ARM secure micros USN format

Ref: SPEC98H06
Revision B

MAXIM INTEGRATED– CONFIDENTIALITY

Revision History

Rev A	2015-Apr-14	1st release
Rev B	2016-Jan-21	2nd release: MAX32560 added

Disclaimer

To our valued customers

We constantly strive to improve the quality of all our products and documentation. We have spent an exceptional amount of time to ensure that this document is correct. However, we realize that we may have missed a few things. If you find any information that is missing or appears in error, please contact us via www.maximintegrated.com/support. We appreciate your assistance in making this a better document.

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Maxim Integrated Office.

Maxim Integrated Technologies may only be used in life-support devices or systems with the express written approval of Maxim Integrated, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Table of Contents

References

[1] AN10S09: USIP Serial Number Format. Rev G. Jan-2008

[2] SPEC21H32: MAX32590 USN Format. RevC. May-2013

1 USN format

This document presents the format of the Unique Serial Number (USN) to be embedded in any ARM secure micro. The USN format is based on the MAX32590 USN format (see [2]) and USIP USN format (described in [1]).

1.1 Requirements

- The USN shall be unique for every chip,
- The USN format shall be the same for every chip platform and model
- There shall not be any (reasonable) risk of S/N shortage,
- Any corruption or unintended modification shall be detected,
- The USN shall contains every information needed for chip tracking,
- The USN should not be modified once written,
- The USN shall allow multiple wafer sort and final test facilities
- The USN shall allow flexible production capacity management.
    - Lot split on different testers during wafer sort and final test must be possible
    - Allocation of several testers to test the same product must be possible
- It shall be possible for the tester to generate the USN on the fly during electrical wafer sort i.e. right before the die is tested

1.2 Format description

The 13-byte (104-bit) USN format is described in the Figure 1.

Byte#	length	Description
0	1	Die type and revision
1	1	Family code
2..5	4	Foundry batch information
6..8	3	Die position on the wafer: • $byte^{6}_{0..7}$ | $byte^{7}_{0..3}$:12 bits for position Y • $byte^{7}_{4..7}$ | $byte^{8}_{0..7}$:12 bits for position X
9..10	2	16 bits: • $byte^{9}_{0..4}$:5 bits:Year: 2010..2041 • $byte^{9}_{5..6}$:2 bits: wafer fab id • $byte^{9}_{7}$| $byte^{10}_{0}$:2 bits: wafer sort id ***(optional)***; value=00 • $byte^{10}_{1..6}$: 6 bits: wafer value • $byte^{10}_{7}$:1 bit: RFU;value=0
11..12	2	Check value bytes

Figure 1 USN format

- Fields description:
  - the “die type and revision” byte follows specifications provided by the Operations manager. Current examples are the following:
    - MAX32590 B2 is 0xB2
    - MAX32590 B3 is 0xB3
    - MAX32590 B4 is 0xB4
    - MAX32550 A3 is 0xA3
    - MAX32555 A1 is 0xA1
  - the family code is related to customer-specific programming or configuration: it is worthwhile this value be written at the end of the final test, avoiding “tagging” too early chips for customers,
    - MAX32590 family code is 0x59
    - MAX32550 family code is 0x67
    - MAX32555 family code is 0x68
    - MAX32560 family code is 0x69
  - foundry batch information: this contains the genuine information about batch value, coming from the foundry: it is converted into 4 bytes,
  - position on the wafer: this provides the X-Y location on the wafer (X and Y values ranges in 0..4095),
  - Year: the year value ranges from 2010 to 2041 (value 0 matches 2010), provided by the foundry batch info c_3.
  - Wafer fab id: this indicates on two bits the reference of the foundry fab
  - Wafer sort id: this indicates on two bits the reference of the wafer sort facility: this field is **optional**: in that case, the bits are null.
  - Wafer value:
    - The wafer sort facility uses physical wafer number (read by OCR for instance). The physical wafer number only is recorded.
  - the check value is computed by using the AES algorithm, in ECB mode. The check value operation is:

    Compute (concatenate) $D = USN_{0..10} \mid 00\ 00\ 00\ 00\ 00$,

    Compute $E = AES_{CVK}(D)$, where CVK is the null key,

    Truncate E to the first two bytes: $CV = E_{1..0}$

1.3 Example

Consider the USN: `B5590011180515D0020430C834`

- Die Rev: 0xB5
- Family code: 0x59 (MAX32590)
- Wafer : 24=0x18
- X die=45=0x02d
- Y Die : 21=0x15

- Year : 2014
    - CRC bytes are:

AES_{00000}(b5590011180515d00204300000000000)=34c84b68130f09f1c8dbfec5f861dded

So, CRC bytes are 0x34 and 0xC8

2 USN address location

- For MAX32590, the USN is stored in the Maxim OTP area, at offset `0x10`.
- For MAX32550, the USN is stored in the Maxim OTP area, at offset `0x00`

3 USN generation tool

The USN is generated using a tool provided and maintained by Maxim.

4 USN verification tool

The USN can be verified and its fields described using tool provided and maintained by Maxim.

Maxim Integrated

http://www.maximintegrated.ccom

for support, goto www.maximintegrated.com/support