Internet Draft
Doc: draft-petrie-sipping-ua-prof-framewk-reqs-00.txt
24 June 2002
Expires: December 2002

D. Petrie
Pingtel Corp.
C. Jennings
Cisco Systems

Requirements for SIP User Agent Profile Delivery Framework

1 Abstract

This document attempts to identify the requirements for a protocol framework to provide SIP user and device profiles to SIP user agents. The objective is not to invent new special purpose protocols, but to identify the requirements such that a rational decision can be made as to what existing protocol(s) should be used to solve the problem of providing user and device profiles to SIP user agents. This document also contains an evaluation of a set of applicable protocols.

2 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" this document are to be interpreted as described in RFC-2119 [RFC2119].

Table of Contents

1 Abstract....1
2 Conventions used in this document....1
3 Overview....3
3.1 Background....3
3.2 Functional Groups....3
3.3 Terminology....4
4 Requirements....4
4.1 General....4
4.1.1 Roaming....4
4.1.2 Open and Extensible for Vendor....5
4.1.3 NAT/Firewall Support....5
4.1.4 Availability of Development Tools....6
4.2 Discovery....6
4.3 Enrollment....6
4.4 Profile Retrieval....8
4.5 Change Notification....8
4.6 Profile Upload....8
4.7 Security....9
4.8 Data Container....9
5 Protocol Evaluation....10
5.1 Evaluation Criteria....10
5.2 SNMP....11
5.3 LDAP....12
5.4 ACAP....12
5.5 SLP....13
5.6 SIP Events....14
5.7 HTTP....15
5.8 DHCP Options....16
5.9 DNS....16
5.10 XML....16
5.11 RFC 822....16
6 Security Considerations....16
7 Conclusion....16
8 References....18
9 Acknowledgments....19
10 Author's Addresses....19

3 Overview

3.1 Background

There is a general need to standardize methods for adding, enabling, and maintaining user and device profiles used by SIP user agents within a VoIP system. When one considers the effort needed to set up systems with hundreds or thousands of users and user agents, the need for reducing set up time is obvious. After a system is set up, ongoing maintenance in the form of changing the user and device profiles on a large population of user agents, is likely to be necessary and requires a similar administrative effort.

In addition to these scaling problems, it is likely that the population of user agents in any given VoIP system will be heterogeneous: the configuration strategy must be flexible enough to accommodate different needs for different users. Consequently, for VoIP system administration sanity and cost practicality, a multi-vendor profile delivery standard is needed.
This requirements document and protocol evaluation is a more formalized update to previous work in progress (e.g. expired draft draft-petrie-sip-config-framewk-reqs-00.txt) and evaluation performed by the authors.

3.2 Functional Groups

The requirements for the configuration of a SIP user agent can be divided into the following high-level functions:

- Discovery
- Enrollment
- Profile Retrieval
- Change Notification
- Profile Upload
- Security
- Data Container

These functional groups are intended only to provide a means to think about and organize the requirements. They are not required to be discrete steps, and they are not intended to dictate a specific

model.

Discovery û is the means by which a new SIP user agent can automatically discover how and where to enroll and retrieve desired device and user profile(s).

Enrollment û is the means by which the user agent makes the profile server(s) aware of its presence and desire of specific users and/or device profiles.

Profile Retrieval û is the means by which the user agent gets the desired profiles(s).

Change Notification û is the means by which the profile server tells the user agent that profiles of interest have changed. Typically the intension would be for the user agent to get those changes or updated profiles.

Profile Upload û this is the means by which the user agent or other entities in the network can update or propagate changes to a profile on the server.

Security û primarily the focus is on protecting the profiles from unauthorized access or change as well as integrity.

Data Container û the container or object model for the profile data during transport to and from the server. The primary issues are structure and hierarchy.

> Note: The specific content is considered out of scope in this document. The content requirements are addressed in [EP-CONFIG]. Ideally the container would be considered with the content requirements instead of the profile retrieval requirements. However as some of the protocols evaluated have an inherent data container the requirements are included in this document to keep the comparison on an apples-to-apples basis.

3.3 Terminology

This document uses the following terminology:

Server or Profile Server û the server(s) that provide the profile delivery framework functions defined above.

