Alert notifications – a powerful tool but how to do it right?[1]

Merete Ask
Gjøvik University College
Martin Onstad
Telenor Norway AS
Jose J. Gonzalez
Gjøvik University College

Abstract

A steadily increasing number of different organizations utilize alert notifications to inform stakeholders in different situations and have developed their own solutions for the purpose. This being said, alert notifications are only vaguely covered in traditional, generic and holistic literatures, "best practices" and standards. There is little general information specifically related to how, what, when and why one would choose to alert notify. "Made as one goes", based on "organizational subjective" experience, current, mature alert notification solutions have to be deemed the current "state of the art". This occurs with little or no solid anchorage in standards or "best practices", challenged to keep up with rapid technological development, increased expectations to keep a growing set of (claimed) stakeholders informed while maintaining the desired level of alert notification quality.

The current general societal expectation about telecom and data services is that they should be resilient, stable and available for use, at all times, everywhere. No matter how resilient, robust and secure these services are designed to be, though, they require maintenance and incidents do happen. Stakeholders expect to be kept proactively informed about maintenance activities that may impact their quality of service. When incidents happen, service providers are expected to handle them efficiently, professionally, in a predictable manner and keep relevant stakeholders informed.

This article presents a 2014 master thesis that assembled alert notification relevant information from different literatures and combined these with Telenor knowledge and experience gained as a mature utilizer of alert notifications. This was used to provide a generic, but alert notification specific set of recommendations. A set defined as guidelines intended for any arbitrary organization considering establishment and continuous improvement of well-structured, secure and efficient alert notifications.

[1] Presented at the Norwegian Information Security Conference 2014 (NSIK-2014)

1. Introduction

This article prepared for NISK 2014, presents the master thesis "Well structured, secure and efficient alert notifications" [1], written by Merete Ask to complete a Master of Information Security Management at Gjøvik University College during the spring of 2014. The thesis assembled and presented a set of organization generic, but alert notification specific recommendations. They should be seen as guidelines intended for any arbitrary organization considering establishment and continuous improvement of well-structured, secure and efficient alert notifications.

1.1. Problem

Several organizations are required by law to alert notify authorities in certain situations and have developed their own solutions for the purpose. A steadily increasing number of different other organizations also utilize alert notifications to inform stakeholders in different situations. As figure 1 illustrates, the public is in general familiar with the concept of alert notifications and its various natures, but not necessarily *consciously* familiar with it.

Figure 1: "The various natures of alert notifications"

As figure 2 illustrates, however, alert notifications are only vaguely covered in traditional, generic and holistic literature, "best practices" and standards. Except for some industry specific guidelines issued by specific authorities that provide a bit more detail of their expectations regarding alert notifications and their content, there is little general information specifically related to how, what, when and why one would choose to alert notify. Relevant fragments can be drawn from some traditional, generic and holistic sources, but none of them provide detailed, alert notification specific recommendations as to how these can be used as a business beneficiary communication tool. This makes it hard for most to maintain a very familiar conscious relation to the concept of alert notifications.

Figure 2: "The specific concept of alert notifications remains vague in generic, holistic literature."

Several organizations have established alert notification solutions to utilize as part of their normal operation. These solutions are most often based on government requirements and customer/end-user increasing expectations and requirements. Solutions continuously improve, based on obtained but quite "organizationally subjective" experiences.

On this basis and in close dialog with the thesis topic provider (the Operation Management Section of Telenor Norway AS), the following problem statement was defined for the thesis [1]:

"Is it possible to define a set of alert notification specific recommendations that any arbitrary organization can utilize to establish and continuously improve a well-structured, secure and efficient alert notification solution?"

1.2. State of the art

An alert notification is a simple communication tool that can support service providers, keeping relevant stakeholders informed about the progress in a professional manner. Informed stakeholders are enabled to "work around" planned maintenance activities or incidents occurred and maintain "business as usual" more efficiently. As defined by The Norwegian 22-07 Commission of Inquiry [2] (and utilized as a basis definition for the thesis [1]), an alert notification can be defined by its purpose:

"A main purpose of alert notifications is that the notification should lead to the receiver performing an action. One type of action may be as simple as the receiver's consideration whether any measures should be initiated."

