Example TEEP Manifest

IETF 111 online

TEEP Manifest Example

- The TEE uses OP-TEE on TFA-A on TrustZone
- The TEE's secure storage is in RPMB
- The TA is to be saved in the file "edd94cd8-9d9c-4cc8-9216-b3ad5a2d5b8a.ta" in RPMB
- The TA developer doesn't want to use a second TAM, just an HTTPS server, to supply the personalization data
  - The TAM delivers a unique Personalization Data manifest to each TA instance. Each Personalization Data manifest has a dependency on the TA manifest
  - The Personalization Data manifest and TA binary manifest are delivered in the TEEP Update message
  - The Personalization Data is delivered via an HTTPS URI

Personalization Manifest: Auth

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
2:<<[
  digest: <<[
   / algorithm-id / -16 / "sha256" /,
   / digest-bytes /
     h'a7fd6593eac32eb4be578278e6540c5c'
     h'09cfd7d4d234973054833b2b93030609'
  ]>>
]>>
```

Personalization Manifest: Common/Deps

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ dependencies / 1:[
  {
    / dependency-digest / 1:[
      / algorithm-id / -16 / "sha256" /,
      / digest-bytes /
      h'd6c1fc7200483092e2db59d4907f9b15'
      h'05cb3af2795cf78f7ae3d88166fdf743'
    ],
  }
]
```

Personalization Manifest: Common/Comps

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ components / 2:[
  [
    h'4f502d544545' / OPT-EE /,
    h'44f301', / Encoding error? /
    h'636f6e6669672e6a736f6e'
      / config.json /
  ]
]

This component was supposed to be:
["OP-TEE","RPMB","config.json"]
```

Personalization Manifest: Common/setup

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ common-sequence / 4:<<[
  / directive-set-component-index / 12,0 ,
  / directive-override-parameters / 20,{
    / vendor-id / 1:h'ec41787224345ae580003de697ff8d43'
                  / ec417872-2434-5ae5-8000-3de697ff8d43 /,
    / class-id / 2:h'eb1701b48be85709aca0adf89f056a64'
                  / eb1701b4-8be8-5709-aca0-adf89f056a64 /,
    / image-digest / 3:<<[
      / algorithm-id / -16 / "sha256" /,
      / digest-bytes /
        h'aaabcccdeeef00012223444566678889'
        h'abbbcdddefff01112333455567778999'
    ]>>,
  } ,
  / condition-vendor-identifier / 1,15 ,
  / condition-class-identifier / 2,15
]>>,
```

Personalization Manifest: Dependencies

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
<<[
  / directive-set-dependency-index /
13,0 ,
  / directive-set-parameters / 19,{
    / uri / 21:'tam.teep.example/'
                'edd94cd8-9d9c-4cc8-'
                '9216-b3ad5a2d5b8a.suit',
  } ,
  / directive-fetch / 21,2 ,
  / condition-image-match / 3,15
]>>,
```

Personalization Manifest: Install

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
<<[
  / directive-set-component-index / 12,0 ,
  / directive-set-parameters / 19,{
    / uri / 21:
     'http://tam.teep.example/config.json',
  } ,
  / directive-set-dependency-index / 13,0 ,
  / directive-process-dependency / 18,0 ,
  / directive-set-component-index / 12,0 ,
  / directive-fetch / 21,2 ,
  / condition-image-match / 3,15
]>>
```

Personalization Manifest: Validate/Run

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ validate / 10:<<[
  / directive-set-component-index / 12,0 ,
  / condition-image-match / 3,15 ,
  / directive-set-dependency-index / 13,0 ,
  / directive-process-dependency / 18,0
]>>,
/ run / 12:<<[
  / directive-set-dependency-index / 13,0 ,
  / directive-process-dependency / 18,0
]>>,
```

Personalization Manifest: Text

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ text / 13:<<{
  [h'4f502d544545', h'44f301',
h'636f6e6669672e6a736f6e']:{
    / model-name / 2:
      'Personalised OP-TEE on TF-A on TrustZone',
    / vendor-domain / 3:'tam.teep.example',
  },
  [
    h'4f502d544545',
    h'44f301',
    h'edd94cd89d9c4cc89216b3ad5a2d5b8a',
    h'7461'
  ]:{
    / model-name / 2:'OP-TEE on TF-A on TrustZone',
    / vendor-domain / 3:'teep.example',
  }
}>>,
```

TA Manifest: Auth

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
<<[
  digest: <<[
    / algorithm-id / -16 / "sha256" /,
    / digest-bytes /
h'd6c1fc7200483092e2db59d4907f9b15’
h'05cb3af2795cf78f7ae3d88166fdf743’
  ]>>,
  signature: <<18([
    / protected / <<{
      / alg / 1:-7 / "ES256" /,
    }>>,
    / unprotected / {},
    / payload / F6 / nil /,
    / signature / <trimmed for brevity>
  ])>>
]>>
```

TA Manifest: Common/components

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:5,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ components / 2:[
  [
    h'4f502d544545’,
    h'44f301’,
    h'edd94cd89d9c4cc89216b3ad5a2d5b8a’,
    h'7461’
  ]
],
```

```
This component was supposed to be:
["OP-TEE","RPMB","edd94cd8-9d9c-4cc8-9216-
b3ad5a2d5b8a","ta"]
```

TA Manifest: Common/setup

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:5,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ common-sequence / 4:<<[
  / directive-override-parameters / 20,{
    / vendor-id /
1:h'c0ddd5f15243566087db4f5b0aa26c2f’,
    / class-id /
2:h'db42f7093d8c55baa8c5265fc5820f4e’,
    / image-digest / 3:<<[
      / algorithm-id / -16 / "sha256" /,
      / digest-bytes /
h'00112233445566778899aabbccddeeff'
h'0123456789abcdeffedcba9876543210’
    ]>>,
    / image-size / 14:76778,
  } ,
  / condition-vendor-identifier / 1,15 ,
  / condition-class-identifier / 2,15
]>>,
```

TA Manifest: install

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:5,
    common,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ install / 9:<<[
  / directive-set-parameters / 19,{
    / uri / 21:
'https://teep.example/edd94cd8-9d9c-4cc8-9216-
b3ad5a2d5b8a.ta',
  } ,
  / directive-fetch / 21,2 ,
  / condition-image-match / 3,15
]>>,
```

TA Manifest: Validate & Run

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:5,
    common,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ validate / 10:<<[
  / condition-image-match / 3,15
]>>,
/ run / 12:<<[
  / directive-run / 23,2
]>>,
```

TA Manifest: Text

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:5,
    common,
    install,
    validate,
    run,
    text
  }>>,
})
```

```
/ text / 13:<<{
 [
   h'4f502d544545',
   h'44f301',
   h'edd94cd89d9c4cc89216b3ad5a2d5b8a',
   h'7461'
 ]:{
   / model-name / 2:
     'OP-TEE on TF-A on TrustZone',
   / vendor-domain / 3:'teep.example'
 }
}>>,
```