The Core Session Initiation Protocol User Agent Profile Data Set
draft-petrie-sipping-sip-dataset-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/lid-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 12, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document defines the properties and format for the core SIP user agent profile data set. The properties defined in this document are expected to be common to most SIP user agents regardless of whether the user agent support audio, video, text or any combination of media. These core SIP properties are considered to be a data set.
Several datasets may be combined into documents or profiles that are provided to SIP user agents so that they can operate with the desired behavior.

Table of Contents

1. Motivation .................................................. 3
2. Introduction ................................................ 3
   2.1 Requirements Terminology .................................. 3
   2.2 Profile Data Terminology ................................ 3
   2.3 Overview ................................................ 4
3. Core SIP Data Set ............................................. 5
   3.1 Transport Protocol Data Set ............................... 5
      3.1.1 transport_protocols Data Set Properties Definitions . 5
      3.1.2 transport_protocols Element Definition ................ 6
      3.1.3 Merging Different Sources of a transport_protocol
            Data Set ............................................. 6
   3.2 outbound_proxy ........................................... 7
      3.2.1 outbound_proxy Data Set Properties Definitions ... 7
      3.2.2 outbound_proxies Element Definition ................ 7
      3.2.3 outbound_proxies Merging Different Sources of a
            Data Set ............................................. 7
   3.3 sip_methods ............................................... 7
      3.3.1 sip_methods Data Set Properties Definitions .......... 8
      3.3.2 sip_methods Element Definition ....................... 8
      3.3.3 sip_methods Merging Different Sources of a Data Set . 8
   3.4 sip_option_tags ......................................... 8
      3.4.1 sip_option_tags Data Set Properties Definitions .... 8
      3.4.2 sip_option_tags Element Definition .................... 8
      3.4.3 sip_option_tags Merging Different Sources of a
            Data Set ............................................. 9
4. Example Profiles and Use ..................................... 9
   4.1 Merge Two Data Sets ...................................... 9
   4.2 Policy Filtering ......................................... 11
   4.3 Override ................................................ 11
5. Security Considerations ...................................... 11
6. Changes from draft-petrie-sipping-profile-datasets-01 .......... 11
7. References .................................................. 11
   Authors’ Addresses .......................................... 12
A. SIP Protocol Dataset Schema ................................ 13
B. Acknowledgments ............................................. 16
   Intellectual Property and Copyright Statements .............. 17
1. Motivation

The SIP Profile Data Sets defined in this document support the principle to enable SIP User Agents to obtain and use profile data sets from multiple sources in order to support a wide range of applications without undue complexity.

The SIP Protocol Data Set is intended to be the lowest common denominator among all user agent types regardless of capability. This data set contains properties that all user agents require. That does not mean that all of these properties are mandatory.

2. Introduction

This document defines the properties and format for the core SIP user agent profile data set. The following properties are defined in this document:

- `transport_protocols`
- `outbound_proxies`
- `sip_methods`
- `sip_option_tags`

and, are expected to be common to most SIP user agents regardless of whether the user agent support audio, video, text or any combination of media. These core SIP properties are considered to be a data set.

2.1 Requirements Terminology

Keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT" and "MAY" that appear in this document are to be interpreted as described in RFC 2119.[RFC2119]

2.2 Profile Data Terminology

property - a named configurable characteristic of a user agent. A given property has a well-defined range of possible values. A given property may be defined to have range of values, allow for simultaneous use of many values (as in a list of allowed possibilities), or be a set of related values that collectively form a single profile information item.

setting - the binding of a specific value or set of values to a given property.

profile - a collection of settings to be applied for a specific user, device, or local network.
device - SIP user agent, either software or hardware appliance. This is a logical concept, as there may be no physical dedicated device or it may be part of an assembly of devices. In this document, the terms "user agent" and "device" are interchangeable.