There are different types of alert notifications, but the thesis scope of alert notifications was focused on the following two types:

(1) **Proactive maintenance alert notifications**, to inform relevant stakeholders of planned maintenance activities which have the potential to affect quality of service.
(2) **Reactive incident alert notifications**, to keep relevant stakeholders informed about detected incidents and the progress of incident response.

Mature and experienced users of alert notifications know that, when done successfully, alert notifications provide a common situational awareness amongst receivers. Valuable for stakeholders that later may have to take more active action should an incident situation escalate (e.g. members of internal crisis management team) and enable other stakeholders to make more correct decisions for themselves more efficiently (e.g. how long an undesirable effect of an incident can be endured before end user has to initiate own internal business recovery and/or contingency processes).

Societal, corporate and governmental dependency on telecom and data services has been steadily increasing. Increased dependency leads to increased expectations and demands towards service providers in general. For suppliers of telecom and data services (like Telenor), the current general expectation is that the services are resilient, stable and available for use, at all times, everywhere. No matter how resilient, robust and secure these services are designed to be, though, they do require maintenance. Also, incidents will happen and they do. Stakeholders expect to be kept proactively informed about planned maintenance activities that may impact their quality of service. When incidents happen, service providers are expected to handle them efficiently, professionally and in

a predictable manner, keeping relevant stakeholders informed. Suppliers of telecom and data services in Norway, such as Telenor, are required by the Norwegian Post and Telecommunications Authority, as warranted by the Norwegian Regulations on electronic communication networks and services [3, §8-5], to proceed as follows:

"Supplier is required to alert the Norwegian Post and Telecommunications Authority about events that may have or have reduced the availability of electronic communication services considerably. The Norwegian Post and Telecommunications Authority can define more detailed alerting procedures."

Due to the lack of publicly available, organization generic, alert notification specific methods/models/set of recommendations, most current, mature solutions for alert notification are historically based on solutions implemented merely to comply with legal requirements. Over the years such solutions are often expanded and improved based on experience, internal requirements for increased efficiency and increased expectations from end users/customers (e.g. included as requirements in Service Level Agreements). Some also provide alert notification as a payable service end users/customers can get assigned to. "Made as one goes", based on quite "organizational subjective" experience, these current, mature solutions have to be deemed the current "state of the art". The lack of publicly available alert notification specific guidelines and lack of experience shared within and across industries, the developed alert notification solutions have little or no anchorage in objective standards and "best practices". It also represents a challenge for those utilizing alert notification as a communication tool, since it makes it hard for them to improve their solutions based on anything else than subjective experience (typical "trial and error based subjective improvement"). The alert notification suppliers also face challenges in relation to efficiently keep up with increased information expectations from a growing set of (claimed) stakeholders, adjust efficiently for rapid technological development of infrastructure and services and at the same time maintain the desired level of alert notification quality.

1.3. Research goals

Based on the current "state of the art" situation, the following challenges were defined as relevant for the thesis:

- Although alert notification relevant elements can be found and utilized from different literatures, "best practices" and standards, these are most often not specific as to how, what, when and why one should alert notify.
- Several different suppliers within different industries are required by law to alert notify and have working alert notification solutions for that purpose, but their extent of structure, security and efficiency are not publicly known and also limitedly shared amongst suppliers and across industries.
- Due to governmental requirements, alert notification receiving authorities have defined some regulations and guidelines, but these are merely based on information they expect to receive (i.e. useful as a basis but represent a "least required minimum" for organizations required by law to alert notify).

