ISO/IEC 29341-13-10

Edition 1.0 2008-11

INTERNATIONAL STANDARD

Information technology – UPnP Device Architecture – Part 13-10: Device Security Device Control Protocol – Device Security Service

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE X

ICS 35.200

ISBN 2-8318-1012-8

CONTENTS

LIST OF TABLES

LIST OF FIGURES

INFORMATION TECHNOLOGY – UPNP DEVICE ARCHITECTURE –

Part 13-10: Device Security Device Control Protocol – Device Security Service

FOREWORD

1) ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

3) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.

4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

5) In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

7) All users should ensure that they have the latest edition of this publication.

8) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

9) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

IEC and ISO draw attention to the fact that it is claimed that compliance with this document may involve the use of patents as indicated below.

ISO and IEC take no position concerning the evidence, validity and scope of the putative patent rights. The holders of the putative patent rights have assured IEC and ISO that they are willing to negotiate free licences or licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of the putative patent rights are registered with IEC and ISO.

Intel Corporation has informed IEC and ISO that it has patent applications or granted patents.

Information may be obtained from:

Intel Corporation
Standards Licensing Department
5200 NE Elam Young Parkway
MS: JFS-98
USA – Hillsboro, Oregon 97124

Microsoft Corporation has informed IEC and ISO that it has patent applications or granted patents as listed below:

6101499 / US; 6687755 / US; 6910068 / US; 7130895 / US; 6725281 / US; 7089307 / US; 7069312 / US; 10/783 524 /US

Information may be obtained from:

Microsoft Corporation
One Microsoft Way
USA – Redmond WA 98052

Philips International B.V. has informed IEC and ISO that it has patent applications or granted patents.

Information may be obtained from:

Philips International B.V. – IP&S
High Tech campus, building 44 3A21
NL – 5656 Eindhoven

NXP B.V. (NL) has informed IEC and ISO that it has patent applications or granted patents.

Information may be obtained from:

NXP B.V. (NL)
High Tech campus 60
NL – 5656 AG Eindhoven

Matsushita Electric Industrial Co. Ltd. has informed IEC and ISO that it has patent applications or granted patents.

Information may be obtained from:

Matsushita Electric Industrial Co. Ltd.
1-3-7 Shiromi, Chuoh-ku
JP – Osaka 540-6139

Hewlett Packard Company has informed IEC and ISO that it has patent applications or granted patents as listed below:

5 956 487 / US; 6 170 007 / US; 6 139 177 / US; 6 529 936 / US; 6 470 339 / US; 6 571 388 / US; 6 205 466 / US

Information may be obtained from:

Hewlett Packard Company
1501 Page Mill Road
USA – Palo Alto, CA 94304

Samsung Electronics Co. Ltd. has informed IEC and ISO that it has patent applications or granted patents.

Information may be obtained from:

Digital Media Business, Samsung Electronics Co. Ltd.
416 Maetan-3 Dong, Yeongtang-Gu,
KR – Suwon City 443-742

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29341-13-10 was prepared by UPnP Implementers Corporation and adopted, under the PAS procedure, by joint technical committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

The list of all currently available parts of the ISO/IEC 29341 series, under the general title *Universal plug and play (UPnP) architecture*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

ORIGINAL UPNP DOCUMENTS
(informative)

Reference may be made in this document to original UPnP documents. These references are retained in order to maintain consistency between the specifications as published by ISO/IEC and by UPnP Implementers Corporation. The following table indicates the original UPnP document titles and the corresponding part of ISO/IEC 29341:

