to any basic C type.The valid hint values are a bitmask and can be independently set. This parameter allows Trusted Applications to refer to various pools of memory or to
request special characteristics for the allocated memory by using an
implementation-defined hint. Future versions of this specification may introduce additional standard hints.

Parameters

size	The size of the buffer to be allocated.
hint	A hint to the allocator.

Returns

Upon successful completion, with size not equal to zero, the function returns a pointer to the allocated space.

10.32.1.16 TEE_OpenPersistentObject()

```
TEE_Result TEE_OpenPersistentObject (
        uint32_t storageID,
        const void * objectID,
        uint32_t objectIDLen,
        uint32_t flags,
        TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_OpenPersistentObject() - Opens a handle on an existing persistent object.

This function returns a handle which can be used to access the object's attributes and data stream.

Parameters

storageID	The storage to use
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success else error occured.

10.32.1.17 TEE_ReadObjectData()

```
TEE_Result TEE_ReadObjectData (
        TEE_ObjectHandle object,
            void * buffer,
            uint32_t size,
            uint32_t * count )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_ReadObjectData() - Attempts to read size bytes from the data stream associated with the object into the buffer pointed to by buffer.

The bytes are read starting at the position in the data stream currently stored in the object handle. The handle's position is incremented by the number of bytes actually read. On completion of TEE_ReadObjectData sets the number of bytes actually read in the "uint32_t" pointed to by count. The value written to ∗count may be less than size if the number of bytes until the end-of3067 stream is less than size. It is set to 0 if the position at the start of the read operation is at or beyond the end-of-stream. These are the only cases where ∗count may be less than size.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write
count	size of the buffer.

Returns

TEE_SUCCESS if success else error occured.

10.32.1.18 TEE_Realloc()

```
void * TEE_Realloc (
            void * buffer,
            uint32_t newSize )
```

TEE_Realloc() - Changes the size of the memory object pointed to by buffer to the size specified by new size.

This function describes the content of the object remains unchanged up to the lesser of the new and old sizes. Space in excess of the old size contains unspecified content. If the new size of the memory object requires movement of the object, the space for the previous instantiation of the object is deallocated. If the space cannot be allocated, the original object remains allocated, and this function returns a NULL pointer.

Parameters

buffer	The pointer to the object to be reallocated.
newSize	The new size required for the object

Returns

Upon successful completion, TEE_Realloc returns a pointer to the (possibly moved) allocated space. If there is not enough available memory, TEE_Realloc returns a NULL pointer and the original buffer is still allocated and unchanged.

10.32.1.19 TEE_WriteObjectData()

```
TEE_Result TEE_WriteObjectData (
        TEE_ObjectHandle object,
        const void * buffer,
        uint32_t size )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_WriteObjectData() - Writes the buffer data in to persistent objects.

In this function it checks if object is present or not, the encryption/ decryption buffer is taken by calling mbedtls_aes←↩_crypt_cbc() then that buffer data is encrypted and mapped to object.On the base of object creation TEE_SUCCESS appears else TEE_ERROR_GENERIC appears.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write

Returns

TEE_SUCCESS if success else error occured.

10.32.1.20 wc_ocall_genseed()

```
int wc_ocall_genseed (
        void * nonce,
        uint32_t len )
```

wc_ocall_genseed() To generate random data.

This function describes the return value of random generated data. if generated random value is not equal to length of buffer then panic
reason occurs.

Parameters

nonce	pointer of buffer
len	length of the buffer.

Returns

0 on success else error will occur based on panic raised inside trusted application.

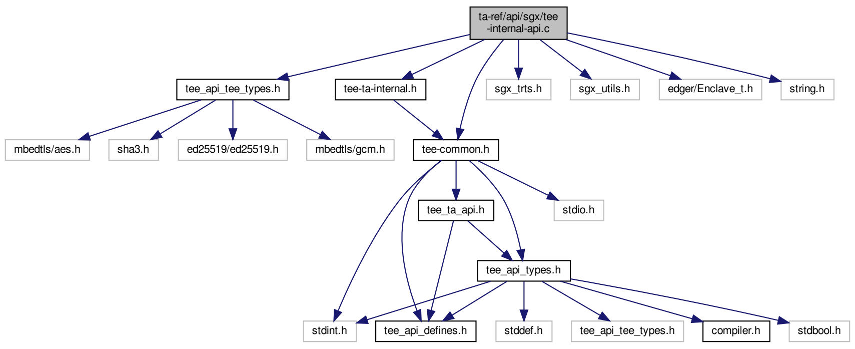
10.32.2 Variable Documentation

10.32.2.1 rngstr `WC_RNG rngstr [static]`

10.32.2.2 wc_rng_init `int wc_rng_init = 0 [static]`

10.33 ta-ref/api/sgx/tee-internal-api.c File Reference

```
#include "tee_api_tee_types.h"
#include "tee-common.h"
#include "tee-ta-internal.h"
#include "sgx_trts.h"
#include "sgx_utils.h"
#include "edger/Enclave_t.h"
#include <string.h>
```
Include dependency graph for tee-internal-api.c:



Functions

- void __attribute__ ((noreturn))
- void TEE_GetREETime (TEE_Time ∗time)

  Core Functions, Time Functions.
- void TEE_GetSystemTime (TEE_Time ∗time)

  Core Functions, Time Functions.
- TEE_Result GetRelTimeStart (uint64_t start)

  Core Functions, Time Functions.
- TEE_Result GetRelTimeEnd (uint64_t end)

  Core Functions, Time Functions.
- static int flags2flags (int flags)
- static int set_object_key (const void ∗id, unsigned int idlen, TEE_ObjectHandle object)
- static TEE_Result OpenPersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle ∗object, int ocreat)
- TEE_Result TEE_CreatePersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle attributes, const void ∗initialData, uint32_t initialDataLen, TEE_ObjectHandle ∗object)

  Core Functions, Secure Storage Functions (data is isolated for each TA)

- TEE_Result TEE_OpenPersistentObject (uint32_t storageID, const void ∗objectID, uint32_t objectIDLen, uint32_t flags, TEE_ObjectHandle ∗object)

    Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_GetObjectInfo1 (TEE_ObjectHandle object, TEE_ObjectInfo ∗objectInfo)

    Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_WriteObjectData (TEE_ObjectHandle object, const void ∗buffer, uint32_t size)

    Core Functions, Secure Storage Functions (data is isolated for each TA)
- TEE_Result TEE_ReadObjectData (TEE_ObjectHandle object, void ∗buffer, uint32_t size, uint32_t ∗count)

    Core Functions, Secure Storage Functions (data is isolated for each TA)
- void TEE_CloseObject (TEE_ObjectHandle object)

    Core Functions, Secure Storage Functions (data is isolated for each TA)
- void TEE_GenerateRandom (void ∗randomBuffer, uint32_t randomBufferLen)

    Crypto, common.
- static WC_RNG ∗ get_wc_rng (void)

Variables

- static int wc_rng_init = 0
- static WC_RNG rngstr

10.33.1 Function Documentation

10.33.1.1 __attribute__() `void __attribute__ ( (noreturn) )`

TEE_Panic() - Raises a Panic in the Trusted Application instance

When a Trusted Application calls the TEE_Panic function, the current instance shall be destroyed and all the resources opened by the instance shall be reclaimed.

Parameters

ec	An informative panic code defined by the TA. May be displayed in traces if traces are available.

10.33.1.2 flags2flags() `static int flags2flags ( int flags ) [inline], [static]`

flags2flags() - Checks the status for reading or writing of the file operational.

This function is to check the status for reading or writing of the file operational.

Parameters

flags	Flags of the referencing node.

Returns

0 if success else error occured.

10.33.1.3 get_wc_rng()

