

# ISO/IEC 10181-3:1996-09 (E)

## Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework

---

| <b>Contents</b> |   | <b>Page</b> |
|-----------------|---|-------------|
| <b>1</b>        | <b>Scope.....</b>   | <b>1</b>    |
| <b>2</b>        | <b>Normative references.....</b>  | <b>2</b>    |
| 2.1             | Identical Recommendations   International Standards .....                             | 2           |
| 2.2             | Paired Recommendations   International Standards equivalent in technical content..... | 2           |
| <b>3</b>        | <b>Definitions .....</b>  | <b>2</b>    |
| <b>4</b>        | <b>Abbreviations.....</b>   | <b>4</b>    |
| <b>5</b>        | <b>General discussion of access control.....</b>                                      | <b>4</b>    |
| 5.1             | Goal of access control.....   | 4           |
| 5.2             | Basic aspects of access control.....  | 5           |
| 5.2.1           | Performing access control functions.....  | 5           |
| 5.2.2           | Other access control activities .....   | 7           |
| 5.2.3           | ACI forwarding.....   | 8           |
| 5.3             | Distribution of access control components .....                                       | 9           |
| 5.3.1           | Incoming access control .....   | 10          |
| 5.3.2           | Outgoing access control .....   | 10          |
| 5.3.3           | Interposed access control.....  | 10          |
| 5.4             | Distribution of access control components across multiple security domains.....       | 10          |
| 5.5             | Threats to access control.....  | 10          |
| <b>6</b>        | <b>Access control policies .....</b>  | <b>11</b>   |
| 6.1             | Access control policy expression .....  | 11          |
| 6.1.1           | Access control policy categories .....  | 11          |
| 6.1.2           | Groups and roles.....   | 11          |
| 6.1.3           | Security labels .....   | 11          |
| 6.1.4           | Multiple Initiator access control policies.....                                       | 12          |
| 6.2             | Policy management.....  | 12          |
| 6.2.1           | Fixed policies.....   | 12          |
| 6.2.2           | Administratively-imposed policies .....   | 12          |
| 6.2.3           | User-selected policies .....  | 12          |
| 6.3             | Granularity and Containment.....  | 12          |
| 6.4             | Inheritance rules.....  | 12          |
| 6.5             | Precedence among access control policy rules .....                                    | 13          |
| 6.6             | Default access control policy rules .....   | 13          |
| 6.7             | Policy mapping through cooperating security domains.....                              | 13          |
| <b>7</b>        | <b>Access control Information and facilities .....</b>                                | <b>13</b>   |
| 7.1             | ACI .....   | 13          |
| 7.1.1           | Initiator ACI .....   | 14          |
| 7.1.2           | Target ACI .....  | 14          |
| 7.1.3           | Access request ACI.....   | 14          |
| 7.1.4           | Operand ACI.....  | 14          |
| 7.1.5           | Contextual information .....  | 14          |
| 7.1.6           | Initiator-bound ACI.....  | 15          |
| 7.1.7           | Target-bound ACI .....  | 15          |
| 7.1.8           | Access request-bound ACI .....  | 15          |
| 7.2             | Protection of ACI .....   | 15          |
| 7.2.1           | Access control certificates.....  | 15          |
| 7.2.2           | Access control tokens .....   | 16          |

|   |  |    |
|---|--|----|
| 7.3   | Access control facilities.....   | 16 |
| 7.3.1   | Management related facilities.....                                       | 16 |
| 7.3.2   | Operation related facilities.....  | 17 |
| 8   | Classification of access control mechanisms.....                         | 19 |
| 8.1   | Introduction.....  | 19 |
| 8.2   | ACL scheme.....  | 20 |
| 8.2.1   | Basic features.....  | 20 |
| 8.2.2   | ACI.....   | 20 |
| 8.2.3   | Supporting mechanisms.....   | 20 |
| 8.2.4   | Variations of this scheme.....   | 21 |
| 8.3   | Capability scheme.....   | 22 |
| 8.3.1   | Basic features.....  | 22 |
| 8.3.2   | ACI.....   | 22 |
| 8.3.3   | Supporting mechanisms.....   | 22 |
| 8.3.4   | Variation of this scheme - Capabilities without specific Operations..... | 22 |
| 8.4   | Label based scheme.....  | 23 |
| 8.4.1   | Basic features.....  | 23 |
| 8.4.2   | ACI.....   | 23 |
| 8.4.3   | Supporting mechanisms.....   | 23 |
| 8.4.4   | Labeled Channels as targets.....   | 24 |
| 8.5   | Context based scheme.....  | 24 |
| 8.5.1   | Basic features.....  | 24 |
| 8.5.2   | ACI.....   | 25 |
| 8.5.3   | Supporting mechanisms.....   | 25 |
| 8.5.4   | Variations of this scheme.....   | 25 |
| 9   | Interaction with other security services and mechanisms.....             | 25 |
| 9.1   | Authentication.....  | 25 |
| 9.2   | Data integrity.....  | 25 |
| 9.3   | Data confidentiality.....  | 26 |
| 9.4   | Audit.....   | 26 |
| 9.5   | Other access-related services.....                                       | 26 |
| Annex A - Exchange of access control certificates among components.....   |  | 27 |
| A.1   | Introduction.....  | 27 |
| A.2   | Forwarding access control certificates.....                              | 27 |
| A.3   | Forwarding multiple access control certificates.....                     | 27 |
| A.3.1   | Example.....   | 27 |
| A.3.2   | Generalization.....  | 28 |
| A.3.3   | Simplifications.....   | 28 |
| Annex B - Access control in the OSI reference model.....                  |  | 29 |
| B.1   | General.....   | 29 |
| B.2   | Use of access control within the OSI layers.....                         | 29 |
| B.2.1   | Use of access control at the network layer.....                          | 29 |
| B.2.2   | Use of access control at the transport layer.....                        | 29 |
| B.2.3   | Use of access control at the application layer.....                      | 29 |
| Annex C - Non-uniqueness of access control identities.....                |  | 30 |
| Annex D - Distribution of access control components.....                  |  | 31 |
| D. 1  | Aspects considered.....  | 31 |
| D.2   | AEC and ADC locations.....   | 31 |
| D.3   | Interactions among access control components.....                        | 32 |
| Annex E - Rule-based versus identity-based policies.....                  |  | 34 |
| Annex F - A mechanism to support ACI forwarding through an initiator..... |  | 35 |
| Annex G - Access control security service outline.....                    |  | 36 |