PSA FF 1.0.0 Alignment Update

Edison Ai

Agenda

- Programming API Update
- Manifest Update
- Partition ID distribution
- Service ID distribution
- Future works

Note

- Only focus on the main difference with PSA FF 1.0 bet0 which will affect SP developers.

Programming APIs Update

- Introduced message type parameter to the psa_call().
  psa_status_t psa_call(psa_handle_t handle, int32_t type, const psa_invec *in_vec, size_t in_len, psa_outvec *out_vec, size_t out_len);

  - The caller indicates a specific operation using the type parameter.
  - This can be any positive value.
  - If the RoT Service only has a single operation, PSA_IPC_CALL can be used as the type.
  - Break the 28 bits service signal limitation.

```
switch (msg.type) {
  case PSA_IPC_CONNECT:
    break;
  case PSA_IPC_CALL:
    break;
  case PSA_IPC_DISCONNECT:
break;
  default:
    tfm_abort();
  }
```

```
if (msg.type >= 0) {
} else if (msg.type == PSA_IPC_CONNECT) {
} else if (msg.type == PSA_IPC_DISCONNECT) {
} else {
        // cannot get here? [broken SPM]
        psa_panic();
}
```


arm

Programming APIs Update

- Add psa_panic()
  - It will terminate execution within the calling Secure Partition and will not return.
  - This function can be used by a Secure Partition when it detects an Internal fault to halt execution.
- More error detect for the input parameters.
- The most of PROGRAMMER ERROR and panic error will cause the system reset.

Manifest Update

- <psa_manifest/pid.h> is added for the Secure Partition macro definitions that map from Secure Partition names to Secure Partition IDs:

  #define name id-value

Note: the partition name is a macro now, please add postfix for other using.

Manifest Update

- “dependencies” support.
  - This attribute lists the RoT Services which the Secure Partition code depends on and is authorized to access.
  - The attribute is a list of the RoT Service names.
  - If access between a client Secure Partition and an RoT Service is not specified in the manifest, then the client is not allowed to connect to the RoT Service.

- Multiple mmio region support.

Manifest Update

- “psa_framework_version” is required to indicate the version of the PSA FF specification this manifest conforms to.
- “heap_size” is removed for TF-M does not support HEAP APIs yet.
- “signal” is removed. Signal macro is derived from service name, such as:
  #define name_SIGNAL VALUE
- minor_version -> version, minor_policy -> version_policy.
- line_name of irqs to “source”

Partition ID distribution

- The distribution policy is on discussing.
- The current usage is as this:

Partition name	Partition ID
Reserved	0-255
TFM_SP_STORAGE	256
TFM_SP_ITS	257
TFM_SP_AUDIT_LOG	258
TFM_SP_CRYPTO	259
TFM_SP_PLATFORM	260
TFM_SP_INITIAL_ATTESTATION	261
TFM_SP_CORE_TEST	262
TFM_SP_CORE_TEST_2	263
TFM_SP_SECURE_TEST_PARTITION	264
TFM_SP_IPC_SERVICE_TEST	265
TFM_SP_IPC_CLIENT_TEST	266
TFM_IRQ_TEST_1	267
TFM_SP_SST_TEST	268

Service ID distribution

- The vendor ID distribution policy is on discussing.
- The current usage is as this:

Services	Vendor ID(20 bits)	Function ID(12 bits)
audit_logging	0x00000	0x000-0x01F
initial_attestation	0x00000	0x020-0x03F
platform	0x00000	0x040-0x05F
secure_storage	0x00000	0x060-0x07F
crypto	0x00000	0x080-0x09F
internal_trusted_storage	0x00000	0x0A0-0x0BF
test_secure_service	0x0000F	0x000-0x01F
core_test	0x0000F	0x020-0x03F
core_test_2	0x0000F	0x040-0x05F
tfm_ipc_client	0x0000F	0x060-0x07F
tfm_ipc_service	0x0000F	0x080-0x09F
tfm_irq_test_service_1	0x0000F	0x0A0-0x0BF
tfm_sst_test_service	0x0000F	0x0C0-0x0DF

arm

Future works

- PSA architecture test suite (IPC module) integrate with TF-M.
- Function enhancement for where are defined as “IMPLEMENTATION DEFINED” if necessary.
- Bugs fix.

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה