

| Operand ID | Explicit/<br>Implicit | Class                                  | Operand                       | Description                                                    |
|------------|-----------------------|----------------------------------------|-------------------------------|----------------------------------------------------------------|
| 0          | Explicit              | GPR                                    | RAX                           | Explicit input operand RAX                                     |
| 1          | Explicit              | GPR                                    | RCX                           | Explicit input operand RCX                                     |
| 2          | Explicit              | GPR                                    | RDX                           | Explicit input operand RDX                                     |
| 3          | Explicit              | GPR                                    | RBX                           | Explicit input operand RBX                                     |
| 5          | Explicit              | GPR                                    | RBP                           | Explicit input operand RBP                                     |
| 6          | Explicit              | GPR                                    | RSI                           | Explicit input operand RSI                                     |
| 7          | Explicit              | GPR                                    | RDI                           | Explicit input operand RDI                                     |
| 8          | Explicit              | GPR                                    | R8                            | Explicit input operand R8                                      |
| 9          | Explicit              | GPR                                    | R9                            | Explicit input operand R9                                      |
| 10         | Explicit              | GPR                                    | R10                           | Explicit input operand R10                                     |
| 11         | Explicit              | GPR                                    | R11                           | Explicit input operand R11                                     |
| 12         | Explicit              | GPR                                    | R12                           | Explicit input operand R12                                     |
| 13         | Explicit              | GPR                                    | R13                           | Explicit input operand R13                                     |
| 14         | Explicit              | GPR                                    | R14                           | Explicit input operand R14                                     |
| 15         | Explicit              | GPR                                    | R15                           | Explicit input operand R15                                     |
| 64         | Explicit              | Component of explicit input            | ATTRIBUTES                    | TD_PARAMS.ATTRIBUTES                                           |
| 65         | Explicit              | Component of explicit input            | XFAM                          | TD_PARAMS.XFAM                                                 |
| 66         | Explicit              | Component of explicit input            | EXEC_CONTROLS                 | TD_PARAMS.CONFIG_FLAGS                                         |
| 67         | Explicit              | Component of explicit input            | EPTP_CONTROLS                 | TD_PARAMS.EPTP_CONTROLS                                        |
| 68         | Explicit              | Component of explicit input            | MAX_VCPUS                     | TD_PARAMS.MAX_VCPUS                                            |
| 69         | Explicit              | Component of explicit input            | CPUID_CONFIG                  | TD_PARAMS.CPUID_CONFIG                                         |
| 70         | Explicit              | Component of explicit input            | TSC_FREQUENCY                 | TD_PARAMS.TSC_FREQUENCY                                        |
| 71         | Explicit              | Component of explicit input            | NUM_L2_VMS                    | TD_PARAMS.NUM_L2_VMS                                           |
| 72         | Explicit              | Component of explicit input            | IA32_ARCH_CAPABILITIES_CONFIG | TD_PARAMS.IA32_ARCH_CAPABILITIES_CONFIG                        |
| 95         | Explicit              | Component of explicit input            | PAGE                          | PAGE PA array entry                                            |
| 96         | Explicit              | Component of explicit input            | TDMR_INFO_PA                  | TDMR_INFO_PA array entry                                       |
| 97         | Explicit              | Component of explicit input            | GPA_LIST_ENTRY                | GPA_LIST array entry                                           |
| 98         | Explicit              | Component of explicit input            | MIG_BUFF_LIST_ENTRY           | Migration buffer list entry                                    |
| 99         | Explicit              | Component of explicit input            | NEW_PAGE_LIST_ENTRY           | New page list entry                                            |
| 100        | Explicit              | Component of explicit input            | KEYNAME                       | KEYREQUEST.KEYNAME                                             |
| 101        | Explicit              | Component of explicit input            | TDSIGSTRUCT                   | TDSIGSTRUCT header or reserved fields                          |
| 102        | Explicit              | Component of explicit input            | SIGNATURE                     | TDSIGSTRUCT.SIGNATURE                                          |