User Agent or Device û the client wishing to get or update the user or device profile(s) as defined by the above functional framework.

4 Requirements

The requirements are categorized by the functional groups defined in 3.2. In addition a general set requirements are defined up front. Each requirement is given a unique identifier for cross referencing.

4.1 General

This section contains miscellaneous requirements across all functional groups.

4.1.1 Roaming

GENRREQ-1: The profile delivery framework MUST support the ability

for profiles to roam.

That is, a user may go to another user agent within the serverÆs domain and with proper authorization, the user agent must be able to retrieve from the server and use the userÆs profile.

4.1.2 Open and Extensible for Vendor

GENOREQ-10: The profile framework MUST allow vendor differentiation on both the server and user agent sides.

> This is largely an issue of how easy it is to make a more intelligent or active server or client without breaking the standard.

GENOREQ-11: The profile server MUST be able to opaquely support vendor extensions to profiles.

> That is the server should be able to handle uploading of vendor specific data in a profile without requiring a new profile definition or schema.

4.1.3 NAT/Firewall Support

There are two primary models in which VoIP systems are deployed:

- Hosted VoIP Services ("Centrex" Model)
- Locally Administered VoIP systems ("PBX" Model)

In the extreme case of a hosted model, the only customer premises equipment is the LAN and user agents. In the locally administered model all equipment, servers, gateways and user agents are on the local premises. There is of course a spectrum of variations between. In addition there are multi-site enterprise deployments that in some aspects may appear more like the hosted model. The user agent in either model may be present in an commercial or in a residential environment.

The primary issue relating to the profile delivery framework is the presence of NATs and/or firewalls between the profile server and the user agent. It is assumed that if NATs or firewalls are present (in between) the user agents are on the inside and the profile server is effectively on the outside (e.g. public Internet).

GENNREQ-20: The user agent MUST be able to reach the profile server through a NAT or firewall to perform all of the functions in the delivery framework.

GENNREQ-21: The firewall or NAT SHOULD not require any additional configuration to enable the profile delivery framework to work.

It is assumed that certain protocols are typically enabled on the NAT or firewall by default (e.g. HTTP access to servers outside). It is assumed that SIP access in both directions is enabled or the user agent is not likely to be of much use.

4.1.4 Availability of Development Tools

The platforms (server and user agent) upon which this profile delivery framework must be deployed are very different in capability. The user agents are largely embedded systems with limited resources for code and data size as well as CPU power (pure software based user agents are less constrained). The profile server is likely to run on general purpose servers and therefore not as resource constrained.

For wide spread adoption of the profile delivery system, the tools protocol implementations required to build the profile server should be readily available.

GENAREQ-30: The protocol stack implementations needed to build a profile server SHOULD be commercially and/or publicly available, preferably with reference or open-source implementations available.

GENAREQ-31: There SHOULD be multiple implementations of the protocol stacks required in the profile server readily available.

GENAREQ-32: There SHOULD be multiple implementations of the protocol stacks required in the user agent readily available.

GENAREQ-33: There SHOULD be multiple implementations of the protocol stacks required in the user agent suitable for embedded systems.

4.2 Discovery

The purpose of discovery is to provide the means by which zero or minimal user interaction is required when plugging in a user agent for the first time in a specific profile server domain. It is likely that there is no single protocol solution for discovery due to the wide variety of typical network configurations including but not limited to networks:

- not connected to the Internet
- with no DHCP server
- with no DNS SRV support
- with a non-configurable DNS server

DISREQ-1: The user agent SHOULD be able to discover the profile server without human input.

DISREQ-2: It MUST be possible to manually set the location of the profile server for a user agent.

> This is primarily a user agent implementation issue not a protocol issue.

4.3 Enrollment

ENREQ-1: A user agent must be able to provide a unique identity to the profile server which does not change for the life of the UA.

This allows user and device profiles to be associated with a particular user agent.

ENREQ-2: A user agent requiring profiles SHOULD make itself known to the profile server.

ENREQ-3: The user agent MUST identify profiles that it requires.

ENREQ-4: The profile server MAY be provisioned to know what profiles a user agent needs by default.