user profile - the profile that applies to a specific user. This is best illustrated by the "hotelling" use case - a user has an association for some period of time with a particular device. The user profile is that set of profile data the user wants to associate with that device (e.g. ringtones used when someone calls them, the user’s shortcuts).

device profile - data profile that applies to a specific device. In the "hotelling" use case, this is the data that is bound to the device itself independent of the user. It relates to specific capabilities of the device and/or preferences of the owner of the device.

local network profile - data that applies to the user agent in the context of the local network. This is best illustrated by roaming applications; a new device appears in the local network (or a device appears in a new network, depending on the point of view). The local network profile includes settings and perhaps policies that allow the user agent to function in the local network (e.g. how to traverse NAT or firewall, bandwidth constraints).

data set - a collection of properties.

working profile - the set of property values actually set in a SIP User Agent as a result of merging the profiles from all sources; the actual effective profile for the user agent.

merging - the operation of resolving overlapping settings from multiple profiles. Overlap occurs when the same property occurs in multiple profiles (e.g. user, device, local network).

2.3 Overview

The Core SIP UA profile data set is defined in Section 3 and complies with the guidelines provided in Section 5 of [I-D.petrie-sipping-profile-datasets]

Section 4 provides illustrative example profiles and use cases for merging. Security considerations are addressed in Section 5.

The following is an example instance of the SIP protocol data set. Note the use of the policy attribute.
<property_set>
  <transport_protocols>
    <transport_protocol policy="allow">
      <name>UDP</name>
      <port>5060</port>
    </transport_protocol>
    <transport_protocol policy="allow">
      <name>TCP</name>
      <port>5060</port>
    </transport_protocol>
    <transport_protocol policy="allow">
      <name>TLS</name>
      <port>5061</port>
    </transport_protocol>
  </transport_protocols>
  <outbound_proxies>
    <outbound_proxy policy="mandatory">
      sip:outproxy.example.com
    </outbound_proxy>
  </outbound_proxies>
  <sip_methods>
    <sip_method policy="disallow">INFO</sip_method>
  </sip_methods>
  <sip_option_tags>
    <sip_option_tag policy="disallow">join</sip_option_tag>
  </sip_option_tags>
</property_set>

3. Core SIP Data Set

The XML schema defined in this document extends the root element "property_set" schema defined in I-D.petrie-sipping-profile-datasets.

3.1 Transport Protocol Data Set

3.1.1 transport_protocols Data Set Properties Definitions

transport_protocols - This property contains properties related to SIP transport protocols, and is an XML element that extends on the XML "setting_container" element contained in the root "property_set" element. It serves as a container for a list of SIP transport protocols to allow or disallow. There may be zero or one elements.
3.1.2 transport_protocols Element Definition

transport_protocol - The "transport_protocol" is an XML element that extends the "setting" element contained in the "transport_protocols" element. The "transport_protocol" element contains properties related to a SIP transport protocol. It names the transport protocol, defines whether the protocol is enabled or not and defines the port to which that protocol is bound. If the protocol is named it defaults to enabled if not explicitly set. If the port property is not set, it defaults to the default specified by the specification which binds the protocol to SIP. The user agent should enable all the set transport protocols that are supported by the user agent. The user agent ignores protocol bindings that it does not support. The user agent may default transport protocols that it supports to enabled, if a protocol property for that transport protocol is not present in the data set. The order of the list of transport_protocol setting values indicated by the "q" attribute indicates the order of preference. There may be zero or more "transport_protocol" elements in the "transport_protocols" element.

name - This XML element identifies the specific transport protocol, and extends the "setting" element contained in transport_protocols. There must be exactly one "name" element in a "transport_protocol".

port - This element identifies the port for binding the transport protocol, and extends the "setting" element contained in transport_protocols. There must be exactly one "port" element in a "transport_protocol".

