

# ISO 20828:2006-07 (E)

## Road vehicles - Security certificate management

---

| <b>Contents</b>                                                                   | <b>Page</b> |
|-----------------------------------------------------------------------------------|-------------|
| Foreword .....                                                                    | iv          |
| Introduction .....                                                                | v           |
| 1 Scope .....                                                                     | 1           |
| 2 Normative references .....                                                      | 1           |
| 3 Terms and definitions .....                                                     | 2           |
| 4 Symbols and abbreviated terms .....                                             | 3           |
| 5 Certificate Management Principles .....                                         | 4           |
| 5.1 Establishment of trust .....                                                  | 4           |
| 5.2 Certificates .....                                                            | 7           |
| 5.3 Certification authorities .....                                               | 8           |
| 5.4 Certificate validity .....                                                    | 10          |
| 5.5 Certificate policies .....                                                    | 12          |
| 5.6 Certificate Paths .....                                                       | 17          |
| 6 Certificate structure .....                                                     | 21          |
| 7 Certificate components and extensions .....                                     | 22          |
| 7.1 General .....                                                                 | 22          |
| 7.2 Certificate version .....                                                     | 22          |
| 7.3 Certificate serial number .....                                               | 22          |
| 7.4 Certificate signature algorithm identifier .....                              | 22          |
| 7.5 Certificate issuer .....                                                      | 22          |
| 7.6 Certificate validity .....                                                    | 23          |
| 7.7 Certificate subject .....                                                     | 23          |
| 7.8 Certificate subject public key .....                                          | 23          |
| 7.9 Certificate issuer unique identifier .....                                    | 23          |
| 7.10 Certificate subject unique identifier .....                                  | 24          |
| 7.11 CA key identifier extension .....                                            | 24          |
| 7.12 Certificate subject key identifier extension .....                           | 24          |
| 7.13 Extended key usage extension .....                                           | 24          |
| 7.14 Certificate policies extension .....                                         | 24          |
| 7.15 Vehicle identification number extension .....                                | 26          |
| 7.16 Path information extension .....                                             | 26          |
| Annex A (normative) Security Certificate Management ASN.1 module definition ..... | 28          |
| Annex B (informative) Certificate examples .....                                  | 31          |