3GPP TSG-CN Meeting #24 **NP-040272**
02 – 04 June 2004, Seoul, KOREA

Source: **CN5 (OSA)**

Title: **Rel-6 CR 29.198-14 OSA API Part 14: Presence and Availability Management (PAM) (Correction of introduction of PAM Provisioning Interfaces)**

Agenda item: **9.7 (OSA Enhancements [OSA3])**

Document for: **APPROVAL**

Doc-1st-	Spec	CR	Rev	Phase	Subject	Cat	Version	Doc-2nd-	Workite
NP-040272	29.198-14	020	-	Rel-6	Correction of introduction of PAM Provisioning Interfaces	F	6.0.1	N5-040110	OSA3

CR-Form-v7

CHANGE REQUEST

⌘ 29.198-14 CR 020 ⌘rev - ⌘ Current version: 6.0.1 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction of introduction of PAM Provisioning Interfaces
Source:	⌘	CN5 Ultan Mulligan, ETSI PTCC
Work item code:	⌘	OSA3
Date:	⌘	6/02/2004
Category:	⌘	**F**
Release:	⌘	*REL-6*

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The PAM Provisioning interfaces were introduced in 3GPP for the first time, at the creation of the Release 6 PAM specification. However, the service properties for PAM either forbid the use of PAM Provisioning, or refer to its being out of scope.
Summary of change:	⌘	Add text in clause 4 referring to creation and use of identities, which was removed from the Release 5 PAM specification since the interfaces for creation of identies were out of scope of Release 5 Modify the service properties in clause 10 to remove some of the restriction on what interfaces to use in 3GPP. All the PAM Provisioning interfaces are now within the scope of 3GPP, so there is no need to explicitly list all interfaces as obtainable: listing them would in fact require all interfaces to be obtainable. Likewise for the events: Release 5 PAM both permitted and required the use of 3 events - many more are applicable for Release 6, but listing them has the effect of requiring their support, which might not be desirable. The description of TpPAMAttributeDef in clause 11 referred to it's being unused in the 3GPP specification - this is no longer the case with the introduction of the PAM Provisioning interfaces.
Consequences if not approved:	⌘	The PAM Provisioning Intefaces, although described in the Release 6 PAM specification, would be forbidden to be used, in the same specification, by implementations of 3GPP Release 6 PAM.

Clauses affected:	⌘	4, 10, 11

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

Change in Clause 4

4 Presence and Availability Management SCF

4.1 Introduction

The goal of these interfaces is to establish a standard for maintaining, retrieving and publishing information about

- Presence and Availability of entities for various forms of communication and the contexts in which they are available.

4.2 Motivation

Consider the following simple but desirable scenario for a communication service: An end-user wishes to receive instant messages from her management at any time on her mobile phone, from co-workers only on her desktop computer, and in certain cases for the messages to be forwarded to e-mail or even a fax machine/printer. The senders may know her availability for various forms of communication in the way she chooses to reveal it or alternatively the senders may never know how she will be receiving their messages. This scenario spans over multiple services and protocols and can only be solved currently by a proprietary solution that maintains the required information in an ad-hoc fashion within the application.

PAM is not a replacement for the protocols being standardized for various communication and network services. PAM attempts to standardize the management and sharing of presence and availability information across multiple services and networks.

The PAM specification is motivated by the observations that

- The notions of Identity, Presence and Availability are common to but independent of the various communication technologies, protocols and applications that provide services using these technologies.
- Presence does not necessarily imply availability. End-users or organizations require greater control over making themselves available through various communication devices.
- Presence based services need to address privacy concerns on who can access presence information and under what conditions.

Management of availability will span over multiple communication services and service providers.

4.3 Goals

The purpose of this document is to adopt the first release of a Presence and Availability Management interface specification created by an industry consortium, PAM forum, established for this purpose harmonized with the IETF model for presence (RFC 2778). This specification is also consistent with the ongoing work in 3GPP for defining the requirements and architecture for a standard presence service in the network.