The above challenges were redefined into the following five research goals (RG1-RG5) required solved, to resolve the thesis main problem statement (ref. section 1.1):

- **RG1:** Find a way to define a generic set of recommendations that can be utilized by an arbitrary organization (i.e. ability to take the most complex into account without limiting the simple and enable tailoring towards individual organization's purpose, needs and capabilities).
- **RG2:** Research, identify and utilize as found relevant, the limited, little alert notification specific, but relevant elements of available literature, "best practices" and standards (i.e. should be utilized to ensure additional anchorage and justification for efforts made in relation to alert notification within an arbitrary organization).
- **RG3:** Collect mature alert notification experience and include it to support limited published relevant material. Make the most out of the topic provider, Telenor, as a case basis for the thesis.
- **RG4:** As found relevant, research, collect and include recommendations from other experienced third party actors and relevant experience gained from other documented crisis/disaster investigations.
- **RG5:** To cover both the aspect of establishment and improvement, make sure the generic set of recommendations include recommended/suggested ways to measure improvement.

The resolution to the problem statement, supported by defined research goals, was focused towards the definition of an organization generic alert notification specific set of recommendations related to the following two main types of alert notifications: (1) Proactive maintenance alert notifications and (2) reactive incident alert notifications.

2. Method

The current "state of the art" defined challenges (ref. section 1.3. of this article), justified the applicability of the alert notification topic in general. It led to the acknowledgement that large parts of the thesis would have to rely upon Telenor's available knowledge as a mature and experienced user of alert notifications, but also put some implications towards the thesis methodology. The extent of structure, security and efficiency of current "state of the art" alert notification solutions developed and utilized by different organizations were (and is) not publicly known. Also there were no known, established tradition for these organizations to share actual gained experience and knowledge on alert notification within or across industries. This further enhanced the acknowledged importance to seize the opportunity and use Telenor as a case basis for the thesis. As such, the known current situation and "state of the art" did put some implications towards choice of thesis methodology, but the candidate resolved the defined problem statement within the thesis timeline as illustrated in Figure 3 below.

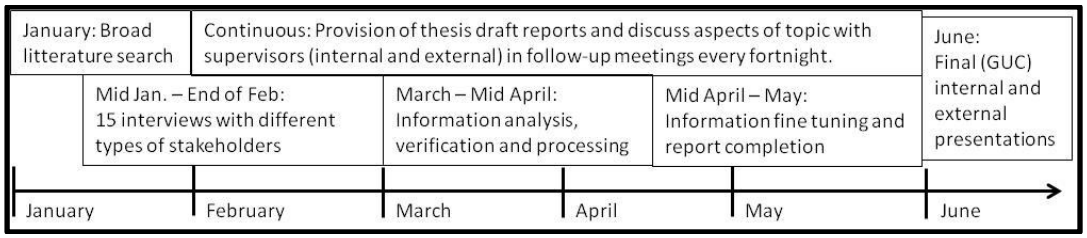

Figure 3: "Thesis timeline"

To resolve the problem statement through research question resolution, the work on the thesis took a qualitative approach [4, Chapter 6, page 140] with the aim to be

descriptive (i.e. reveal the multifaceted nature of alert notifications as a topic) and interpretative (i.e. allow for the researcher to gain insights into the topic). The work was initiated by performing a broad literature search. The search was aimed to identify alert notification relevant elements in documentation of related topics (e.g. literature, standards, "best practices", guidelines etc.)[2], which could be extracted and utilized to form alert notification specific but organization generic recommendations. The literature search was supported with empirical data collection from 15 open-ended interviews. The interviews were conducted by the candidate as open-ended interviews with different semi-structured [4, Chapter 6, page 154, "Interviews"] follow-up questions (related to their alert notification perspectives, e.g. main importance, challenges, relevant aspects to improve etc.) depending on the interview subject (i.e. different types of alert notification stakeholders). The interviews were aimed to cover two main objectives: (1) Gain broad and adequate insight into Telenor alert notification utilization to use Telenor as a case basis for the thesis and (2) draw relevant elements from interviews and reformulate these into generic alert notification recommendations (i.e. with specific interest towards "how, when, why and what"). The interview subjects were Telenor alert notification stakeholders (12) and third party experts (3), all with different perspectives on alert notification as a topic. Additional support and insights during the five months period of working on the thesis, was gained by the candidate's access to office space in the Telenor Operations department (i.e. ability to work close to and observe the operational thesis relevant environment), received Telenor Operation Management alert notifications (i.e. for additional observational purposes), opportunities to discuss key findings of the work with Telenor operation managers, and information/clarifications provided by the thesis external supervisor from Telenor upon direct request from the candidate.