There are a number of reasons for the above requirements. In large scale deployments this may be important for load balancing purposes. This may be needed by the profile server so that it can understand which user agents are dependent upon which profiles.

ENREQ-5: A user agent MAY request additional or different user profiles beyond the default provisioned for the user agent.

This is primarily to support the notion of roaming.

ENREQ-6: The user agent MUST provide specific information which may needed by the server to customize the profile(s) for the user agent.

It may be necessary to provide different views of a profile based upon the specific configuration of the user agent. (for example, Vendor, Model number, Software or firmware version, serial number, MAC address, etc.).

ENREQ-7: It SHOULD be possible for the profile server to deliver different views of a profile based upon characteristics of the user agent.

Though the objective is to provide a standardized profile that has the same content for all vendors user agents, in reality there are changes or differences to work around. That is it may be desirable to put intelligence in the profile server to work around differences in user agent behavior or changes in the standardized profile content specification.

ENREQ-8: It MUST be possible to reassigned device-specific profiles, stored in the server, to a different user agent.

This is to facilitate hardware swap out.

ENREQ-9: It MUST be possible for the profile server, over time, to

change the location(s) from which configuration data is retrieved.

The intension is to allow server handoff as the result of failure, administration changes, load balancing, etc.

ENREQ-10: The user agent SHOULD re-enroll periodically.

The user agent basically should check in periodically with the profile server in case a network problem prevented change notification from getting to the user agent.

4.4 Profile Retrieval

PRREQ-1: It MUST be possible for the user agent to retrieve the profile(s) it requires on demand.

PRREQ-2: It MUST be possible for the entire population of user agents to request and retrieve the required profiles in a short period of time.

This is a scalability requirement: e.g. during a power outage tens or hundreds of thousands of user agents may power up at once.

4.5 Change Notification

CNREQ-1: The profile server MUST be able to notify dependent user agents of profile changes.

CNREQ-2: The user agent MUST be able to get the new updated profile.

CNREQ-3: The server MAY specify in advance that a configuration change is to occur.

That is the profile server may schedule changes.

CNREQ-4: The user agent MAY defer making profile changes effective until it is safe to do so.

Some profile changes may disrupt the operation of the user agent. The user agent should use discretion as to whether the change will disrupt critical operation (e.g. a call) of the user agent. [Should there be a means of specifying immediate or when safe?]

4.6 Profile Upload

PUREQ-1: A user agent MUST be able to upload changes to a profile on the profile server.

This is to facilitate changes made either via a user interface on the user agent which are desired to be permanent as well as a

means by which a external interface (e.g. a rich GUI on a general purpose computer) may interface with the profile server.

PUREQ-2: The profile server should provide an access control mechanism to constrain who can read, write, delete, or by notified about change to profile data.

4.7 Security

User and device profiles may contain sensitive data such as passwords and identities. It MUST be possible to protect the profiles and information about the profiles.

SECREQ-1: The profile server SHOULD not provide access to profile data without authentication and authorization.

SECREQ-2: The profile server MUST not allow a user agent to update profile data without authentication and authorization.

SECREQ-3: The profile data, when transmitted over the network, SHOULD be protected against man in the middle attacks and snooping.

SECREQ-4: The profile server SHOULD not allow enrollment without authentication and authorization.

SECREQ-5: The profile server SHOULD not provide change notification of profiles without authentication and authorization.

SECREQ-6: The user agent SHOULD not interact with or trust any information from the profile server before authenticating the profile server.

SECREQ-7: The information exchanged between the user agent and the profile server SHOULD be integrity protected.

4.8 Data Container

DAREQ-1: The data container MUST support hierarchical and structured date. Note: for a better understanding of rational for this requirement see [EP-CONFIG]

DAREQ-2: It MUST be possible to define a standardized set of profile data that all user agents SHOULD support.

DAREQ-3: It MUST be possible for user agent vendors to add vendor specific data without breaking the standardized data set or requiring the creation of additional profiles.

DAREQ-4: The data container MUST be flexible enough to contain additional data without breaking the profile server or the user agent.

e.g. non-standard, vendor specific or standard updates

DAREQ-5: The user agent must be able to determine the differences when a profile has changed.

Note: this can be either by getting only the added, removed or changed data or by calculating the difference between two profiles.