```
static WC_RNG * get_wc_rng (
    void ) [static]
```

get_wc_rng() - Gets the seed (from OS) and key cipher for rng(random number genertor).

This function returns the random number or unique number of "rngstr".

Returns

random number if success else error occured.

10.33.1.4 GetRelTimeEnd()

```
TEE_Result GetRelTimeEnd (
    uint64_t end )
```

Core Functions, Time Functions.

GetRelTimeStart() - find the real time of the end timing.

This function prints the End timing.

Parameters

end	End timing

Returns

0 if success else error occured

10.33.1.5 GetRelTimeStart()

```
TEE_Result GetRelTimeStart (
    uint64_t start )
```

Core Functions, Time Functions.

GetRelTimeStart() - Gets the real time of the start timing.

Ths function prints the start timing.

Parameters

start	start timing

Returns

0 if success else error occured.

10.33.1.6 OpenPersistentObject()

```
static TEE_Result OpenPersistentObject (
        uint32_t storageID,
        const void * objectID,
        uint32_t objectIDLen,
        uint32_t flags,
        TEE_ObjectHandle * object,
        int ocreat )  [static]
```

OpenPersistentObject() - Opens a handle on an existing persistent object.

The flags parameter is a set of flags that controls the access rights and sharing permissions with which the object handle is opened. The value of the flags parameter is constructed by a bitwise-inclusive OR of flags TEE_DATA↩_FLAG_ACCESS_READ, the object is opened with the read access right. This allows the Trusted Application to call the function TEE_ReadObjectData. TEE_DATA_FLAG_ACCESS_WRITE, the object is opened with the write access right. TEE_DATA_FLAG_ACCESS_WRITE_META, the object is opened with the write-meta access right.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	length of the identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion.

Returns

0 if success else error occured.

10.33.1.7 set_object_key()

```
static int set_object_key (
        const void * id,
        unsigned int idlen,
        TEE_ObjectHandle object )  [static]
```

set_object_key - To initalize report and then attest enclave with file.

This function describes objectID as key_id to make the key dependent on it sgx report key is 128-bit. Fill another 128-bit with seal key. seal key doesn't change with enclave. Better than nothing, though. random nonce can not use for AES here because of persistency. the digest of attestation report and objectID as the last resort has been used.

Parameters

id	id of the object.
idlen	length of the id.
object	TEE_ObjectHandle type handle.

Returns

0 if success else error occured.

10.33.1.8 TEE_CloseObject()

```
void TEE_CloseObject (
        TEE_ObjectHandle object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_CloseObject() - Function closes an opened object handle.

The object can be persistent or transient.For transient objects, TEE_CloseObject is equivalent to TEE_Free↩
TransientObject.

Parameters

object	Handle of the object

Returns

TEE_SUCCESS if success else error occured.

10.33.1.9 TEE_CreatePersistentObject()

```
TEE_Result TEE_CreatePersistentObject (
        uint32_t storageID,
        const void * objectID,
        uint32_t objectIDLen,
        uint32_t flags,
        TEE_ObjectHandle attributes,
        const void * initialData,
        uint32_t initialDataLen,
        TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_CreatePersistentObject() - Creates a persistent object with initial attributes.

An initial data stream content, and optionally returns either a handle on the created object, or TEE_HANDLE_NULL upon failure.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
attributes	A handle on a persistent object or an initialized transient object from which to take the persistent object attributes
initialData	The initial data content of the persistent object
initialDataLen	The initial data content of the persistent object
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success, else error occured.

10.33.1.10 TEE_GenerateRandom()

```
void TEE_GenerateRandom (
        void * randomBuffer,
        uint32_t randomBufferLen )
```

Crypto, common.

TEE_GenerateRandom() - Generates random data.

This function generates random data of random bufferlength and is stored in to randomBuffer by calling sgx_read←_rand().

Parameters

randomBuffer	Reference to generated random data
randomBufferLen	Byte length of requested random data

10.33.1.11 TEE_GetObjectInfo1()

```
TEE_Result TEE_GetObjectInfo1 (
        TEE_ObjectHandle object,
        TEE_ObjectInfo * objectInfo )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_GetObjectInfo1() - Function returns the characteristics of an object.

It returns a handle that can be used to access the object's attributes and data stream.

Parameters

objectInfo	Pointer to a structure filled with the object information
object	Handle of the object

Returns

0 if success else error occured.

10.33.1.12 TEE_GetREETime()

```
void TEE_GetREETime (
        TEE_Time * time )
```

Core Functions, Time Functions.

TEE_GetREETime() - Function retrieves the current REE system time.

This function retrieves the current time as seen from the point of view of the REE.

Parameters

time	Filled with the number of seconds and milliseconds.

10.33.1.13 TEE_GetSystemTime()

```
void TEE_GetSystemTime (
        TEE_Time * time )
```

Core Functions, Time Functions.

TEE_GetSystemTime() - Retrieves the current system time.

The system time has an arbitrary implementation-defined origin that can vary across TA instances

Parameters

time	Filled with the number of seconds and milliseconds.

10.33.1.14 TEE_OpenPersistentObject()

```
TEE_Result TEE_OpenPersistentObject (
        uint32_t storageID,
        const void * objectID,
        uint32_t objectIDLen,
        uint32_t flags,
        TEE_ObjectHandle * object )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_OpenPersistentObject() - Opens a handle on an existing persistent object.

This function returns a handle that can be used to access the object's attributes and data stream.

Parameters

storageID	The storage to use.
objectID	The object identifier
objectIDLen	The object identifier
flags	The flags which determine the settings under which the object is opened.
object	A pointer to the handle, which contains the opened handle upon successful completion

Returns

0 if success, else error occured.

10.33.1.15 TEE_ReadObjectData()

```
TEE_Result TEE_ReadObjectData (
    TEE_ObjectHandle object,
    void * buffer,
    uint32_t size,
    uint32_t * count )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_ReadObjectData() - Attempts to read size bytes from the data stream associated with the object object into the buffer pointed to by buffer.

The bytes are read starting at the position in the data stream currently stored in the object handle. The handle's position is incremented by the number of bytes actually read. On completion TEE_ReadObjectData sets the number of bytes actually read in the uint32_t pointed to by count. The value written to ∗count may be less than size if the number of bytes until the end-of3067 stream is less than size. It is set to 0 if the position at the start of the read operation is at or beyond the end-of-stream. These are the only cases where ∗count may be less than size.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write
count	size of the buffer.

Returns

TEE_SUCCESS if success, else error occured.

10.33.1.16 TEE_WriteObjectData()

```
TEE_Result TEE_WriteObjectData (
        TEE_ObjectHandle object,
        const void * buffer,
        uint32_t size )
```

Core Functions, Secure Storage Functions (data is isolated for each TA)

TEE_WriteObjectData() - writes size bytes from the buffer pointed to by buffer to the data stream associated with the open object handle object.

If the current data position points before the end-of-stream, then size bytes are written to the data stream, overwriting bytes starting at the current data position. If the current data position points beyond the stream's end, then the data stream is first extended with zero bytes until the length indicated by the data position indicator is reached, and then size bytes are written to the stream.

Parameters

object	Handle of the object
buffer	The buffer containing the data to be written
size	The number of bytes to write

Returns

TEE_SUCCESS if success else error occured.

