SIF Targeted Event & Notify Distribution Proposal

|  |  |  |  |
| --- | --- | --- | --- |
| Author: | John Chapman, BECTA | | |
| Date: | 29 June 2010 | | |
| Document history: |  | | |
| 29/06/10 | 0.1 | John Chapman | Initial draft of proposal. Andy Widdess wrote |
| 02/08/10 | 0.2 | Rob Potter | Updated proposal following conference call with Infrastructure WG. |
| 26/09/10 | 0.3 | Ron Kleinman | Updated proposal following US Tech Board conference call and incorporating additional comments posted in the discussion group. Identified required changes to the specification and remaining open issues. |

# Modifications to the Original Proposal

1. It now applies to Notify as well as Event messages

2. It limits the Destination field within the SIF\_Header to only one identified recipient.

# Actual Changes to the SIF Specification

Under the present proposal, the only major change to the existing proposal occurs in Table 5.1.2-1: SIF\_Header, where the text in red would need to be added to the definition of “SIF\_DestinationId”:

SIF\_Request messages MAY have this element set to the Id of a specific agent if the requesting agent wishes to direct the SIF\_Request to a specific responder. If present, the ZIS will route the SIF\_Request to the agent referenced in the element subject to the access control policies in effect for the zone.

SIF\_ServiceInput messages MAY have this element set to the Id of a specific agent if the invoking agent wishes to direct the SIF\_ServiceInput to a specific responder. If present, the ZIS will route the SIF\_ServiceInput to the agent referenced in this element; otherwise, if not present, the ZIS will route the message to the Provider of the service referenced in the SIF\_ServiceInput. In both cases the ZIS will route messages subject to the access control policies in effect for the zone.

SIF\_Event messages MAY have this element set to the Id of a specific agent if the posting agent wishes to direct the SIF\_Event to a specific agent. The agent may or may not be a subscriber to the events for the indicated object type. If present, the ZIS will route the SIF\_Event only to the agent referenced in the element. **This will be done irrespective of the access control policies in effect for the zone.** Otherwise, if not present, the ZIS will route the message to all subscribers of the events of that object type subject to the access control policies in effect for the zone.

SIF\_ServiceNotify messages MAY have this element set to the Id of a specific agent if the invoking agent for the service wishes to direct the SIF\_ServiceNotify to a specific agent. The agent may or may not be a subscriber for the notifications of that service. If present, the ZIS will route the SIF\_ServiceNotify only to the agent referenced in this element. **This will be done irrespective of the access control policies in effect for the zone.** Otherwise, if not present, the ZIS will route the message to all subscribers of the notifications of that service subject to the access control policies in effect for the zone.

This element SHOULD NOT be used in any other SIF Infrastructure messages. If the element is present, it will be ignored by the ZIS.

# Since both Directed Event and Directed Notify are now limited to only a single identified destination (as SIF\_Request and SIF\_ServiceInput already are) there is no change required to the SIF\_Header elements. That part of the original proposal has been eliminated.

This proposal also has a minor impact on the Event and Notify ZIS message flow sections.

# Open Issues (A-C)

**A. Special Provisioning Extensions may be needed in SIF\_AgentACL and SIF\_Provision**

There were primary two use cases identified, and each has some unresolved “behavioral” questions which need to be considered:

1. **The publisher wants to send the Event to one or more recipients who otherwise cannot normally receive them (i.e. who are not allowed to subscribe to them).**

This would cover the case of a work study program, in which 5 of 500 students were enrolled. Student Events for only those 5 should be published to the agent representing the work study program, which must not receive any of the others.

**Open Issue: Therefore that agent cannot be allowed to subscribe to Student Events, but must still be able to receive a Directed Student Event. This either requires an additional field in the Provisioning logic or (as documented above) would require the ZIS to deliver events to Agents who never subscribed to them, or who were specifically excluded from being able to subscribe to them.**

In either case, it would require the SIS application to “know” all about this situation and which students were in the work study program.

It would then be required to perform the following additional logic:

After posting a Student Event, if it was for one of those students, repost a Directed Student Event to the Work Study agent.

1. **The publisher wants to send an Event to one or more recipients who can receive them, but who are also entitled to see “more” information than the general class of event subscriber**

This addresses the case of an external application which is cleared to monitor say the health or disciplinary information of a student in addition to other student information. The application is subscribed to and receives StudentPersonal Events, but when one of a set of “hidden” elements is changed, the SIS sends out a Directed Event to only that application.

This is an alternative technique to XML Filtering, as it rolls the security decisions back into the source of the data, rather than relying on security policies previously established within the ZIS. Both techniques protect unauthorized subscribers from viewing changes to restricted data.

But this raises the question of how these two can be coordinated, since only some of the fields should be visible to all Requesters.

**Open Issue: Agents subscribing to an Event in this case will not receive all the data due to XML filtering restrictions enforced by the ZIS. Yet the destination agent in a Directed Event will receive these restricted fields, even though there is no current field in the Provisioning logic which identifies them as being able to do so.**

1. **More reasons ZIS Provisioning for these messages may be needed**

In the first use case above, the receiver of the Directed Event is an application that is not allowed to subscribe to events of that type. It was noted that this can be problematic. If the publisher is mistaken about the recipient’s ability to accept a Directed Event, an application which never subscribed to Event type A (or any events at all for that matter) will now receive a Directed Event of type A. The application’s supplied provisioning options are effectively violated.

The suggestion was made that there may need to be the equivalent of another column in the ZIS-defined provisioning matrix which allows an application to “receive Directed Events of type A, even when reception of type A Events isn’t allowed”. To be consistent, this column would need to be reflected in a Zone Status element and in the Provisioning arguments (and even in the CSQ matrix of all certified applications). An additional column might be required for the ability to accept “Directed ServiceNotify” messages as well.

Open Issue: Assume there is no change to the Provisioning matrix to accommodate “Ability to receive Directed Events”. Does an application even have to register in a Zone to receive a Directed Event? The answer to this needs to be clearly indicated in the specification.

Open Issue: How much of this if anything do we need to think through and document (as requirements, recommendations, best practices … or for that matter, warnings) in the standard itself, or in associated collateral, when the Directed Event capability is initially released?

**B. Error Handling**

Published Events & Notifications only “fail” when they are clearly erroneous. They do not fail if a subscriber can’t receive them (or even if there are no subscribers at all).

Both the Directed Event and Directed Notify contain the publisher-provided address of a specific recipient (as opposed to just posting it to any / all subscribers unknown to the poster). This indicates there may be a need to alert the publisher that the **specified** recipient will not receive the directed message because:

* The recipient is not currently registered in the Zone
* The recipient cannot receive Directed Events or Notifications
* <For ServiceNotifies> The packet size is too large

**Open Issue: If some error notification is required, how exactly would it be provided to the publisher of a Directed Event or Directed Notification?**

**C. Release Differences**

UK Release 1.3-E1 will support the results of this proposal as “experimental”. It will become finalized in SIF US Release 2.5

**Open Issue: Does support for this proposal need to be the same in both releases? If not, some examples of differences might include:**

* **Specific provisioning hooks (as described above)**
* **Extension of “specified recipient” from Directed Event to include Directed Notify**
* **Some mechanism for error notification**
* **Documentation of best practices (or more formal functional profiles) for Directed Event usage**