Software Design Specification

Node Provisioning QR Code Format (S2, Smart Start)

Description:	Format for representing S2 DSK as well as various product properties in QR codes
Written By:	Z-Wave Alliance, Inc.
Date:	18 March, 2021
Reviewed By:	SWG
Restrictions:	Public

Approved by:
Z-Wave Alliance Board of Directors

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20170411	ABR	ALL	First revision
3	20170628	NOBRIOT	3.1.1 3.3	Added TLV representation paragraph Updated the example with the new combined Type/Critical values
4	20170811	ABR	3.3	Updated examples
-	20170911	ABR	Some	Further clarifications to the Type/Critical field encoding
5	20180305	BBR	All	Added Silicon Labs template
6	20180903	NOBRIOT	3.2	Changed the minimum QR Code size

Table of Contents

Table of Tables

1 ABBREVIATIONS

Abbreviation	Explanation

2 INTRODUCTION

The S2 specification defines a human-readable DSK string format and requires that a QR code representation is also provided. This document presents the QR code format for S2 and Smart Start devices.

The QR code format supports basic S2 devices as well as Smart Start enabled devices applications; allowing for efficient warehouse logistics and portal-centric commissioning via connected gateways as well as production bundled kits.

The Z-Wave QR code format is an improved variant of the format originally presented in the Z-Wave Security 2 specification. The format allows for more compact QR codes.
The table below shows the original S2 QR code and a Smart Start QR code using the improved format of this specification. The first-generation S2 code only holds the DSK. The Smart Start code further holds information for device provisioning.

Gen 1 (S2)	Gen 2 (S2 & Smart Start)

3 REQUIREMENTS

This chapter presents requirements to the format of the Z-Wave S2 and Smart Start QR code.

3.1 QR code format

The following requirements apply to the Z-Wave QR code.

The QR code MUST NOT contain other characters than the decimal digits 0..9.
The QR code MUST contain the all fields until and including the DSK.
The QR code MUST contain TLV types 0 and 1. Refer to [2].
The QR code MAY contain additional TLV blocks. Refer to [2].
The QR code MUST comply with Table 1.
The QR code MUST be encoded as QR Code Type “Text”.
The QR code SHOULD be encoded with QR Code Error Correction Level “L”.

The Version field defined in Table 1 should not be confused with the QR Version referenced in Table 2. The QR Version primarily defines the number of pixels in the QR code.

The mandatory TLV types ensure that S2 devices produced prior to the official release of the Smart Start technology can be firmware upgraded to perform as native Smart Start devices.