5 Protocol Evaluation

The following set of protocols are those that have been suggested for the purpose of SIP user agent profile delivery framework both on the SIP and SIPPING mailing lists as well as at past work group meetings.

SNMP
LDAP
ACAP
SLP
SIP Events
HTTP
DHCP Options
DNS
XML
RFC 822

This is of course not an exhaustive list of possible protocols, but a pragmatic list.

5.1 Evaluation Criteria

The requirements defined in section 4 define a set of criteria for by which protocols may be evaluated for use in the profile delivery framework.

The following table indicates the functional area for which the protocols are considered. This table indicates which requirements will be evaluated for each of the protocols. As no single protocol provides all of the functional areas, the objective is to find a small set of protocols that will best satisfy the requirements. All protocols are evaluated against the general requirements in section 4.1.

	SNMP	LDAP	ACAP	SLP	HTTP	SIP	XML	822	DHCP	DNS
Discovery				X					X	X
Enrollment	X		X	X		X				
Profile Retrieval	X	X	X		X					
Change Notification	X		X			X				

Profile Upload	X	X	X		X	
Security	X	X	X	X	X	X

			xxxxx			
Data Container	X	X	X		X	X

In each of the following subsections to section 5 a general over evaluation is made of the protocol. In addition the requirements which are NOT satisfied fully or as well as other protocols are explicitly listed or discussed. Those requirements that are satisfied are generally not explicitly called out or listed.

5.2 SNMP

SNMPv3 [SNMP] is evaluated and referred to as SNMP in this document. SNMP has no discovery mechanism.

General

There are two aspects of the roaming requirement (GENRREQ-1), neither of which are solved very well by SNMP.

- Physical relocation of a user agent in a different LAN
- Users moving to a different user agent which subsequently requires a new user profile

It is very difficult to support a user whose preferences are stored outside the local management domain. This physical relocation of a user agent (e.g. user agent on a laptop in a visited LAN) is a very desirable scenario. Because of its security model, SNMP does not work very well outside of its local domain.

To support a user (one or more) temporarily using a user agent, the user agent would have to support the access of multiple, variable user profiles. MIBs do support the ability to have arrays or multiple instances of an object (typically leaf nodes). However MIBs do not support multiple instances of a hierarchy (e.g. multiple user profiles each with a hierarchy of content).

It is difficult to make an active SNMP server. SNMP is primarily a push model. It is difficult to make an intelligent profile server where traps are not designed into the standard profile MIB (GENOREQ-10).

MIBs have a very rigid schema that makes it difficult to add vendor specific data without breaking the MIB or having to create a new MIB (GENOREQ-11). Supporting the vendor differentiation through MIBs would make management difficult.

SNMP will not work through a NAT or firewall by default. It is also likely that a firewall administrator will have serious concerns letting SNMP traffic through their firewall.

Enrollment

ENREQ-5 has the same issues with multiple user profiles as described above for general requirement GENRREQ-1.

ENREQ-7 has the same issues as GENOREQ-10 and GENOREQ-11 described above.

Profile Retrieval

As SNMP uses a push model, the user agent must throw a trap or inform to tell the server to push a profile to the user agent. In addition the issue with multiple user profiles, described above with GENRREQ-1, make it difficult to satisfy PRREQ-1.

SNMP does not scale very well to individual dynamic nodes. It is difficult to build a system managing more than tens of thousands of users. User agents from some vendors do not have sufficient persistent memory to store a whole user or device profile. After a power outage tens or hundreds of thousands of user agents would all power up, throw traps requesting profiles.

The push model of SNMP make it difficult to make changes from the user agent (PUREQ-2). A solution perhaps could be built using a trap. However this would not enable other entities (non-user agents) to set profile data.

Change Notification

There is no delayed setting of MIB data. A SNMP agent either accepts the change or rejects it immediately (CNREQ-3 and CNREQ-4).

Data Container
DAREQ-3 and DAREQ-4 are not well supported due to the rigid nature of MIBs described above relative to GENOREQ-11.

5.3 LDAP

The authors did not have sufficient time to complete a thorough evaluation of LDAP.

