**AES** **Registers**

AES plaintext register (128 bit)

IV register (128 bit)

Ciphertext register (128 bit)

AES Control and Status Register (CSR) (Used 7 bits):

* Encryption/decryption flag (1 bit) (rw)
* Mode selection (3-bit) (rw)
* Start flag (1 bit) (rw)
* Busy flag (1 bit) (ro)
* Done (1 bit) (ro)

**HMAC Registers**

HMAC plaintext register (128-bit)

Digest0 register (256-bit)

Digest1 register (256-bit)

HMAC CSR (Used 10 bits):

* Key length (8-bit) (rw)
* Start flag (1 bit) (rw)
* Busy flag (1 bit) (ro)
* Done (1 bit) (ro)

**PRNG Registers**

Seed (128-bit)

Generated random number (128-bit)

PRNG CSR (Used 4 bits):

* Seed used or not (1 bit) (rw)
* Start flag (1 bit) (rw)
* Busy flag (1 bit) (ro)
* Done (1 bit) (ro)

**Comparator Registers**

COMP CSR:

* Equal (1 bit) (ro)

**DSA Verify Registers**

R register (160-bit)

S register (160-bit)

V register (160-bit)

CSR (used 2 bits):

* Start flag (rw)
* Busy (ro)
* Verification finished (ro)

|  |  |
| --- | --- |
| 0 | AES\_plaintext (128) |
| 1 | IV register (128) |
| 2 | AES\_ciphertext (128) |
| 3 | AES\_CSR (7) |
| 4 | HMAC\_plaintext (128) |
| 5 | Hash0 (256) |
| 6 | Hash1 (256) |
| 7 | HMAC\_CSR (10) |
| 8 | PRNG\_Seed (128) |
| 9 | PRNG\_Generated (128) |
| 10 | PRNG\_CSR (4) |
| 11 | COMP\_CSR (1) |
| 12 | DSA\_R (160) |
| 13 | DSA\_S (160) |
| 14 | DSA\_V (160) |
| 15 | DSA\_CSR (3) |