10.33.2 Variable Documentation

10.33.2.1 rngstr

```
WC_RNG rngstr [static]
```

10.33.2.2 wc_rng_init

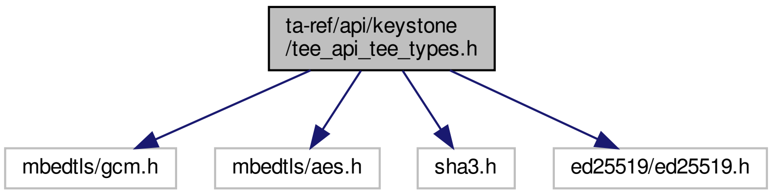
```
int wc_rng_init = 0 [static]
```

10.34 ta-ref/api/keystone/tee_api_tee_types.h File Reference

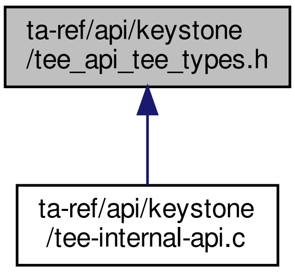
```
#include "mbedtls/gcm.h"
#include "mbedtls/aes.h"
#include "sha3.h"
```

```
#include "ed25519/ed25519.h"
```

Include dependency graph for tee_api_tee_types.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct __TEE_OperationHandle
- struct __TEE_ObjectHandle

10.35 tee_api_tee_types.h

Go to the documentation of this file.

```
/*
 * SPDX-License-Identifier: BSD-2-Clause
 *
 * Copyright (C) 2019 National Institute of Advanced Industrial Science
 *                           and Technology (AIST)
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */

#ifndef TEE_API_TYPES_KEYSTONE_H
#define TEE_API_TYPES_KEYSTONE_H

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define MBEDCRYPT 1
#define WOLFCRYPT 2
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

#if CRYPTLIB==MBEDCRYPT
#ifndef DOXYGEN_SHOULD_SKIP_THIS
# define MBEDTLS_CONFIG_FILE "mbed-crypto-config.h"
# define AES256 1
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
# include "mbedtls/gcm.h"
# include "mbedtls/aes.h"
# include "sha3.h"
# include "ed25519/ed25519.h"
#elif CRYPTLIB==WOLFCRYPT
#ifndef DOXYGEN_SHOULD_SKIP_THIS
# define HAVE_AESGCM 1
# define HAVE_AES_CBC 1
# define HAVE_AES_DECRYPT 1
# define HAVE_FIPS 1
# define HAVE_FIPS_VERSION 2
# define HAVE_ED25519 1
# define HAVE_ED25519_SIGN 1
# define HAVE_ED25519_VERIFY 1
# define WOLFSSL_SHA512 1
# define WOLFSSL_SHA3 1
# define WOLFSSL_SHA3_SMALL 1
# define WOLFCRYPT_ONLY 1
# define WOLF_CRYPT_PORT_H
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
# include "wolfssl/wolfcrypt/sha3.h"
# include "wolfssl/wolfcrypt/aes.h"
# include "wolfssl/wolfcrypt/sha512.h"
# include "wolfssl/wolfcrypt/ed25519.h"
#else
# include "sha3.h"
# include "ed25519/ed25519.h"
# include "tiny_AES_c/aes.h"
#ifndef DOXYGEN_SHOULD_SKIP_THIS
# define AES256 1
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
#endif

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define SHA_LENGTH (256/8)
#define TEE_OBJECT_NONCE_SIZE 16
#define TEE_OBJECT_KEY_SIZE 32
#define TEE_OBJECT_SKEY_SIZE 64
#define TEE_OBJECT_AAD_SIZE 16
#define TEE_OBJECT_TAG_SIZE 16
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

struct __TEE_OperationHandle
{
  int mode;
  int flags;
  int alg;
#if CRYPTLIB==MBEDCRYPT
  sha3_ctx_t ctx;
  mbedtls_aes_context aectx;
  mbedtls_gcm_context aegcmctx;
#elif CRYPTLIB==WOLFCRYPT
  wc_Sha3 ctx;
  Aes aectx;
  Aes aegcmctx;
  unsigned int aegcm_aadsz;
  unsigned char aegcm_aad[TEE_OBJECT_AAD_SIZE];
  ed25519_key key;
#else
  sha3_ctx_t ctx;
  struct AES_ctx aectx;
#endif
  int aegcm_state;
  unsigned char aeiv[TEE_OBJECT_NONCE_SIZE];
  unsigned char aekey[32];
  unsigned char pubkey[TEE_OBJECT_KEY_SIZE];
  unsigned char prikey[TEE_OBJECT_SKEY_SIZE];
};

struct __TEE_ObjectHandle
{
  unsigned int type;
  int flags;
  int desc;
#if CRYPTLIB==MBEDCRYPT
  mbedtls_aes_context persist_ctx;
  unsigned char persist_iv[TEE_OBJECT_NONCE_SIZE];
#elif CRYPTLIB==WOLFCRYPT
  Aes persist_ctx;
  unsigned char persist_iv[TEE_OBJECT_NONCE_SIZE];
  ed25519_key key;
#else
  struct AES_ctx persist_ctx;
#endif
  unsigned char public_key[TEE_OBJECT_KEY_SIZE];
  unsigned char private_key[TEE_OBJECT_SKEY_SIZE];
};

// defined in tee_api_defines.h
// enum Data_Flag_Constants {
//   TEE_DATA_FLAG_ACCESS_READ = 0x00000001,
//   TEE_DATA_FLAG_ACCESS_WRITE = 0x00000002,
//   //TEE_DATA_FLAG_ACCESS_WRITE_META = 0x00000004,
//   //TEE_DATA_FLAG_SHARE_READ = 0x00000010,
//   //TEE_DATA_FLAG_SHARE_WRITE = 0x00000020,
//   TEE_DATA_FLAG_OVERWRITE = 0x00000400
// };
// enum Data_Flag_Constants {
//   TEE_DATA_FLAG_ACCESS_READ = 0x00000001,
//   TEE_DATA_FLAG_ACCESS_WRITE = 0x00000002,
//   //TEE_DATA_FLAG_ACCESS_WRITE_META = 0x00000004,
//   //TEE_DATA_FLAG_SHARE_READ = 0x00000010,
//   //TEE_DATA_FLAG_SHARE_WRITE = 0x00000020,
//   TEE_DATA_FLAG_OVERWRITE = 0x00000400
// };
#endif
```

10.36 ta-ref/api/optee/tee_api_tee_types.h File Reference

10.37 tee_api_tee_types.h

Go to the documentation of this file.

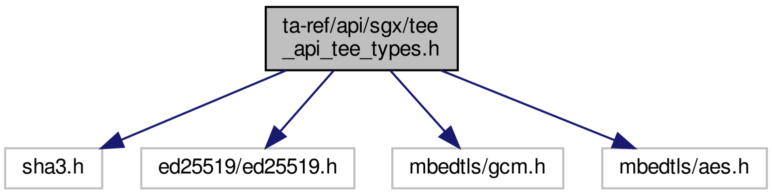
```
// empty
```

10.38 ta-ref/api/sgx/tee_api_tee_types.h File Reference

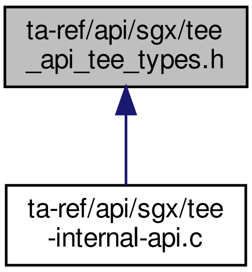
```
#include "sha3.h"
#include "ed25519/ed25519.h"
#include "mbedtls/gcm.h"
```

```
#include "mbedtls/aes.h"
```

Include dependency graph for tee_api_tee_types.h:



