



# ST1331, ST1333 ST1353

## 6-Contact Memory Card IC 272-bit EEPROM with Advanced Security Mechanisms

DATA BRIEFING

- 5 V Single Supply Voltage
- Counting Capability (two options)
  - up to 32767 ( $8^5 - 1$ )
  - 8 times reloadable, up to 4095 ( $8^4 - 1$ )
- Active Authentication Function (ST1333/1353)
- Cipher Block Chaining Function (ST1353)
- Memory Divided into :
  - 16 bits of Circuit Identification
  - 48 bits of Card Identification
  - 40 bits of Count Data
  - 16 bits for Validation Certificate
  - 24 bits of Transport Code
  - 64 bits of Issuer Data (ST1331) or Authentication Secret Key (ST1333/1353)
  - 32 bits of Anti-tearing Flags (optional)
  - 56 bits of User data (optionally not erasable)
- 1 Million Erase/Write Cycle (minimum)
- 10 Year Data Retention (minimum)
- 3.5 ms Programming Time at 5 V (typical)
- 500  $\mu$ A Supply Current at 5 V (typical)
- 250  $\mu$ A Stand-by Current at 5 V (typical)

### DESCRIPTION

The members of the ST1331/1333/1353 family are principally designed for use in prepaid Phonocard applications. Each is a 272-bit EEPROM device, with associated security logic and special fuses to control memory access. The memory is arranged as a matrix of 34 x 8 cells, accessed in a serial bit-wise fashion for reading and programming, and in