| 103        | Explicit              | Component of explicit input            | PAGE_LIST_ENTRY               | Entry of a page list<br>Upper 16 bits are the list entry index |
| 104        | Explicit              | Component of explicit input            | NRX_DESCRIPTOR                | NRX Descriptor                                                 |
| 105        | Explicit              | Component of explicit input            | MEM_SCAN_CONTEXT              | Memory scan context                                            |
| 106        | Explicit              | Component of explicit input            | GPA_RANGE_LIST_ENTRY          | Memory scan GPA range list entry                               |
| 128        | Implicit              | Physical Page                          | TDR                           | TDR Page                                                       |
| 129        | Implicit              | Physical Page                          | TDCX                          | TDCX Page                                                      |
| 130        | Implicit              | Physical Page                          | TDVPR                         | TDVPR Page                                                     |
| 132        | Implicit              | Physical Page                          | REG_PAGE                      | PT_REG private page                                            |
| 144        | Implicit              | TD logical control structure           | TDCS                          | TDCS Logical Structure                                         |
| 145        | Implicit              | TD logical control structure           | TDVPS                         | TDVPS Logical Structure                                        |
| 146        | Implicit              | TD logical control structure           | SEPT_TREE                     | Secure EPT Tree                                                |
| 147        | Implicit              | TD logical control structure           | SEPT_ENTRY                    | Secure EPT Entry                                               |
| 168        | Implicit              | Component of logical control structure | RTMR                          | TDCS.RTMR                                                      |
| 169        | Implicit              | Component of logical control structure | TD_EPOCH                      | TDCS.TD_EPOCH                                                  |
| 170        | Implicit              | Component of logical control structure | L2_VAPIC_GPA                  | TDVPS.L2_VAPIC_GPA                                             |
| 171        | Implicit              | Component of logical control structure | MIGSC                         | TDCS.MIGSC_LINK and MIGSC page                                 |
| 172        | Implicit              | Component of logical control structure | OP_STATE                      | TDCS.OP_STATE                                                  |
| 173        | Implicit              | Component of logical control structure | MIG                           | TDCS Migration Context                                         |
| 174        | Implicit              | Component of logical control structure | SERVTD_BINDINGS               | Service TD bindings table                                      |
| 175        | Implicit              | Component of logical control structure | PASID_TRK                     | PASID tracking information                                     |
| 176        | Implicit              | Component of logical control structure | METADATA_FIELD                | Metadata field                                                 |
| 177        | Implicit              | Component of logical control structure | NUM_VCPUS                     | TDCS.NUM_VCPUS                                                 |
| 178        | Implicit              | Component of logical control structure | CPUID_FIXED0_BITMAP           | TDCS.CPUID_FIXED0_BITMAP                                       |
| 184        | Implicit              | Abstract item                          | SYS                           | Intel TDX Module                                               |
| 185        | Implicit              | Abstract item                          | TDMR                          | TDMR                                                           |
| 186        | Implicit              | Abstract item                          | KOT                           | KOT                                                            |
| 187        | Implicit              | Abstract item                          | KET                           | KET                                                            |
| 188        | Implicit              | Abstract item                          | WBCACHE                       | TDH.PHYMEM.CACHE.WB State                                      |
| 189        | Implicit              | Abstract item                          | NRX                           | NRX                                                            |
| 190        | Implicit              | Abstract item                          | MEM_SCAN_STATE                | Memory scan internal state                                     |
| 256        | Implicit              | TDX I/O abstract item                  | PASIDMT                       | PASID metadata table                                           |
| 257        | Implicit              | TDX I/O abstract item                  | MMIOMT                        | MMIO physical page metadata table                              |
| 258        | Implicit              | TDX I/O abstract item                  | SPDMMT                        | SPDM metadata table                                            |
| 320        | Implicit              | Global control structure               | DMAR                          | Trusted DMA remapping structure                                |