3.1.3 Merging Different Sources of a transport_protocol Data Set

The "transport_protocol" property uses the "policy" attribute to identify whether the transport protocol is mandatory, allowed or disallowed. The "q" attribute is used for ordering of the list. In addition, a visibility attribute may be present.

If there are matches on multiple "name" element values, the "policy" attribute will determine which is mandatory. As defined in Merging Datasets [I-D.petrie-sipping-profile-datasets] properties with a "policy" attribute value of "mandatory" are used over those with other "policy" attribute values. If there are multiple "transport_protocol" elements from different profiles with the same "name" element value and "policy" attribute values of "allows", then the resulting merged "transport_protocols" element will contain one "transport_protocol" element having a "name" element of that value. The "port" element value will be determined in the following order of the source profile, when there are multiple "transport_protocol" elements from different profiles with the same "name" element value.
and "policy" attribute value of "allow":
Local
Device
User
Application

3.2 outbound_proxy

3.2.1 outbound_proxy Data Set Properties Definitions

outbound_proxies - The "outbound_proxies" property is an XML element that extends on the XML "setting" element contained in the root "property_set" element. It serves as a container for a list of outbound proxies. There may be zero or one element. The default outbound proxy, through which all SIP requests, not explicitly routed, should be sent. The format of this parameter is of name-addr as specified in [RFC3261]. This property is optional. If absent or not set, SIP requests are sent to directly to the URI of the request. If set the effect of this property is to add a loose route as defined in [RFC3261] for the next hop destination.

3.2.2 outbound_proxies Element Definition

outbound_proxies - The "outbound_proxy" is an XML element that extends the XML "setting" element contained in "outbound_proxies". There may be zero, one or many "outbound_proxy" elements. It provides default value for an outbound proxy, through which all SIP requests, not explicitly routed, should be sent. The format of this parameter is of name-addr as specified in [RFC3261]. This property is optional. If absent or not set, SIP requests are sent to directly to the URI of the request. If set the effect of this property is to add a loose route as defined in [RFC3261] for the next hop destination. Multiple "outbound_proxy" elements may be contained in the "outbound_proxies" element to form a route set.

3.2.3 outbound_proxies Merging Different Sources of a Data Set

The aggregation approach is used to resolve conflicts. By aggregating the multiple outbound proxies, the local network profile provided outbound proxy allows the signaling to get out of the local network and the device profile provided outbound proxy is able to monitor all SIP signaling from the user agent. The order of the resulting merged, route set is determined by the "q" attribute.

3.3 sip_methods
3.3.1 sip_methods Data Set Properties Definitions

sip_methods - This property contains properties related to SIP Methods, and is an XML element that extends on the XML "setting" element contained in the root "property_set" element. It serves as a container for a list of SIP request methods to allow or disallow. Typically, only provide by the device dataset. The "sip_methods" element is intended to provide a means of enabling or disabling features in the SIP user agent based upon the SIP request method.

3.3.2 sip_methods Element Definition

sip_method - An element to specify a SIP method, and extends the "setting" element contained in the "sip_methods" element. There may be zero or more elements. For user agents that support the method indicated, this element serves as a switch to enable or disable the named SIP method as indicated by the "policy" attribute.

3.3.3 sip_methods Merging Different Sources of a Data Set

The "sip_methods" Data Set uses the aggregation merging policy defined in [I-D.petrie-sipping-profile-datasets]. When multiple "sip_method" elements with the same value are provided, the "policy" attribute is used to determine precedence.

3.4 sip_option_tags

3.4.1 sip_option_tags Data Set Properties Definitions

sip_option_tags - This property specifies a container for a list of SIP option tags that are allowed or disallowed, and is an XML element that extends on the XML "setting" element contained in the root "property_set" element. For user agents that support features indicated by option tags, this element serves as a list of features to turn on or off as indicated by the "policy" attribute in the "sip_option_tag" element.