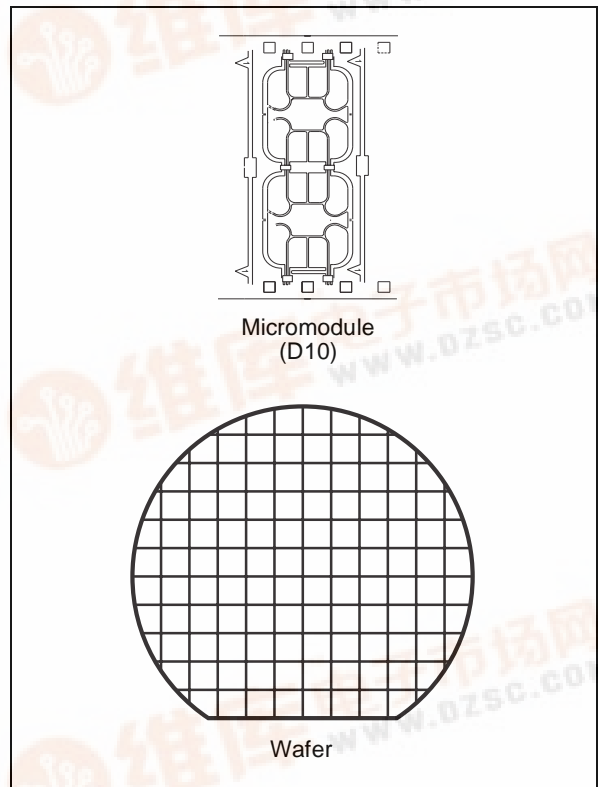


Figure 1. Logic Diagram

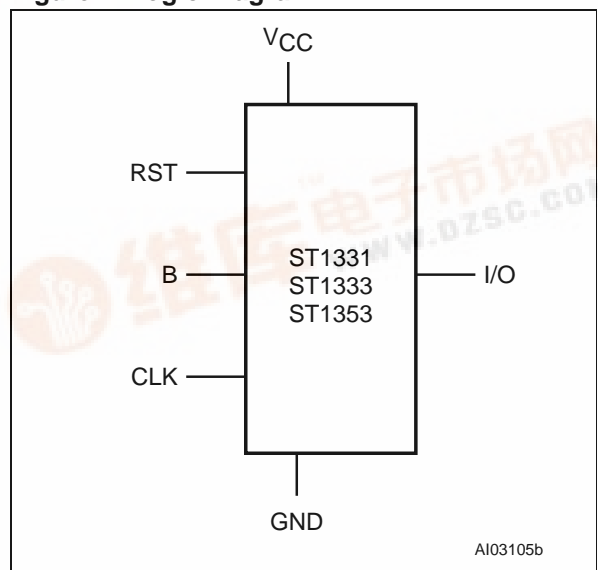
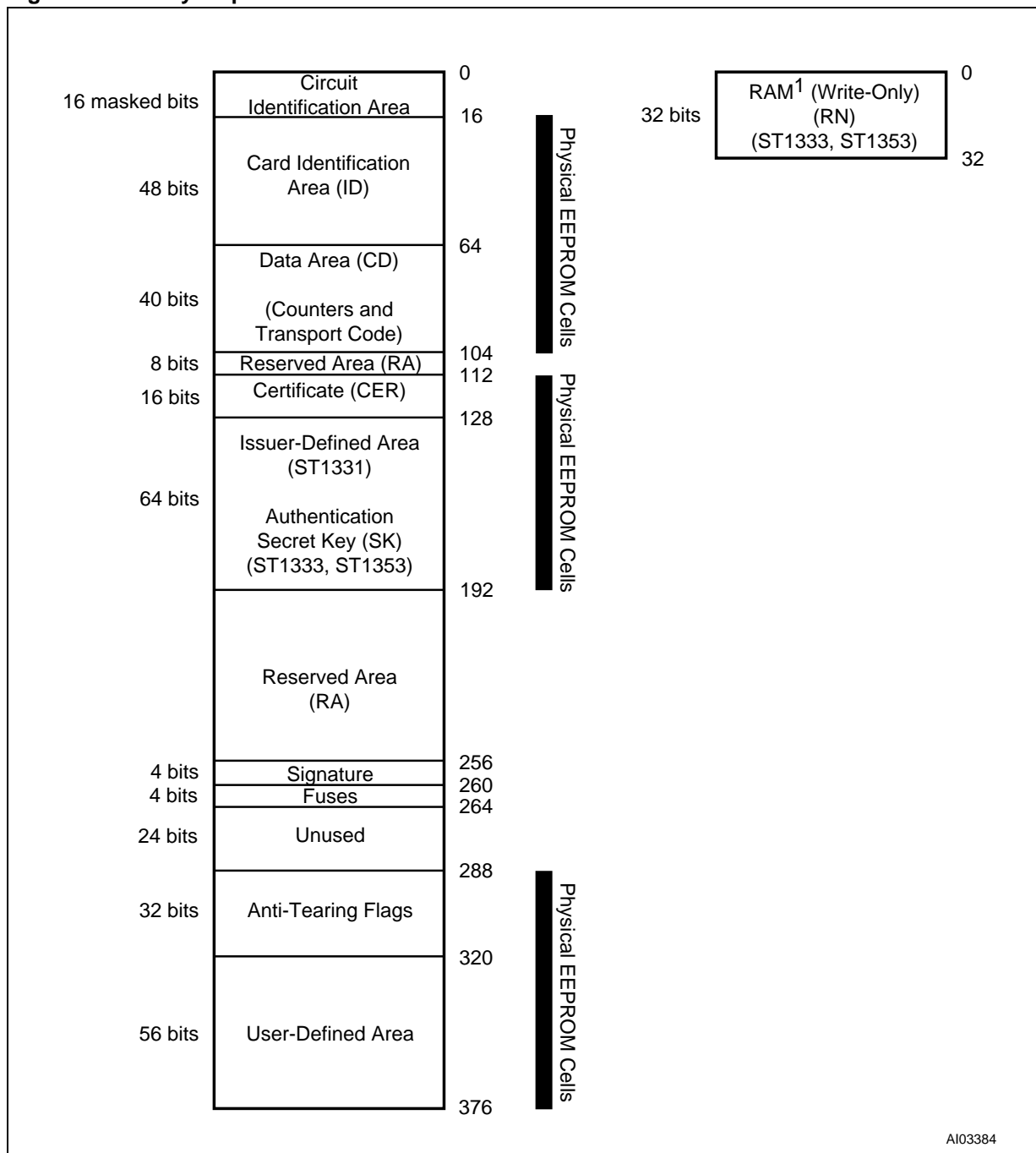


Table 1. Signal Names

CLK	Clock
RST	Function code
B	
I/O	Data Input / Output
VCC	Supply Voltage
GND	Ground



Figure 2. Memory Map



Note: 1. The write-only RAM area (RN) is applicable only for the User Configuration.

a byte-wise fashion for internal erasing. An on-chip address counter provides an internal address space of up to 512 bits.

