Updates on TF-M HAL API
Agenda

Write in your subtitle here

• HAL for Secure Partitions
• HAL for Secure Partition Manager
• Progress
SPM HAL

- Was a full stack, heavy HAL
- Is a very light-weight, thin HAL

APIs

- Log API – not changed
- Interrupt API - WIP
- Loader API – Removed
  - Feature design, currently no use case
- Platform API - Tailored a bit
  - Removed one API
  - Simplified one API
  - became the old HAL API
- Isolation API – totally new design
  - Simplified
  - Closer to HW
## API Changes

<table>
<thead>
<tr>
<th>Previous version</th>
<th>Current version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform APIs</strong></td>
<td></td>
</tr>
<tr>
<td>tfm_hal_init_platform()</td>
<td>tfm_hal_init_platform()</td>
</tr>
<tr>
<td>tfm_hal_reset_platform()</td>
<td>tfm_hal_reset_platform()</td>
</tr>
<tr>
<td>tfm_hal_get_meminfo()</td>
<td></td>
</tr>
<tr>
<td><strong>Isolation APIs</strong></td>
<td></td>
</tr>
<tr>
<td>tfm_hal_create_isolation_region()</td>
<td>tfm_hal_set_spe_boundary()</td>
</tr>
<tr>
<td>tfm_hal_destroy_isolation_region()</td>
<td>tfm_hal_isolation_init()</td>
</tr>
<tr>
<td>tfm_hal_switch_isolation_regions()</td>
<td>tfm_hal_enable_memory_access()</td>
</tr>
<tr>
<td>tfm_hal_config_isolation_region()</td>
<td>tfm_hal_disable_memory_access()</td>
</tr>
<tr>
<td>tfm_hal_access_to_region()</td>
<td>tfm_hal_memory_has_access()</td>
</tr>
</tbody>
</table>
Progress

• Design Docs
  • Platform API – API finalized
  • Log API - API finalized
  • Isolation API

• Platform API
  • “Implemented”

• Log API
  • SPM log – patch for review
  • SP log – coming soon

• Isolation API
  • isolation feature branch
  • Re-implemented Isolation L1 and L2
  • Prototyping on Isolation L3
Thank You
Danke
Merci
Merci
谢谢
ありがとうございます
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה