signal_enclave_interface

Generated by Doxygen 1.8.17

0.1 code/enclave_interface_documentation.c File Reference

Functions

- sgx_status_t **sgxsd_ocall_reply** (const sgxsd_msg_header_t *reply_header, const uint8_t *reply_data, size_t reply_data_size, sgxsd_msg_tag_t msg_tag)

  The enclave uses this OCALL to pass the result of the contact discovery to the service.
- sgx_status_t **sgxsd_enclave_node_init** (sgx_enclave_id_t eid, sgx_status_t *retval, const sgxsd_node_↩ init_args_t *p_args)

  This ECALL will initialize the enclave.
- sgx_status_t **sgxsd_enclave_server_start** (sgx_enclave_id_t eid, sgx_status_t *retval, const sgxsd_↩ server_init_args_t *p_args, sgxsd_server_state_handle_t state_handle)

  Used to start the server specified with state_handle.
- sgx_status_t **sgxsd_enclave_server_call** (sgx_enclave_id_t eid, sgx_status_t *retval, const sgxsd_↩ server_handle_call_args_t *p_args, const sgxsd_msg_header_t *msg_header, const uint8_t *msg_data, size_t msg_size, sgxsd_msg_tag_t msg_tag, sgxsd_server_state_handle_t state_handle)

  Used to make a server call.
- sgx_status_t **sgxsd_enclave_get_next_report** (sgx_enclave_id_t eid, sgx_status_t *retval, sgx_target_↩ info_t qe_target_info, sgx_report_t *p_report)

  Used to get the enclave measurement.
- sgx_status_t **sgxsd_enclave_set_current_quote** (sgx_enclave_id_t eid, sgx_status_t *retval)

  This function sets the old keypair equal to the newly generated keypair during a sgxsd_enclave_get_next_report call.
- sgx_status_t **sgxsd_enclave_negotiate_request** (sgx_enclave_id_t eid, sgx_status_t *retval, const sgxsd_request_negotiation_request_t *p_request, sgxsd_request_negotiation_response_t *p_response)

  Used to establish a shared secret using ECDH.
- sgx_status_t **sgxsd_enclave_server_stop** (sgx_enclave_id_t eid, sgx_status_t *retval, const sgxsd_↩ server_terminate_args_t *p_args, sgxsd_server_state_handle_t state_handle)

  This function will find the intersection between registered users and the discovery requests and stop the server.

0.1.1 Function Documentation

0.1.1.1 sgxsd_enclave_get_next_report()

```
sgx_status_t sgxsd_enclave_get_next_report (
            sgx_enclave_id_t eid,
            sgx_status_t * retval,
            sgx_target_info_t qe_target_info,
            sgx_report_t * p_report )
```

Used to get the enclave measurement.

Parameters

qe_target_info	Target info.
p_report	Will contain the measurement after the function is finished.

0.1.1.2 sgxsd_enclave_negotiate_request()

```
sgx_status_t sgxsd_enclave_negotiate_request (
            sgx_enclave_id_t eid,
            sgx_status_t * retval,
            const sgxsd_request_negotiation_request_t * p_request,
            sgxsd_request_negotiation_response_t * p_response )
```

Used to establish a shared secret using ECDH.

This function needs to be called before making a server call. It will register a pending request and set all fields in the response parameter.

Parameters

p_request	Contains the client public key.
p_response	Will contain the enclave's 2 public keys when this call is finished.

0.1.1.3 sgxsd_enclave_node_init()

```
sgx_status_t sgxsd_enclave_node_init (
            sgx_enclave_id_t eid,
            sgx_status_t * retval,
            const sgxsd_node_init_args_t * p_args )
```

This ECALL will initialize the enclave.

This function must be called first, before all other ECALLS.
It can only be called once. Calling it more than once will result in an error.
It will perform the enclave setup.

Parameters

p_args	Used to calculate the size of the memory region used for storing client contact discovery requests.

0.1.1.4 sgxsd_enclave_server_call()

```
sgx_status_t sgxsd_enclave_server_call (
            sgx_enclave_id_t eid,
            sgx_status_t * retval,
            const sgxsd_server_handle_call_args_t * p_args,
            const sgxsd_msg_header_t * msg_header,
            const uint8_t * msg_data,
            size_t msg_size,
            sgxsd_msg_tag_t msg_tag,
            sgxsd_server_state_handle_t state_handle )
```

Used to make a server call.

This function can be used to send an encrypted contact discovery request to the server.
The message is decrypted and is stored behind previous messages in a byte array.
Message meta-data is stored in the server state in a linked list.

Parameters

p_args	Contains the amount of contacts in the request.
msg_header	Contains the IV and MAC used by the enclave for decrypting the request.
msg_data	The encrypted message.
msg_size	The encrypted message size.
msg_tag	Used for indicating which client this request belongs to.
state_handle	Used as index to fetch the appropriate server state.

0.1.1.5 sgxsd_enclave_server_start()

```
sgx_status_t sgxsd_enclave_server_start (
             sgx_enclave_id_t eid,
             sgx_status_t * retval,
             const sgxsd_server_init_args_t * p_args,
             sgxsd_server_state_handle_t state_handle )
```

Used to start the server specified with state_handle.

This function starts the server specified with the state_handle argument.
It can only be called once for each server.
Zeroes the region of memory corresponding to the server state, then initializes the server state.
Must be called once on a server before this server can be used to make calls.

Parameters

p_args	Used to calculate size of server state.
state_handle	Used as index to fetch the appropriate server state. Must be smaller than the max allowed amount of servers (256).

0.1.1.6 sgxsd_enclave_server_stop()

```
sgx_status_t sgxsd_enclave_server_stop (
             sgx_enclave_id_t eid,
             sgx_status_t * retval,
             const sgxsd_server_terminate_args_t * p_args,
             sgxsd_server_state_handle_t state_handle )
```

This function will find the intersection between registered users and the discovery requests and stop the server.

This function will find the intersection between registered users and the discovery requests.
After that, the server is terminated.
It will call the OCALL with the encrypted reply.

Parameters

p_args	Contains the list of registered users.
state_handle	Used to indentify the server that needs to be stopped.

0.1.1.7 sgxsd_enclave_set_current_quote()

```
sgx_status_t sgxsd_enclave_set_current_quote (
             sgx_enclave_id_t eid,
             sgx_status_t * retval )
```

This function sets the old keypair equal to the newly generated keypair during a sgxsd_enclave_get_next_report call.

0.1.1.8 sgxsd_ocall_reply()

```
sgx_status_t sgxsd_ocall_reply (
             const sgxsd_msg_header_t * reply_header,
             const uint8_t * reply_data,
             size_t reply_data_size,
             sgxsd_msg_tag_t msg_tag )
```

The enclave uses this OCALL to pass the result of the contact discovery to the service.

This function will be called after a server is stopped using the sgxsd_enclave_server_stop ECALL.
The enclave will pass the result of the contact discovery requests to the service.
The result consists of 1 byte for each contact that was in the request. This byte will be 1 in case the contact is a registered users, 0 in case the contact isn't registered.

Parameters

reply_header	Contains the IV and MAC used for decrypting the reply.
reply_data	Contains a 0 byte for each contact in the request that is not registered and a 1 byte for each contact that is registered.
reply_data_sise	The size of the reply in bytes, 1 byte for earch contact in the request.
msg_tag	Indicates to which client this reply should be sent.