

# ISO/IEC 29341-13-10:2008-11 (E)

## Information technology\_ - UPnP Device Architecture\_ - Part\_13-10: Device Security Device Control Protocol\_ - Device Security Service

---

### CONTENTS

FOREWORD .....	5
ORIGINAL UPNP DOCUMENTS (informative) .....	7
<b>1. Overview and Scope.....</b>	<b>9</b>
1.1. Acknowledgements .....	11
<b>2. Service Modeling Definitions .....</b>	<b>12</b>
2.1. Service Type .....	12
2.2. Namespaces .....	12
2.3. Referenced Specifications .....	12
2.4. MustUnderstand .....	12
2.5. State Variables .....	13
2.5.1. NumberOfOwners .....	13
2.5.2. LifetimeSequenceBase .....	13
2.5.3. TimeHint.....	14
2.5.4. TotalACLSize .....	14
2.5.5. FreeACLSize .....	14
2.5.6. TotalOwnerListSize .....	14
2.5.7. FreeOwnerListSize.....	14
2.5.8. TotalCertCacheSize .....	14
2.5.9. FreeCertCacheSize .....	14
2.5.10. A_ARG_TYPE_string .....	14
2.5.11. A_ARG_TYPE_base64 .....	14
2.5.12. A_ARG_TYPE_int .....	14
2.5.13. A_ARG_TYPE_boolean .....	15
2.6. Eventing and Moderation .....	15
2.7. Actions.....	16
2.8. Cryptographic Notation for Selected Actions.....	17
2.9. Actions Invoked by Both CP and SC.....	17
2.9.1. GetPublicKeys.....	17
2.9.2. GetAlgorithmsAndProtocols.....	18
2.9.3. GetACLSizes.....	19
2.9.4. CacheCertificate .....	20
2.9.5. SetTimeHint .....	22
2.9.6. GetLifetimeSequenceBase .....	23
2.9.7. SetSessionKeys .....	24
2.9.8. ExpireSessionKeys .....	26
2.9.9. DecryptAndExecute .....	27
2.10. Actions Invoked by SC only .....	28
2.10.1. TakeOwnership .....	28
2.10.2. GetDefinedPermissions .....	30
2.10.3. GetDefinedProfiles .....	31
2.10.4. ReadACL .....	33
2.10.5. WriteACL .....	34
2.10.6. AddACLEntry.....	35
2.10.7. DeleteACLEntry.....	36
2.10.8. ReplaceACLEntry .....	37
2.10.9. FactorySecurityReset .....	38
2.10.10. GrantOwnership .....	39
2.10.11. RevokeOwnership .....	40
2.10.12. ListOwners .....	41
2.11. Relationships among Actions .....	43

2.11.1.	Relationships among Actions invoked by Security Console.....	43
2.11.2.	Relationships among Actions invoked by normal Control Point.....	43
2.11.3.	ACLVersion .....	44
2.12.	Common Error Codes .....	45
<b>3.</b>	<b>Supporting Information.....</b>	<b>46</b>
3.1.	Glossary .....	46
3.2.	XML Strings as UPnP Arguments.....	46
3.3.	BASE32 Encoding.....	47
3.4.	Namespaces .....	47
<b>4.</b>	<b>Data Structures .....</b>	<b>48</b>
4.1.	Namespaces .....	48
4.2.	Access Control List (ACL) Structure .....	48
4.2.1.	Note on date and time format: ISO 8601 .....	49
4.3.	Owner List .....	49
4.4.	Certificates .....	50
4.4.1.	Authorization Certificate .....	50
4.4.2.	Name Definition Certificate .....	51
4.5.	Permission Language .....	52
4.5.1.	<all> .....	52
4.5.2.	<set> .....	52
4.5.3.	<elt> .....	52
4.5.4.	<prefix> .....	52
4.5.5.	<range> .....	52
4.6.	RSA Encryption Padding.....	53
4.6.1.	SetSessionKeys .....	54
4.6.2.	TakeOwnership.....	54
4.6.3.	Counteracting attacks on PKCS#1 V 1.5 padding .....	54
4.6.4.	Historical note about padding and padding attacks .....	55
4.7.	Public Keys and their hashes .....	55
4.8.	Symmetric cipher mode and padding.....	56
4.9.	Canonical BASE64 Encoding.....	56
<b>5.</b>	<b>Theory of Operation .....</b>	<b>58</b>
5.1.	Access Control Lists and Certificates.....	58
5.1.1.	ACL and Certificate Processing Model .....	59
5.2.	Signature block format .....	59
5.2.1.	Sequence Numbering .....	61
5.2.2.	Hashing and Canonicalization.....	62
5.2.3.	UPnP Certificate Transport.....	62
5.2.4.	IDs for XML-Signature .....	63
5.2.5.	Signature Processing Model.....	63
<b>6.</b>	<b>XML Service Description.....</b>	<b>64</b>
	<b>Annex A (normative) Device Security Schema .....</b>	<b>71</b>
	<b>Annex B (informative) Security Ceremonies .....</b>	<b>79</b>
B.1	Background .....	79
B.2	Security Model.....	79
B.2.1	Security Policy Data .....	81
B.3	Secure Component Discovery .....	81
B.3.1	Discovery of Secured Devices .....	82
B.3.2	Discovery of a Secured CP or SC.....	84

B.4	Ownership .....	84
B.4.1	TakeOwnership.....	85
B.4.2	ListOwners .....	86
B.4.3	GrantOwnership.....	87
B.4.4	RevokeOwnership.....	87
B.4.5	FactorySecurityReset.....	88
B.5	Session Keys.....	88
B.6	ACL Editing .....	89
B.7	Certificate caching.....	90
B.8	References.....	92

## LIST OF TABLES

Table 1:	State variable.....	13
Table 2:	Event Moderation.....	15
Table 3:	Actions invoked by both Control Point and Security Console.....	16
Table 4:	Actions invoked by a Security Console only .....	16

## LIST OF FIGURES

Figure B.1:	Message Security Flowchart.....	80
Figure B.2:	Device discovery ceremony and TakeOwnership.....	82
Figure B.3:	Discovery of CP and SC nodes.....	84
Figure B.4:	Taking ownership via private cable.....	85
Figure B.5:	ListOwners .....	86
Figure B.6:	GrantOwnership.....	87
Figure B.7:	RevokeOwnership.....	87
Figure B.8:	FactorySecurityReset.....	88
Figure B.9:	Setting Session Keys .....	89
Figure B.10:	ACL Editing .....	90
Figure B.11:	Certificate caching on the device .....	91
Figure B.12:	Delivering certificates to the CP.....	92