SUIT
Internet-Draft
Intended status: Standards Track
Expires: 8 September 2022

B. Moran
Arm Limited

7 March 2022

Update Management Extensions for Software Updates for Internet of Things (SUIT) Manifests

draft-ietf-suit-update-management-00

Abstract

This specification describes extensions to the SUIT manifest format defined in [I-D.ietf-suit-manifest]. These extensions allow an update author, update distributor or device operator to more precisely control the distribution and installation of updates to IoT devices. These extensions also provide a mechanism to inform a management system of Software Identifier and Software Bill Of Materials information about an updated device.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 September 2022.

Copyright Notice

Table of Contents

1. Introduction

Full management of software updates for unattended, connected devices, such as Internet of Things devices requires a cooperation

between the update author(s) and management, distribution, policy enforcement, and auditing systems. This specification provides the extensions to the SUIT manifest ([I-D.ietf-suit-manifest]) that enable an author to coordinate with these other systems. These extensions enable authors to instruct devices to examine update

priority, local update authorisation, update lifetime, and system properties. They also enable devices to report and distributors to collect Software Bill of Materials information.

Extensions in this specification are OPTIONAL to implment and OPTIONAL to include in manifests unless otherwise designated.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Additionally, the following terminology is used throughout this document:

* SUIT: Software Update for the Internet of Things, also the IETF working group for this standard.

3. Extension Metadata

Some additional metadata makes management of SUIT updates easier:

* CoSWID, CoMID, CoRIM

* Text descriptions of requirements

3.1. suit-coswid

a CoSWID can enable Software Bill-of-Materials use-cases. A CoMID can enable monitoring of expected hardware. A CoRIM (which may contain both CoSWID and CoMID) can enable both of these use-cases, but can also act as the transport for expected values to an attestation Verifier. Tightly coupling update and attestation

ensures that verification infrastructure always knows what software to expect on each device.

suit-coswid is a member of the suit-manifest. It contains a Concise Software Identifier (CoSWID) as defined in [I-D.ietf-sacm-coswid]. This element SHOULD be made severable so that it can be discarded by the Recipient or an intermediary if it is not required by the Recipient.

suit-coswid typically requires no processing by the Recipient. However all Recipients MUST NOT fail if a suit-coswid is present.

suit-coswid is RECOMMENDED to implement and RECOMMENDED to include in manifests.

NOTE: CoRIM comprises a list of CoSWID and a list of CoMID, so it may be preferable to a CoSWID.

NOTE: CoMID may be a preferable alternative to Vendor ID/Class ID, however it consumes more bandwidth, so a UUID based on CoMID may be appropriate.

3.2. text-version-required

suit-text-version-required is used to represent a version-based dependency on suit-parameter-version as described in Section 4.4 and Section 5.5. To describe a version dependency, a Manifest Author SHOULD populate the suit-text map with a SUIT_Component_Identifier key for the dependency component, and place in the corresponding map a suit-text-version-required key with a free text expression that is representative of the version constraints placed on the dependency. This text SHOULD be expressive enough that a device operator can be expected to understand the dependency. This is a free text field and there are no specific formatting rules.

By way of example only, to express a dependency on a component "['x', 'y']", where the version should be any v1.x later than v1.2.5, but not v2.0 or above, the author would add the following structure to the suit-text element. Note that this text is in cbor-diag notation.

```
[h'78',h'79'] : {
```

```
    7 : ">=1.2.5,<2"
}
```

4. Extension Parameters

Several parameters are needed to define the behaviour of the commands specified in Section 5. These parameters follow the same considerations as defined in Section 8.4.8 of [I-D.ietf-suit-manifest].

Name	CDDL Structure	Reference
Use Before	suit-parameter-use-before	Section 4.1
Minimum Battery	suit-parameter-minimum-battery	Section 4.2
Update Priority	suit-parameter-update-priority	Section 4.3
Version	suit-parameter-version	Section 4.4
Wait Info	suit-parameter-wait-info	Section 4.5

Table 1

4.1. suit-parameter-use-before

An expiry date for the use of the manifest encoded as the positive integer number of seconds since 1970-01-01. Implementations that use this parameter MUST use a 64-bit internal representation of the integer. Used with Section 5.1

4.2. suit-parameter-minimum-battery

This parameter sets the minimum battery level in mWh. This parameter is encoded as a positive integer. Used with suit-condition-minimum-battery (Section 5.3).

4.3. suit-parameter-update-priority

This parameter sets the priority of the update. This parameter is encoded as an integer. It is used along with suit-condition-update-authorized (Section 5.4) to ask an application for permission to initiate an update. This does not constitute a privilege inversion because an explicit request for authorization has been provided by the Update Authority in the form of the suit-condition-update-authorized command.