UPnP Document Title	**ISO/IEC 29341 Part**
UPnP Device Architecture 1.0	ISO/IEC 29341-1
UPnP Basic:1 Device	ISO/IEC 29341-2
UPnP AV Architecture:1	ISO/IEC 29341-3-1
UPnP MediaRenderer:1 Device	ISO/IEC 29341-3-2
UPnP MediaServer:1 Device	ISO/IEC 29341-3-3
UPnP AVTransport:1 Service	ISO/IEC 29341-3-10
UPnP ConnectionManager:1 Service	ISO/IEC 29341-3-11
UPnP ContentDirectory:1 Service	ISO/IEC 29341-3-12
UPnP RenderingControl:1 Service	ISO/IEC 29341-3-13
UPnP MediaRenderer:2 Device	ISO/IEC 29341-4-2
UPnP MediaServer:2 Device	ISO/IEC 29341-4-3
UPnP AV Datastructure Template:1	ISO/IEC 29341-4-4
UPnP AVTransport:2 Service	ISO/IEC 29341-4-10
UPnP ConnectionManager:2 Service	ISO/IEC 29341-4-11
UPnP ContentDirectory:2 Service	ISO/IEC 29341-4-12
UPnP RenderingControl:2 Service	ISO/IEC 29341-4-13
UPnP ScheduledRecording:1	ISO/IEC 29341-4-14
UPnP DigitalSecurityCamera:1 Device	ISO/IEC 29341-5-1
UPnP DigitalSecurityCameraMotionImage:1 Service	ISO/IEC 29341-5-10
UPnP DigitalSecurityCameraSettings:1 Service	ISO/IEC 29341-5-11
UPnP DigitalSecurityCameraStillImage:1 Service	ISO/IEC 29341-5-12
UPnP HVAC_System:1 Device	ISO/IEC 29341-6-1
UPnP HVAC_ZoneThermostat:1 Device	ISO/IEC 29341-6-2
UPnP ControlValve:1 Service	ISO/IEC 29341-6-10
UPnP HVAC_FanOperatingMode:1 Service	ISO/IEC 29341-6-11
UPnP FanSpeed:1 Service	ISO/IEC 29341-6-12
UPnP HouseStatus:1 Service	ISO/IEC 29341-6-13
UPnP HVAC_SetpointSchedule:1 Service	ISO/IEC 29341-6-14
UPnP TemperatureSensor:1 Service	ISO/IEC 29341-6-15
UPnP TemperatureSetpoint:1 Service	ISO/IEC 29341-6-16
UPnP HVAC_UserOperatingMode:1 Service	ISO/IEC 29341-6-17
UPnP BinaryLight:1 Device	ISO/IEC 29341-7-1
UPnP DimmableLight:1 Device	ISO/IEC 29341-7-2
UPnP Dimming:1 Service	ISO/IEC 29341-7-10
UPnP SwitchPower:1 Service	ISO/IEC 29341-7-11
UPnP InternetGatewayDevice:1 Device	ISO/IEC 29341-8-1
UPnP LANDevice:1 Device	ISO/IEC 29341-8-2
UPnP WANDevice:1 Device	ISO/IEC 29341-8-3
UPnP WANConnectionDevice:1 Device	ISO/IEC 29341-8-4
UPnP WLANAccessPointDevice:1 Device	ISO/IEC 29341-8-5
UPnP LANHostConfigManagement:1 Service	ISO/IEC 29341-8-10
UPnP Layer3Forwarding:1 Service	ISO/IEC 29341-8-11
UPnP LinkAuthentication:1 Service	ISO/IEC 29341-8-12
UPnP RadiusClient:1 Service	ISO/IEC 29341-8-13
UPnP WANCableLinkConfig:1 Service	ISO/IEC 29341-8-14
UPnP WANCommonInterfaceConfig:1 Service	ISO/IEC 29341-8-15
UPnP WANDSLLinkConfig:1 Service	ISO/IEC 29341-8-16
UPnP WANEthernetLinkConfig:1 Service	ISO/IEC 29341-8-17
UPnP WANIPConnection:1 Service	ISO/IEC 29341-8-18
UPnP WANPOTSLinkConfig:1 Service	ISO/IEC 29341-8-19
UPnP WANPPPConnection:1 Service	ISO/IEC 29341-8-20
UPnP WLANConfiguration:1 Service	ISO/IEC 29341-8-21
UPnP Printer:1 Device	ISO/IEC 29341-9-1
UPnP Scanner:1.0 Device	ISO/IEC 29341-9-2
UPnP ExternalActivity:1 Service	ISO/IEC 29341-9-10
UPnP Feeder:1.0 Service	ISO/IEC 29341-9-11
UPnP PrintBasic:1 Service	ISO/IEC 29341-9-12
UPnP Scan:1 Service	ISO/IEC 29341-9-13
UPnP QoS Architecture:1.0	ISO/IEC 29341-10-1
UPnP QosDevice:1 Service	ISO/IEC 29341-10-10
UPnP QosManager:1 Service	ISO/IEC 29341-10-11
UPnP QosPolicyHolder:1 Service	ISO/IEC 29341-10-12
UPnP QoS Architecture:2	ISO/IEC 29341-11-1
UPnP QOS v2 Schema Files	ISO/IEC 29341-11-2