With a desired goal of rapid acceptance and usage, the specification has been deliberately designed to be as simple as possible with an attempt to include a minimal set of functionality that is sufficient for use in non-trivial applications. Often, this has been at the cost of some useful features, which would have made the specification baroque and cumbersome if not controversial.

4.4 Concepts

This chapter briefly describes the various concepts involved in this specification to serve as the context for the rest of the document.

4.4.1 Identity

Identity, for purposes of the PAM specification, is a limited electronic representation of an entity (i.e., an individual or an organization) that participates in PAM-enabled applications and services. This concept corresponds to the concept of Presentity as described in the IETF Common Presence and Instant Messaging Model (RFC 2778).

The main characteristic of an entity that is central to PAM specifications is the name (or handle) by which entities are identified by applications and services. Entities may have multiple names, login ids, account names, etc., by which they are identified. As PAM attempts to abstract over multiple networks and services, it does not assume that a single name will necessarily identify entities across all application domains.

The generalized structure available in 3GPP for user names that may contain various formats for addressing has been adopted for these specifications.

To enable entities to be identified by any of the names associated with them, PAM identities can be assigned aliases. A name and a namespace pair can be defined as an alias of another name and namespace pair. It is important to note that aliases are just synonyms and hence have limited semantics. In particular, they are not powerful enough to model personas each with their own capabilities and privacy requirements.

An identity can represent a single entity or a group of identities. Group identities have similar semantics to non-group identities but, in addition, maintain a list of identities that constitute the group. As an example, a sales department may be modelled as a group identity with the identities of the members of the department being member identities of the group. Group identities and their member identities do not inherit anything from each other.

No other relationships between identities are within the scope of the PAM specifications.

For flexibility and extensibility, attribute lists are used to associate additional data with identities. Identities are typed to provide a way to manage such attribute lists. An identity type may be associated with a specific set of attributes and all identities of that type inherit instances of such attributes.

For consistency with IETF (RFC 2778) defined presence data models, PAM pre-defines an identity type Presentity with a list of presence attributes as defined in TS 22.141 based on the definitions in RFC 2778.

PAM implementations may map certain existing directory and database data to one or more types to allow access via PAM interfaces. PAM specifications do not specify how the data within the profiles are to be stored. They may be stored within the PAM implementation or mapped to data stored on external directories and databases.

4.4.2 Presence

The concept of presence has been used in several application areas, being most explicit in Instant Messaging. Starting from a simple notion of online/offline status, it has expanded to include other context information around the status such as disposition (out to lunch, away from the computer, etc.) and activity status (on the phone, idle, etc.). Location information, on the other hand, has largely been kept separate from what has been traditionally considered presence information. PAM specifications broaden the concepts of presence recognizing that all such information, including location, describes different contexts of an entity's existence. The unifying property is that the presence information is continually changing and that there is value in knowing the current information at different points in time for services and applications.

For the purposes of PAM specifications, presence is an extensible set of characteristics that captures the dynamic context in which an identity or an agent exists at any point in time. In contrast to the relatively static information about identities or agents (e.g., names, addresses, capabilities), presence refers to dynamic information such as location, status, disposition, etc. Registrations of presence and location information in existing applications are covered by this definition.

Presence information is differentiated from the more static information associated with identities and agents that are stored in attributes. The rationalization for this design is that the presence information is dynamic and has implications on the implementation. Some of the presence information is too dynamic to be maintained in static data stores such as directories and without this hint about the data characteristics, PAM implementers may make sub-optimal decisions on the way the data is stored. Second, presence information typically has expiration data that needs to be understood by the implementation.

The PAM specification recognizes that devices that provide presence information are not necessarily devices that communicate.

The PAM specification does not specify the methods by which the presence information is derived. For example, an instant messaging client on a desktop computer can register its status based on when a user is logged in. A mobile phone may do an explicit registration on a WAP server for instant messaging. The phone's presence for voice calls, on the other hand, may be inferred implicitly by querying the cellular network for the device being on when requested. The presence of an identity, on the other hand, may be computed using presence information from one or more devices owned by the identity.

