# Software Design Specification

## Z-Wave Plus v2 Device Type Specification

| | |
|---|---|
| **Document No.:** | SDS14224 |
| **Version:** | 10 |
| **Description:** | - |
| **Written By:** | NOBRIOT;DEWASSIE;JFR |
| **Date:** | 2020-07-06 |
| **Reviewed By:** | NOBRIOT;JFR;BBR;COLSEN;PSH;DEWASSIE |
| **Restrictions:** | Public |

| Approved by: | | | | |
|---|---|---|---|---|
| Date | CET | Initials | Name | Justification |
| 2020-07-06 | 03:54:22 | NTJ | Niels Johansen | |

| | | | **REVISION RECORD** | |
|---|---|---|---|---|

| Doc. Rev | Date | By | Pages affected | Brief description of changes |
|---|---|---|---|---|
| 1 | 20180226 | NOBRIOT | ALL | First revision |
| 2 | 20180304 | NOBRIOT | ALL | Updated document template |
| 3 | 20180701 | NOBRIOT | 4.8.2<br><br>4.5.1, 4.5.2, 4.5.6 & 4.5.5 | Added indicator, version 3 mandatory control for the Generic Controller DT.<br>Changed Basic Report Mapping for the Lock DT, Motorized Barrier DT, Sound Switch DT and Thermostat DT |
| 4 | 20181001 | NOBRIOT | Various<br><br>3.6.8.4 | Contributions 2018C:<br>• Added small clarifications and naming consistency updates along the document<br>• Clarified that the QR Code must comply with the "Gen2" determination from [9] |
| 5 | 20190101 | DEWASSIE NOBRIOT | 3.8<br>4.8.1 | Contributions 2018D:<br>• Removed S2 Learn Mode DSK statement obsoleted by SmartStart<br>• Updated the minimum Z/IP CC required version for Gateway DT and clarified the Gateway DT Command Class control requirements |
| 6 | 20190401 | NOBRIOT DEWASSIE | 3.6.8.7<br><br><br>4.7.2<br>3.9.10, 3.9.11 | Contributions 2019A:<br>• Moved the Security discovery for Association group in the Association and Multi Channel Association Command Classes<br>• Added IR Repeater Device Type<br>• Added required documentation requirements for Basic and Notification Command Classes. |
| 7 | 20190701 | NOBRIOT | 4.1 | Contributions 2019B:<br>• Clarified that Root Device MAY aggregate actuator Command Classes from different Device Type for their end points. |
| 8 | 20191001 | DEWASSIE | 3.9.10<br>4.8.1<br>4.8.2 | Contributions 2019C:<br>• Updated the documentation requirement of Basic Command Class support<br>• Clarified the use of Gateway DT<br>• Clarified the use of Generic Controller DT |
| 9 | 20200101 | DEWASSIE NOBRIOT | 3.3<br>3.9.13<br>4.8.1 & 4.8.2<br>3.6.1 & 3.7.1 | Contributions 2019D:<br>• Updated the Identify function of a Z-Wave Plus v2 node<br>• Added a documentation requirement regarding Identify function<br>• Added the Anti-Theft Unlock Command Class mandatory to control for all controllers Device Types |
| 10 | 20200701 | NOBRIOT<br><br>DEWASSIE | 3.6.8.2.2<br><br>3.6<br>4.8.1, 4.8.2<br>4.8.1.4<br><br>3.6.3.2<br><br>4.5.1, Table 5<br>4.6.4.2 | Contributions 2020A:<br>• Removed requirement to request S2 Unauthenticated when the highest requested key is S2 Authenticated<br>• Removed the bridging device requirement<br>• Removed UI requirements for the Gateway and Generic DT.<br>• Changed Node Provisioning command class support from MUST to SHOULD for the Gateway DT<br>• Clarified that Multi Channel multi-endpoint bit addressing must trigger a Lifeline Report.<br>• Updated optional supported command classes for Lock device type.<br>• Updated the recommended supported command classes for Meter Sensor device type. |

# Table of Contents

# List of Figures

# List of Tables

SDS14224-10     Z-Wave Plus v2 Device Type Specification     2020-07-06

# 1    Abbreviations

| Abbreviation | Explanation |
|---|---|
| AGI | Association Group Information (Command Class) |
| AOS | Always On Slave |
| CSC | Central Static Controller |
| DNS | Domain Name System |
| DT | Device Type |
| IP | Internet Protocol |
| LAN | Local Area Network |
| LSB | Less significant bit |
| LSS | Listening Sleeping Slave |
| MSB | Most significant bit |
| NIF | Node Information Frame |
| NOP | No Operation (Command Class) |
| PAN | Personal Area Network |
| PC | Portable Controller |
| PS | Portable Slave |
| QR | Quick Reponse |
| RPC | Reporting Portable Controller |
| RSS | Reporting Sleeping Slave |
| RT | Role Type |
| S0 | Security 0 Command Class |
| S2 | Security 2 Command Class |

| Abbreviation | Explanation |
|---|---|
| SIS | SUC NodeID Server |
| SSC | Sub Static Controller |
| SUC | Static Update Controller |
| Z/IP | Z-Wave for IP |

## 2    Introduction

### 2.1    Purpose

This document describes the requirement associated to the Z-Wave Plus v2 compliant Device Types. It contains a list of requirements applying for all Z-Wave Plus v2 compliant nodes as well as requirements specifics to each defined Device Type.

### 2.2    Audience and prerequisites

This document is public. The reader is expected to be familiar with Z-Wave development, Command Classes and Role Types.

### 2.3    Precedence of definitions

Individual Z-Wave Plus Role Type, Z-Wave Plus v2 Device Type and Command Class Specifications approved as a final version during the type/class development process MUST take precedence over this document temporarily until such individual specifications have been integrated into this document.

### 2.4    Terms used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document MUST be interpreted as described in IETF RFC 2119 [1].

## 3    Common Z-Wave Plus v2 Device Type requirements

### 3.1    How to detect Z-Wave Plus v2 compliant nodes

DT:00.11.0001.1    A Z-Wave Plus v2 node MUST advertise version 0x02 in the Z-Wave Plus Version field of the Z-Wave Plus Info Report. Multi Channel End Points MUST advertise the same version number in their Z-Wave Plus Info Report.

DT:00.11.0002.1    A Z-Wave Plus v2 node MUST set the Optional Functionality bit to 1 in its NIF.
For the NIF's description, refer to [3].

### 3.2    Command Classes support requirements

DT:00.11.0003.1    A Z-Wave Plus v2 node MUST support the command classes listed in the following sections. When a version number is indicated, the node MUST support or control the indicated version or a newer one.

#### 3.2.1    Root Device level

DT:00.11.0004.1    All Root Devices or nodes MUST support:

- Association, version 2
- Association Group Information
- Device Reset Locally
- Firmware Update Meta Data, version 5
- Indicator, version 3
- Manufacturer Specific
- Multi Channel Association, version 3
- Powerlevel
- Security 2
- Supervision
- Transport Service, version 2
- Version, version 2
- Z-Wave Plus Info, version 2

#### 3.2.2    End Point level

DT:00.11.0005.1    All Multi Channel End Points MUST support:

- Association, version 2
- Association Group Information
- Multi Channel Association, version 3
- Supervision
- Z-Wave Plus Info, version 2

### 3.3 Identify

DT:00.11.0006.2    A Z-Wave Plus v2 node MUST support an Identify indicator (Indicator ID 0x50) which can be used for an Identify function.

DT:00.12.0004.1    The node is RECOMMENDED to use a visible LED for an identify function if it has an LED. If the node is itself a light source, e.g. a light bulb, this MAY be used in place of a dedicated LED.

DT:00.11.0007.1    The Root Device of a node MUST support the Indicator Command Class, version 3 or newer and support the Indicator ID 0x50 (Identify) and Properties ID 0x03, 0x04 and 0x05.

DT:00.13.0001.1    Multi Channel devices MAY support an Identify indicator on End Points, if the corresponding End Point has its own LED or light source.

DT:00.11.0008.1    If a Multi Channel device only implements a single indicator for the entire device, the End Points MUST NOT support the Identify Indicator, while the Root Device MUST support the Identify Indicator.

### 3.4 Dynamic Capabilities and node discovery

DT:00.11.0009.1    A controller MUST have a menu or method for an (advanced) end user to request the controller to perform a capability discovery for a given node (i.e. to perform a complete commissioning interview)

DT:00.13.0002.1    Nodes (and their End Points) MAY change capabilities based on a user action, such as changing configuration parameters or the physical addition/removal of a module.

DT:00.11.000A.1    End Point changing capabilities based on a user action MUST NOT be advertised as Dynamic End Points.

DT:00.13.0003.1    If supporting Configuration Command Class, nodes MAY issue a Configuration Report advertising a dynamic capabilities parameter value change in order to let the lifeline destination(s) know that some capabilities have changed.

DT:00.11.000B.1    However, a controlling node MUST NOT perform the node interview unless instructed to do so by the end user.