Applications MAY define their own meanings for the update priority. For example, critical reliability & vulnerability fixes MAY be given negative numbers, while bug fixes MAY be given small positive numbers, and feature additions MAY be given larger positive numbers, which allows an application to make an informed decision about whether and when to allow an update to proceed.

4.4. suit-parameter-version

Indicates allowable versions for the specified component. Allowable versions can be specified, either with a list or with range matching. This parameter is compared with version asserted by the current component when suit-condition-version (Section 5.5) is invoked. The current component may assert the current version in many ways, including storage in a parameter storage database, in a metadata object, or in a known location within the component itself.

The component version can be compared as:

* Greater.

* Greater or Equal.

* Equal.

* Lesser or Equal.

* Lesser.

Versions are encoded as a CBOR list of integers. Comparisons are done on each integer in sequence. Comparison stops after all integers in the list defined by the manifest have been consumed OR after a non-equal match has occurred. For example, if the manifest defines a comparison, "Equal [1]", then this will match all version sequences starting with 1. If a manifest defines both "Greater or Equal [1,0]" and "Lesser [1,10]", then it will match versions 1.0.x up to, but not including 1.10.

While the exact encoding of versions is application-defined, semantic versions map conveniently. For example,

* 1.2.3 = [1,2,3].

* 1.2-rc3 = [1,2,-1,3].

* 1.2-beta = [1,2,-2].

* 1.2-alpha = [1,2,-3].

* 1.2-alpha4 = [1,2,-3,4].

suit-condition-version is OPTIONAL to implement.

Versions SHOULD be provided as follows:

1. The first integer represents the major number. This indicates breaking changes to the component.

2. The second integer represents the minor number. This is typically reserved for new features or large, non-breaking changes.

3. The third integer is the patch version. This is typically

reserved for bug fixes.

4. The fourth integer is the build number.

Where Alpha (-3), Beta (-2), and Release Candidate (-1) are used, they are inserted as a negative number between Minor and Patch numbers. This allows these releases to compare correctly with final releases. For example, Version 2.0, RC1 should be lower than Version 2.0.0 and higher than any Version 1.x. By encoding RC as -1, this works correctly: [2,0,-1,1] compares as lower than [2,0,0]. Similarly, beta (-2) is lower than RC and alpha (-3) is lower than RC.

4.5. suit-parameter-wait-info

suit-directive-wait (Section 5.6) directs the manifest processor to pause until a specified event occurs. The suit-parameter-wait-info encodes the parameters needed for the directive.

The exact implementation of the pause is implementation-defined. For example, this could be done by blocking on a semaphore, registering an event handler and suspending the manifest processor, polling for a notification, or aborting the update entirely, then restarting when a notification is received.

suit-parameter-wait-info is encoded as a map of wait events. When ALL wait events are satisfied, the Manifest Processor continues. The wait events currently defined are described in the following table.

+=======================+==========+==========================+

Name	Encoding	Description
suit-wait-event-authorization	int	Same as suit-parameter-update-priority
suit-wait-event-power	int	Wait until power state
suit-wait-event-network	int	Wait until network state
suit-wait-event-other-device-version	See below	Wait for other device to match version
suit-wait-event-time	uint	Wait until time (seconds since 1970-01-01)
suit-wait-event-time-of-day	uint	Wait until seconds since 00:00:00
suit-wait-event-time-of-day-utc	uint	Wait until seconds since 00:00:00 UTC
suit-wait-event-day-of-week	uint	Wait until days since Sunday
suit-wait-event-day-of-week-utc	uint	Wait until days since Sunday UTC

Table 2

suit-wait-event-other-device-version reuses the encoding of suit-parameter-version-match. It is encoded as a sequence that contains an implementation-defined bstr identifier for the other device, and a list of one or more SUIT_Parameter_Version_Match.

5. Extension Commands

The following table defines the semantics of the commands defined in this specification in the same way as in the Abstract Machine Description, Section 6.4, of [I-D.ietf-suit-manifest].