This graph shows which files directly or indirectly include this file:


ta-ref/api/sgx/tee_api_tee_types.h
ta-ref/api/sgx/tee-internal-api.c

Classes

- struct __TEE_OperationHandle
- struct __TEE_ObjectHandle

10.39 tee_api_tee_types.h

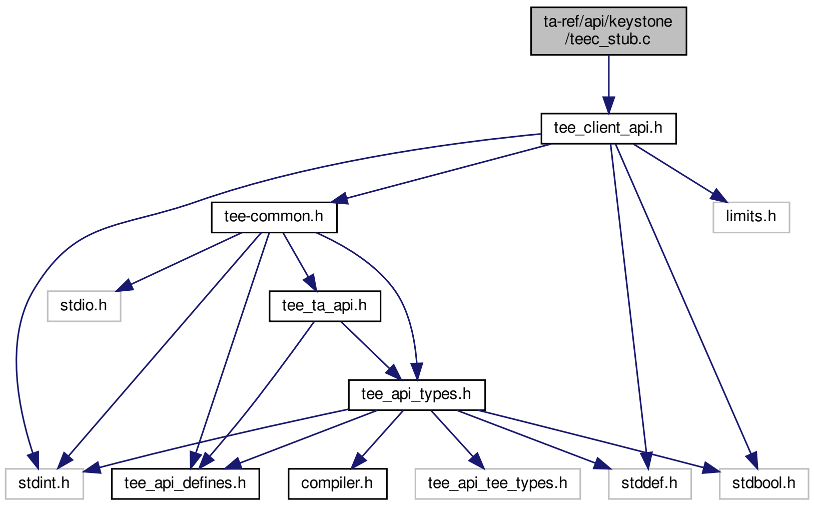
Go to the documentation of this file.

```
/*
 * SPDX-License-Identifier: BSD-2-Clause
 *
 * Copyright (C) 2019 National Institute of Advanced Industrial Science
 *                           and Technology (AIST)
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 * this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 * this list of conditions and the following disclaimer in the documentation
 * and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
 * POSSIBILITY OF SUCH DAMAGE.
 */

#ifndef TEE_API_TYPES_KEYSTONE_H
#define TEE_API_TYPES_KEYSTONE_H

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define MBEDCRYPT 1
#define WOLFCRYPT 2
#define SHA_LENGTH (256/8)
#define AES256 1
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

#include "sha3.h"
#include "ed25519/ed25519.h"

#if CRYPTLIB==MBEDCRYPT
#ifndef DOXYGEN_SHOULD_SKIP_THIS
# define MBEDTLS_CONFIG_FILE "mbed-crypto-config.h"
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
# include "mbedtls/gcm.h"
# include "mbedtls/aes.h"
#elif CRYPTLIB==WOLFCRYPT
#ifndef DOXYGEN_SHOULD_SKIP_THIS
# define HAVE_AESGCM 1
# define HAVE_AES_CBC 1
# define HAVE_AES_DECRYPT 1
# define HAVE_FIPS 1
# define HAVE_FIPS_VERSION 2
# define HAVE_ED25519 1
# define HAVE_ED25519_SIGN 1
# define HAVE_ED25519_VERIFY 1
# define WOLFSSL_SHA3 1
# define WOLF_CRYPT_PORT_H
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/
# include "wolfssl/wolfcrypt/sha3.h"
# include "wolfssl/wolfcrypt/aes.h"
# include "wolfssl/wolfcrypt/sha512.h"
# include "wolfssl/wolfcrypt/ed25519.h"
#else
# include "tiny_AES_c/aes.h"
#endif

#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define TEE_OBJECT_NONCE_SIZE 16
#define TEE_OBJECT_KEY_SIZE 32
#define TEE_OBJECT_SKEY_SIZE 64
#define TEE_OBJECT_AAD_SIZE 16
#define TEE_OBJECT_TAG_SIZE 16
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

struct __TEE_OperationHandle
{
  int mode;
  int flags;
  int alg;
#if CRYPTLIB==MBEDCRYPT
  sha3_ctx_t ctx;
  mbedtls_aes_context aectx;
  mbedtls_gcm_context aegcmctx;
#elif CRYPTLIB==WOLFCRYPT
  wc_Sha3 ctx;
  Aes aectx;
  Aes aegcmctx;
  unsigned int aegcm_aadsz;
  unsigned char aegcm_aad[TEE_OBJECT_AAD_SIZE];
  ed25519_key key;
#else
  sha3_ctx_t ctx;
  struct AES_ctx aectx;
#endif
  int aegcm_state;
  unsigned char aeiv[TEE_OBJECT_NONCE_SIZE];
  unsigned char aekey[32];
  unsigned char pubkey[TEE_OBJECT_KEY_SIZE];
  unsigned char prikey[TEE_OBJECT_SKEY_SIZE];
};

struct __TEE_ObjectHandle
{
  unsigned int type;
  int flags;
  int desc;
#if CRYPTLIB==MBEDCRYPT
  mbedtls_aes_context persist_ctx;
  unsigned char persist_iv[TEE_OBJECT_NONCE_SIZE];
#elif CRYPTLIB==WOLFCRYPT
  Aes persist_ctx;
  unsigned char persist_iv[TEE_OBJECT_NONCE_SIZE];
  ed25519_key key;
#else
  struct AES_ctx persist_ctx;
#endif
  unsigned char public_key[TEE_OBJECT_KEY_SIZE];
  unsigned char private_key[TEE_OBJECT_SKEY_SIZE];
};

// Minimal constant definitions
#ifndef DOXYGEN_SHOULD_SKIP_THIS
#define TEE_HANDLE_NULL 0
#endif /*DOXYGEN_SHOULD_SKIP_THIS*/

#endif
```

10.40 ta-ref/api/keystone/teec_stub.c File Reference

`#include <tee_client_api.h>`

Include dependency graph for teec_stub.c:



Functions

- TEEC_Result TEEC_InitializeContext (const char ∗name, TEEC_Context ∗context)
- void TEEC_FinalizeContext (TEEC_Context ∗context)
- TEEC_Result TEEC_OpenSession (TEEC_Context ∗context, TEEC_Session ∗session, const TEEC_UUID ∗destination, uint32_t connectionMethod, const void ∗connectionData, TEEC_Operation ∗operation, uint32↩ _t ∗returnOrigin)

- void TEEC_CloseSession (TEEC_Session ∗session)
- TEEC_Result TEEC_RegisterSharedMemory (TEEC_Context ∗context, TEEC_SharedMemory ∗shared↩ Mem)
- TEEC_Result TEEC_AllocateSharedMemory (TEEC_Context ∗context, TEEC_SharedMemory ∗shared↩ Mem)
- void TEEC_ReleaseSharedMemory (TEEC_SharedMemory ∗sharedMemory)
- void TEEC_RequestCancellation (TEEC_Operation ∗operation)

10.40.1 Function Documentation

10.40.1.1 TEEC_AllocateSharedMemory()

```
TEEC_Result TEEC_AllocateSharedMemory (
        TEEC_Context * context,
        TEEC_SharedMemory * sharedMem )
```

TEEC_AllocateSharedMemory() - Allocate shared memory for TEE.

Parameters

context	The initialized TEE context structure in which scope to open the session.
sharedMem	Pointer to the allocated shared memory.

Returns

TEEC_SUCCESS The registration was successful.

TEEC_ERROR_OUT_OF_MEMORY Memory exhaustion.

TEEC_Result Something failed.

10.40.1.2 TEEC_CloseSession()

```
void TEEC_CloseSession (
        TEEC_Session * session )
```

TEEC_CloseSession() - Closes the session which has been opened with the specific trusted application.

Parameters

session	The opened session to close.

10.40.1.3 TEEC_FinalizeContext()

```
void TEEC_FinalizeContext (
        TEEC_Context * context )
```

TEEC_FinalizeContext() - Destroys a context holding connection information on the specific TEE.

This function finalizes an initialized TEE context, closing the connection between the client application and the TEE. This function must only be called when all sessions related to this TEE context have been closed and all shared memory blocks have been released.

Parameters

context	The context to be finalized.

10.40.1.4 TEEC_InitializeContext()

```
TEEC_Result TEEC_InitializeContext (
        const char * name,
        TEEC_Context * context )
```

TEEC_InitializeContext() - Initializes a context holding connection information on the specific TEE, designated by the name string.