DT:00.11.000C.1    The configuration of Command Classes that are available before and after a capability change MUST remain unchanged. For instance, the Lifeline Association Group destination and Wake Up destination MUST stay identical when a node changes capabilities.

DT:00.11.000D.1    A node MUST stay compliant and observe Z-Wave Plus v2 Device Type requirements when and after changing capabilities. A node MAY change its Device Type when altering its capabilities.

DT:00.11.000E.1    A node being able to change between a secure only Device Type (S2 Access Control) and a regular S2 Device Type MUST observe the S2 Access Control Device Type requirements (3.6.8.2.1) even if configured to be a regular Device Type.

### 3.5   Controller Functionalities

A controller plays an important role in a Z-Wave network because this device hosts important functionality to create, maintain and configure the network and the home automation application. The following sections describe important rules to ensure that a controller is capable of fulfilling this important role.

#### 3.5.1   Interoperability

DT:00.11.0011.1

To ensure interoperability, a controller MUST comply with the following requirements:

1.  It is not acceptable to block interoperability by any means.

2.  It is not acceptable to prevent inclusion of certified devices into a system or force exclusion of non-preferred devices after inclusion.

3.  Devices from non-preferred manufacturers MAY be placed in a special section of the user interface; this section should be referred to as "Additional Z-Wave Ecosystem Devices". Additionally, it is acceptable to inform the user, upon inclusion of non-preferred devices that the device being included is not part of the vendors preferred ecosystem, and that control and support of the device by the vendor may be limited.

    a.  It is not permitted to display additional pop-ups, ask for pin codes or implement any other blocking or discouraging behavior for inclusion or control of non-preferred devices.

    b.  The Z-Wave Alliance recommends wording as follows. "You are about to include a Z-Wave compatible device that is not promoted by *'service provider name'* for use in this application. While the device will work as expected the device may or may not support all of the features of the *'service provider name'* recommended device."

#### 3.5.2   Minimal Control Functionality

DT:00.11.0012.1

If a controller product supports short range wireless non-Z-Wave technology smarthome products (e.g. light bulbs, thermostats, door locks and the like) and Z-Wave technology products, it MUST, at a minimum, control the following Command Classes:

- Door Lock Command Class
- Binary Switch Command Class
- Multilevel Switch Command Class
- Thermostat Mode Command Class
- Thermostat Setpoint Command Class

It is acceptable to provide additional controlling functionalities for nodes from a preferred manufacturer as long as the controller provides the minimal required control functionalities for all nodes. Refer to [7] for Command Class control requirements.

### 3.6    Command Class support specific requirements

Certain rules must be fulfilled depending on which command classes are supported. The following subsections detail the requirements of special command classes. Details about individual Command Classes can be found in [3], [4], [5] and [6].

#### 3.6.1    Anti-theft Command Class

DT:00.11.002A.1    If the Anti-Theft Command Class is supported, it MUST be version 3 or newer.

#### 3.6.2    Application Status Command Class

DT:00.11.0015.1    If a node is temporarily not capable to service a Get or Set Command request, it MUST support the Application Status Command Class and return an Application Busy Report Command to the initiator of the Get or Set.

DT:00.13.0004.1    If a node is always capable of servicing the Get and Set requests, it is OPTIONAL to support the Application Status Command Class.

### 3.6.3　Association requirements

#### 3.6.3.1　Mandatory groups

DT:00.11.0016.1　The Root Device and End Points of a Z-Wave Plus v2 node MUST advertise the Association Groups indicated in Table 1 as a minimum.

**Table 1, Z-Wave Plus v2 minimum required AGI table**

| Group identifier | Profile 2 bytes | Command Class & Command (list) N bytes | Group Name (UTF-8) M bytes |
|---|---|---|---|
| 1 | General:Lifeline | Refer to 3.6.3.2 Lifeline reports | Lifeline |

DT:00.11.0017.1　A Node or Root Device MUST advertise a "Max Nodes Supported" value of 1 or more for the Lifeline Association group in the Association Report and Multi Channel Association Report Commands.

DT:00.11.0018.1　End Points MUST advertise a "Max Nodes Supported" of 0 for the Lifeline Group and MUST report their Lifeline Commands via the Root Device's Lifeline Group when an End Point Association is established for the Lifeline Group. (Refer to Multi Channel Association Command Class)

#### 3.6.3.2　Lifeline reports

DT:00.11.0019.1　A Z-Wave Plus v2 node MUST issue all the commands defined in [8] via the Lifeline Association Group to reflect its state changes if the corresponding command is supported by the node.

DT:00.12.0001.1　Report or Notification Commands SHOULD NOT be issued while performing a transitions from a Command Class state to another, but only when the supporting node has reached a final state. Intermediate transition state values SHOULD be advertised only if a long transition takes place (e.g. transition longer than 1 minute)

DT:00.12.0002.1　Any other Command Class state or configuration relevant to the control of the node or relevant for GUI information SHOULD be reported via the Lifeline when changed.

DT:00.11.001A.1　If the state change was triggered by other means than a Z-Wave Command, a node MUST issue the corresponding Report/Notification Command immediately to the lifeline destination(s).

If the state change was triggered by a Z-Wave Command:

DT:00.12.0003.1　
- A node SHOULD NOT issue any Report/Notification Commands via the Lifeline if the actual lifeline destination issued the Set Command.

DT:00.11.001B.1　
- A node MUST NOT issue any Report/Notification Command after a Command received via Multicast/broadcast addressing.

DT:00.11.002D.1　
- A node MUST issue a Report/Notification Command after a Command received via Singlecast using Multi Channel multi-endpoint bit addressing.

DT:00.11.001C.1　
- Unless the lifeline destination issued the command, a node MUST issue a Report/Notification Command after a command was received using singlecast addressing (including Multi Channel multi-End Point destination) via the Lifeline.

DT:00.11.001D.1　
- If a node has more than one lifeline destination, it MUST issue a Report/Notification Command after a command was received using singlecast addressing (including Multi Channel multi-End Point destination) via the Lifeline.

An example of the expected frame flow is shown in Figure 1.
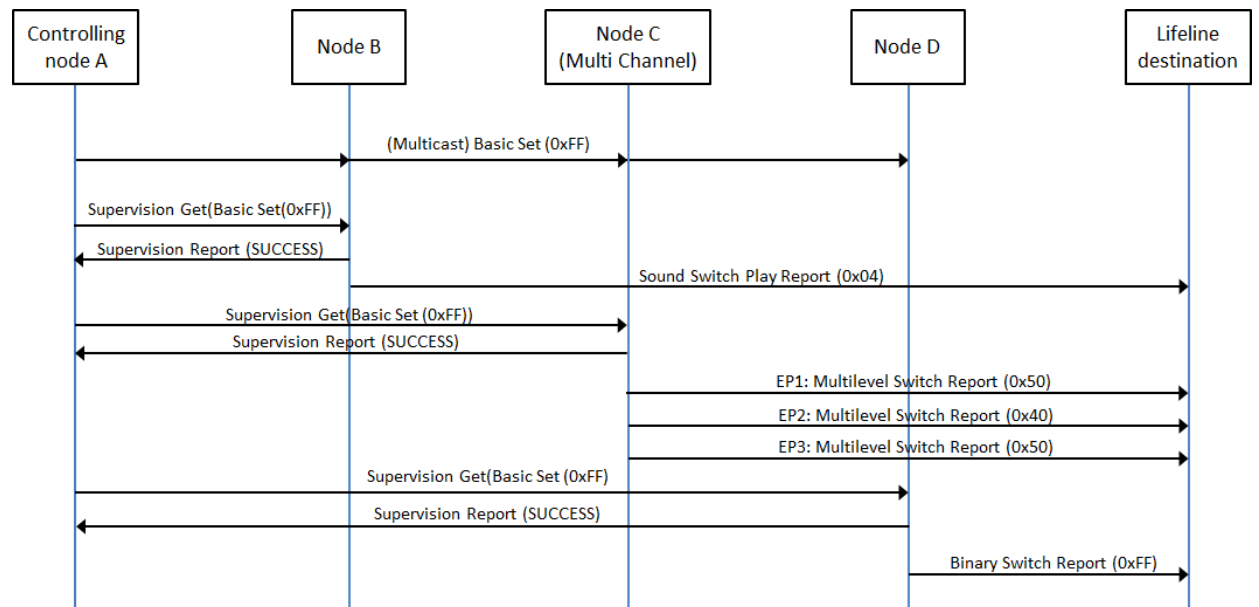


**Figure 1, Lifeline status reports frame flow after multicast (example)**

### 3.6.4    Configuration Command Class

DT:00.11.001E.1    If the Configuration Command Class is implemented, it MUST NOT replace any existing Command Class functionality.

DT:00.11.001F.1    If the Configuration Command Class is supported, it MUST be version 4 as a minimum.

### 3.6.5    Firmware Update Meta Data Command Class

DT:00.11.0020.1    The configuration of Command Classes that are available before and after a firmware update MUST remain unchanged. For instance, the Lifeline Association Group destination, Wake Up destination and any command class setting MUST stay identical before and after performing a firmware update.