5.4 ACAP

General

ACAP was not designed to be active on the server side. It has more of a database model. It is probably possible to make the data access active or intelligent, however this is make more difficult by the lack of implementations (GENOREQ-10).

ACAP [ACAP] over TLS [ACAP-TLS] is evaluated to satisfy the security requirements. The authors were not able to find a commercially or publicly available version of ACAP written in C, C++ or Java (GENAREQ-30, GENAREQ-31, GENAREQ-32, GENAREQ-33).

ACAP does not support any discovery mechanism and was not evaluated for this functional area.

Enrollment

Due to the difficulty of making the profile server active for Change Notification (as described above in the general requirements evaluation of ACAP), it is also difficult to provide different views of data based upon characteristics of the user agent (ENREQ-7). The different views would have to be designed into the schema requiring coordination on both the user agent and server sides.

Without an event mechanism (see below) or a means to redirect profile data requests to another server it is difficult to re-assign a user agent to an alternative ACAP server (ENREQ-9).

Change Notification

ACAP does not support an event mechanism. It uses a polling model. This makes it difficult to make profile data changes effective immediately. A very short polling time must be used which does not scale well with large numbers of user agents. Alternatively with a longer pooling period, user agents will be slow to make the profile changes effective (CNREQ-1, CNREQ-2, CNREQ-3 and CNREQ-4).

Profile Retrieval

ACAP meets the requirements for profile retrieval.

Profile Upload

ACAP provides a means of updating the profile data with access control.

Security

Security is provided via TLS.

Data Container

ACAP does have a rich hierarchal structure for containing profile data. In addition it has a powerful means of describing access control and modification time stamping of data.

5.5 SLP

SLP [SLP] is primarily a LAN based solution for discovery of services. It allows the discovery of URL or server and port for a well named service. SLP is not appropriate for profile retrieval, change notification or profile update. Nor does it provide a data container.

General

As SLP is primarily for LAN based discovery where roaming functionality is not applicable (GENRREQ-1). Likewise vendor

differentiation in the server and user agent are less applicable (GENOREQ-10 and GENOREQ-11).

It is difficult to make SLP work through NATs or firewalls (GENNREQ-20, GENNREQ-21).

Enrollment

The ability to provision or create active responses to user agent request makes ENREQ-3, ENREQ-4, ENREQ-5 and ENREQ-6 more appropriately performed with protocols other than SLP.

As SLP does not get involved with the profile retrieval, update or change notification enrollment requirements: ENREQ-7, ENREQ-8, ENREQ-9 and ENREQ-10 are not applicable to SLP.

Security

For the above reason security requirements: SECREQ-1, SECREQ-2, SECREQ-3 and SECREQ-5 are also not applicable.

SLP does not authenticate or authorize the user agent. It assumes that is preformed by the server performing the profile retrieval, upload and change notification functions (SECREQ-4).

5.6 SIP Events

The only appropriate use of SIP is for its event mechanism [SIP-EVENTS]. SIP is evaluated assuming SIPS and S/MIME [SIP] support for the security functionality. SIP provides a very powerful event framework through the SUBSCRIBE and NOTIFY messages.

SIP is not appropriate for profile retrieval or upload. It is not a data transport protocol. Nor does SIP provide a data container. SIP does support multicast that could be used as a discovery mechanism. However it is not evaluated for discovery features.

General

The primary requirement for vendor differentiation is in the enrollment, profile retrieval, update and change notification. SIP does allow active server and client side components. However this is not considered necessary for this requirement (GENOREQ-10) and considered not applicable.

As SIP is not consider appropriate for profile retrieval or upload it is consider not applicable to GENOREQ-11.

Enrollment

The SIP SUBSCRIBE mechanism of [SIP-EVENTS] satisfies all of the enrollment functional requirements.

Change Notification

CNREQ-2 is not applicable to SIP. It is more related to the profile retrieval mechanism used.

The deferral of making profile changes effective is a user agent implementation issue in the context of [SIP-EVENTS]. CNREQ-4 is considered to be not applicable to SIP.

Security

As SIP is not proposed as a data transport for profile data SECREQ-2 and SECREQ-3 are not applicable.

The security capabilities of [SIP] are considered to satisfy the other security requirements.