Parameters

name	A zero-terminated string identifying the TEE to connect to. If name is set to NULL, the default TEE is connected to. NULL is the only supported value in this version of the API implementation.
context	The context structure which is to be initialized.

Returns

TEEC_SUCCESS The initialization was successful.

TEEC_Result Something failed.

10.40.1.5 TEEC_OpenSession()

```
TEEC_Result TEEC_OpenSession (
        TEEC_Context * context,
        TEEC_Session * session,
        const TEEC_UUID * destination,
        uint32_t connectionMethod,
        const void * connectionData,
        TEEC_Operation * operation,
        uint32_t * returnOrigin )
```

TEEC_OpenSession() - Opens a new session with the specified trusted application.

Parameters

context	The initialized TEE context structure in which scope to open the session.
session	The session to initialize.
destination	A structure identifying the trusted application with which to open a session.
connectionMethod	The connection method to use.

Paramter list continued on next page

connectionData	Any data necessary to connect with the chosen connection method. Not supported, should be set to NULL.
operation	An operation structure to use in the session. May be set to NULL to signify no operation structure needed.
returnOrigin	A parameter which will hold the error origin if this function returns any value other than TEEC_SUCCESS.

Returns

TEEC_SUCCESS OpenSession successfully opened a new session.

TEEC_Result Something failed.

10.40.1.6 TEEC_RegisterSharedMemory()

```
TEEC_Result TEEC_RegisterSharedMemory (
        TEEC_Context * context,
        TEEC_SharedMemory * sharedMem )
```

TEEC_RegisterSharedMemory() - Register a block of existing memory as a shared block within the scope of the specified context.

Parameters

context	The initialized TEE context structure in which scope to open the session.
sharedMem	pointer to the shared memory structure to register.

Returns

TEEC_SUCCESS The registration was successful.

TEEC_ERROR_OUT_OF_MEMORY Memory exhaustion.

TEEC_Result Something failed.

10.40.1.7 TEEC_ReleaseSharedMemory()

```
void TEEC_ReleaseSharedMemory (
        TEEC_SharedMemory * sharedMemory )
```

TEEC_ReleaseSharedMemory() - Free or deregister the shared memory.

Parameters

sharedMem	Pointer to the shared memory to be freed.

10.40.1.8 TEEC_RequestCancellation() `void TEEC_RequestCancellation ( TEEC_Operation * operation )`

TEEC_RequestCancellation() - Request the cancellation of a pending open session or command invocation.

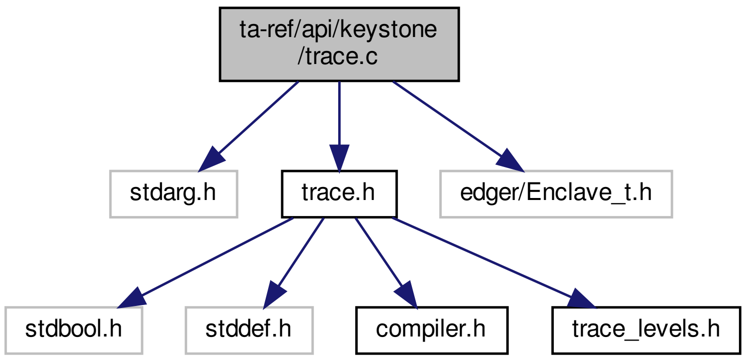
Parameters

operation	Pointer to an operation previously passed to open session or invoke.

10.41 ta-ref/api/keystone/trace.c File Reference

```
#include <stdarg.h>
#include "trace.h"
#include "edger/Enclave_t.h"
```

Include dependency graph for trace.c:



Functions

- void trace_vprintf (const char ∗func, int line, int level, bool level_ok, const char ∗fmt, va_list ap)
- void trace_printf (const char ∗func, int line, int level, bool level_ok, const char ∗fmt,...)

10.41.1 Function Documentation

10.41.1.1 trace_printf()

```
void trace_printf (
        const char * func,
        int line,
        int level,
        bool level_ok,
        const char * fmt,
         ... )
```

trace_printf() - Prints the formatted data to stdout.

This function returns the value of ap by calling va_end().

Parameters

func	Pointer to a buffer where the resulting C-string is stored.
line	integer type of line
level_ok	boolen value
fmt	C string that contains a format string
ap	A value identifying a variable arguments list

Returns

Total number of characters is returned.

10.41.1.2 trace_vprintf()

```
void trace_vprintf (
        const char * func,
        int line,
        int level,
        bool level_ok,
        const char * fmt,
        va_list ap )
```

trace_vprintf() - Writes the formatted data from variable argument list to sized buffer.

This function returns the buffer character by calling ocall_print_string()

Parameters

func	Pointer to a buffer where the resulting C-string is stored.
line	integer type of line
level_ok	boolen value
fmt	C string that contains a format string
ap	A value identifying a variable arguments list

Returns

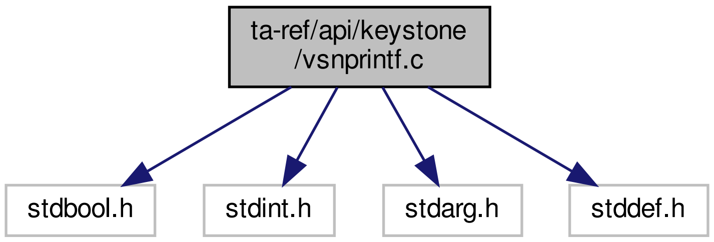
buf The total number of characters written is returned.

10.42 ta-ref/api/keystone/vsnprintf.c File Reference

```
#include <stdbool.h>
#include <stdint.h>
#include <stdarg.h>
```

```
#include <stddef.h>
```

Include dependency graph for vsnprintf.c:



Classes

- struct out_fct_wrap_type

Typedefs

- typedef void(∗ out_fct_type) (char character, void ∗buffer, size_t idx, size_t maxlen)

Functions

- static void _out_buffer (char character, void ∗buffer, size_t idx, size_t maxlen)
- static void _out_null (char character, void ∗buffer, size_t idx, size_t maxlen)
- static void _out_char (char character, void ∗buffer, size_t idx, size_t maxlen)
- static void _out_fct (char character, void ∗buffer, size_t idx, size_t maxlen)
- static unsigned int _strlen (const char ∗str)
- static bool _is_digit (char ch)
- static unsigned int _atoi (const char ∗∗str)
- static size_t _ntoa_format (out_fct_type out, char ∗buffer, size_t idx, size_t maxlen, char ∗buf, size_t len, bool negative, unsigned int base, unsigned int prec, unsigned int width, unsigned int flags)
- static size_t _ntoa_long (out_fct_type out, char ∗buffer, size_t idx, size_t maxlen, unsigned long value, bool negative, unsigned long base, unsigned int prec, unsigned int width, unsigned int flags)
- static int _vsnprintf (out_fct_type out, char ∗buffer, const size_t maxlen, const char ∗format, va_list va)
- int sprintf (char ∗buffer, const char ∗format,...)
- int snprintf (char ∗buffer, size_t count, const char ∗format,...)
- int vsnprintf (char ∗buffer, size_t count, const char ∗format, va_list va)
- int fctprintf (void(∗out)(char character, void ∗arg), void ∗arg, const char ∗format,...)