### 3.6.6    Wake Up Command Class

DT:00.11.0021.1    If the node supports the Wake Up Command Class, the node MUST support manual Wake Up triggered by a user activation.

### 3.6.7    Multi Channel support

DT:00.11.0022.1    Actuator functionalities MUST reside in individual Multi Channel End Points according to the list of actuator Device Types.

DT:00.11.0023.1    Multi Channel devices MUST support the Multi Channel Command Class, version 4 or newer

DT:00.11.0024.1    A node supporting the Multi Channel Command Class MUST issue commands to the Lifeline destination from all of its End Points if an End Point Association has been established on the Root Device Lifeline association group.

DT:00.11.0025.1    A command issued to the Lifeline destination from a Multi Channel End Point MUST be Multi Channel encapsulated if an End Point Association has been established.

### 3.6.8    Security 2 Command Class

### 3.6.8.1    S2 bootstrapping and functionalities

DT:00.21.0001.1    After network inclusion, a node MUST consider S2 Bootstrapping as started after receiving the S2 KEX Get Command.

DT:00.21.0002.1    If a node times out waiting for security bootstrapping after network inclusion, it MUST NOT consider that bootstrapping failed and MUST consider that it was included non-securely.

DT:00.23.0001.1    If S2 bootstrapping started and did not complete successfully, a supporting node MAY remove support of its implemented command classes until re-included. Refer to [3] chapter 3 regarding NIF contents depending on network inclusion and security bootstrapping.

DT:00.21.0003.1    A node supporting S2 MUST consider any Security Class lower than its highest granted Security Class as unsecure communication.
Certain command classes, such as Transport Service or Z-Wave Plus Info, must always be supported non-securely and present in the NIF if they are supported by a node. In this case, non-secure support requirements are specified in each individual command class definition. A list of these special Command Classes is also available in [11], under "Additional Comments".

DT:00.21.0004.1    By default, a node supporting S2 MUST support its Command Classes only at the highest granted Security Class. If no Security Class was granted, the node MUST support all its Command Class using non-secure communication.

This does not apply to S2 Access Control nodes, which MAY (or sometimes MUST) remove support for some Command Classes if a particular Security Class has not been granted.

### 3.6.8.2    S2 Security Classes requirements

Security 2 Command Class defines several Security Classes [5].

DT:00.21.0005.1    A Z-Wave Plus v2 node MUST request either S2 Access Control or S2 Authenticated as its highest key.

DT:00.21.0006.1    An S2 supporting node MUST comply with the requirements indicated in the subsection below (3.6.8.2.1 or 3.6.8.2.2) associated to its highest requested Security Class during S2 bootstrapping.

DT:00.21.0007.1    Nodes requesting the S0 Security Class MUST also comply with requirement indicated in 3.6.8.3.

DT:00.21.0008.1    A Multi Channel Root Device and all its End Points MUST share the same highest S2 Security Class.

### 3.6.8.2.1 S2 Access Control Security Class

The S2 Access Control Class is the most trusted class and is intended for home access control devices such as door locks, garage door openers or central controllers.

DT:00.21.0009.1 A node requesting the S2 Access Control Security Class MUST carry a representation of its DSK on itself and/or make it visible on its UI at any time when Learn Mode is enabled. Refer to 3.6.8.4 for DSK format and representation.

DT:00.21.000A.1 A node based on a controlling Device Type (4.3) requesting S2 Access Control Security Class MUST request S2 Authenticated and S2 Unauthenticated Security Classes when being S2 bootstrapped.

DT:00.23.0002.1 A node based on a controlling Device Type (4.3) requesting the S2 Access Control Security Class MAY decide to not support a set of its implemented Command Classes if it has not been granted a certain Security Class during S2 bootstrapping.

DT:00.23.0003.1 A node based on a supporting Device Type (4.2) requesting S2 Access Control Security Class MAY request any other Security Class for control purposes.

DT:00.21.000B.1 A node based on a supporting Device Type (4.2) MUST support its Command Classes depending on Security bootstrapping as follows:

DT:00.21.000C.1
- If security bootstrapped, it MUST support its Command Classes only if the highest granted key is S0 or S2 Access Control Security Class. It MUST NOT support its Command Classes at all if its highest granted Security Class is any other class than S0 or S2 Access Control.

DT:00.21.000D.1
- If it timed out waiting for security bootstrapping or S0/S2 bootstrapping failed, it MUST NOT support its Command Classes non-securely.

DT:00.21.000E.1
- The above two requirements MUST NOT apply for Command Classes that MUST always be in the NIF (refer to 3.6.8.1 and [11]).

### 3.6.8.2.2 S2 Authenticated Security Class

The S2 Authenticated Class is the 2nd most trusted class and is intended for secure applications in home control deployments.

DT:00.21.000F.1 A node requesting the S2 Authenticated Security Class MUST carry a representation of its DSK on itself and/or make it visible on its UI at any time when Learn Mode is enabled. Refer to 3.6.8.4 for DSK format and representation.

### 3.6.8.3 S0 Security Class requirements

The S0 Class is used for backwards compatibility with S0 supporting nodes.

DT:00.21.0011.1 An S2 node MUST NOT request the S0 Security Class if it does not support the Security 0 Command Class. An S2 node MUST NOT request the S0 Security Class without requesting an S2 Security Class.

DT:00.22.0001.1 Nodes with controlling capabilities and controllers SHOULD request the S0 Security Class for application control purposes.

### 3.6.8.4    DSK format and representations

The S2 Command Class defines a Device Specific Key (DSK) that enables authentication as part of the S2 Bootstrapping process.

The DSK can be represented with the following pre-defined formats: PIN code, DSK string and QR code.

DT:00.21.0012.1   The PIN code MUST be 5 decimal digits representing the value of the first 2 bytes of the node's DSK and MUST be constructed according to Figure 2.

ECDH Public Key[1..16]:    {0x84,0xEC,0x5C,0x75,0x51,0xCA,0xB5,0x0A,0x83,0xD2,0x1D,0x07,0xDD,0xF5,0x38,0xD9}

⇩

0x84EC

⇩

Pin code:    34028
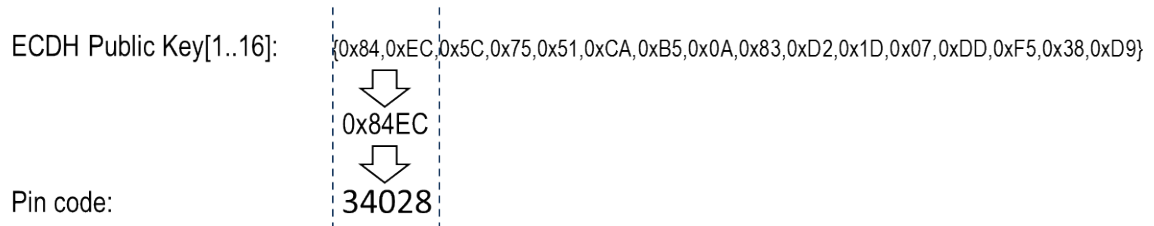
**Figure 2, PIN code format**

DT:00.21.0013.1   The DSK string MUST be 8 groups of 5 decimal digits, each representing 2 bytes of the DSK, separated with hyphens and MUST be constructed according to Figure 3.

ECDH Public Key[1..16]:    {0x84,0xEC,0x5C,0x75,0x51,0xCA,0xB5,0x0A,0x83,0xD2,0x1D,0x07,0xDD,0xF5,0x38,0xD9}

⇩  ⇩  ⇩  ⇩  ⇩  ⇩  ⇩  ⇩

0x84EC  0x5C75  0x51CA  0xB50A  0x83D2  0x1D07  0xDDF5  0x38D9

⇩  ⇩  ⇩  ⇩  ⇩  ⇩  ⇩  ⇩

DSK string:    DSK:34028-23669-20938-46346-33746-07431-56821-14553
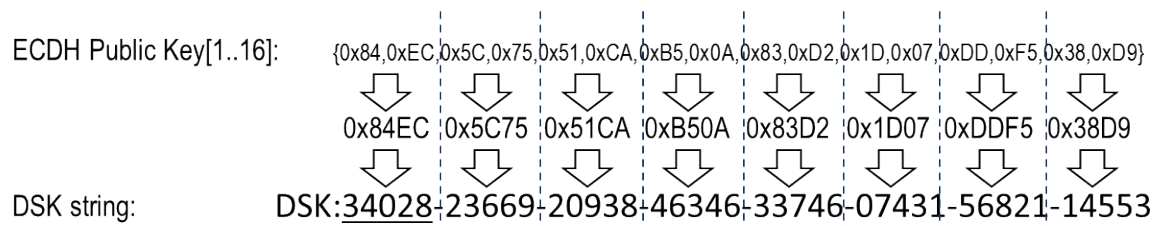
**Figure 3, DSK String format**

DT:00.21.0014.1   The first five digits of the DSK string MUST be underlined to help the user identify the PIN code portion of the DSK string.

DT:00.21.0015.2   The QR code format MUST comply with the "Gen2" format defined in [9]. The QR code MUST include two TLV blocks: Type 0 (Product Type) and TLV Type 1 (Product ID) as defined by [10].