3. Limitations

The thesis validity (i.e. accuracy, meaningfulness and credibility) [4, Chapter 4, page 101, "Considering the Validity of Your Method"], could be adversely affected by lack of topic-specific information (ref. section 1.1), which forced us to rely much upon Telenor as a thesis case basis (ref. section 2). The same lack of topic-specific information did, however, verify the thesis applicability and meaningfulness, enhancing the importance to utilize Telenor as a case basis to increase the thesis credibility.

A thesis replication by third parties would be challenging, owing to the chosen interview method, which does not necessarily provide comparable results between conducted interviews of stakeholders with different perspectives. Also, the actual recorded minutes were excluded from the thesis, since they contained sensitive information that would prohibit the thesis from being published. In addition, there is the fact that the interview method's output quality rely much upon the interviewer's individual skills and capabilities, i.e. different interviewers will not necessarily get the same result interviewing the same set of interview subjects.

The thesis generalization abilities are yet to be proven, but they are found to be promising. The organization generic, alert notification specific set of recommendations resulting from the thesis are new and as such need to be "exercised" in different types of

[2] For more details about the literature search including more literature references, refer the published thesis [1].

research projects (or through utilization in the industry) to determine its actual ability to be generalized. The thesis did however include a set of reflections made in relation to the results' ability to strengthen known third party audit methods, combined with a high level summary of results from an evaluation of Telenor's alert notification solution towards the set of recommendations. Generalization abilities will also be dependent of the ability of the utilizing party to tailor the alert notification specific set of recommendations to the individual organizations needs, purpose and capabilities.

4. Results

The thesis does provide a set of alert notification specific recommendations for any organization to utilize to establish and continuously improve well structured, secure and efficient alert notifications. Table 1 below lists the thesis provided complete set of alert notification specific recommendations (i.e. A.1-A.5, R.1.1-R3.6 and improvement suggestions 1-7) with a short description.

ASSUMPTIONS		**SHORT DESCRIPTION**
#	**Assumption**	A.1-A.5: Assumptions/preconditions any arbitrary organization should comply with before utilizing the following set of organizationally generic alert notification recommendations efficiently. Way of compliance is, however, organizationally individual and may, as such differ between arbitrary organizations. (IR=Incident Response, BR=Business Recovery and CM=Change Management.)
A.1	IR and BR processes are in place	
A.2	CM processes are in place	
A.3	Alert notification provision tool is available	
A.4	Alert notification trigger is in place	
A.5	Ability to tailor generic recommendations to the need and purpose of the organization.	
PREPARATIONS		R1.1-R1.5: Recommended preparations organizations should perform (or review) prior to establishing (or improving) alert notification. The definitions, identifications and descriptions made as part of these preparations are highly relevant in relation to the organization's ability to later utilize this as a basis for continuous improvements as outlined by the below included 7 improvement suggestions. By identification of alert notification triggers in current processes (R1.2), the organization will also find the key on where to extend current processes with a process to alert notify.
#	**Recommendation**	
R1.1	Define the main purpose of alert notification aligned with the organization's main business objectives.	
R1.2	Identify alert notification triggers in current processes	
R1.3	Define alert notification requirements relevant to fulfill its purpose	
R1.4	Define alert notification relevant roles with descriptions.	
R1.5	Identify and describe alert notification stakeholders relevant to its purpose.	
ALERT NOTIFICATION SOLUTION		R2.1-R2.5: Recommendations regarding the overall alert notification solution (i.e. independent of chosen technology utilized to alert). These recommendations are generic recommendations relevant to be able to use alert notifications efficiently within a timely manner with an adequate level of quality.
#	**Recommendation**	
R2.1	Maintain and control the list of alert notification stakeholders (i.e. receivers) continuously.	
R2.2	Avoid serial processing as far as practically possible.	
R2.3	Automate for increased efficiency, where found possible.	
R2.4	Operate based on a clearly defined regime for incident classification.	
R2.5	Operate under strict change control.	