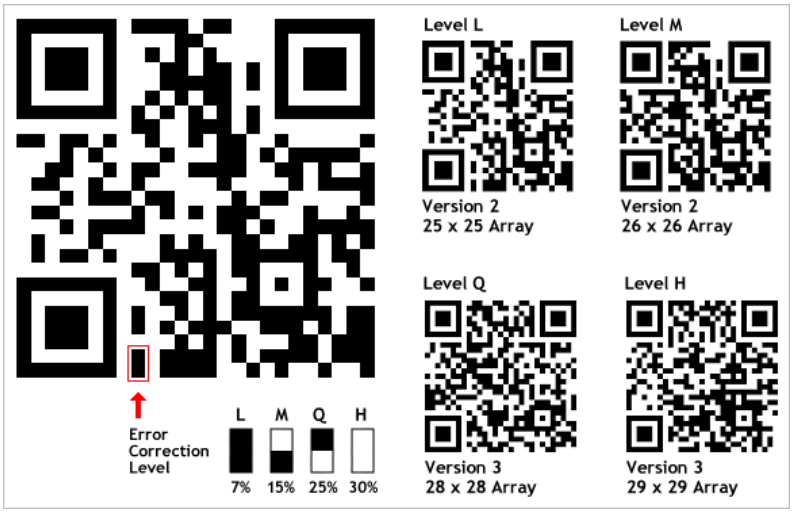

Table 1, Z-Wave QR Code format

Field name	Dec digit blocksize	Description
Lead-in	2	Must be 90, representing ASCII character “Z”. Allows for an initial detection of Z-Wave QR codes. An application MUST also validate the checksum before evaluating other fields.
Version	2	MUST be set to 0 for S2-only devices. MUST be set to 1 for Smart Start enabled devices.
Checksum	5	This field allows an application to ensure that the actual QR code does indeed contain valid Z-Wave Smart Start data. It serves as a simple checksum and has no cryptographic purpose. This field MUST advertise a 5 digit decimal value representing the first two bytes of the SHA-1 hash calculated over all digits following this field. When calculating the SHA-1 value, the digits MUST be treated as ASCII characters. Example: If the string "0123456789" follows after the Checksum field, the first two bytes of the SHA-1 value are "87AC". The Checksum value 0x87AC in decimal representation is 34732.
Requested Keys	3	This field carries an 8 bit value as 3 decimal digits. The value MUST reflect the Requested Keys byte as defined by the S2 specification.
DSK	5 (8 blocks)	This field MUST carry a full 16 byte DSK as defined by the S2 specification. The field MUST be organized as 8 groups of 5 decimal digits without any delimiter characters. If any data follows the DSK, it MUST be a TypeCritical field.
TypeCritical (T)	2	This field advertises the type of data carried in this TLV block and the criticality of this information. The Type MUST be encoded in bits 7..1. The Critical flag MUST be encoded in bit 0. Refer to section 3.1.1 and [2]. A Length field MUST follow this field.
Len (L)	2	This field MUST advertise the number of decimal digits carried in the Value field of this TLV block. Refer to 3.1.1 and [2]. A Value field MUST follow this field.
Value (V)	(depends on type)	Data complying with the advertised type and length. Refer to 3.1.1 and [2]. Another TLV block MAY follow this field. If any data follows the Value field, it MUST be a TypeCritical field

3.1.1 QR Code TLV representation

The TLV fields indicated in [2] MUST be mapped into the QR Code format described below.

TypeCritical (2 decimal digits)

When carried in a QR code, the Critical flag and the Type field MUST be combined into one 8-bit value, where the Type is mapped to bits 7..1 and the Critical flag is mapped to bit 0.
That combined value MUST be in the range 0..99.

Length (2 decimal digits)

In QR Codes, the length MUST indicate the number of decimal digits used to represent the Value field.

Value (variable length)

In QR Codes, 8 bits value fields with allowed values in the range 0..99 MUST be represented using decimal representation with 2 decimal digits.

In QR Codes, 8 bits value fields with allowed values higher than 99 MUST be represented using decimal representation with 3 decimal digits.

In QR Codes, 16 bits value fields MUST be represented using decimal representation with 5 decimal digits.

In QR Codes, multiple of 16 bits value fields MUST be represented using decimal representation with N blocks of 5 decimal digits each representing 16 bits.

3.2 S2 QR code presentation requirements

Guidelines for formatting QR Codes are given in [3], it is RECOMMENDED that QR codes are at least 10x10mm.

Printing technology may be the constraining factor when printing on plastics, e.g. a light bulb, causing QR code edges to be slightly blurred. In that case, the QR code SHOULD be made slightly bigger.

The combination of different TLV blocks may cause the information density to grow. A QR code grows in significant steps. Assuming that a low level of data correction and that numeric text encoding is used, the following applies.

Table 2, QR Code block sizes

QR Version	Pixels	Decimal digits	Sample	Comment
1	21x21	1..41		*(too small for S2 and Smart Start)*
2	25x25	42..77		*(too small for S2 and Smart Start)*
3	29x29	78..127		A basic Smart Start code occupies 90 digits.
4	33x33	128..187		A Smart Start code with UUID16 occupies 134 digits

Most Smart Start devices will fit into a QR Version 3 QR code while the addition of significant amounts of data, such as a UUID16 field, may necessitate QR Version 4.

An S2 QR code has the same size as a basic Smart Start QR code.

3.3 QR code examples

3.3.1 Acme Light Dimmer

A Smart Start device advertises Z-Wave QR code version 1.

Field name	Decimal	Dec digit block size	Comment
Lead-in	90	2	ASCII character “Z”
Version	01	2	Version 1: SmartStart device
Checksum	32782	5	First 16 bits of SHA-1; covering all following bytes. 16 bit decimal representation.
Requested Keys	003	3	Requesting [S2 Unauthenticated] + [S2 Authenticated] keys. 8 bit decimal representation.
DSK	51525 35455 41424 34445 31323 33435 21222 32425	5 (8 blocks)	S2 DSK. 16 bit decimal block representation.
TypeCritical	00	2	ProductType, 16 bit decimal representation.
Len	10	2	Number of digits in ProductType
ProductType	04353 01537	5 (2 blocks)	QRProductType: Z-Wave Device Type = [Light Dimmer Switch] 0x11.0x01 = 04353 Z-Wave Installer Icon Type = LIGHT_DIMMER_SWITCH_PLUGIN = 0x0601 = 01537 16 bit decimal block representation.
TypeCritical	02	2	ProductID, 16 bit decimal representation.
Len	20	2	Number of digits in ProductID
ProductID	65520 00100 00003 00578	5 (4 blocks)	QRProductID: Z-Wave Manufacturer ID = Acme Corp = 0xFFF0 = 65520 Z-Wave Product Type = 00100 (0x0064) Z-Wave Product ID = 00003 Z-Wave Application Version = 0x02.0x42 = 00578 16 bit decimal block representation.