Additional formatting requirements for the market certification are given by the Z-Wave Alliance, refer to [12].

### 3.6.8.5    Mandatory DSK representations

DT:00.21.0016.1   The DSK representations present on a product MUST comply with Table 2 and the subsections below.

**Table 2, Mandatory DSK representations for Z-Wave Plus v2 nodes**

|  | On the product | On the leaflet | On the box/package |
|---|---|---|---|
| **PIN Code** | At least one REQUIRED | OPTIONAL | OPTIONAL |
| **DSK String** |  | - | |
|  | REQUIRED in at least 1 place | | |
| **QR Code** | REQUIRED if the node | OPTIONAL | RECOMMENDED |

| | supports to be included using SmartStart inclusion | | |
|---|---|---|---|

#### 3.6.8.5.1   DSK on the product or UI

DT:00.21.0017.1   A product MUST have a QR code printed on the its outside or on its UI if it supports to be included using SmartStart inclusion.

DT:00.21.0018.1   A product MUST carry or display the DSK string or PIN code.

DT:00.21.0019.1   If the product carries the PIN code representation of the DSK, the product leaflet, documentation or packaging MUST contain the DSK string.

#### 3.6.8.5.2   DSK on documentation or leaflet

DT:00.22.0002.1   It is RECOMMENDED that a leaflet inside the product's box, advertises the QR code and the full DSK string.

#### 3.6.8.5.3   DSK on the product's box/package

DT:00.22.0003.1   The product packaging SHOULD carry the QR code and DSK string on its outside.

#### 3.6.8.6   Filtering Security Class for controlling nodes

DT:00.23.0004.1   For Command Classes always supported non-securely (always in the NIF), a controlling node MAY accept a command at any security level shared with a sending S2 node.

DT:00.21.001A.1   For Command Classes supported securely, a controlling node MUST discard the command from a supporting node if not received at the highest common security level between the controlling node and the sending S2 node.

DT:00.21.001B.1   A controlling node MUST NOT discard a command if the sending node does not support the S2 Command Class.

A node is considered controlling or supporting based on which command it sends or receives. Each command node's role is marked in [11].

### 3.6.8.7   Controlling nodes: Security Class learning

DT:00.21.001D.2

Any Z-Wave Plus v2 node controlling Command Classes (not using association groups) MUST discover the destination capabilities using every Security Class. If it intends to create associations between 2 other nodes, it MUST also discover which keys have been granted to both nodes.

DT:00.22.0005.1

If the controller is the SIS, it SHOULD skip the discovery as it knows which keys have been granted. If the controller is not the SIS or does not know which security levels to use with a destination, the following discovery algorithm is RECOMMENDED:

1. Request the NIF and read its contents, look for S2/Supervision and S0
2. If S2 is supported, for every S2 key starting from the highest:
    a. Issue the S2 Commands Supported Get
        i. If receiving no answer (or S2 Nonce Reports), conclude that the corresponding Security Class has not been granted to the node
        ii. If receiving an S2 Commands Supported Report with an empty list, conclude that the corresponding Security Class has been granted and is not the highest
        iii. If received an S2 Commands Supported Report with a non-empty list, conclude that the corresponding Security Class has been granted and is the highest.
3. If S0 is supported, discover if S0 key was granted:
    a. Issue a S0 encrypted S0 Security Command Supported Get command
    b. If S2 was in the NIF :
        i. If not receiving any response, conclude that the S0 Security Class has not been granted to the node
        ii. If receiving an S0 Commands Supported Report with an empty list, conclude that the S0 Security Class has been granted and is not the highest
        iii. If receiving an S0 Commands Supported Report with a non-empty list, conclude that the S0 Security Class has been granted and is the highest
    c. If S2 was not in the NIF:
        i. If receiving an S0 Commands Supported Report, conclude that S0 is the highest granted key
        ii. If not receiving any response, conclude that the S0 Security Class has not granted to the node

The Role Type specification [2] provides recommended timeouts when waiting for responses to get type commands.

### 3.7    Command Class control specific requirements

Certain rules must be fulfilled depending on which command classes are controlled. The following subsections detail the requirements of special command classes. Details about individual Command Class control can be found in [7].

### 3.7.1    Anti-Theft Command Class

Control of this command class is limited to an entity that has been granted permission by the Z-Wave Alliance to control this Command Class and has been granted a locking entity ID. The list of granted locking entity IDs is defined in [13].

Any node controlling this Command Class without authorization will be failed in certification.

DT:00.11.002B.1    A node controlling this Command Class MUST NOT provide access to the locking functionality feature of the Command Class to a consumer/end-user of the node; i.e. end users MUST NOT be able to lock nodes themselves.

DT:00.11.002C.1    Control of this command class by a node which is also offered in a non-service market where an end consumer has access to network control features MUST use a different Product ID and Product Type ID between the service and consumer versions of the product.

### 3.8    SmartStart requirements

DT:00.11.0026.1    A Z-Wave Plus v2 node MUST either support to be included in a network using SmartStart inclusion or provide SmartStart inclusion of other nodes. A controller providing SmartStart inclusion of other nodes MAY also support being included in a network using SmartStart inclusion.

DT:00.11.0027.1    A SmartStart product documentation MUST respect the requirements described in 3.9.4 Documentation related to SmartStart.

DT:00.11.0028.1    A node supporting to be included using SmartStart inclusion MUST have a QR code printed on its outside or its UI. (refer to 3.6.8.5 Mandatory DSK representations). The QR code MUST indicate version 1 (SmartStart enabled nodes).

DT:00.11.0029.2    A SmartStart node MUST carry and keep the same Learn Mode DSK during its entire lifetime. Refer to 3.6.8.2 and 3.6.8.4.

### 3.9     Required Documentation

The following requirements for end user documentation apply to all Z-Wave Plus v2 compliant products. The documentation may be provided as product manuals, quick start guides, electronic help files, web pages, etc.

### 3.9.1     Terminology

DT:00.31.0001.1

The product documentation MUST use the terminology indicated in Table 3 for Z-Wave related functionality.

**Table 3, Z-Wave Z-Wave Plus v2 documentation terminology**

| Z-Wave functionality | Documentation terminology | Example |
|---|---|---|
| Inclusion | Add | The process of adding a node to the Z-Wave network. |
| Exclusion | Remove | The process of removing a node from the Z-Wave network. |
| Replication | Copy | The process of copying network information from one controller to another. |

### 3.9.2     Additional documentation required for Z-Wave Certification

DT:00.31.0002.1

In addition to the rules defined above the following technical documentation MUST be made available to the certification test lab upon submitting the product for certification:

- Documentation about how to activate any functionality available in the device related to Z-Wave behavior

- If any *special* procedures are REQUIRED to test any item in the certification form, such procedures MUST be clearly described

- If the product is a Z-Wave controller, documentation on how to send any controlled command from the controller MUST be included, refer to [7].

### 3.9.3     Documentation for Classic Inclusion, Exclusion and Replication

DT:00.31.0003.1

For Z-Wave slave Role Types, the documentation MUST describe:

- How to include and exclude the device in an existing network when using Classic inclusion.

DT:00.31.0004.1

For Z-Wave controller Role Types, the documentation MUST describe:

- How to include and exclude the device in an existing network using classic inclusion.
- How to include and exclude other devices.
- How to initiate a replication of network information from the controller to another controller.
- How to put the controller into learn mode to receive network information from another controller.

### 3.9.4    Documentation related to SmartStart

DT:00.31.0005.1    The documentation MUST describe:

- How to locate the DSK representation(s) on the product.
- How to access the DSK representation(s) via the UI, if available.

DT:00.31.0006.1    For nodes supporting the SmartStart inclusion, the documentation MUST include a short description of what is SmartStart. The following wording is RECOMMENDED:

> *SmartStart enabled products can be added into a Z-Wave network by scanning the Z-Wave QR Code present on the product with a controller providing SmartStart inclusion. No further action is required and the SmartStart product will be added automatically within 10 minutes of being switched on in the network vicinity.*

DT:00.31.0007.1    For controllers providing the SmartStart functionality, the documentation MUST describe:

- How to perform a secure inclusion of a SmartStart node (adding the node in the Node Provisioning List and powering up/installing the node)
- How to access and edit the Node Provisioning List.

### 3.9.5    Documentation related to devices from multiple manufacturers

DT:00.31.0008.1    The product documentation MUST include a section which describes how products from different manufacturers and product categories can be a part of the same Z-Wave network, and that the different mains powered nodes can act as repeaters regardless of manufacturers.

The following is the RECOMMENDED wording:

> *This product can be operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers. All mains operated nodes within the network will act as repeaters regardless of vendor to increase reliability of the network.*

### 3.9.6    Documentation for Association Command Class

DT:00.31.0009.1    The documentation MUST include a description of the association groups available in the product.

DT:00.31.000A.1    Each group MUST include the following information:

- Grouping identifier
- Maximum number of devices that can be added to the group
- Description of how the association group is used and/or triggered by the product

- Description of any mapping between groups (e.g. Root Device mirrored End Point group)

### 3.9.7    Documentation for Configuration Command Class

DT:00.31.000B.1    If the product implements support of the Configuration Command Class, the documentation MUST include a description of each configuration parameter available in the product.