10.42.1 Typedef Documentation

10.42.1.1 out_fct_type `typedef void(* out_fct_type) (char character, void *buffer, size_t idx, size_t maxlen)`

10.42.2 Function Documentation

10.42.2.1 _atoi()

```
static unsigned int _atoi (
    const char ** str ) [static]
```

10.42.2.2 _is_digit()

```
static bool _is_digit (
    char ch ) [inline], [static]
```

10.42.2.3 _ntoa_format()

```
static size_t _ntoa_format (
    out_fct_type out,
    char * buffer,
    size_t idx,
    size_t maxlen,
    char * buf,
    size_t len,
    bool negative,
    unsigned int base,
    unsigned int prec,
    unsigned int width,
    unsigned int flags ) [static]
```

10.42.2.4 _ntoa_long()

```
static size_t _ntoa_long (
    out_fct_type out,
    char * buffer,
    size_t idx,
    size_t maxlen,
    unsigned long value,
    bool negative,
    unsigned long base,
    unsigned int prec,
    unsigned int width,
    unsigned int flags ) [static]
```

10.42.2.5 _out_buffer()

```
static void _out_buffer (
    char character,
    void * buffer,
    size_t idx,
    size_t maxlen ) [inline], [static]
```

10.42.2.6 _out_char()

```
static void _out_char (
    char character,
    void * buffer,
    size_t idx,
    size_t maxlen ) [inline], [static]
```

10.42.2.7 _out_fct()

```
static void _out_fct (
    char character,
    void * buffer,
    size_t idx,
    size_t maxlen ) [inline], [static]
```

10.42.2.8 _out_null()

```
static void _out_null (
    char character,
    void * buffer,
    size_t idx,
    size_t maxlen ) [inline], [static]
```

10.42.2.9 _strlen()

```
static unsigned int _strlen (
    const char * str ) [inline], [static]
```

10.42.2.10 _vsnprintf()

```
static int _vsnprintf (
    out_fct_type out,
    char * buffer,
    const size_t maxlen,
    const char * format,
    va_list va ) [static]
```

10.42.2.11 fctprintf()

```
int fctprintf (
    void(*)(char character, void *arg) out,
    void * arg,
    const char * format,
     ... )
```

10.42.2.12 snprintf()

```
int snprintf (
    char * buffer,
    size_t count,
    const char * format,
     ... )
```

10.42.2.13 sprintf()

```
int sprintf (
    char * buffer,
    const char * format,
     ... )
```

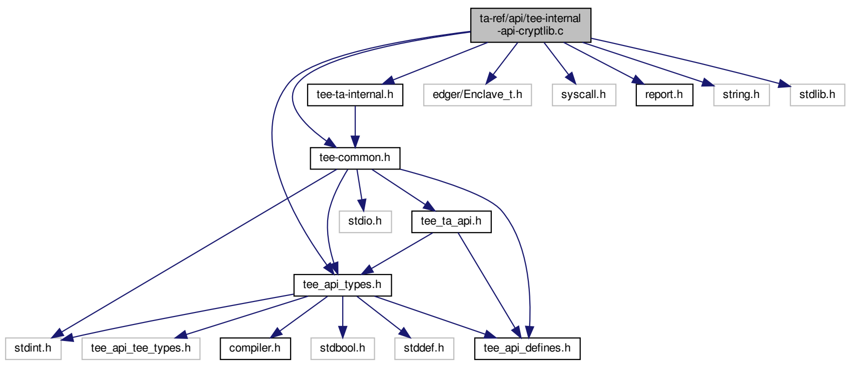
10.42.2.14 vsnprintf()

```
int vsnprintf (
    char * buffer,
    size_t count,
    const char * format,
    va_list va )
```

10.43 ta-ref/api/tee-internal-api-cryptlib.c File Reference

```
#include "tee_api_types.h"
#include "tee-common.h"
#include "tee-ta-internal.h"
#include "edger/Enclave_t.h"
#include "syscall.h"
#include "report.h"
#include <string.h>
#include <stdlib.h>
```

Include dependency graph for tee-internal-api-cryptlib.c:



Functions

- void wolfSSL_Free (void ∗p)
- void ∗ wolfSSL_Malloc (size_t n)
- TEE_Result TEE_AllocateOperation (TEE_OperationHandle ∗operation, uint32_t algorithm, uint32_t mode, uint32_t maxKeySize)

  Crypto, for all Crypto Functions.
- void TEE_FreeOperation (TEE_OperationHandle operation)

  Crypto, for all Crypto Functions.
- void TEE_DigestUpdate (TEE_OperationHandle operation, const void ∗chunk, uint32_t chunkSize)

  Crypto, Message Digest Functions.

- TEE_Result TEE_DigestDoFinal (TEE_OperationHandle operation, const void ∗chunk, uint32_t chunkLen, void ∗hash, uint32_t ∗hashLen)
- TEE_Result TEE_SetOperationKey (TEE_OperationHandle operation, TEE_ObjectHandle key)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEInit (TEE_OperationHandle operation, const void ∗nonce, uint32_t nonceLen, uint32_t tagLen, uint32_t AADLen, uint32_t payloadLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- void TEE_AEUpdateAAD (TEE_OperationHandle operation, const void ∗AADdata, uint32_t AADdataLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEUpdate (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEEncryptFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen, void ∗tag, uint32_t ∗tagLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_AEDecryptFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen, void ∗tag, uint32_t tagLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- void TEE_CipherInit (TEE_OperationHandle operation, const void ∗nonce, uint32_t nonceLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_CipherUpdate (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)

    Crypto, Authenticated Encryption with Symmetric key Verification Functions.
- TEE_Result TEE_CipherDoFinal (TEE_OperationHandle operation, const void ∗srcData, uint32_t srcLen, void ∗destData, uint32_t ∗destLen)
- TEE_Result TEE_GenerateKey (TEE_ObjectHandle object, uint32_t keySize, const TEE_Attribute ∗params, uint32_t paramCount)

    Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_AllocateTransientObject (TEE_ObjectType objectType, uint32_t maxKeySize, TEE_ObjectHandle ∗object)

    Crypto, Asymmetric key Verification Functions.
- void TEE_InitRefAttribute (TEE_Attribute ∗attr, uint32_t attributeID, const void ∗buffer, uint32_t length)

    Crypto, Asymmetric key Verification Functions.
- void TEE_InitValueAttribute (TEE_Attribute ∗attr, uint32_t attributeID, uint32_t a, uint32_t b)

    Crypto, Asymmetric key Verification Functions.
- void TEE_FreeTransientObject (TEE_ObjectHandle object)

    Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_AsymmetricSignDigest (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗digest, uint32_t digestLen, void ∗signature, uint32_t ∗signatureLen)

    Crypto, Asymmetric key Verification Functions.
- TEE_Result TEE_AsymmetricVerifyDigest (TEE_OperationHandle operation, const TEE_Attribute ∗params, uint32_t paramCount, const void ∗digest, uint32_t digestLen, const void ∗signature, uint32_t signatureLen)

    Crypto, Asymmetric key Verification Functions.

10.43.1 Function Documentation

10.43.1.1 TEE_AEDecryptFinal()

```
TEE_Result TEE_AEDecryptFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen,
        void * tag,
        uint32_t tagLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEDecryptFinal() - Processes data that has not been processed by previous calls to TEE_AEUpdate as well as data supplied in srcData.

This function completes the AE operation and compares the computed tag with the tag supplied in the parameter tag .The operation handle can be reused or newly initialized.The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation may be in either initial or active state and enters initial state afterwards.

Parameters

operation	Handle of a running AE operation
srcData	Reference to final chunk of input data to be encrypted
srcLen	length of the input data
destData	Output buffer. Can be omitted if the output is to be discarded.
destLen	length of the buffer.
tag	Output buffer filled with the computed tag
tagLen	length of the tag.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output

TEE_ERROR_MAC_INVALID If the computed tag does not match the supplied tag

10.43.1.2 TEE_AEEncryptFinal()

```
TEE_Result TEE_AEEncryptFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen,
        void * tag,
        uint32_t * tagLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEEncryptFinal() - processes data that has not been processed by previous calls to TEE_AEUpdate as well as data supplied in srcData .

