Technical Specification Group Services and System Aspects **TSGS#23(04)0174**

Meeting #23, Phoenix, USA, 15 - 18 March 2004

Source: **Alcatel, Lucent Technologies**

Title: **OSA High Availability**

Document for: **Decision**

Agenda Item:

At SA#22, a Stage 1 CR on "OSA High Availability" was discussed. Several companies raised issues with the need for such a CR, whereas other companies felt that the requirement was needed. SA agreed "to send the issue to CN WG5 to determine the need for this functionality, or whether the functionality is already included in the specifications and feed back to TSG SA, copied to SA WG1 (via LS) to help towards a decision on this." CN5 have provided a response to this issue in SP-040003, with an update on the CN5 discussions in SP-040xxx . The LSs clearly show that there is no consensus between the OSA experts in CN5 as to the need for support of High Availability to be visible at the API level. What is clear is that there is consensus on the need for OSA solutions that interoperate and have High Availability, the issue is simply on whether there is a need to do this in a manner that is visible at the API layer.

Operators are looking for the ability to ensure that the applications are available whenever needed, otherwise the operator will lose revenue or even subscribers, if the application is not available when needed. In a multi-vendor environment, standards are used to ensure that operators are able to build a network from equipment sourced from various vendors. Standards ensure that the equipment interoperate, but effort is made to only standardise what is essential for interoperability. Over standardisation can reduce vendors' abilities to innovate and hence reduce the cost of their equipment. Typically, the solutions for ensuring that equipment has high availability have been left to the vendors to solve.

In the particular use case being considered in the SA1 CR the assumption is that the platform supporting the application is not highly available and so the operator is configuring a back up platform (in a different location) to take over if the application fails. To do this, the application will need to inform the network side of the API of the primary and backup addresses. This is currently supported in OSA with the "Set call back" command and the command is available to all APIs. However, only the Call Control API includes the call flows to describe how to use the command, which may be the reason why some companies believe that the command is not available for all APIs. n order for the backup instance of the application to be able to pick up the OSA Service Session if the primary fails, it will need to be aware of the state of each context the primary is supporting. For example, if the primary application instance has set a trigger for a location update if a UE has changed location, then the backup instance will need to know what this update relates to if it receives the update instead of the primary. All of this complicates the application design, especially when meeting the requirement that the two instances may be geographically separate. This support of High Availability at the API level exists, but its use does result in more complex application design, which can be provided by other means.

In summary, the requirement as described in CP-040092 is already supported across the APIs, but it must be noted that its use does complicate the application design. Based on this, the **Reasons for Change** and the **Consequences if not approved** are incorrect as summarised below.

Comments on the CR (SP-040092) itself:

Reasons for change:

The CR currently states that:

> *The support for High Availability in OSA is currently limited to a small subset of the available OSA features, e.g., Call Control. The absence of a fully defined high availability approach for OSA requires vendor specific solutions for realizing high availability including geographical redundancy. These vendor specific solutions are neither technology independent nor interoperable in a multi-vendor deployment.*

SA had asked CN5 to respond to the concern that the current support for High Availability is not complete and is only available for some SCSs, and the concern that the current support for High Availability is not interoperable. CN5 have not yet provided a response on either of these issues in SP-04003/SP-0400xx, so the reasons as stated in the CR coversheet are debatable. However, as described above, the **Reason for Change** is actually:

> *OSA already provides the ability for the application to provide the network side with the address of a backup instance of the application. This means that the network side can communicate with the backup instance of the application in the case of a failure of the primary instance. However, this capability is not visible in the stage 1 requirements.*

Consequences if not approved:

The CR current states:

> *Currently, OSA only provides High Availability support for a small subset of the available OSA features, e.g., Call Control. SA2 and CN5 cannot start the stage2/3 work to define a complete solution for OSA High Availability until SA1 has approved an OSA High Availability requirement. The consequence is that vendor specific solutions for High Availability will emerge that are not interoperable in a multi-vendor environment.*

It is proposed that this is changed to:

> *The stage 1 does not reflect the capabilities available to the application developer and this has caused confusion over the ability of OSA to support backup instances of the application.*

Conclusion

It is recommended that the **Reason for Change** and **Consequences if not approved** are changed on the CR and the category is changed to "F" before approval. If these are not changed then the CR should be postponed until CN5 has confirmed the **Reasons for Change** as described.