DT:00.31.000C.1    Each configuration parameter MUST be listed with the following information:

- Parameter number
- Description of parameter and its effect on the product
- Default value and allowed values
- Size (number of bytes)

DT:00.32.0001.1    The documentation SHOULD also list other configuration parameter properties such as read-only or advanced flag, etc.

### 3.9.8    Documentation for Wake Up Command Class

DT:00.31.000D.1    If the node supports the Wake Up Command Class, the product documentation MUST describe how to manually Wake Up the node.

### 3.9.9    Documentation for Security 2 Command Class

DT:00.31.000E.2    If a node based on a slave Role Type supports its Command Classes only when granted the Access Control Security key, the documentation MUST indicate that an S2 security enabled controller is required to operate the product.

DT:00.31.000F.1    The documentation MUST list the supported Command Classes, their version and their required Security class if any.

For example, a Lock Device Type list and a Binary Switch Device Type list are given in Table 4.

**Table 4, Lock DT/Binary Switch DT Supported Command Classes documentation example**

| Lock DT example | | | Binary Switch DT example | | |
|---|---|---|---|---|---|
| **Command Class** | **Version** | **Required Security Class** | **Command Class** | **Version** | **Required Security Class** |
| Association | 2 | S0 or Access Control | Association | 2 | Highest granted Security Class |
| Association Group Information | 3 | S0 or Access Control | Association Group Information | 3 | Highest granted Security Class |
| Basic | 2 | S0 or Access Control | Basic | 2 | Highest granted Security Class |
| Device Reset Locally | 1 | S0 or Access Control | Binary Switch | 2 | Highest granted Security Class |
| Door Lock | 4 | S0 or Access Control | Device Reset Locally | 1 | Highest granted Security Class |
| Firmware Update Meta Data | 5 | S0 or Access Control | Firmware Update Meta Data | 5 | Highest granted Security Class |
| Indicator | 3 | S0 or Access Control | Indicator | 3 | Highest granted Security Class |
| Manufacturer Specific | 1 | S0 or Access Control | Manufacturer Specific | 1 | Highest granted Security Class |
| Multi Channel Association | 3 | S0 or Access Control | Multi Channel Association | 3 | Highest granted Security Class |
| Powerlevel | 1 | S0 or Access Control | Powerlevel | 1 | Highest granted Security Class |
| Security 0 | 1 | None | Security 2 | 1 | None |
| Security 2 | 1 | None | Supervision | 1 | None |
| Supervision | 1 | None | Transport Service | 2 | None |
| Transport Service | 2 | None | Version | 3 | Highest granted Security Class |
| Version | 3 | S0 or Access Control | Z-Wave Plus Info | 2 | None |
| Z-Wave Plus Info | 2 | None | | | |

### 3.9.10  Documentation for Basic Command Class

DT:00.31.0014.2   If the product supports Basic Command Class, the product documentation MUST include information on the usage of the Basic Command Class and the resulting product behavior

### 3.9.11  Documentation for Notification Command Class

DT:00.31.0015.1   If the product implements support of the Notification Command Class, the documentation MUST specify the implemented Notification Type(s) and Event(s).

### 3.9.12  Documentation for dynamic capabilities

DT:00.31.0010.1   If the product can alter its capabilities depending on a configuration parameter or based on a user interaction, the documentation MUST include a list of all events that can trigger capability change and describe:

- How to perform such actions
- What capabilities are being altered.

DT:00.31.0011.1   The product documentation MUST indicate to the end user that it is necessary to ask a controlling node to rediscover the product's capabilities after altering capabilities.

DT:00.31.0012.1   The product documentation MUST indicate that it is necessary to re-include the node in the network if the controller does not have any capability rediscovery option.

DT:00.31.0013.1   For nodes based on a controlling Device Type (4.3), the documentation MUST describe how an (advanced) end user can perform a capability rediscovery of a chosen node.

### 3.9.13  Documentation for Identity function

DT:00.31.0016.1   The product documentation MUST describe how product can be identified using the Indicator Command Class with the Indicator ID 0x50 (identify).

## 4    Z-Wave Plus v2 Device Type Definition

### 4.1    Optional Command Classes

DT:00.11.000F.1   Device Types MAY support optional Command Classes on top of the minimum mandatory set of supported Command Classes. However, the following Command Classes MUST NOT be supported optionally in a Device Type:

- Barrier Operator
- Color Switch
- Window Covering
- Multilevel Switch
- Thermostat Mode
- Thermostat Setpoint
- Thermostat Setback
- Sound Switch
- Simple AV Control
- Door Lock
- Binary Switch

DT:00.11.0010.1    It means that if supported, these command classes MUST fit the exact actuator Command Class list of a Device Type. If several actuator Command Classes not belonging to the Device Type need to be supported, they MUST be partitioned in End Points which match the actuator Command Class list of a Device Type.

Multi Channel Root Devices MAY still aggregate some of the above mentioned Command Classes from their end points for backwards compatibility. The optional Command Class rule applies:

- For the node (Root Device) if the node does not support Multi Channel Command Class
- For each and every end point if the node supports the Multi Channel Command Class

## 4.2   Supporting Device type overview

The Z-Wave Plus v2 certification program defines a new set of Device Type based on which Command Classes are supported. They are classified into 3 categories:

- Actuator supporting device types.
- Data reporting devices types
- Other devices types.

The Supporting Device Type overview is shown in Table 5.

**Table 5, Supporting Device Types overview**

| Actuator supporting Types | | | |
|---|---|---|---|
| **Device Type** | **Mandatory** | **Recommended options** | **Role Types** |
| Lock | Door Lock, v4<br><br>Security 0 (S0) | User Code<br>Entry Control<br>Generic Schedule<br>Authentication<br>Authentication Media Write | All |
| Motorized barrier | Barrier Operator<br><br>Notification, v8<br><br>Security 0 (S0) | - | All |
| Color Switch | Color Switch, v3<br><br>Multilevel Switch v4 or<br>Binary Switch v2 | Multi Command | All |
| Window Covering | Multilevel Switch, v4<br>Window covering | - | All |
| Thermostat | Thermostat Mode, v3<br><br>Thermostat Setpoint | Clock (support) or Time (control)<br>Multilevel Sensor<br>Schedule, v4<br>Thermostat Setback | All |
| Sound Switch | Sound Switch | - | All |
| AV Control Point | Simple AV Control | - | All |
| Multilevel Switch | Multilevel Switch, v4 | - | All |
| Binary Switch | Binary Switch, v2 | - | All |
| Data reporting supporting Types | | | |
| **Device Type** | **Mandatory** | **Recommended options** | **Role Types** |
| Entry Control Keypad | Entry Control<br>Security 0 (S0) | - | All |
| Multilevel Sensor | Multilevel Sensor, v11 | Multi Command (control) | All |
| Notification Sensor | Notification, v8 | Multi Command (control) | All |
| Meter Sensor | Meter, v5 | Multi Command (control) | All |
| Central Scene | Central Scene, v3 | Basic (control) | All |

| Other Types | | | |
|---|---|---|---|
| **Device Type** | **Mandatory** | **Recommended options** | **Role Types** |
| Repeater | No command class other than 3.2.1 | - | AOS |
| IR Repeater | IR Repeater Command Class | | AOS |

<u>Note</u>: green background indicates Device Types that operate at the S2 Access Control Security Class only.

## 4.3    Controlling Device type overview

The Z-Wave Plus v2 certification program defines a new set of Device Type for controllers based on which Command Classes are supported and controlled.

The controlling Device Type overview is shown in Table 6.

**Table 6, Controlling Device Types overview**

| Controller Types | | | |
|---|---|---|---|
| **Device Type** | **Mandatory (support)** | **Mandatory (control)** | **Role Types** |
| Gateway | CRC-16 Encapsulation<br>Multi Command<br>Node Provisioning<br>Security 0 (S0)<br>Time | Association, version 2<br>Basic<br>Central Scene, version 3<br>CRC-16 Encapsulation<br>Firmware Update Meta Data, version 5<br>Indicator, version 3<br>Meter, version 5<br>Multi Channel, version 4<br>Multi Channel Association, version 3<br>Multilevel Sensor, version 11<br>Notification, version 8<br>Security 0 (S0)<br>Security 2 (S2)<br>Version, version 2<br>Wake Up, version 2 | CSC |
| Generic Controller | Multi Command | Basic<br>Indicator, version 3<br>Multi Channel, version 4<br>The actuator Command Classes of at least 1 actuator Device Type | CSC, SSC, RPC, PC, NAS |

**4.4    From Z-Wave Plus to Z-Wave Plus v2 certification**

Table 7 indicates the recommended transitions from a Z-Wave Plus Device Type to a Z-Wave Plus v2 Device Type.