3.4.2 sip_option_tags Element Definition

sip_option_tag - An element to specify a SIP option tag, and extends the "setting" element and is contained in "sip_option_tags" element. There may be zero or more elements "sip_option_tag". For user agents that support features indicated by option tags, this element serves as a switch to enable or disable the named SIP option as indicated by the policy attribute in the
"sip_option_tag" element.

### 3.4.3 sip_option_tags Merging Different Sources of a Data Set

The sip_option_tags Data Set uses the default aggregation merging policy defined in [I-D.petrie-sipping-profile-datasets]. When multiple "sip_method" elements with the same value are provided, the "policy" attribute is used to determine precedence.

#### 4. Example Profiles and Use

##### 4.1 Merge Two Data Sets

Consider the use case described in [I-D.petrie-sipping-profile-datasets] where the user wishes to indicate that only secure SIP transport should be used. The device profile may contain SIP Protocol Data Set (see Section 3.1) settings that look like the following:

```xml
<property_set>
  <transport_protocols>
    <transport_protocol policy="allow">
      <name>UDP</name>
      <port>5060</port>
    </transport_protocol>
    <transport_protocol policy="allow">
      <name>TCP</name>
      <port>5060</port>
    </transport_protocol>
    <transport_protocol policy="allow">
      <name>TLS</name>
      <port>5061</port>
    </transport_protocol>
  </transport_protocols>
  <outbound_proxies>
    <outbound_proxy policy="mandatory">
      sip:outproxy.example.com
    </outbound_proxy>
  </outbound_proxies>
  <sip_methods>
    <sip_method policy="disallow">INFO</sip_method>
  </sip_methods>
  <sip_option_tags>
    <sip_option_tag policy="disallow">join</sip_option_tag>
  </sip_option_tags>
</property_set>
```
The user profile which indicates that only TLS should be used would look like (Note: this example also indicates that port 5061 should be used with a mandatory policy as well. This may be more constrained than the user really wants.):

```xml
<property_set>
  <transport_protocols>
    <transport_protocol policy="mandatory">
      <name>TLS</name>
      <port>5061</port>
    </transport_protocol>
    <transport_protocol policy="disallow">
      <name>UDP</name>
    </transport_protocol>
    <transport_protocol policy="disallow">
      <name>TCP</name>
    </transport_protocol>
  </transport_protocols>
</property_set>
```

The merged result of the device and user profile would look like:

```xml
<property_set>
  <transport_protocols>
    <transport_protocol policy="mandatory">
      <name>TLS</name>
      <port>5061</port>
    </transport_protocol>
    <transport_protocol policy="disallow">
      <name>UDP</name>
    </transport_protocol>
    <transport_protocol policy="disallow">
      <name>TCP</name>
    </transport_protocol>
  </transport_protocols>
  <outbound_proxies>
    <outbound_proxy policy="mandatory">
      sip:outproxy.example.com
    </outbound_proxy>
  </outbound_proxies>
  <sip_methods>
    <sip_method policy="disallow">INFO</sip_method>
  </sip_methods>
  <sip_option_tags>
    <sip_option_tag policy="disallow">join</sip_option_tag>
  </sip_option_tags>
</property_set>
```
4.2 Policy Filtering

(allowed and disallowed protocols)

4.3 Override

(device prefers default ports 5060, local net requires port 11000)

5. Security Considerations

Security is mostly a profile delivery problem. The delivery framework MUST provide a secure means of delivering the profile data as it may contain sensitive data that would be undesirable if it were stolen or sniffed. Storage of the profile on the profile delivery server and user agent is an implementation problem. The profile delivery server and the user agent MUST provide protection that prevents unauthorized access of the profile data. The profile delivery server and the user agent MUST enforce the access control policies defined in the profile data sets if present.

6. Changes from draft-petrie-sipping-profile-datasets-01

The core SIP profile data set was split out from the examples in draft-petrie-sipping-profile-datasets-01 to create a stand alone data set definition.