UPnP Document Title	ISO/IEC 29341 Part
UPnP QosDevice:2 Service	ISO/IEC 29341-11-10
UPnP QosManager:2 Service	ISO/IEC 29341-11-11
UPnP QosPolicyHolder:2 Service	ISO/IEC 29341-11-12
UPnP RemoteUIClientDevice:1 Device	ISO/IEC 29341-12-1
UPnP RemoteUIServerDevice:1 Device	ISO/IEC 29341-12-2
UPnP RemoteUIClient:1 Service	ISO/IEC 29341-12-10
UPnP RemoteUIServer:1 Service	ISO/IEC 29341-12-11
UPnP DeviceSecurity:1 Service	ISO/IEC 29341-13-10
UPnP SecurityConsole:1 Service	ISO/IEC 29341-13-11

1. Overview and Scope

The Device Security service provides the services necessary for strong authentication, authorization, replay prevention and privacy of UPnP SOAP actions. Under this architecture, a Device enforces its own access control but its access control policy is established and maintained by an administrative application, the Security Console (see SecurityConsole:1), which uses some of the actions provided as part of this service. Nothing prevents a device with the proper user interface capabilities from providing its own administration interface, although presumably it is a valuable ability to administer access from one location for an entire household network. In what follows, the term "Security Console" refers to any Control Point that chooses to exercise the administrative functions defined here in DeviceSecurity.

DeviceSecurity implements access control for itself and for other Services in the same Device (or embedded Device). There are two classes of access control grant defined here: ownership and normal permission. Each security-aware Device has an ownership list capable of holding at least one entry. Any Security Console listed as an owner has full rights to the Device, specifically to all actions including the DeviceSecurity actions that specify other access control. In addition to the owner list, the Device usually has an access control list (ACL) maintained by DeviceSecurity. Entries in the ACL grant a Security Console or other Control Point symbolic permissions that, in turn, grant access to sets of actions. Those permissions typically grant less than the full access that ownership grants. A Security Console, at the option of the Device vendor, might also be granted the permission to delegate rights to others without having to be a full owner of the device or to define named groups of Control Points to be granted access as a group in a single operation. These last two capabilities depend on the implementation of certificate processing by the Device and that is an optional feature of DeviceSecurity.

A device implementing DeviceSecurity will need to support the basic cryptographic algorithms used in this service:

1. AES 128-bit, for symmetric bulk encryption, labeled "AES-128-CBC", with blocks padded as described in section 4.8 below.

2. SHA1 HMAC, for symmetric signatures and for TakeOwnership, labeled "SHA1-HMAC"

3. RSA 1024-bit, for identification and for establishing secure sessions, and possibly for other operations, labeled "RSA". In the current version of this DeviceSecurity specification, there is no reason for a device to have a public-key algorithm signature key. Therefore a device will offer a public confidentiality key but does not need to offer a signature key at this time. [In particular, actions that are authorized by public-key algorithm signatures do not have digitally signed responses.] The algorithm identifier "RSA" when used for encryption in this service implies (RSA, PKCS#1) and when used for signing implies (RSA, SHA-1, PKCS#1).

Other algorithms may be added to this list, if these develop flaws and need to be supplanted. For example, if another hash algorithm were to be added, one would need to identify it and also identify RSA using it for signing. So, for example, if one adds the hash algorithm FOOBLA, one would need to add RSA-FOOBLA and FOOBLA-HMAC to the algorithm list.

The logic of operation, from the point of view of the security-aware device, is as follows:

1. If a device has a display or printing capability and also has a source of randomness, then it is preferable for the device to generate a new password and new public key pair on any power-up when it is in factory reset state. It would then display or print the generated password and the hash of the new public key. For devices without those abilities, the password and public key pair will have been created by the manufacturer and will remain constant over the lifetime of the device. In that case, the manufacturer will have printed the password and the Security ID (hash of the device's public key) on a card or a label attached to the device case, or both. The password does not need to be longer than about 6 upper case alphanumeric characters, provided it was generated randomly for that device and is used by TakeOwnership shortly after the device is plugged into the network. [Note: passwords or keys are not to be used in common across a set of devices. Such usage would be a security flaw.]

2. The device announces itself via SSDP, perhaps giving real details or perhaps describing itself only as "Security Aware Device", if the device wants to prevent inventory by an unauthorized control point.

3. A Security Console (SC), presumably that of the device's owner, calls the GetPublicKeys, GetLifetimeSequenceBase and TakeOwnership actions, supplying the device's password to prove

authorization to take control of the device. As a result of a successful TakeOwnership action, that Security Console is listed as the device's Owner. An Owner is a control point that is empowered to edit the device's Access Control List (ACL). Subsequent TakeOwnership attempts MUST be ignored. If the device generated its password dynamically, then the password used in this TakeOwnership action should not be valid again.