5.7 HTTP

HTTP [HTTP] is considered for the purpose of transporting the data profiles (profile retrieval and upload). To satisfy the security requirements [HTTPS] is assumed.

General

As HTTP is used primarily for transport GENOREQ-11 is consider to be non-applicable. However active HTTP pages could be used to help support this requirement.

Enrollment

Enrollment is considered to be mostly not applicable to the proposed use of HTTP. However ENREQ-7 can be satisfied as part of profile retrieval. This would require active pages on the profile server.

Profile Retrieval

HTTP satisfies all of the profile retrieval requirements.

Change Notification

Enrollment is considered to be mostly not applicable to the proposed use of HTTP. However CNREQ-2 can be satisfied as profile retrieval.

Profile Upload

HTTP provides gross level access control of profile. However to get atomic level access control on elements of the profile data requires the development of active pages on the profile server (PUREQ-2).

The security capabilities of [HTTPS] are considered to satisfy the security requirements.

5.8 DHCP Options

[SIP-DHCP]

General
Discovery

5.9 DNS

[DNS]
[DNSSRV]

General
Discovery

5.10 XML

General
Data Container

5.11 RFC 822

General
Data Container

6 Security Considerations

Security considerations are covered in section 4.7.

7 Conclusion

The following tables rate the protocols according the the requirements. The rating indcates how well the protocol satisfies the requirment. The notation used is defined as follows:

No : No support of requirement
L : Low suppport of requirement
H : High support of requirement
- : Not applicable to requirement

	SNMP	ACAP	SLP	HTTP	SIP	XML	822	DHCP	DNS
GENRREQ-1	No	H	-	H	H	-	-	-	-
GENOREQ-10	L	L	-	H	-	-	-	-	-
GENOREQ-11	L	H	-	-	-	H	M	-	-

GENNREQ-20	L	H	L	H	H	-	-	-	H
GENNREQ-21	No	H	L	H	H	-	-	-	H
GENAREQ-30	H	L	L	H	H	H	H	H	H
GENAREQ-31	H	L	L	H	H	H	H	H	H

GENAREQ-32	H	L	L	H	H	H	H	H	H
GENAREQ-33	L	L	L	H	H	H	H	H	H
DISREQ-1			H					H	H
DISREQ-2			-					-	-
ENREQ-1	H	H	H		H				
ENREQ-2	H	H	H		H				
ENREQ-3	H	H	L		H				
ENREQ-4	H	H	L		H				
ENREQ-5	L	H	L		H				
ENREQ-6	H	H	No		H				
ENREQ-7	L	L	-	H*1	H				
ENREQ-8	H	H	-		H				
ENREQ-9	H	No	-		H				
ENREQ-10	H	H	-		H				

*1 Note: this capability could be provided either as part of enrollment or profile retrieval. Therefore HTTP is evaluated here as providing ENREQ-7 as part of profile retrieval.

	SNMP	ACAP	SLP	HTTP	SIP	XML	822	DHCP	DNS
PRREQ-1	L	H		H					
PRREQ-2	L	L		H					
CNREQ-1	H	No			H				
CNREQ-2	H	No		H*2	-				
CNREQ-3	No	No			H				
CNREQ-4	L	No			-				

*2 Note: this capability could be provided either as part of change notification or profile retrieval. Therefore HTTP is evaluated here as providing CNREQ-2 as part of profile retrieval.

	SNMP	ACAP	SLP	HTTP	SIP	XML	822	DHCP	DNS
PUREQ-1	H	H		H					
PUREQ-2	L	H		L					
SECREQ-1	H	H	-	H	H				
SECREQ-2	H	H	-	H	-				
SECREQ-3	H	H	-	H	-				
SECREQ-4	H	H	No	H	H				
SECREQ-5	H	-	-	H	H				
SECREQ-6	H	H	H	H	H				
SECREQ-7	H	H	H	H	H				
DAREQ-1	H	H				H	L		
DAREQ-2	-	-				-	-		
DAREQ-3	L	H				H	H		
DAREQ-4	L	H				H	H		

DAREQ-5	H	H			H	H

The discovery solution is best addressed separately. Due to the varied nature of most network environments, there is no single solution that will work everywhere. It is probably necessary to support multiple protocols. Due to the widespread deployment and use of DHCP and DNS they are the best two candidates for discovery, although SLP can be used in network that already support it.