**Table 7, Equivalent Z-Wave Plus and Z-Wave Plus v2 Device Types**

| Z-Wave Plus DT(s) | Suggested Z-Wave Plus v2 DT(s) | Z-Wave Plus DT(s) | Suggested Z-Wave Plus v2 DT(s) |
|---|---|---|---|
| On/Off Power Switch Power Strip Valve – Open/close Irrigation control | Binary Switch | Remote Control – Multi purpose Remote control – Simple Wall controller | Generic Controller Central Scene |
| Siren | Binary Switch Sound Switch | Sub Energy Meter Whole Home Meter | Meter Sensor |
| Door Lock – Keypad Lockbox | Lock | Gateway Central Controller | Gateway |
| Light Dimmer Switch Fan Switch | Multilevel Switch | Thermostat – HVAC Thermostat – Setback | Thermostat |
| Set Top box TV Sub System Controller | Gateway Generic Controller | Remote control -AV | Generic Controller |
| | | Window Covering | Window Covering |

The following Device Types are unchanged and have the same equivalent Device Type in the Z-Wave Plus v2 certification program:

- Sensor - Notification
- Sensor - Multilevel
- AV Control Point
- Sound Switch
- Barrier Operator
- Entry Control keypad
- Repeater

The following Device Type is discontinued:

- Display - Simple

---

### 4.5    Actuator supporting types

### 4.5.1    Lock DT

The Lock Device Type is intended for nodes implementing a lock mechanism with optional handles. It can be a door lock, a lockbox as well as a safe.

#### 4.5.1.1    Generic and Specific Device Class

DT:01.11.0001.1    The Lock Device Type MUST use the following Device Classes:

- GENERIC_TYPE_ENTRY_CONTROL (0x40)
- SPECIFIC_TYPE_DOOR_LOCK (0x01)

#### 4.5.1.2    S2 Security Classes

DT:01.11.0002.1    The Root Device MUST request Access Control Security Class if it (or any End Point) uses this Device Type.

#### 4.5.1.3    Mandatory Command Classes

DT:01.11.0003.1    The Lock MUST support the following Command Classes:

- Door Lock, version 4
- Basic, version 2
- Security 0 (S0)


Recommended optional command classes for advanced applications:

- User Code
- Entry Control
- Generic Schedule
- Authentication
- Authentication Media Write


#### 4.5.1.4    Basic Command Class Requirements

DT:01.11.0004.1    The Basic Command Class MUST be mapped according to Table 8.

**Table 8, Lock Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Door Lock Operation Set (Door Lock Mode) |
| Basic Report (Current Value = 0x00) | Door Lock Operation Report (Door Lock Mode = 0x00) |
| Basic Report (Current Value = 0xFF) | Door Lock Operation Report (Door Lock Mode > 0x00) |

### 4.5.2    Motorized Barrier DT

The Motorized Barrier Device Type is intended for barriers, gates or garage doors devices.

#### 4.5.2.1    Generic and Specific Device Class

DT:02.11.0001.1    The Motorized Barrier Device Type MUST use the following Generic Device Class:

- GENERIC_TYPE_ENTRY_CONTROL (0x40)

DT:02.11.0002.1    The Motorized Barrier Device Type MUST use one of the following Specific Device Classes based on its capabilities within the Barrier Operator Command Class:

- SPECIFIC_TYPE_SECURE_GATE (0x06) if it can both open and close
- SPECIFIC_TYPE_SECURE_BARRIER_OPEN_ONLY (0x08) if it can open only
- SPECIFIC_TYPE_SECURE_BARRIER_CLOSE_ONLY (0x09) if it can close only

#### 4.5.2.2    S2 Security Classes

DT:02.11.0003.1    The Root Device MUST request Access Control Security Class if it (or any End Point) uses this Device Type.

#### 4.5.2.3    Mandatory Command Classes support

DT:02.11.0004.1    The Motorized Barrier Devices MUST support the following Command Classes:

- Barrier Operator
- Notification, version 8
- Basic, version 2
- Security 0 (S0)

#### 4.5.2.4    Basic Command Class Requirements

DT:02.11.0005.1    The Basic Command Class MUST be mapped according to Table 9.

**Table 9, Motorized Barrier Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Barrier Operator Set (Target Value) |
| Basic Report (Current Value = 0x00) | Barrier Operator Report (State = 0x00) |
| Basic Report (Current Value = 0xFF) | Barrier Operator Report (State > 0x00) |

### 4.5.3    Color Switch DT

The Color Switch Device Type is intended for a lighting product having the ability to change its color.

#### 4.5.3.1    Generic and Specific Device Class

DT:03.11.0001.1    The Color Switch Device Type MUST use the following Generic Device Classes:

- GENERIC_TYPE_SWITCH_BINARY (0x10) if supporting Binary Switch
- GENERIC_TYPE_SWITCH_MULTILEVEL (0x11) if supporting Multilevel Switch

DT:03.11.0002.1    The Color Switch Device Type MUST use the following Specific Device Classes:

- SPECIFIC_TYPE_COLOR_TUNABLE_BINARY (0x02) if supporting Binary Switch
- SPECIFIC_TYPE_COLOR_TUNABLE_MULTILEVEL (0x02) if supporting Multilevel Switch

#### 4.5.3.2    Mandatory Command Classes

DT:03.11.0003.1    The Color Switch MUST support the following Command Classes:

- Color Switch, version 3
- Multilevel switch, version 4 or Binary Switch, version 2
- Basic, version 2

#### 4.5.3.3    Basic Command Class Requirements

DT:03.11.0004.1    The Basic Command Class MUST be mapped according to Table 10 if supporting the Binary Switch Command Class or Table 11 if supporting the Multilevel Switch Command Class.

**Table 10, Color Switch Device Type Basic mapping for Binary Switch**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Binary Switch Set (Target Value) |
| Basic Report (Current Value, Target Value, Duration) | Binary Switch Report (Current Value, Target Value, Duration) |

**Table 11, Color Switch Device Type Basic mapping for Multilevel Switch**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Multilevel Switch Set (Value) |
| Basic Report (Current Value, Target Value, Duration) | Multilevel Switch Report (Current Value, Target Value, Duration) |

#### 4.5.4    Window Covering DT

The Window Covering Device Type is intended for curtains or blinds allowing the end user to control the amount of light going through windows.

##### 4.5.4.1       Generic and Specific Device Class

DT:04.11.0001.1    The Window Covering Device Type MUST use the following Generic Device Classes:

- GENERIC_TYPE_SWITCH_MULTILEVEL (0x11)

DT:04.11.0002.1    The Window Covering Device Type MUST use one of the following Specific Device Classes based on its capabilities within the Window Covering Command Class:

- SPECIFIC_TYPE_CLASS_A_MOTOR_CONTROL (0x05) if no position/endpoint awareness
- SPECIFIC_TYPE_CLASS_B_MOTOR_CONTROL (0x06) if endpoint aware
- SPECIFIC_TYPE_CLASS_C_MOTOR_CONTROL (0x07) if position and endpoint aware

##### 4.5.4.2    Mandatory Command Classes

DT:04.11.0003.1    The Window Covering MUST support the following Command Classes:

- Window Covering, version 1
- Multilevel Switch, version 4 (MUST be redundant to Window Covering, i.e. actuating the same hardware)
- Basic, version 2

##### 4.5.4.3        Basic Command Class Considerations

DT:04.11.0004.1    The Basic Command Class MUST be mapped according to Table 12.

**Table 12, Window Covering Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value=0xFF) | Multilevel Switch Set (0xFF) if endpoint aware<br>Start level change(Up/down) if not endpoint aware |
| Basic Set (Value=0x00) | Multilevel Switch Set (0x00) if endpoint aware<br>Stop level change() if not endpoint aware |
| Basic Set (Value=0x01..0x63) | Multilevel Switch Set (0x01..0x63) if position aware<br>Start level change(Up/down) if not position aware |
| Basic Report (Current Value, Target Value, Duration) | Multilevel Switch Report (Current Value, Target Value, Duration)<br>Current Value and Target Value MUST be set to 0xFE if not position aware |

#### 4.5.5    Thermostat DT

The Thermostat Device Type is intended by thermostats that support set points and modes. It is typically used for all mainstream thermostats that can support e.g. Heating, Cooling and Fans.

##### 4.5.5.1    Generic and Specific Device Class

The Thermostat Device Type MUST use the following Device Classes:

DT:05.11.0001.1

- GENERIC_TYPE_THERMOSTAT (0x08)
- SPECIFIC_TYPE_THERMOSTAT_GENERAL_V2 (0x06)

##### 4.5.5.2    Mandatory Command Classes

DT:05.11.0002.1    The Thermostat MUST support the following Command Classes:

- Thermostat Mode, version 3
- Thermostat Set Point
- Basic, version 2

Recommended optional command classes:

- Multilevel Sensor, supporting Sensor Type 0x01 (temperature)
- Clock
- Schedule, version 4
- Thermostat Setback

As an alternative to supporting Clock, the node can also control:

- Time

##### 4.5.5.3    Basic Command Class Considerations

DT:05.11.0003.1    The Basic Command Class MUST be mapped according to Table 13.