Command Name	CDDL Identifier	Semantic of the Operation
Use Before	suit-condition-use-before	assert(now() < current.params[use-before])
Check Image Not Match	suit-condition-image-not-match	assert(not binary-match(digest(current), current.params[digest]))
Check Minimum Battery	suit-condition-minimum-battery	assert(battery >= current.params[minimum-battery])
Check Update Authorized	suit-condition-update-authorized	assert(isAuthorized(current.params[priority]))
Check Version	suit-condition-version	assert(version_check(current, current.params[version]))
Wait For Event	suit-directive-wait	until event(arg), wait

Table 3

5.1. suit-condition-use-before

Verify that the current time is BEFORE the specified time. suit-condition-use-before is used to specify the last time at which an update should be installed. The recipient evaluates the current time against the suit-parameter-use-before parameter (Section 4.1), which must have already been set as a parameter, encoded as seconds after 1970-01-01 00:00:00 UTC. Timestamp conditions MUST be evaluated in 64 bits, regardless of encoded CBOR size. suit-condition-use-before is OPTIONAL to implement.

5.2. suit-condition-image-not-match

Verify that the current component does not match the suit-parameter-image-digest (Section 8.4.8.6 of [I-D.ietf-suit-manifest]). If no digest is specified, the condition fails. suit-condition-image-not-match is OPTIONAL to implement.

5.3. suit-condition-minimum-battery

suit-condition-minimum-battery provides a mechanism to test a Recipient's battery level before installing an update. This condition is primarily for use in primary-cell applications, where the battery is only ever discharged. For batteries that are charged, suit-directive-wait is more appropriate, since it defines a "wait" until the battery level is sufficient to install the update. suit-condition-minimum-battery is specified in mWh. suit-condition-minimum-battery is OPTIONAL to implement. suit-condition-minimum-battery consumes suit-parameter-minimum-battery (Section 4.2).

5.4. suit-condition-update-authorized

Request Authorization from the application and fail if not authorized. This can allow a user to decline an update. suit-parameter-update-priority (Section 4.3) provides an integer priority level that the application can use to determine whether or not to authorize the update. Priorities are application defined. suit-condition-update-authorized is OPTIONAL to implement.

5.5. suit-condition-version

suit-condition-version allows comparing versions of firmware. Verifying image digests is preferred to version checks because digests are more precise. suit-condition-version examines a component's version against the version info specified in suit-parameter-version (Section 4.4)

5.6. suit-directive-wait

suit-directive-wait directs the manifest processor to pause until a specified event occurs. Some possible events include:

1. Authorization
2. External Power
3. Network availability

4. Other Device Firmware Version

5. Time

6. Time of Day

7. Day of Week

6. IANA Considerations

IANA is requested to:

* allocate key 14 in the SUIT Envelope registry for suit-coswid

* allocate key 14 in the SUIT Manifest registry for suit-coswid

* allocate key 7 in the SUIT Component Text registry for suit-text-version-required

* allocate the commands and parameters as shown in the following tables

6.1. SUIT Commands

Label	Name	Reference
4	Use Before	Section 5.1
25	Image Not Match	Section 5.2
26	Minimum Battery	Section 5.3
27	Update Authorized	Section 5.4
28	Version	Section 5.5
29	Wait For Event	Section 5.6

Table 4

6.2. SUIT Parameters

Label	Name	Reference
4	Use Before	Section 4.1
26	Minimum Battery	Section 4.2
27	Update Priority	Section 4.3
28	Version	Section 4.4
29	Wait Info	Section 4.5

Table 5

7. Security Considerations

This document extends the SUIT manifest specification. A detailed security treatment can be found in the architecture [RFC9019] and in the information model [I-D.ietf-suit-information-model] documents.

8. References

8.1. Normative References

[I-D.ietf-sacm-coswid]
Birkholz, H., Fitzgerald-McKay, J., Schmidt, C., and D. Waltermire, "Concise Software Identification Tags", Work in Progress, Internet-Draft, draft-ietf-sacm-coswid-20, 26 January 2022, <https://www.ietf.org/archive/id/draft-ietf-sacm-coswid-20.txt>.

[I-D.ietf-suit-manifest]
Moran, B., Tschofenig, H., Birkholz, H., and K. Zandberg, "A Concise Binary Object Representation (CBOR)-based Serialization Format for the Software Updates for Internet

of Things (SUIT) Manifest", Work in Progress, Internet-Draft, draft-ietf-suit-manifest-16, 25 October 2021, <https://www.ietf.org/archive/id/draft-ietf-suit-manifest-16.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9019] Moran, B., Tschofenig, H., Brown, D., and M. Meriac, "A Firmware Update Architecture for Internet of Things", RFC 9019, DOI 10.17487/RFC9019, April 2021, <https://www.rfc-editor.org/info/rfc9019>.

8.2. Informative References

[I-D.ietf-suit-information-model]
Moran, B., Tschofenig, H., and H. Birkholz, "A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices", Work in Progress, Internet-Draft, draft-ietf-suit-information-model-13, 8 July 2021, <https://www.ietf.org/archive/id/draft-ietf-suit-information-model-13.txt>.

