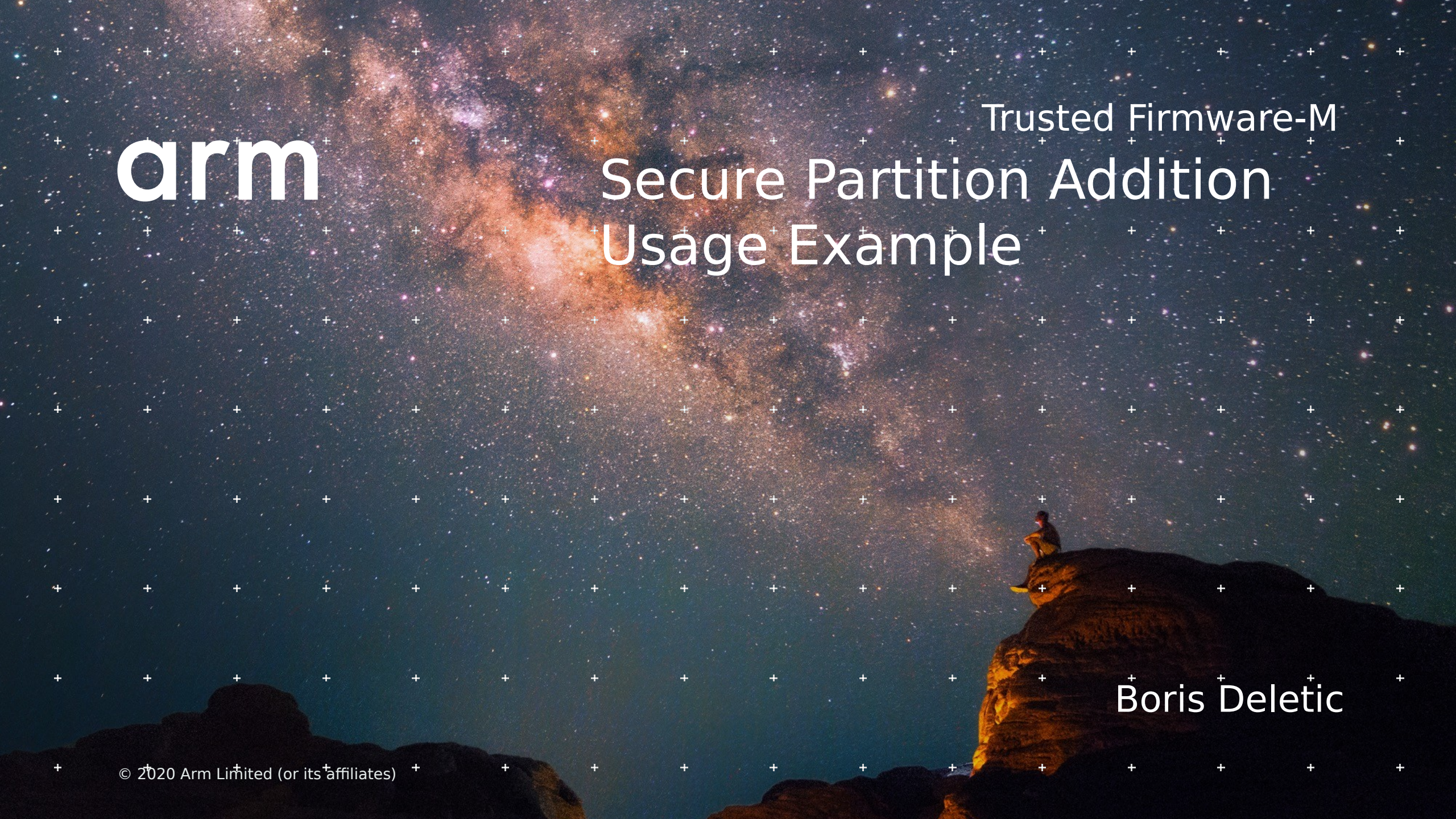


Introduction

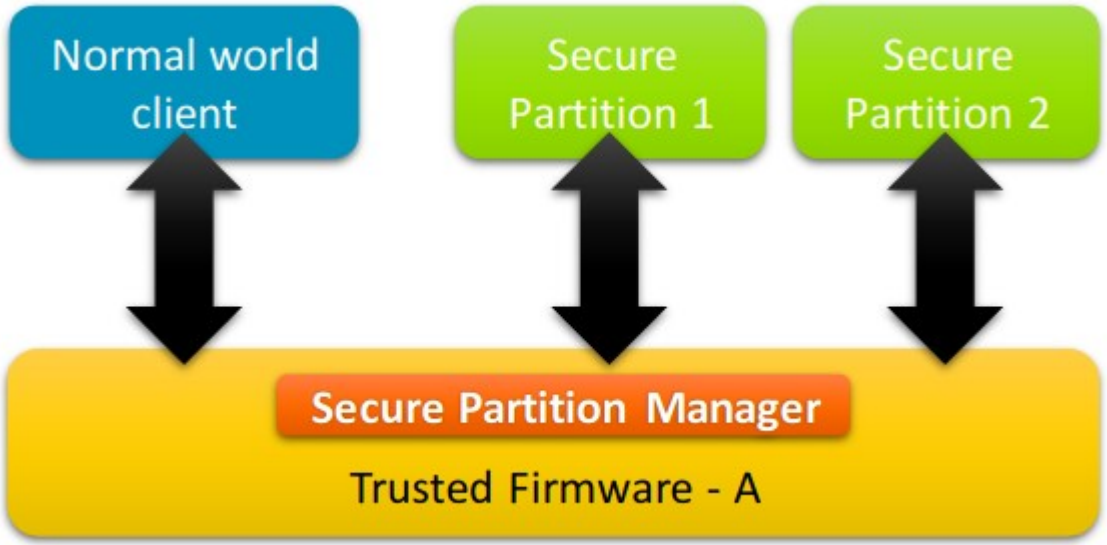
Boris Deletic

- Usage examples for new users
- Implementations of core functionality
- Expanding existing documentation

Adding a Secure Partition

Core functionality

- Secure partitions are the backbone of TF-M
  - Implement RoT secure services
- Simple “Hello world” example service



arm

Implementation

Create Secure Partition

- Outline manifest
- Declare secure services
  - New service ‘ROT_A’

```
{
  "psa_framework_version": 1.0,
  "name": "TFM_SP_EXAMPLE",
  "type": "PSA-ROT",
  "priority": "HIGH",
  "entry_point": "EXAMPLE_main",
  "stack_size": "0x0200",
  "services" : [
    {
      "name": "ROT_A",
      "sid": "0x0000F000",
      "non_secure_clients": true,
      "version": 1,
      "version_policy": "STRICT"
    }
  ],
  "mmio_regions": [
    {
      "name": "TFM_PERIPHERAL_A",
      "permission": "READ-WRITE"
    }
  ],
  "irqs": [
    {
      "source": "TFM_A_IRQ",
      "signal": "SPM_CORE_A_IRQ",
      "tfm_irq_priority": 64,
    }
  ],
  "linker_pattern": {
    "object_list": [
      "*EXAMPLE.*"
    ]
  }
}
```

Implementation

Create the Secure Service

- Define unique service ID (SID)
- Entry point function
  - Handles signals
- Implement PSA functionality for returning “Hello World” message on connection

```
void example_main(void *param)
{
    uint32_t signals = 0;

    while (1) {
            signals = psa_wait(PSA_WAIT_ANY, PSA_BLOCK);
        if (signals & ROT_A_SIGNAL) {
                rot_A();
        } else {
            /* Should not come here */
            tfm_abort();
        }
    }
}
```

Demonstration

Add test demonstration

- Add a test case to call the new service
- Run example on FVP model
- “Hello World!”

```
> Executing 'TFM_IPC_TEST_1014'
  Description: 'Get reply from example service from example partition'
TFM service support version is 1.
psa_call is successful!
outvec1 is: Hello World.
outvec2 is: Hello World.
  TEST PASSED!
```

Future

- Expand the documentation
- More usage examples for advanced functionality
  - Interrupt Requests
  - Peripherals

arm

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