**Table 13, Thermostat Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value=0xFF) | Thermostat Mode Set (Mode = 0x01, 0x02 or 0x03) |
| Basic Set (Value=0x00) | Thermostat Mode Set (Mode = 0x00, 0x0B, 0x0C or 0x0D) |
| Basic Report (Current Value = 0xFF) | Thermostat Mode Report (Mode = 0x01, 0x02 or 0x03) |
| Basic Report (Current Value = 0x00) | Thermostat Mode Report (Mode = 0x00, 0x0B, 0x0C or 0x0D) |

### 4.5.6    Sound Switch DT

The Sound Switch Device Type is intended for products with the ability to issue sound notifications with a pre-programmed sound inventory. It can be used for a doorbell, chime, siren, alarm clock or any device issuing sounds.

#### 4.5.6.1    Generic and Specific Device Class

DT:06.11.0001.1    The Sound Switch Device Type MUST use the following Device Classes:

- GENERIC_TYPE_AV_CONTROL_POINT (0x03)
- SPECIFIC_TYPE_SOUND_SWITCH (0x01)

#### 4.5.6.2    Mandatory Command Classes

DT:06.11.0002.1    The Sound Switch MUST support the following Command Classes:

- Sound Switch
- Basic, version 2

#### 4.5.6.3    Basic Command Class Considerations

DT:06.11.0003.1    The Basic Command Class MUST be mapped according to Table 14.

**Table 14, Sound Switch Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Sound Switch Tone Play Set (Tone Identifier) |
| Basic Report (Current Value = 0x00) | Sound Switch Tone Play Report (Tone Identifier = 0x00) |
| Basic Report (Current Value = 0xFF) | Sound Switch Tone Play Report (Tone Identifier > 0x00) |

### 4.5.7    AV Control Point DT

The AV Control Point Device Type is intended for products with the ability to receive IR codes. It can be a TV, DVD player or any multimedia device that can now be also controller via Z-Wave.

#### 4.5.7.1      Generic and Specific Device Class

DT:07.11.0001.1    The AV Control Point Device Type MUST use the following Device Classes:

- GENERIC_TYPE_AV_CONTROL_POINT (0x03)
- SPECIFIC_TYPE_NOT_USED (0x00)

#### 4.5.7.2      Mandatory Command Classes

DT:07.11.0002.1    The AV Control Point Device Type MUST support the following Command Classes:

- Simple AV Control
- Basic, version 2

#### 4.5.7.3      Basic Command Class Considerations

DT:07.11.0003.1    The Basic Command Class MUST be mapped according to Table 15.

**Table 15, AV Control Point Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Simple AV Set (Command). The associated AV Codes Commands to the values 0x00 and 0xFF chosen be the manufacturer MUST switch the node's main functionality On and Off. (such as play/pause or volume up/volume down) |
| Basic Report (Current Value) | None The reported value MAY indicate if the node's main functionality is On or Off. (such as play/paused) else current value SHOULD be set to 0x00. |

### 4.5.8    Multilevel Switch DT

The Multilevel Switch Device Type is intended for products that can be switched between more than 2 discrete levels or states, such a light dimmer, water valve or a fan.

#### 4.5.8.1      Generic and Specific Device Class

DT:08.11.0001.1    The Multilevel Switch Device Type MUST use the following Device Classes:

- GENERIC_TYPE_SWITCH_MULTILEVEL (0x11)
- SPECIFIC_TYPE_NOT_USED (0x00)

#### 4.5.8.2      Mandatory Command Classes

DT:08.11.0002.1    The Multilevel Switch Device Type MUST support the following Command Classes:

- Multilevel Switch, version 4
- Basic, version 2

#### 4.5.8.3      Basic Command Class Requirements

DT:08.11.0003.1    The Basic Command Class MUST be mapped according to Table 16.

**Table 16, Multilevel Switch Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Multilevel Switch Set (Value) |
| Basic Report (Current Value, Duration) | Multilevel Switch Report (Value, Duration). |

### 4.5.9    Binary Switch DT

The Binary Switch Device Type is intended for any actuator functionality that can only be switched between 2 states (On and Off). It can be a valve, a light switch, a plug-in module.

#### 4.5.9.1    Generic and Specific Device Class

DT:09.11.0001.1    The Binary Switch Device Type MUST use the following Device Classes:

- GENERIC_TYPE_SWITCH_BINARY (0x10)
- SPECIFIC_TYPE_NOT_USED (0x00)

#### 4.5.9.2    Mandatory Command Classes

DT:09.11.0002.1    The Binary Switch MUST support the following Command Classes:

- Binary Switch, version 2
- Basic, version 2

DT:09.12.0001.1    If the node can measure energy, water or gas consumption, it is RECOMMENDED to support:

- Meter, version 5

#### 4.5.9.3    Basic Command Class Requirements

DT:09.11.0003.1    The Basic Command Class MUST be mapped according to Table 17.

**Table 17, Binary Switch Device Type Basic mapping**

| Basic Command | Mapped Command |
|---|---|
| Basic Set (Value) | Binary Switch Set (Value) |
| Basic Report (Current Value, Duration) | Binary Switch Report (Value, Duration). |

### 4.6    Reporting supporting Device Types

#### 4.6.1    Entry Control Keypad DT

The Keypad Device Type is intended for keypads or authentication devices reporting user input to a controlling application.

##### 4.6.1.1    Generic and Specific Device Class

DT:11.11.0001.1    The Entry Control Keypad Device Type MUST use the following Device Classes:

- GENERIC_TYPE_ENTRY_CONTROL (0x40)
- SPECIFIC_TYPE_SECURE_KEYPAD (0x0B)

##### 4.6.1.2    S2 Security Classes

DT:11.11.0002.1    The Root Device MUST request Access Control Security Class if it (or any End Point) uses this Device Type.

##### 4.6.1.3    Mandatory Command Classes

DT:11.11.0003.1    The Entry Control Keypad MUST support the following Command Classes:

- Entry Control
- Security 0 (S0)

Recommended optional command classes:

- Indicator, version 3 (with other Indicator IDs than Identify)

##### 4.6.1.4    Basic Command Class Requirements

DT:11.11.0004.1    Basic Command Class MUST NOT be supported

### 4.6.2    Multilevel Sensor DT

The Multilevel Sensor Device Type is intended for sensor reporting instantaneous numerical readings or measurements.

#### 4.6.2.1    Generic and Specific Device Class

DT:12.11.0001.1   The Multilevel Sensor Device Type MUST use the following Device Classes:

- GENERIC_TYPE_SENSOR_MULTILEVEL (0x21)
- SPECIFIC_TYPE_ROUTING_MULTILEVEL_SENSOR (0x01)

#### 4.6.2.2    Mandatory Command Classes

DT:12.11.0002.1   The Multilevel Sensor MUST support the following Command Classes:

- Sensor Multilevel, version 11

DT:12.12.0001.1   If the node issues more than one command regularly, it is RECOMMENDED to control:

- Multi Command

#### 4.6.2.3    Basic Command Class Requirements

DT:12.11.0003.1   Basic Command Class MUST NOT be supported

### 4.6.3    Notification Sensor DT

The Notification Sensor Device Type is intended for sensors reporting events or local state changes.

#### 4.6.3.1      Generic and Specific Device Class

DT:13.11.0001.1    The Notification Sensor Device Type MUST use the following Device Classes:

- GENERIC_TYPE_SENSOR_NOTIFICATION (0x07)
- SPECIFIC_TYPE_NOTIFICATION_SENSOR (0x01)

#### 4.6.3.2      Mandatory Command Classes

DT:13.11.0002.1    The Notification Sensor MUST support the following Command Classes:

- Notification, version 8

DT:13.12.0001.1    If the node issues more than one command regularly, it is RECOMMENDED to control:

- Multi Command

#### 4.6.3.3      Basic Command Class Requirements

DT:13.11.0003.1    Basic Command Class MUST NOT be supported

### 4.6.4    Meter Sensor DT

The Meter Sensor Device Type is intended for sensors measuring cumulated values. The most typical application is an electricity meter, but it can also be used for sensor measuring gas or water consumption.

#### 4.6.4.1    Generic and Specific Device Class

DT:14.11.0001.1    The Meter Sensor Device Type MUST use the following Device Classes:

- GENERIC_TYPE_METER (0x31)
- SPECIFIC_TYPE_NOT_USED (0x00)

#### 4.6.4.2    Mandatory Command Classes

DT:14.11.0002.1    The Meter Sensor MUST support the following Command Classes:

- Meter, version 5

DT:14.12.0001.1    If the node issues more than one command regularly, it is RECOMMENDED to control:

- Multi Command

DT:14.12.0002.1    For advanced metering applications, it is RECOMMENDED to support the following command classes:

- Meter Table Monitor, version 2
- Meter Table Push Configuration
- Rate Table Monitor

#### 4.6.4.3    Basic Command Class Requirements

DT:14.11.0003.1    Basic Command Class MUST NOT be supported

### 4.6.5    Central Scene DT

The Central Scene Device Type is intended for nodes with buttons or GUI allowing to report user input/button press to a central application, which in turn will actuate or control other nodes.