Finally, the PAM specification does not require that the presence information be stored explicitly (i.e., in a materialized fashion) in a PAM implementation. An implementation may infer the presence information on demand from the underlying services or networks.

For compatibility with the presence model from IETF (RFC 2778), a type called Presentity is pre-defined with the attributes consistent with the IETF Presence model.

4.4.3 Availability

Availability is a property of an identity denoting its ability and willingness to share information about itself or to communicate with another identity based on factors such as the type of communication requested, the identity of the calling entity and the preferences and policies that are associated with the recipient. This is the primary means by which the current PAM specification enables controls for privacy. While presence is, in most applications, a necessity for availability, presence does not necessarily imply availability to all.

Availability is always with respect to a context. A context in PAM specifications is a set of attributes defining the state in which the availability is requested. For example, the query "Is Jane available for IM for Rob?" identifies the type of communication and the identity of the asker as the context. PAM allows for availability to be differentiated based on any attribute of a context. A context, "Communication" is pre-defined in PAM.

Most queries for presence in existing applications can be mapped into PAM availability queries to control the information being given out. Alternatively, queries can be mapped directly into PAM presence queries in situations where privacy controls and policies are not required or all presence data is open to the entity querying. This allows PAM specifications to be consistent with existing presence servers and to serve as the basis for presence services across multiple protocols while providing uniform and flexible privacy controls.

PAM specification does not specify whether the availability is computed on demand or stored explicitly. In some applications, the availability may be pre-computed and stored explicitly while in some, it may be computed at each request for availability.

While the PAM specification provides a mechanism to associate preferences with an Identity to control availability, it neither specifies the syntax and semantics of the preferences nor the process by which the availability is computed. These aspects are left to the implementation.

For example, a particular implementation may provide the facility to store preferences as rules such as "I prefer to receive my instant messages on my computer rather than my cell phone unless the message is from my boss or the computer is off, etc.".

As an example, a computation of availability for communication may consist of the following algorithm:

1) Find all devices of the identity being called that are capable of the specified form of communication AND have registered their presence status as available.

2) Evaluate the rules associated with the identity being called to select the preferred device(s) from the set of present devices determined in Step 1.

3) If there are any devices available satisfying Step 2, indicate the availability of the identity being called via the available devices.

An implementation can chose to provide one or more means to specify preferences. It is expected that if there is industry standardization on the specification of preferences, the implementations will support such a standard. This is currently outside the scope of PAM.

4.4.4 Events

Events are representations of certain identified occurrences related to the concepts described above. The PAM specification provides for registering interest (i.e., callbacks) in being notified of such occurrences. Any entity that subscribes to the Event is a "watcher" in the IETF terminology (RFC 2778). An implementation is expected to provide such notifications.

Examples of events include,

- Creation/deletion of an identity.
- Change in the presence information of an identity
- Change in availability of an identity for a particular form of communication

PAM specifications contain a set of pre-defined events. Each event is defined by a name of the event, a set of input attribute value pairs that must be provided when an event is registered for and a set of attribute value pairs that are included in the notifications sent out when the event of interest occurs.

4.5 Scope of PAM information

Presence and Availability Management has the following types of information in its scope:

- Identities, which consist of names and aliases of entities participating in communications.
- Presence information, which consists of an identity's dynamic characteristics such as status and geographical location.
- Availability information, which consists of preferences associated with identities and computation of availability, based on the devices present and the current preferences.
- Notification of changes to the above pieces of information.
- Security issues for access to this information.

The PAM specification consists of interfaces to manage or access the above information.

The specification purposefully does not include

- Storage design or storage requirements for any of the presence and availability information.

These are to be decided by specific implementations of the PAM specification.