4. The owning SC establishes a set of session keys by calling GetLifetimeSequenceBase and SetSessionKeys. These session keys will be used for digitally signing future action messages using XML-Signature with symmetric key signature.

5. The owning SC will then be free to use the GetACLSizes action to discover whether access permissions can be granted by ACL entries directly or need to be encoded as certificates, because the device has too little room to store an ACL.

6. The owning SC will probably also invoke GetDefinedPermissions in order to learn what permissions it might grant to chosen Control Points.

7. If the SC grants access by certificate, that operation happens without invoking any actions on the device. Otherwise, the SC grants access to desired Control Points (CPs) by way of AddACLEntry. It also reads the current ACL contents, for display to its human operator, by using ReadACL. The actions WriteACL, ReplaceACLEntry and DeleteACLEntry are also available for ACL editing. These actions will be omitted from DeviceSecurity in those implementations that do not provide any memory for an ACL.

8. A CP that wants to conduct a control session with a security aware device may call GetAlgorithmsAndProtocols, in order to confirm interoperability, and will then call SetSessionKeys, to establish a secure session with the device. These sessions do not hold network connections open and could be very long-lived, depending on the storage capacity of the Device and the CP.

9. Once a CP has established a session with the device, it invokes actions by sending normal action messages, digitally signed using XML-Signature with a symmetric signature key (e.g., HMAC) established during SetSessionKeys and with a sequence number initialized by that action. The sequence numbers during a session must be monotonically increasing but need not be sequential.

10. If a CP needs an action message to be confidential, it uses the DecryptAndExecute action, one argument of which is the ciphertext of an encrypted action. The reply from that action is then encrypted and returned in the reply to the DecryptAndExecute action.

11. A session may be ended intentionally, by ExpireSessionKeys, or may time out at the device's discretion.

12. In the event that the device's owner wants to share ownership, either with another person or (for fault-tolerance) with another SC operated by him- or her-self, a current owning SC can invoke GrantOwnership. This assumes that GetACLSizes shows that there is room in the device to record the additional owner. Ownership can be revoked via RevokeOwnership. Current owners can be listed via the action ListOwners.

13. Should a device be sold to someone else, it can be reinitialized via the FactorySecurityReset action. It is strongly recommended that a device also include some physical means for achieving the same end, although that means should not necessarily be convenient (e.g., might require opening the case). The physical Reset mechanism is to cover the case when a Security Console takes ownership of the device, has not granted any access or any co-ownership, and then dies irretrievably, leaving the device owned by an SC that can never again be used.

14. It is conceivable that a device manufacturer might want to define some UPnP maintenance actions to which it alone retains authority. To do this under UPnP DeviceSecurity, the manufacturer needs to create a separate device with its own instance of DeviceSecurity and take ownership of that sub-device at time of manufacture. Simply initializing the normal ACL with access permissions granted to the manufacturer's key(s) does not allow the manufacturer to retain control, since a device owner can delete any entries in the normal ACL. This separate sub-device would not have its ACL affected by FactorySecurityReset.

Enhancements

15. A device may, if it chooses, define named sets of permissions, called Profiles, and a Security Console may read those definitions via GetDefinedProfiles. These Profiles could be role names, for example, like Parent, Child, or Administrator. The Profile names can be used in the user interface provided by the Security Console.

16. If a CP has certificates to present to the device, in order to gain access, and if the device shows via GetACLSizes that it has certificate cache memory available, the CP may send those certificates to the device via the CacheCertificate action. Such certificates would then be available on the device over multiple subsequent actions. Implementation of certificate caches is up to the device, but it would make sense to validate certificates at the time they are cached. It might also make sense to derive implied ACL entries from validated certificates and current ACL entries, and store those derived entries at the time a certificate is cached.

1.1. Acknowledgements

The authors and the chair of the UPnP Security Working Committee would like to acknowledge significant contributions made by other UPnP members to help complete this work. Markus Wischy of Siemens was one of the initiators of this effort, and he made many important contributions along the way, including work on securing device discovery and leading one of the sample implementation development teams. Andrew Fiddian-Green of Siemens provided detailed technical feedback on the specification and single-handedly developed one of the sample implementations. Sony Electronics, LG Electronics, GlobespanVirata, and Atinav contributed sample implementations and provided feedback on the specification. Microsoft contributed to the specification and also enhanced the certification test tool to enable testing of secure devices.