<table>
<tr><td colspan="2">ALERT NOTIFICATION MESSAGE (Message type: M= Maintenance, I= Incident)</td><td rowspan="14">Recommendations regarding proactive maintenance (M) and reactive incident (I) messages regarding generic and type specific alert message content. These recommendations are closely tied to the following 6 generic recommendations (R3.1-3.6) regarding response control, content, structure, basis of support, language and quality control of alert messages. It should be noted that the chosen media to use in alert notification (e.g. public webpage/similar, directly addressed messages by e-mail/sms/similar, etc.) most often will have some effect on content, level of detail and language. It is however still relevant to consider the here listed recommendations and determine how to handle each one of them best in relation to chosen media.</td></tr>
<tr><td>Type</td><td>Recommended content</td></tr>
<tr><td rowspan="3">M&I</td><td>From</td></tr>
<tr><td>To</td></tr>
<tr><td>Title</td></tr>
<tr><td rowspan="3">M</td><td>Time interval</td></tr>
<tr><td>What</td></tr>
<tr><td>Consequence</td></tr>
<tr><td rowspan="8">I</td><td>Type of alert with case number reference</td></tr>
<tr><td>Consequence</td></tr>
<tr><td>Expected correction time</td></tr>
<tr><td>Detection time</td></tr>
<tr><td>Mitigations implemented</td></tr>
<tr><td>Cause</td></tr>
<tr><td>Additional info</td></tr>
<tr><td>#</td><td>Recommendation</td></tr>
<tr><td>R3.1</td><td>Include suitable response control</td></tr>
<tr><td>R3.2</td><td>Ensure only fact based content is included</td></tr>
<tr><td>R3.3</td><td>Content structure</td></tr>
<tr><td>R3.4</td><td>Alert notifications content quality control</td></tr>
<tr><td>R3.5</td><td>Utilize available, relevant guidelines and knowledge for support</td></tr>
<tr><td>R3.6</td><td>Adapt language to target audience</td></tr>
<tr><td colspan="2">MEASURE, JUSTIFY AND IMPROVE</td><td rowspan="9">7 suggestions regarding alert notification improvement, based on measurements and justification. Provides generic suggested means to continuously improve with references to research goal RG5 (ref. section 1.3).
Measures for improvements are tightly linked to the organization’s individual purpose and capabilities and that is the reason behind these being listed as “suggestions” rather than “recommendations”. Suggestions do, however, cover measurements related to success rate of the established/improved by use of before/after measurements. In addition, KPI-based performance measurements used in relation to organization individually defined goals/requirements and alert notification stakeholder’s feedback on perceived value (versus organizational alert notification purposes).</td></tr>
<tr><td>#</td><td>Suggestions</td></tr>
<tr><td>1</td><td>Proactive maintenance alerts issued in accordance with time requirements?</td></tr>
<tr><td>2</td><td>Maintenance activities completed successfully within alert notification defined maintenance window?</td></tr>
<tr><td>3</td><td>New incident alert notifications issued within time requirement from detection?</td></tr>
<tr><td>4</td><td>Update incident alert notifications issued at least within time defined interval?</td></tr>
<tr><td>5</td><td>Incident alert notification closed within first defined expected correction time?</td></tr>
<tr><td>6</td><td>Precision in incident classification level definition?</td></tr>
<tr><td>7</td><td>Stakeholder’s made able to utilize alert notifications in accordance with its defined purpose?</td></tr>
</table>