4.6 Security and privacy

As the Presence and Availability Management interface is designed to share information across administrative domains and to facilitate availability computation based on the identity of the entity desiring communication, security and privacy issues are addressed in the design. Two of the issues considered to be within the scope of PAM are:

- Access control to an implementation of the PAM specification.
- Use of an authenticated entity's credentials by methods in the specification.

To understand the distinction between the first two issues, consider, for example, an end-user that logs on to an Instant Messaging client and wishes to send a message. The client (or a gateway to which the client talks to) may access a PAM implementation to determine the availability of the destination for the message. The client (or the gateway) will need to be authorized for access to the PAM implementation independent of the user that logs in. A gateway may, in fact, do this access on behalf of a number of clients and, for performance reasons, wish to authenticate itself just once on start up rather than at each invocation. This authentication is handled by the authentication mechanisms in the OSA Framework common to all services within OSA.

Second, each invocation of a particular method will need to contain the credentials of the end-user that logged into the client so that the computation of the availability can take that into account when necessary for privacy issues.

It should be noted that the PAM specification allows for the possibility that the authentication of the end-users is not necessarily done within the PAM implementation itself. As long as the authenticated credentials supplied by the client (or gateway) are acceptable for validation and the client (or the gateway) itself is authenticated by the implementation, the authentication of end-users can occur anywhere outside the PAM implementation. A deployment scenario for a particular application is that one or more authentication services are provided as external services over PAM implementations.

This design does not preclude the possibility that the client (or the gateway) cannot be authenticated. Therefore, the credentials supplied by the client (or the gateway) may be held to stronger authentication criterion than credentials supplied by a trusted client (or gateway).

Finally, the PAM specification does not mandate the use of authentication within an implementation if the environment in which it is used does not require it.

Clause 5.1 explains the mechanism for providing data about the asker to each of the methods with a sequence diagram.

Privacy issues are addressed primarily by providing a mechanism to control the information flowing out of a PAM implementation based on whatever criterion the end user may choose to specify in the availability preferences and independent of any particular application.

The following security issues were considered to be outside the scope of PAM:

- Authentication of the identity of the end-users or entities. As explained above, this authentication may be provided by a third-party authentication service or it may occur through an authentication service written over the PAM platform. The only requirement is that the type of credentials supplied by the authentication service be acceptable to the PAM platform implementation being accessed.
- Encryption of the flow of information between a PAM platform implementation and clients of this implementation. This is dependent on the method of access to the interface which is outside the scope of the PAM specification and hence to be determined by the implementation.

End of Change in Clause 4

Change in Clause 10

10 PAM Service Properties

The following table lists properties relevant to all the PAM SCFs.

Property	Type	Description
P_OBTAINABLE_INTERFACES	STRING_SET	The interfaces obtainable from the service
P_SUPPORTED_ATTRIBUTE_TAGS	STRING_SET	Lists the supported attribute tags defined by TpAttributeTagInfo
P_SUPPORTED_SIMPLE_ATTRIBUTE_TYPES	STRING_SET	Lists the supported attribute types defined by TpSimpleAttributeTypeInfo
P_SUPPORTED_STRUCTURED_ATTRIBUTE_TYPES	STRING_SET	Lists the supported attribute types defined by TpStructuredAttributeType, e.g. P_org/csapi/TpAddress.
P_SUPPORTED_XML	STRING_SET	Lists the supported versions of XML specifications such as XML schema specifications (e.g. through URLs), XML versions (e.g. version 1.0) or XPath (e.g. version 1.0)

Implementations of the PAM APIs shall have the Service Properties set to the indicated values at a minimum:

```
P_SUPPORTED_ATTRIBUTE_TAGS = {
P_SIMPLE_TYPE
}
P_SUPPORTED_SIMPLE_ATTRIBUTE_TYPES = {
```

```
P_STRING,
P_FLOAT,
P_INT32
}
```

~~10.1PAM Provisioning service properties~~

~~Implementations of the PAM Provisioning APIs for 3GPPshall have the Service Properties set to the indicated values:~~

```
~~P_OBTAINABLE_INTERFACES = {}~~
```

~~10.2~~10.1 PAM Access Service

Implementations of the PAM Access APIs for 3GPPshall have the Service Properties set to the indicated values:

```
P_OBTAINABLE_INTERFACES = {
P_PAM_IDENTITY_PRESENCE,
P_PAM_AVAILABILITY
}
```

~~10.3~~10.2 PAM Event Service

PAM Event service has the following property in addition to the above.

