



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 μ A Supply Current at 5 V (typical)
- 250 μ A Stand-by Current at 5 V (typical)

DESCRIPTION

The members of the ST1331/1333/1353 family are principally designed for use in prepaid Phonecard 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

Table 1. Signal Names

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

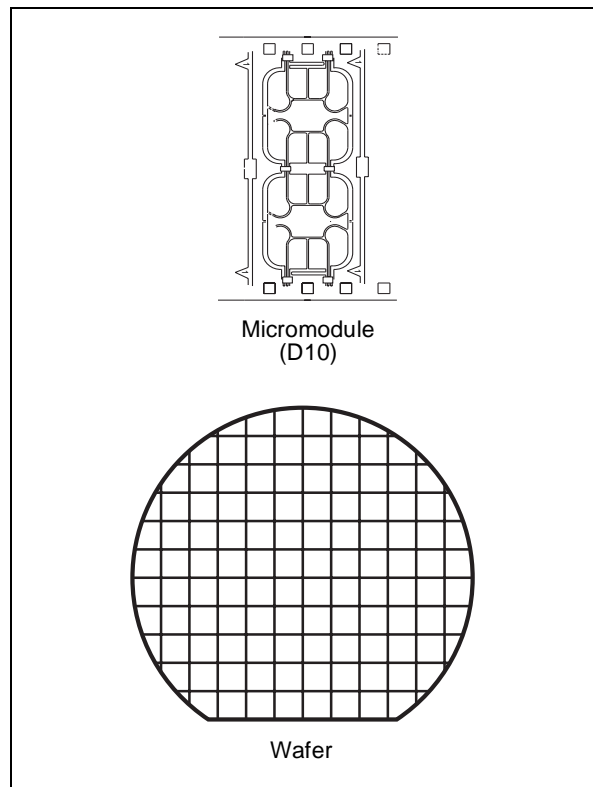


Figure 1. Logic Diagram

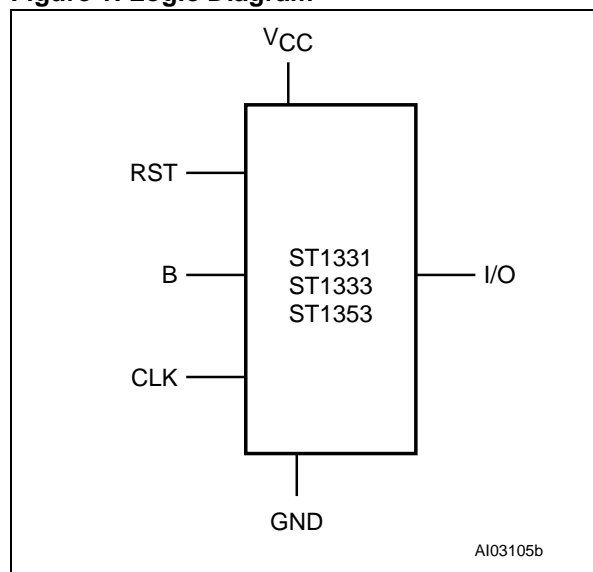
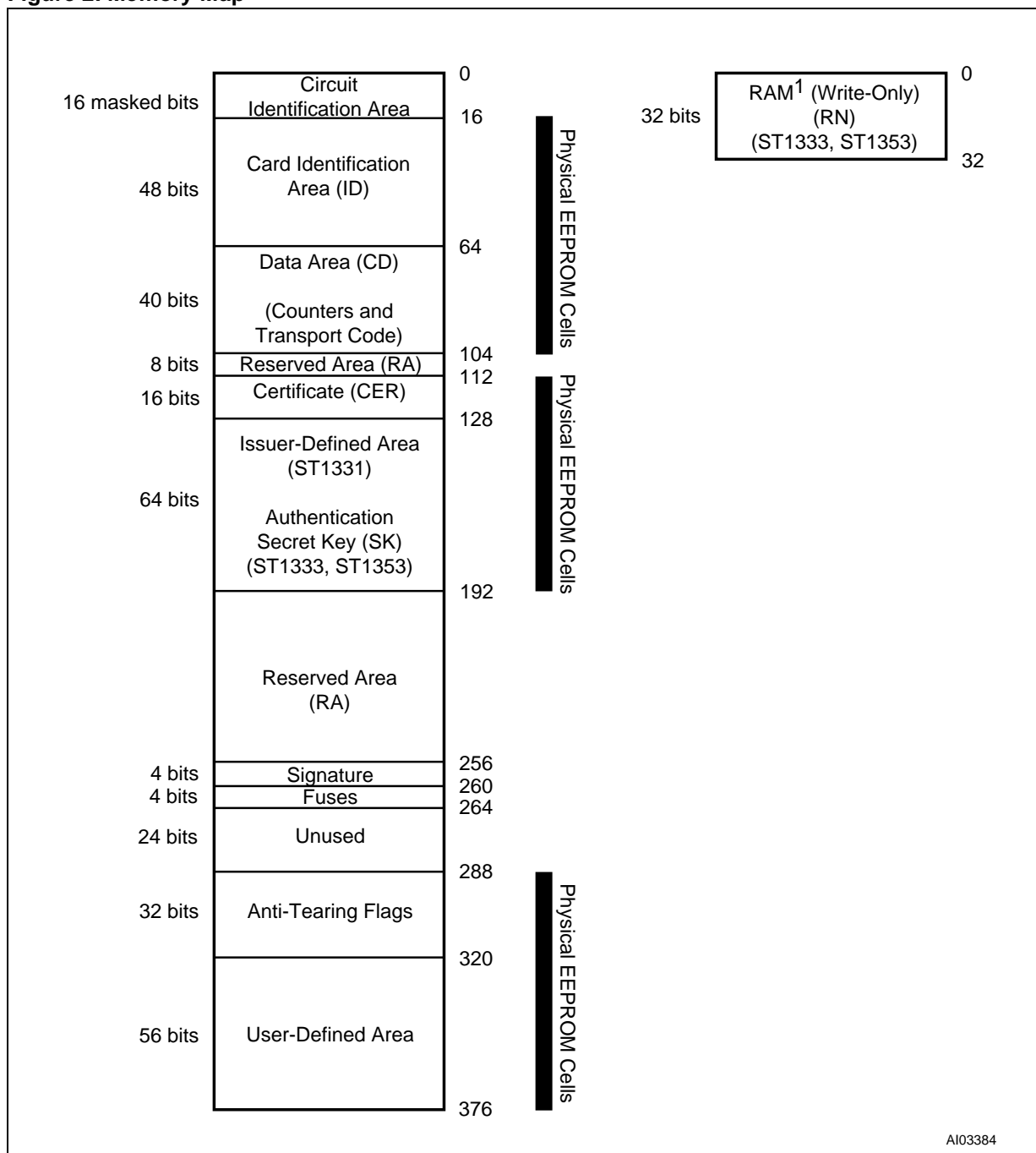


Figure 2. Memory Map



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

