

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	4
5 Concepts	5
5.1 A model for controlling access to resources	5
5.1.1 Overview	5
5.1.2 Relationship between identity management system and access management system	6
5.1.3 Security characteristics of the access method	7
5.2 Relationships between logical and physical access control	7
5.3 Access management system functions and processes	8
5.3.1 Overview	8
5.3.2 Access control policy	8
5.3.3 Privilege management	9
5.3.4 Policy-related attribute information management	10
5.3.5 Authorization	11
5.3.6 Monitoring management	12
5.3.7 Alarm management	12
5.3.8 Federated access control	13
6 Reference architecture	14
6.1 Overview	14
6.2 Basic components of an access management system	15
6.2.1 Authentication endpoint	15
6.2.2 Policy decision point	15
6.2.3 Policy information point	15
6.2.4 Policy administration point	16
6.2.5 Policy enforcement point	16
6.3 Additional service components	16
6.3.1 General	16
6.3.2 Subject centric implementation	16
6.3.3 Enterprise centric implementation	18
7 Additional requirements and concerns	19
7.1 Access to administrative information	19
7.2 AMS models and policy issues	19
7.2.1 Access control models	19
7.2.2 Policies in access management	19
7.3 Legal and regulatory requirements	20
8 Practice	20
8.1 Processes	20
8.1.1 Authorization process	20
8.1.2 Privilege management process	20

8.2	Threats	21
8.3	Control objectives	22
8.3.1	General	22
8.3.2	Validating the access management framework	22
8.3.3	Validating the access management system	24
8.3.4	Validating the maintenance of an implemented AMS	28
	Annex A (informative) Common access control models	31