TEE_AEEncryptFinal completes the AE operation and computes the tag. The operation handle can be reused or newly initialized. The buffers srcData and destData SHALL be either completely disjoint or equal in their starting positions.The operation may be in either initial or active state and enters initial state afterwards.

Parameters

operation	Handle of a running AE operation
srcData	Reference to final chunk of input data to be encrypted
srcLen	length of the input data
destData	Output buffer. Can be omitted if the output is to be discarded.
destLen	length of the buffer.
tag	Output buffer filled with the computed tag
tagLen	length of the tag.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER If the output or tag buffer is not large enoughto contain the output.

10.43.1.3 TEE_AEInit()

```
TEE_Result TEE_AEInit (
            TEE_OperationHandle operation,
            const void * nonce,
            uint32_t nonceLen,
            uint32_t tagLen,
            uint32_t AADLen,
            uint32_t payloadLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEInit() - Initializes an Authentication Encryption operation.

The operation must be in initial state and remains in the initial state afterwards.

Parameters

operation	A handle on the operation.
nonce	The operation nonce or IV
nonceLen	length of nonce
tagLen	Size in bits of the tag
AADLen	Length in bytes of the AAD
payloadLen	Length in bytes of the payload.

Returns

0 on success.

TEE_ERROR_NOT_SUPPORTED If the tag length is not supported by the algorithm.

10.43.1.4 TEE_AEUpdate()

```
TEE_Result TEE_AEUpdate (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEUpdate() - Accumulates data for an Authentication Encryption operation

This function describes Input data does not have to be a multiple of block size. Subsequent calls to this function are possible. Unless one or more calls of this function have supplied sufficient input data,no output is generated. when using this routine to decrypt the returned data may be corrupt since the integrity check is not performed until all the data has been processed. If this is a concern then only use the TEE_AEDecryptFinal routine.

Parameters

operation	Handle of a running AE operation.
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of the input buffer.
destData	Output buffer
destLen	length of the out put buffer.

Returns

0 on success.

TEE_ERROR_SHORT_BUFFER if the output buffer is not large enough to contain the output.

10.43.1.5 TEE_AEUpdateAAD()

```
void TEE_AEUpdateAAD (
        TEE_OperationHandle operation,
        const void * AADdata,
        uint32_t AADdataLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_AEUpdateAAD() - Feeds a new chunk of Additional Authentication Data (AAD) to the AE operation. Subsequent calls to this function are possible.

The TEE_AEUpdateAAD function feeds a new chunk of Additional Authentication Data (AAD) to the AE operation. Subsequent calls to this function are possible.The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation SHALL be in initial state and remains in initial state afterwards.

Parameters

operation	Handle on the AE operation
AADdata	Input buffer containing the chunk of AAD
AADdataLen	length of the chunk of AAD.

10.43.1.6 TEE_AllocateOperation()

```
TEE_Result TEE_AllocateOperation (
        TEE_OperationHandle * operation,
        uint32_t algorithm,
        uint32_t mode,
        uint32_t maxKeySize )
```

Crypto, for all Crypto Functions.

TEE_AllocateOperation() - Allocates a handle for a new cryptographic operation and sets the mode and algorithm type.

If this function does not return with TEE_SUCCESS then there is no valid handle value.Once a cryptographic operation has been created, the implementation shall guarantee that all resources necessary for the operation are allocated and that any operation with a key of at most maxKeySize bits can be performed. For algorithms that take multiple keys, for example the AES XTS algorithm, the maxKeySize parameter specifies the size of the largest key. It is up to the implementation to properly allocate space for multiple keys if the algorithm so requires.

Parameters

operation	reference to generated operation handle.
algorithm	One of the cipher algorithms.
mode	The operation mode.
maxKeySize	Maximum key size in bits for the operation.

Returns

0 in case of success

TEE_ERROR_OUT_OF_MEMORY If there are not enough resources to allocate the operation.

TEE_ERROR_NOT_SUPPORTED If the mode is not compatible with the algorithm or key size or if the algorithm is not one of the listed algorithms or if maxKeySize is not appropriate for the algorithm.

10.43.1.7 TEE_AllocateTransientObject()

```
TEE_Result TEE_AllocateTransientObject (
        TEE_ObjectType objectType,
        uint32_t maxKeySize,
        TEE_ObjectHandle * object )
```

Crypto, Asymmetric key Verification Functions.

TEE_AllocateTransientObject() - Allocates an uninitialized transient object. Transient objects are used to hold a cryptographic object (key or key-pair).

The value TEE_KEYSIZE_NO_KEY should be used for maxObjectSize for object types that do not require a key so that all the container resources can be pre-allocated. As allocated, the container is uninitialized. It can be initialized by subsequently importing the object material,generating an object, deriving an object, or loading an object from the Trusted Storage.

Parameters

objectType	Type of uninitialized object container to be created
maxKeySize	Key Size of the object.
object	Filled with a handle on the newly created key container.

Returns

0 on success

TEE_ERROR_OUT_OF_MEMORY If not enough resources are available to allocate the object handle.

TEE_ERROR_NOT_SUPPORTED If the key size is not supported or the object
type is not supported.

10.43.1.8 TEE_AsymmetricSignDigest()

```
TEE_Result TEE_AsymmetricSignDigest (
            TEE_OperationHandle operation,
            const TEE_Attribute * params,
            uint32_t paramCount,
            const void * digest,
            uint32_t digestLen,
            void * signature,
            uint32_t * signatureLen )
```

Crypto, Asymmetric key Verification Functions.

TEE_AsymmetricSignDigest() - Signs a message digest within an asymmetric operation.

Parameters

operation	Handle on the operation, which SHALL have been suitably set up with an operation key.
params	Optional operation parameters
paramCount	size of param
digest	Input buffer containing the input message digest
digestLen	length of input buffer.
signature	Output buffer written with the signature of the digest
signatureLen	length of output buffer.

Returns

0 on sccess

TEE_ERROR_SHORT_BUFFER If the signature buffer is not large enough to hold the result

10.43.1.9 TEE_AsymmetricVerifyDigest()

```
TEE_Result TEE_AsymmetricVerifyDigest (
        TEE_OperationHandle operation,
        const TEE_Attribute * params,
        uint32_t paramCount,
        const void * digest,
        uint32_t digestLen,
        const void * signature,
        uint32_t signatureLen )
```

Crypto, Asymmetric key Verification Functions.

TEE_AsymmetricVerifyDigest() - verifies a message digest signature within an asymmetric operation.

This function describes the message digest signature verify by calling ed25519_verify().

Parameters

operation	Handle on the operation, which SHALL have been suitably set up with an operation key.
params	Optional operation parameters
paramCount	size of param.
digest	Input buffer containing the input message digest
digestLen	length of input buffer.
signature	Output buffer written with the signature of the digest
signatureLen	length of output buffer.

Returns

TEE_SUCCESS on success

TEE_ERROR_SIGNATURE_INVALID if the signature is invalid.

10.43.1.10 TEE_CipherDoFinal()

```
TEE_Result TEE_CipherDoFinal (
        TEE_OperationHandle operation,
        const void * srcData,
        uint32_t srcLen,
        void * destData,
        uint32_t * destLen )
```

TEE_CipherDoFinal() - Finalizes the cipher operation, processing data that has not been processed by previous calls to TEE_CipherUpdate as well as data supplied in srcData .

This function describes The operation handle can be reused or re-initialized. The buffers srcData and destData shall be either completely disjoint or equal in their starting positions.The operation SHALL be in active state and is set to initial state afterwards.

Parameters

operation	Handle of a running Cipher operation
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of input buffer
destData	output buffer
destLen	ouput buffer length.

Returns

0 on success

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output

10.43.1.11 TEE_CipherInit()

```
void TEE_CipherInit (
    TEE_OperationHandle operation,
    const void * nonce,
    uint32_t nonceLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_CipherInit() - starts the symmetric cipher operation.

