Crypto Engine

Overview

The crypto engine (CE) API is a crypto queue manager.

Requirement

You must put, at the start of your transform context your_tfm_ctx, the structure crypto_engine:

```
struct your_tfm_ctx {
        struct crypto_engine engine;
        ...
};
```

The crypto engine only manages asynchronous requests in the form of crypto_async_request. It cannot know the underlying request type and thus only has access to the transform structure. It is not possible to access the context using container_of. In addition, the engine knows nothing about your structure "`struct your_tfm_ctx`". The engine assumes (requires) the placement of the known member `struct crypto_engine` at the beginning.

Order of operations

You are required to obtain a struct crypto_engine via `crypto_engine_alloc_init()`. Start it via `crypto_engine_start()`. When finished with your work, shut down the engine using `crypto_engine_stop()` and destroy the engine with `crypto_engine_exit()`.

Before transferring any request, you have to fill the context enginectx by providing functions for the following:

- `prepare_crypt_hardware`: Called once before any prepare functions are called.
- `unprepare_crypt_hardware`: Called once after all unprepare functions have been called.
- `prepare_cipher_request`/`prepare_hash_request`: Called before each corresponding request is performed. If some processing or other preparatory work is required, do it here.
- `unprepare_cipher_request`/`unprepare_hash_request`: Called after each request is handled. Clean up / undo what was done in the prepare function.
- `cipher_one_request`/`hash_one_request`: Handle the current request by performing the operation.

Note that these functions access the crypto_async_request structure associated with the received request. You are able to retrieve the original request by using:

```
container_of(areq, struct yourrequesttype_request, base);
```

When your driver receives a crypto_request, you must to transfer it to the crypto engine via one of:

- crypto_transfer_aead_request_to_engine()
- crypto_transfer_akcipher_request_to_engine()
- crypto_transfer_hash_request_to_engine()
- crypto_transfer_kpp_request_to_engine()
- crypto_transfer_skcipher_request_to_engine()

At the end of the request process, a call to one of the following functions is needed:

- crypto_finalize_aead_request()
- crypto_finalize_akcipher_request()
- crypto_finalize_hash_request()
- crypto_finalize_kpp_request()
- crypto_finalize_skcipher_request()