This Device Type can be used for nodes such as wall switches or panels with a set of buttons. Such devices will send Scene Notifications to the Lifeline destination in order to trigger scenes.

#### 4.6.5.1      Generic and Specific Device Class

DT:15.11.0001.1    The Central Scene Device Type MUST use the following Device Classes:

- GENERIC_TYPE_WALL_CONTROLLER (0x18)
- SPECIFIC_TYPE_NOT_USED (0x00)

#### 4.6.5.2      Mandatory Command Classes

DT:15.11.0002.1    The Central Scene MUST support the following Command Classes:

- Central Scene, version 3

#### 4.6.5.3      Basic Command Class Considerations

DT:15.11.0003.1    Basic Command Class MUST NOT be supported.

#### 4.6.5.4    Recommended options

DT:15.12.0001.1    The Central Scene Device Type SHOULD implement controlling capabilities using Association Groups. It is RECOMMENDED to have a group issuing Basic Set Commands.

DT:15.12.0002.1    Multi Channel End Point SHOULD NOT implement this Device Type.

### 4.7     Other Device Types

#### 4.7.1     Repeater DT

The Repeater Device Type is intended for nodes being part of the network with no application functionalities. Such nodes help as Z-Wave repeaters and strengthen the network reliability.

##### 4.7.1.1     Role Type

DT:21.11.0001.1     The Repeater Device Type MUST use the AOS Role Type.

##### 4.7.1.2     Generic and Specific Device Class

DT:21.11.0002.1     The Repeater Device Type MUST use the following Device Classes:

- GENERIC_TYPE_REPEATER_SLAVE (0x0F)
- SPECIFIC_TYPE_REPEATER_SLAVE (0x01)

##### 4.7.1.3     Mandatory Command Classes

DT:21.11.0003.1     The Repeater Device Type MUST NOT support any other command class than the list defined in 3.2.1.

DT:21.11.0004.1     The Repeater Device Type MUST NOT control any Command Class.

##### 4.7.1.4     Basic Command Class Requirements

DT:21.11.0005.1     Basic Command Class MUST NOT be supported

### 4.7.2    IR Repeater DT

The IR Repeater Device Type is intended for nodes having the ability to read or repeat IR signals. They do not have any other application functionality. Such repeater nodes also help as Z-Wave repeaters and strengthen the network reliability.

#### 4.7.2.1    Role Type

The IR Repeater Device Type MUST use the AOS Role Type.

DT:22.11.0001.1

#### 4.7.2.2    Generic and Specific Device Class

The Repeater Device Type MUST use the following Device Classes:

DT:22.11.0002.1

- GENERIC_TYPE_REPEATER_SLAVE (0x0F)
- SPECIFIC_TYPE_IR_REPEATER (0x03)

#### 4.7.2.3    Mandatory Command Classes

The IR Repeater MUST support the following Command Classes:

DT:22.11.0003.1

- IR Repeater, version 1

DT:22.11.0004.1    The IR Repeater Device Type MUST NOT support any additional Command Class (other than the mandatory list above and the list defined in 3.2.1).

DT:22.11.0005.1    The IR Repeater Device Type MUST NOT control any Command Class.

#### 4.7.2.4    Basic Command Class Requirements

Basic Command Class MUST NOT be supported

DT:22.11.0006.1

### 4.8    Controlling Device Types

### 4.8.1    Gateway DT

DT:31.13.0002.1

The Gateway Device Type is intended for all gateway controllers that provide access in and potentially out of the Z-Wave network as well as extensive controlling capabilities over Z-Wave. This DT MAY provide transparent access for all types of IP Packets between several network technologies.

#### 4.8.1.1    Role Type

DT:31.11.0001.1

The Gateway Device Type MUST use the CSC Role Type.

#### 4.8.1.2    Generic and Specific Device Class

DT:31.11.0002.1

The Gateway Device Type MUST use the following Device Classes:

- GENERIC_TYPE_STATIC_CONTROLLER (0x02)
- SPECIFIC_TYPE_GATEWAY (0x07)

#### 4.8.1.3    S2 Security Classes

DT:31.11.0003.1

If bootstrapped in another network, it MUST request all S2 Security Classes. (S2 Access Control, S2 Authenticated and S2 Unauthenticated)

#### 4.8.1.4    Mandatory Command Classes

DT:31.11.0004.1

The Gateway MUST support the following Command Classes in a Z-Wave network:

- CRC-16 Encapsulation
- Inclusion Controller
- Multi Command
- Security 0 (S0)
- Time

DT:31.12.0005.1

The Gateway SHOULD support Node Provisioning Command Class in a Z-Wave network.

DT:31.11.0005.2

The Gateway MUST support the following Command Classes in an IP network:

- Z/IP, version 4

DT:31.12.0001.1

If the Z/IP Gateway relies on a Z/IP client to provide application functionalities, it SHOULD support the following Command Classes in an IP network:

- Z/IP Gateway
- Z/IP ND
- Z/IP Portal
- Mailbox
- Network Management Proxy, version 2
- Network Management Inclusion, version 3
- Network Management Basic, version 2

---

DT:31.11.0006.2     The Gateway MUST control the following Command Classes in a Z-Wave network:

- Anti-Theft Unlock or Anti-Theft, version 3 (refer to 3.7.1)
- Association, version 2
- Association Group Information, version 3
- Basic, version 2
- Central Scene, version 3
- CRC-16 Encapsulation
- Firmware Update Meta Data, version 5
- Indicator, version 3
- Meter, version 5
- Multi Channel, version 4
- Multi Channel Association, version 3
- Multilevel Sensor, version 11
- Notification, version 8
- Security 0 (S0)
- Security 2 (S2)
- Version, version 2
- Wake up, version 2

DT:31.13.0001.1     A Gateway Device Type MAY provide a subset of its capabilities (supported and controlled command classes) if it has the Secondary Controller Role in a network.

### 4.8.1.5     Recommended options

DT:31.12.0002.1     A Gateway Device Type SHOULD support reading and interpreting data form legacy sensors supporting the following Command Classes:

- Alarm Sensor
- Binary Sensor
- Alarm/Notification, version 1.
- Multilevel Sensor
- Meter

DT:31.12.0003.1     In order to achieve this, it is RECOMMENDED to implement a database of known devices.

DT:31.12.0004.2     A Gateway controller SHOULD control the Command Classes from all actuator Device Types (Table 5).

### 4.8.1.6     Basic Command Considerations

DT:31.11.0007.1     Basic Command Class MUST NOT be supported.

#### 4.8.2    Generic Controller DT

The Generic Controller Device Type is intended for all more constrained or simple controllers allowing users to make basic use of the Z-Wave network and controlling a pre-defined set of actuator nodes as well as unknown actuator nodes.

##### 4.8.2.1    Generic and Specific Device Class

DT:32.11.0001.1    The Generic Controller Device Type MUST use the following Device Classes:

- GENERIC_TYPE_GENERIC_CONTROLLER (0x01)
- SPECIFIC_TYPE_NOT_USED (0x00)

##### 4.8.2.2    Mandatory Command Classes

DT:32.11.0002.1    The Generic Controller MUST support the following Command Classes:

- Multi Command

DT:32.11.0003.2    The Generic Controller MUST control the following Command Classes:

- Anti-Theft Unlock or Anti-Theft, version 3 (refer to 3.7.1)
- Basic
- Indicator, version 3
- The mandatory actuator Command Classes of at least one actuator Device Type
- Version, version 2
- Wake up, version 2

##### 4.8.2.3    Recommended options

DT:32.12.0001.2    A Generic Controller SHOULD control Command Classes from as many actuator Device Types as possible.

##### 4.8.2.4    Basic Command Considerations

DT:32.11.0004.1    Basic Command Class MUST NOT be supported.

## 5        References

[1]    IETF RFC 2119, Key words for use in RFC's to Indicate Requirement Levels, http://tools.ietf.org/pdf/rfc2119.pdf

[2]    Silicon Labs, SDS11846, Z-Wave Plus Role Types Specification.

[3]    Silicon Labs, SDS13781, Z-Wave Application Command Class Specification.

[4]    Silicon Labs, SDS13782, Z-Wave Management Command Class Specification.

[5]    Silicon Labs, SDS13783, Z-Wave Transport-Encapsulation Command Class Specification.

[6]    Silicon Labs, SDS13784, Z-Wave Network-Protocol Command Class Specification.

[7]    Silicon Labs, SDS14223, Z-Wave Command Class Control Specification

[8]    Silicon Labs, SDS14222, Association Command Class, list of mandatory commands for the Lifeline Association Group

[9]    Silicon Labs, SDS13937, Node Provisioning QR Code Format (S2, Smart Start)

[10]   Silicon Labs, SDS13944, Node Provisioning Information Type Registry (QR code, Z/IP Gateway, Smart Start)

[11]   Silicon Labs, SDS13548, List of defined Z-Wave Command Classes

[12]   Z-Wave Alliance, Z-Wave Security 2 (S2) Product Labeling Requirements

[13]   Silicon Labs, SDS14622, Anti-Theft Command Class, list of assigned Locking Entity IDs