Each member of the ST1331/1333/1353 family has an identification data area, unit-counters (with an anti-tearing mechanism for reliable usage in open readers), a post validation certificate, an

issuer area (ST1331) or an authentication secret key area (ST1333/1353), and a user area. This is summarized in Figure 2.

The validation certificate allows the recognition of the device by the appropriate security module.

The anti-tearing mechanism guards against extra, spurious count signals being executed when the

card is unexpectedly extracted, while an operation is underway, in an open reader.

**EXTERNAL COMMANDS**

The device uses six contacts: V<sub>CC</sub>, GND, I/O, CLK, RST, B. Four commands distinct can be composed using these external pins:

- RESET: to reset the internal address register to 000d
- READ: to increment the internal address register and read the data bit at the new address
- COMPARE: to allow comparison of the presented code against the internal transport code
- PROGRAM: to program the bit at the current address

**CONFIGURATIONS**

The device works in two distinct configurations:

- Issuer Configuration: for the card manufacturer. Customized data can be written to the chip, to initialize it before release to the end user.
- User Configuration: for use by the end user of the card, but with restricted access.

**OPTIONS**

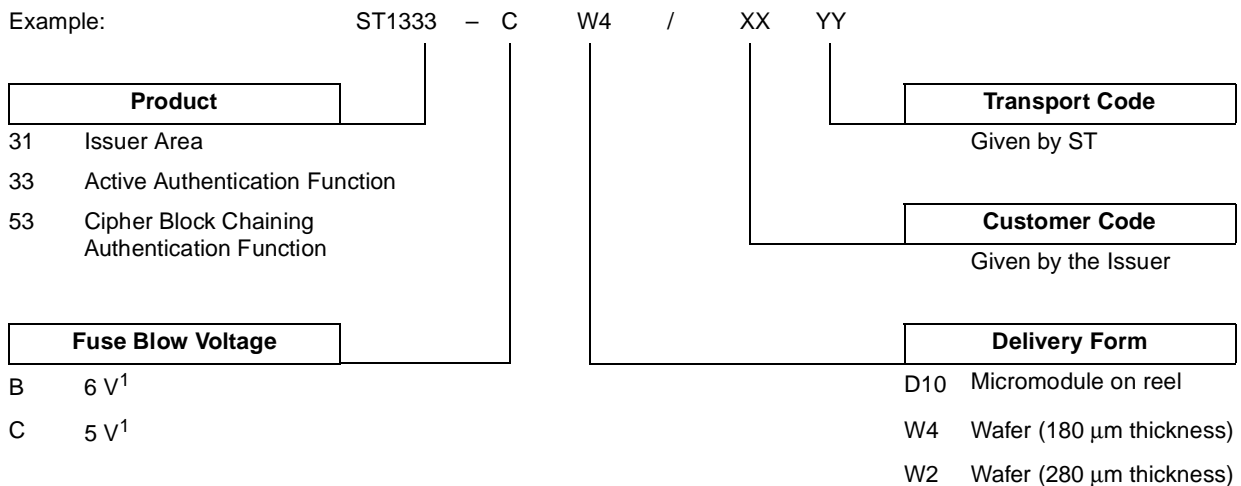
Three options can be chosen on ordering the device:

- The anti-tearing mechanism can be disconnected. In this case, the anti-tearing flag area from bit 288d to bit 319d is unused (Figure 2).
- The user area, from bit 320d to bit 375d, can be defined as “not erasable” in the User Configuration.
- The reload mechanism can be activated. In this case, erasing a bit in the reload counter refreshes the certificate (CER). At this time, the certificate can be programmed with a new value.

**ORDERING INFORMATION**

The notation used for the device number is as shown in Table 2. For a list of available options (speed, package, etc.) or for further information on any aspect of this device, please contact your nearest ST Sales Office.

**Table 2. Ordering Information Scheme**



Note: 1. Please contact your nearest ST Sales Office to check on availability