PSA FF 1.0.0 Alignment Update
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()`.
  
  ```c
  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.

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

```c
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();
}
```
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
  ```


- line_name of irqs to “source”
Partition ID distribution

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

<table>
<thead>
<tr>
<th>Partition name</th>
<th>Partition ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0-255</td>
</tr>
<tr>
<td>TFM_SP_STORAGE</td>
<td>256</td>
</tr>
<tr>
<td>TFM_SP_ITS</td>
<td>257</td>
</tr>
<tr>
<td>TFM_SP_AUDIT_LOG</td>
<td>258</td>
</tr>
<tr>
<td>TFM_SP_CRYPTO</td>
<td>259</td>
</tr>
<tr>
<td>TFM_SP_PLATFORM</td>
<td>260</td>
</tr>
<tr>
<td>TFM_SP_INITIAL_ATTESTATION</td>
<td>261</td>
</tr>
<tr>
<td>TFM_SP_CORE_TEST</td>
<td>262</td>
</tr>
<tr>
<td>TFM_SP_CORE_TEST_2</td>
<td>263</td>
</tr>
<tr>
<td>TFM_SP_SECURE_TEST_PARTITION</td>
<td>264</td>
</tr>
<tr>
<td>TFM_SP_IPC_SERVICE_TEST</td>
<td>265</td>
</tr>
<tr>
<td>TFM_SP_IPC_CLIENT_TEST</td>
<td>266</td>
</tr>
<tr>
<td>TFM_IRQ_TEST_1</td>
<td>267</td>
</tr>
<tr>
<td>TFM_SP_SST_TEST</td>
<td>268</td>
</tr>
</tbody>
</table>
Service ID distribution

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

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