Property	Type	Description
P_EVENT_TYPES	INTEGER_SET	The pre-defined event types that can be registered for

~~Imple~~

~~mentations of the PAM Event APIs for 3GPP shall have the Service Properties set to the indicated values:~~

```
~~P_OBTAINABLE_INTERFACES = {~~
~~P_PAM_EVENT_HANDLER~~
~~}~~
~~P_EVENT_TYPES = {~~
~~PAM_CE_IDENTITY_PRESENCE_SET,~~
~~PAM_CE_AVAILABILITY_CHANGED,~~
~~PAM_CE_WATCHERS_CHANGED~~
~~}~~
```

End of Change in Clause 10

Change in Clause 11

11 PAM Data Definitions

All data types referenced in this document but not defined in this clause are common data definitions which may be found in 3GPP TS 29.198-2.

11.1 Entity Address Definitions

11.1.1 TpPAMFQName

This is the same as TpURN and is used to name entities in PAM Access service.

11.1.2 TpPAMFQNameList

This is a Numbered List of Data Elements of type TpPAMFQName.

11.2 Attribute Data Definitions

11.2.1 TpPAMAttribute

This is a Sequence of Data Elements containing the attribute name, expiration time and value. This is derived from the common attribute type TpAttribute to add the expiration value for dynamic attributes.

Sequence Element Name	Sequence Element Type	Notes
AttributeName	TpString	The name of the attribute.
AttributeValue	TpAttributeValue	The typed value(s) for the attribute.
ExpiresIn	TpPAMTimeInterval	The interval in milliseconds in which the attribute values are valid. A time interval of PAM_MAX_LONGINT indicates static attribute values that never expire. A time interval of 0 or negative values indicate an expired value and the time for which it has expired.

11.2.2 TpPAMAttributeList

This is a Numbered List of Data Elements of type TpPAMAttribute.

11.2.3 TpPAMAttributeDef

This is a Sequence of Data Elements containing the definition of an attribute. This definition constitutes the "schema" for an attribute and contains fields to define the type and behavior of a dynamic attribute. Each definition using these fields results in a TpPAMAttribute with the corresponding name and type and dynamic behavior as defined by the remaining fields. ~~In 3GPP Release 6, no methods exist to create PAM attributes at runtime and hence this type is not used in any method. However, certain pre-defined attributes are defined for identity presence in Section 11.10 using the following fields. This type is included in this document to specify the semantics of the fields in the pre-defined attributes.~~

Sequence Element Name	Sequence Element Type	Notes
Name	TpString	Name of attribute
Type	TpString	Type of attribute. Valid values for Type must include at least TpString, TpInt32 and TpFloat
IsStatic	TpBoolean	True indicates that the attributes is always static and its values never expire. False indicates that the attribute can be dynamic and may contain values that expire.
IsRevertOnExpiration	TpBoolean	True indicates that the attribute reverts to the default value on expiration. False indicates that the attribute will not revert to the default value.
DefaultValues	TpAny	An attribute is always initialized with this value. If the *isRevertOnExpiration* attribute is set to true, a dynamic attribute that has expired while stored in a PAM implementation is reset to this value with the *expiresIn* interval set to PAM_MAX_LONGINT. The default attribute value is interpreted based on the value of the attribute Type.

11.2.4 TpPAMAttributeDefList

This is a Numbered List of Data Elements of type TpPAMAttributeDef.

End of Change in Clause 11