SMS Framework: AAA Considerations

The application of AAA services (authentication, authorisation and accounting) to the SMS Framework creates a number of hurdles in terms of implementation but also will greatly increase the flexibility and ease-of-use of sites which use it. For the purpose of this discussion, the following count as “user-facing” AAA:

- authentication: the initial validation of a user's mobile phone number and the confirmation that the user is the 'owner' of the number provided
- authorisation: the verification of that user's consent to receive messages, the removal of that consent in the event of a STOP message,
- accounting: the collection of billing information and other related events

In terms of “site-facing” AAA, the following additional considerations apply:

- authentication: ensuring that users and processes creating, sending or acting upon messages or message subscriptions are valid users
- authorisation: verifying that authenticated users or processes are (a) sending messages to valid users with a current consent ('opt-in') and in a currently authorised number range (for example, whether authenticated or not, a site-user should not be able to send messages to a premium-rate destination, or an international destination in a single-jurisdiction site)
- accounting: monitoring account balance(s) with gateway provider(s) and generating alerts, correlating 'user' accounting with 'traffic' accounting

The authentication steps, in both cases, are in many ways the easiest: it would be desirable to extend 'user' authentication to allow for models other than that standard Drupal mechanism but that has to be done with care to stay within 'site' authentication and the rules imposed by various regulators[1].

Both authorisation and accounting require further subdivision, into per-subscriber and per-message in the case of authorisation, and per-gateway and per-site accounting (per-site being an aggregate of per-gateway). As it is the simpler of the two areas, accounting will be discussed first.

The accounting needs of most SMS systems are relatively simple: tracking the number of messages sent and received, per MSISDN, per gateway. Financial accounting, in terms of tracking messages in GBP/USD/EUR, is not something that should be done within the “call flow” as the overhead in keeping track of changing message rates for each gateway and each destination is significant, however tracking “MSISDN;gateway;MOvsMT” for each message adds little overhead. It should however be done within the Framework and not within Drupal's standard logging mechanisms: it needs to be audit-able and isolated from other data. It also needs to use a write-once storage mechanism. The message costs and gateway balance do however become important if multiple gateways are used, and a provision should be made for storing rate tables and making such information available for message routing decisions if a true multiple-gateway / multiple-carrier Framework is to be developed in the future.

1 This is not as complex an area as it may seem, in terms of different jurisdictions: starting with the EU norms provides a 'tried and tested' starting place that is more rigorous than many others

Authorisation is the most complex of the three AAA services and also must be the most efficient as it will be necessary to make authorisation calls before each message is sent. In terms of system efficiency there are several ways to reduce the load this incurs, although several are database-specific. For example, additional fields in sms_user could be used to reflect opt-in status, number validity, account status etc, and a single unified view presented to the actual send function, with the non-authorised numbers already removed. The 'user-level' authorisation can be managed in response to changes (for example, an SMS Action can handle STOP messages by changing an “opt-in” field to 'N'): where “site-level” changes are made they will be through the admin interface, and so database updates should not be a complex issue. It is also worth noting that the majority of 'site' authorisation refers to the ability to send any SMS-MT messages whereas the 'user' authorisation refers to the desirability for a specific user to receive a given message.

The sample SQL DDL provided below describes a modified sms_user table, together with a new sms_site table and an sms_accounting table.

```
CREATE TABLE `sms_user` (
  `uid` int(10) unsigned NOT NULL,
  `delta` int(10) unsigned NOT NULL,
  `number` varchar(32) NOT NULL,
  `status` int(10) unsigned NOT NULL,
  `code` varchar(16) NOT NULL,
  `gateway` text,
  'opt-in_type' int(1),
  'account_status' int(1),
  'number_valid' int(1),
  PRIMARY KEY  (`uid`,`delta`)
  )

CREATE TABLE 'sms_site' (
  'gid' int(10) unsigned NOT NULL,
  'number_template' varchar(32) NOT NULL,
  'gway' varchar(32) NOT NULL,
  'priority' int(2) NOT NULL,
  PRIMARY KEY ('number_template', 'priority')
  )

CREATE TABLE 'sms_acct' (
  'id' int(10) unsigned NOT NULL,
  'gid' int(10) unsigned NOT NULL,
  'uid' int(10) unsigned NOT NULL,
  'msidsn' varchar(32) NOT NULL,
  'msgtime'  timestamp NOT NULL,
  'MTvsMO' boolean NOT NULL,
  'msgtxt' varchar(640) NOT NULL,
  'gway' varchar(32) NOT NULL,
  'status' int(2) NOT NULL,
  PRIMARY KEY ('msisdn', 'uid', 'gid', 'MTvsMO')
  )
```

These three tables are not optimal; the 'gway' field should be extracted into a separate table that would enable account balance tracking, the sms_acct table only allows for messages that are four-part multipart, and stores multiple copies of the same message if identical messages are sent to multiple recipients, and so on. They also include several 'phantom' variables, in that they do not currently have meaning in the Framework. For example 'gid' is used in to hold an identity field which would default to a single id per site

but could be used by OG to track SMS usage per group; sms_site includes a 'priority' field that enables the Framework to prioritise which gateway to use for a particular destination “number template”.

More advanced services such as payments can be added once the underlying Framework is expanded to provide the auditing facility; location, MMS and video services are premium cost services and robust auditing is required before these should be considered. Storing the gateway ID in the sms_acct table however enables such services to be offered using multiple providers when they become available, and storing gateway and priority information in the sms_site table enables basic least-cost routing. However functions such as LCR will almost certainly require database-specific features such as materialised views (or an equivalent mechanism) for maximum efficiency in any large-scale environment.