Appendix A. A. Full CDDL

To be valid, the following CDDL MUST be appended to the SUIT Manifest CDDL. The SUIT CDDL is defined in Appendix A of [I-D.ietf-suit-manifest]

```
$$SUIT_severable-members-extensions //= (
    suit-coswid => bstr .cbor concise-software-identity)

$$severable-manifest-members-choice-extensions //= (
```

```
    suit-coswid => bstr .cbor SUIT_Command_Sequence / SUIT_Digest
)

SUIT_Condition //= (
    suit-condition-image-not-match,   SUIT_Rep_Policy)
SUIT_Condition //= (
    suit-condition-use-before,        SUIT_Rep_Policy)
SUIT_Condition //= (
    suit-condition-minimum-battery,   SUIT_Rep_Policy)
SUIT_Condition //= (
    suit-condition-update-authorized, SUIT_Rep_Policy)
SUIT_Condition //= (
    suit-condition-version,           SUIT_Rep_Policy)

SUIT_Directive //= (
    suit-directive-wait,              SUIT_Rep_Policy)

SUIT_Wait_Event = { + SUIT_Wait_Events }

SUIT_Wait_Events //= (suit-wait-event-authorization => int)
SUIT_Wait_Events //= (suit-wait-event-power => int)
SUIT_Wait_Events //= (suit-wait-event-network => int)
SUIT_Wait_Events //= (suit-wait-event-other-device-version
    => SUIT_Wait_Event_Argument_Other_Device_Version)
SUIT_Wait_Events //= (suit-wait-event-time => uint); Timestamp
SUIT_Wait_Events //= (suit-wait-event-time-of-day
    => uint); Time of Day (seconds since 00:00:00)
SUIT_Wait_Events //= (suit-wait-event-day-of-week
    => uint); Days since Sunday
```



```
SUIT_Wait_Event_Argument_Other_Device_Version = [
    other-device: bstr,
    other-device-version: [ + SUIT_Parameter_Version_Match ]
]

SUIT_Parameters //= (suit-parameter-use-before => uint)
SUIT_Parameters //= (suit-parameter-minimum-battery => uint)
SUIT_Parameters //= (suit-parameter-update-priority => uint)
SUIT_Parameters //= (suit-parameter-version =>
    SUIT_Parameter_Version_Match)
SUIT_Parameters //= (suit-parameter-wait-info =>
```

```
    bstr .cbor SUIT_Wait_Event)

SUIT_Parameter_Version_Match = [
    suit-condition-version-comparison-type:
        SUIT_Condition_Version_Comparison_Types,
    suit-condition-version-comparison-value:
        SUIT_Condition_Version_Comparison_Value
]
SUIT_Condition_Version_Comparison_Types /=
    suit-condition-version-comparison-greater
SUIT_Condition_Version_Comparison_Types /=
    suit-condition-version-comparison-greater-equal
SUIT_Condition_Version_Comparison_Types /=
    suit-condition-version-comparison-equal
SUIT_Condition_Version_Comparison_Types /=
    suit-condition-version-comparison-lesser-equal
SUIT_Condition_Version_Comparison_Types /=
    suit-condition-version-comparison-lesser

suit-condition-version-comparison-greater = 1
suit-condition-version-comparison-greater-equal = 2
suit-condition-version-comparison-equal = 3
suit-condition-version-comparison-lesser-equal = 4
suit-condition-version-comparison-lesser = 5

SUIT_Condition_Version_Comparison_Value = [+int]

$$suit-text-component-key-extensions //= (
    suit-text-version-required => tstr)

suit-coswid = 14
suit-condition-use-before        = 4
suit-condition-image-not-match          = 25
suit-condition-minimum-battery          = 26
suit-condition-update-authorized        = 27
suit-condition-version                  = 28
```



```
suit-directive-wait                     = 29

suit-wait-event-authorization        = 1
suit-wait-event-power                = 2
```

```
   suit-wait-event-network              = 3
   suit-wait-event-other-device-version = 4
   suit-wait-event-time                 = 5
   suit-wait-event-time-of-day          = 6
   suit-wait-event-day-of-week          = 7

   suit-parameter-use-before        = 4
   suit-parameter-minimum-battery   = 26
   suit-parameter-update-priority   = 27
   suit-parameter-version           = 28
   suit-parameter-wait-info         = 29

   suit-text-version-required      = 7
```

Author's Address

Brendan Moran
Arm Limited
Email: Brendan.Moran@arm.com