The data container requirements are equally satisfied by XML and ACAP largely due to their ability to support an extensible, hierarchal schema. XML seems to have an advantage as well based on the wide spread availability of development tools that operate on XML. Both ACAP and HTTP address the profile retrieval and upload requirements, although the relative maturity of XML over HTTP is very attractive.

SIP is the only protocol that addressed all the relevant enrollment and change control requirements.There was no single protocol that satisfied all of the requirements in the other functional areas. However a combination of HTTP and SIP satisfies all of the remaining requirements to a high degree. In addition the large number of implementations and development tools make this combination the most attractive solution. The development as well as end user (e.g. administrator) skill sets are much more readily available for these protocols as well. As a second choice ACAP and SIP seems to be the only other reasonable combination.

8 References

[SIP] M. Handley, E. Schooler, and H. Schulzrinne, "SIP: Session Initiation Protocol", RFC2543, Internet Engineering Task Force, Nov 1998.

[SIP] draft-ietf-sip-rfc2543bis-09.txt

[RFC2026] S Bradner, "The Internet Standards Process -- Revision 3", RFC2026 (BCP), IETF, October 1996.

[RFC2119] S. Bradner, "Key words for use in RFCs to indicate requirement levels," Request for Comments (Best Current Practice) 2119, Internet Engineering Task Force, Mar. 1997.

[HTTP] R. Fielding et al, ôHypertext Transfer Protocol -- HTTP/1.1ö, Request for Comments (Standards Track) 2616, Internet Engineering Task Force, June 1999

[HTTPS] E. Rescorla, ôHTTP Over TLSö, Request for Comments 2818, Internet Engineering Task Force, May 2000

[TLS] T. Dierks, C. Allen, ôThe TLS Protocol Version 1.0ö, Request for Comments 2246, Internet Engineering Task Force, Jan. 1999

[EP-CONFIG] draft-stredicke-sipping-ep-config-00.txt

[SNMP] Request for Comments 2570-2576, Internet Engineering Task Force

[ACAP] Request for Comments 2244, Internet Engineering Task Force

[ACAP-TLS] Request for Comments 2595, Internet Engineering Task Force

[SLP] Request for Comments 2608, Internet Engineering Task Force

[SIP-EVENTS] A. Roach, ôEvent Notification in SIPö, <draft-ietf-sip-events-05.txt>, IETF; February 2002, Work in progress.

[DHCP] S. Alexander and R. Droms, "DHCP options and BOOTP vendor extensions," Request for Comments (Draft Standard) 2132, Internet Engineering Task Force, Mar. 1997.

[SIP-DHCP] G.Nair, H.Schulzrinne , ôDHCP Option for SIP Serversö, <draft-ietf-sip-dhcp-06.txt>, IETF; March 1, 2002, Work in progress.

[DNSSRV] M. Mealling and R. Daniel, "The naming authority pointer (NAPTR) DNS resource record," Request for Comments 2915, Internet Engineering Task Force, Sept. 2000.

[XML] T. Bray, J. Paoli, C. Sperberg-McQueen and E. Maler, "Extensible Markup Language (XML) 1.0 (Second Edition)", W3C Recommendation, October 2000, <http://www.w3.org/TR/2000/REC-xml-20001006>

[RFC822] D. Crocker, ôSTANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGESö, Request for Comments 822, Internet Engineering Task Force, Aug. 1982

[UA-PROF-FRAMEWORK] draft-petrie-sipping-config-framework-00.txt

9 Acknowledgments

Thanks to Henry Sinnreich and Henning Schulzrinne for their input and review of this document.

10 Author's Addresses

Daniel G. Petrie
Pingtel Corp.
400 W. Cummings Park
Suite 2200

Woburn, MA 01801
USA
Phone: +1 781 938 5306
Email: dpetrie@pingtel.com

Cullen Jennings
Cisco Systems
170 West Tasman Drive
MS: SJC-21/3
San Jose, CA 95134
USA
Phone: +1 408 527-9132
EMail: fluffy@cisco.com