The checksum is calculated over all fields following the checksum field, according to section 3.1.

String to be encoded in QR code:

900132782003515253545541424344453132333435212223242500100435301537022065520001000000300578

(QR Code Error Correction Level “L”)

3.3.2 Oscorp Door Lock w. UUID

A Smart Start device advertises Z-Wave QR code version 1.

In addition to basic Smart Start QR code fields, this QR code also carries a 16 byte UUID field.

Field name	Deci-mal	Dec digit block size	Comment
Lead-in	90	2	ASCII character “Z”
Version	01	2	Version 1: Smart Start enabled
Checksum	34623	5	First 16 bits of SHA-1; covering all following bytes. 16 bit decimal representation.
Requested Keys	007	3	Requesting [S2 Unauthenticated] + [S2 Authenticated] keys. 8 bit decimal representation.
DSK	51525 35455 41424 34445 31323 33435 21222 32425	5 (8 blocks)	S2 DSK. 16 bit decimal block representation.
TypeCritical	00	2	ProductType, 16 bit decimal representation.
Len	10	2	Number of digits in ProductType
ProductType	16387 00768	5 (2 blocks)	QR ProductType: Z-Wave Device Type = [Door Lock - Keypad] 0x40.0x03 = 16387 Z-Wave Installer Icon Type = DOOR_LOCK_KEYPAD = 0x0300 = 00768 16 bit decimal block representation.
TypeCritical	02	2	ProductID, 16 bit decimal representation.
Len	20	2	Number of digits in ProductID

ProductID	65521 01000 00017 00288	5 (4 blocks)	QR ProductID: Z-Wave Manufacturer ID = Oscorp Inc = 0xFFF1 = 65521 Z-Wave Product Type = 01000 (0x03E8) Z-Wave Product ID = 00017 (0x0011) Z-Wave Application Version = 0x01.0x20 = 00288 16 bit decimal block representation.
TypeCritical	06	2	UUID16, 16 bytes in 16 bit decimal representation.
Len	42	2	Number of digits in UUID16
UUID16	00 21222 32425 41424 34445 11121 31415 31323 33435	(2 digits followed by 8 blocks of 5 digits)	QR UUID16: Presentation Format = 00 UUID = …

The checksum is calculated over all fields following the checksum field, according to section 3.1.

String to be encoded in QR code:

900134623007515253545541424344453132333435212223242500101638700768022065521010000001700288064200212223242541424344451112131415313233343 5

(QR Code Error Correction Level “L”)

3.3.3 Acme Light Dimmer (S2 only – not SmartStart)

An S2 device advertises a basic Smart Start QR code but the Z-Wave QR code version field is set to 0.

Field name	Decimal	Dec digit block size	Comment
Lead-in	90	2	ASCII character “Z”
Version	00	2	Version 0: S2 device
Checksum	32782	5	First 16 bits of SHA-1; covering all following bytes. 16 bit decimal representation.
Requested Keys	003	3	Requesting [S2 Unauthenticated] + [S2 Authenticated] keys. 8 bit decimal representation.

DSK	51525 35455 41424 34445 31323 33435 21222 32425	5 (8 blocks)	S2 DSK. 16 bit decimal block representation.
TypeCritical	00	2	ProductType, 16 bit decimal representation.
Len	10	2	Number of digits in ProductType
ProductType	04353 01537	5 (2 blocks)	QRProductType: Z-Wave Device Type = [Light Dimmer Switch] 0x11.0x01 = 04353 Z-Wave Installer Icon Type = LIGHT_DIMMER_SWITCH_PLUGIN = 0x0601 = 01537 16 bit decimal block representation.
TypeCritical	02	2	ProductID, 16 bit decimal representation.
Len	20	2	Number of digits in ProductID
ProductID	65520 00100 00003 00578	5 (4 blocks)	QRProductID: Z-Wave Manufacturer ID = Acme Corp = 0xFFF0 = 65520 Z-Wave Product Type = 00100 (0x0064) Z-Wave Product ID = 00003 Z-Wave Application Version = 0x02.0x42 = 00578 16 bit decimal block representation.

The checksum is calculated over all fields following the checksum field, according to section 3.1.

String to be encoded in QR code:

900032782003515253545541424344453132333435212223242500100435301537022065520001000000300578

(QR Code Error Correction Level “L”)

REFERENCES

[1] Silicon Labs, SDS13574, Security 2 Command Class Specification

[2] Silicon Labs, SDS13944, Smart Start Provisioning Information Type Registry

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

[4]