7. References

[I-D.ietf-sipping-config-framework]
Petrie, D., "A Framework for Session Initiation Protocol User Agent Profile Delivery",
draft-ietf-sipping-config-framework-06 (work in progress), February 2005.

[I-D.petrie-sipping-profile-datasets]
Petrie, D., "A Schema for Session Initiation Protocol User Agent Profile Data Sets",
draft-petrie-sipping-profile-datasets-00 (work in progress), July 2004.

[I-D.sinnreich-sipdev-req]
Sinnreich, H., "SIP Telephony Device Requirements and Configuration",
draft-sinnreich-sipdev-req-07 (work in progress), June 2005.


Authors’ Addresses

Daniel Petrie
SIPez LLC.
34 Robbins Rd.
Arlington, MA  02476
US

Phone: +1 617 273 4000
Email: dan.ietf AT SIPez DOT com
URI:  http://www.sipez.com/
Appendix A.  SIP Protocol Dataset Schema

The following is the schema for the SIP protocol data set.

<?xml version='1.0' encoding='iso-8859-1' standalone='yes'?>
<!-- XML Schema for SIP Protocol core Data Sets -->
<schema
xmlns:spds='http://sipfoundry.org/schema/sip-ua-profile-07'
targetNamespace='http://sipfoundry.org/schema/sip-protocol-00'
xmlns='http://www.w3.org/2001/XMLSchema'>
<annotation>
<documentation>
SIP Protocol Properties.
</documentation>
</annotation>
<element name="transport_protocols"
substitutionGroup="spds::setting_container">
<annotation>
<documentation>
Container for a set of transport protocol bindings for SIP.
</documentation>
</annotation>

<complexType>
  <sequence minOccurs="0" maxOccurs="unbounded">
    <element ref="transport_protocol" />
  </sequence>
</complexType>

<element name="transport_protocol" substitutionGroup="spds::setting">
  <annotation>
    <documentation>
      Container for the properties for a single transport protocol binding for SIP.
    </documentation>
  </annotation>
  <complexType>
    <sequence>
      <element ref="name" />
      <element ref="port" />
    </sequence>
    <attributeGroup ref="spds:multi_setting_attributes" />
  </complexType>
</element>

<element name="name" type="spds:transport">
  <annotation>
    <documentation>
      Name of the specific transport protocol
    </documentation>
  </annotation>
</element>

<element name="port" type="spds:port_num">
  <annotation>
    <documentation>
      Port binding for the transport protocol
    </documentation>
  </annotation>
</element>

<element name="outbound_proxies" substitutionGroup="spds::setting_container">
  <annotation>
    <documentation>
      Container for outbound_proxy elements which define a preset route set. The q attribute determines the order of the routes in the route set.
    </documentation>
  </annotation>
</element>
<complexType>
  <sequence minOccurs="0" maxOccurs="unbounded">
    <element ref="outbound_proxy" />
  </sequence>
</complexType>

<element name="outbound_proxy" substitutionGroup="spds::setting">
  <annotation>
    <documentation>
      The next hop proxy for SIP requests without a defined route set. Value is of name-addr format. There should probably be a type defined for name-addr that outbound_proxy inherits from.
    </documentation>
  </annotation>
</element>

<element name="sip_methods" substitutionGroup="spds::setting_container">
  <annotation>
    <documentation>
      Container for list of SIP request methods to allow or disallow.
    </documentation>
  </annotation>
</element>

<element name="sip_method" substitutionGroup="spds::setting">
  <annotation>
    <documentation>
      An element to specify a SIP method. For user agents that support the method indicated, this element serves as a switch to enable or disable the named SIP method as indicated by the policy attribute.
    </documentation>
  </annotation>
</element>
Container for list of SIP option tags to allow or disallow. For user agents that support features indicated by option tags, this element serves as a list of features to turn on or off as indicated by the policy attribute in the sip_option_tag element.

Appendix B. Acknowledgments
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.
Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.