The operation shall have been associated with a key. If the operation is in active state, it is reset and then initialized. If the operation is in initial state, it is moved to active state.

Parameters

operation	A handle on an opened cipher operation setup with a key
nonce	Buffer containing the operation Initialization Vector as appropriate.
nonceLen	length of the buffer

10.43.1.12 TEE_CipherUpdate()

```
TEE_Result TEE_CipherUpdate (
    TEE_OperationHandle operation,
    const void * srcData,
    uint32_t srcLen,
    void * destData,
    uint32_t * destLen )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_CipherUpdate() - encrypts or decrypts input data.

Input data does not have to be a multiple of block size. Subsequent calls to this function are possible. Unless one or more calls of this function have supplied sufficient input data, no output is generated. The cipher operation is finalized with a call to TEE_CipherDoFinal .The buffers srcData and destData SHALL be either completely disjoint or equal in their starting positions.The operation SHALL be in active state.

Parameters

operation	Handle of a running Cipher operation
srcData	Input data buffer to be encrypted or decrypted
srcLen	length of input buffer
destData	output buffer
destLen	ouput buffer length.

Returns

0 on success else

TEE_ERROR_SHORT_BUFFER If the output buffer is not large enough to contain the output. In this case, the input is not fed into the algorithm.

10.43.1.13 TEE_DigestDoFinal()

```
TEE_Result TEE_DigestDoFinal (
        TEE_OperationHandle operation,
        const void * chunk,
        uint32_t chunkLen,
        void * hash,
        uint32_t * hashLen )
```

TEE_DigestDoFinal() - Finalizes the message digest operation and produces the message hash.

This function finalizes the message digest operation and produces the message hash. Afterwards the Message Digest operation is reset to initial state and can be reused.

Parameters

operation	Handle of a running Message Digest operation.
chunk	Chunk of data to be hashed.
chunkLen	size of the chunk.
hash	Output buffer filled with the message hash.
hashLen	lenth of the mesaage hash.

Returns

0 on success

TEE_ERROR_SHORT_BUFFER If the output buffer is too small. In this case, the operation is not finalized.

10.43.1.14 TEE_DigestUpdate()

```
void TEE_DigestUpdate (
        TEE_OperationHandle operation,
        const void * chunk,
        uint32_t chunkSize )
```

Crypto, Message Digest Functions.

TEE_DigestUpdate()- Accumulates message data for hashing.

This function describes the message does not have to be block aligned. Subsequent calls to this function are possible.The operation may be in either initial or active state and becomes active.

Parameters

operation	Handle of a running Message Digest operation.
chunk	Chunk of data to be hashed
chunkSize	size of the chunk.

10.43.1.15 TEE_FreeOperation()

```
void TEE_FreeOperation (
        TEE_OperationHandle operation )
```

Crypto, for all Crypto Functions.

TEE_FreeOperation() - Deallocates all resources associated with an operation handle.

This function deallocates all resources associated with an operation handle. After this function is called, the operation handle is no longer valid. All cryptographic material in the operation is destroyed. The function does nothing if operation is TEE_HANDLE_NULL.

Parameters

operation	Reference to operation handle.

Returns

nothing after the operation free.

10.43.1.16 TEE_FreeTransientObject()

```
void TEE_FreeTransientObject (
        TEE_ObjectHandle object )
```

Crypto, Asymmetric key Verification Functions.

TEE_FreeTransientObject() - Deallocates a transient object previously allocated with TEE_AllocateTransientObject .

this function describes the object handle is no longer valid and all resources associated with the transient object shall have been reclaimed after the TEE_AllocateTransientObject() call.

Parameters

object	Handle on the object to free.

10.43.1.17 TEE_GenerateKey()

```
TEE_Result TEE_GenerateKey (
    TEE_ObjectHandle object,
    uint32_t keySize,
    const TEE_Attribute * params,
    uint32_t paramCount )
```

Crypto, Asymmetric key Verification Functions.

TEE_GenerateKey () - Generates a random key or a key-pair and populates a transient key object with the generated key material.

The size of the desired key is passed in the keySize parameter and shall be less than or equal to the maximum key size specified when the transient object was created.

Parameters

object	Handle on an uninitialized transient key to populate with the generated key.
keySize	Requested key size shall be less than or equal to the maximum key size specified when the object container was created
params	Parameters for the key generation.
paramCount	The values of all parameters are copied nto the object so that the params array and all the memory buffers it points to may be freed after this routine returns without affecting the object.

Returns

0 on succes

TEE_ERROR_BAD_PARAMETERS If an incorrect or inconsistent attribute is detected. The checks that are performed depend on the implementation.

10.43.1.18 TEE_InitRefAttribute()

```
void TEE_InitRefAttribute (
    TEE_Attribute * attr,
    uint32_t attributeID,
    const void * buffer,
    uint32_t length )
```

Crypto, Asymmetric key Verification Functions.

TEE_InitRefAttribute() - The helper function can be used to populate a single attribute either with a reference to a buffer or with integer values.

In TEE_InitRefAttribute () only the buffer pointer is copied, not the content of the buffer. This means that the attribute structure maintains a pointer back to the supplied buffer. It is the responsibility of the TA author to ensure that the contents of the buffer maintain their value until the attributes array is no longer in use.

Parameters

attr	attribute structure to initialize.
attributeID	Identifier of the attribute to populate.
buffer	input buffer that holds the content of the attribute.
length	buffer length.

10.43.1.19 TEE_InitValueAttribute()

```
void TEE_InitValueAttribute (
    TEE_Attribute * attr,
    uint32_t attributeID,
    uint32_t a,
    uint32_t b )
```

Crypto, Asymmetric key Verification Functions.

TEE_InitValueAttribute() - The helper function can be used to populate a single attribute either with a reference to a buffer or with integer values.

Parameters

attr	attribute structure to initialize.
attributeID	Identifier of the attribute to populate.
a	unsigned integer value to assign to the a member of the attribute structure.
b	unsigned integer value to assign to the b member of the attribute structure

10.43.1.20 TEE_SetOperationKey()

```
TEE_Result TEE_SetOperationKey (
    TEE_OperationHandle operation,
    TEE_ObjectHandle key )
```

Crypto, Authenticated Encryption with Symmetric key Verification Functions.

TEE_SetOperationKey() - Programs the key of an operation; that is, it associates an operation with a key.

The key material is copied from the key object handle into the operation. After the key has been set, there is no longer any link between the operation and the key object. The object handle can be closed or reset and this will not affect the operation. This copied material exists until the operation is freed using TEE_FreeOperation or another key is set into the operation.

Parameters

operation	Operation handle.
key	A handle on a key object.

Returns

0 on success return

TEE_ERROR_CORRUPT_OBJECT If the object is corrupt. The object handle is closed.

TEE_ERROR_STORAGE_NOT_AVAILABLE If the persistent object is stored in a storage area which is currently inaccessible.

10.43.1.21 wolfSSL_Free() `void wolfSSL_Free ( void * p )`

wolfSSL_Free() - Deallocates the memory which allocated previously.

Parameters

p	This is the pointer to a memory block.

10.43.1.22 wolfSSL_Malloc() `void * wolfSSL_Malloc ( size_t n )`

wolfSSL_Malloc() - Allocates the requested memory and returns a pointer to it.

Parameters

n	size of the memory block.

10.44 ta-ref/docs/building.md File Reference

10.45 ta-ref/docs/gp_api.md File Reference

10.46 ta-ref/docs/how_to_program_on_ta-ref.md File Reference

10.47 ta-ref/docs/overview_of_ta-ref.md File Reference

10.48 ta-ref/docs/preparation.md File Reference

10.49 ta-ref/docs/running_on_dev_boards.md File Reference

Index