Table 1: Summarized thesis result in terms of the provided set of recommendations for alert notifications

The thesis [1] includes a much more detailed description of the recommendations summarized in Table 1 above, with corresponding examples for increased understanding. No matter the type of organization, all recommendations are relevant to visit whether the organization is establishing a new or reviewing a current alert notification solution. If an organization determines one or more of the recommendations “not applicable” to the organization it is recommended that the reasoning behind such a conclusion is documented. This, so that the conclusion may be revisited and altered if

later found applicable (or not applicable for same reason as before) in later reviews based on experience and statistics for alert notification improvement purposes. It is also expected that, when utilized, the recommendations will be tailored towards the needs of the utilizing organization for best possible outcome. Such tailoring is recommended documented in terms of for instance keeping "not applicable" recommendations in the list (but reasoned) with added/adjusted corresponding organizationally individual recommendations included based on organizational individual experience. This way, the organization has a justified basis to discuss experience and tailoring with other experienced users of the framework and use that to share experience and increase the generic, common knowledge on alert notification as a topic.

5. Conclusion, discussion and suggested future work

The thesis has provided a set of recommendations to resolve the thesis problem statement. When done well, alert notifications may contribute to, e.g.:

- Provide an essential common situational awareness amongst many stakeholders
- Keep relevant stakeholders updated (and ready should their additional action be required at any point in time)
- Provide insights enabling relevant stakeholders to make more correct decisions for themselves more efficiently
- Build communication bridges between processes (i.e. Incident Response and Business Recovery and/or Continuity) and those responsible for them (i.e. Incident and Crisis Management, Incident and Change Management etc.)
- Create a generic sense of predictability in less predictable situations and as such increase trust between parties
- Alert notifications that are well-tailored into relevant already established business processes (e.g. Change Management, Incident Response, Business Recovery and/or Continuity etc.) may also provide insights that indirectly also contributes to improvements of the processes initiating alert notifications.

The feasibility of the provided set of recommendations and their ability to be generalized and tailored to individual organizations purposes is yet to be proven. The thesis as such provides an alert notification framework that organizations can utilize as a basis to establish and improve alert notification solutions. It is, however, expected that organizations utilizing the result as a basis, over time "exercising" the framework will be able to further improve the provided set of recommendations, based on experience.

The thesis also represents a basis for future research. Researchers may, based on the thesis provided set of recommendations, further determine their level of usability for arbitrary organizations, organization individual scalability and ability to be generalized. This can for instance be done by utilizing the thesis provided set of recommendations as a basis to audit a set of different organizations that already have alert notification in place, and as such verify the recommendations "working conditions". Also, given the marginal, topic specific research available, any research providing additional direction in relation to alert notifications would be of great value to topic stakeholders. Arbitrary topic stakeholders may also benefit through following up on results from ongoing research projects on related topics to evaluate its usability in alert notification. E.g.

research within areas such as big data analysis, smart emergency response, smart city resilience etc.

6. References

The list below constitutes the list of all relevant sources of information studied and referenced from this article:

1. M. Ask (2014), "*Well structured, secure and efficient alert notifications"*, http://brage.bibsys.no/xmlui/handle/11250/197836, URL visited and verified working (August 2014)
2. A. B. Gjørv et al (2012), *"Report from the 22-7 commission of inquiry"*, NOU 2012:14, ISSN: 0333-2306, ISBN: 978-82-583-1148-2
3. Samferdselsdepartementet, FOR-2004-02-16-401, *"Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)"*, available at: http://lovdata.no/dokument/SF/forskrift/2004-02-16-401?q=ekomforskriften*, URL visited and verified working (August 2014)
4. [5] P. D. Leedy and J. E. Ormrod (2011), 10th ed., *"Practical Research planning and design"*, ISBN-13: 978-0-13-289950-5, ISBN-10: 0-13-289950-7