Web Consultation – benefits and drawbacks of developing the FlexPlan grid planning tool as a cloud-based service – summary of the received feedbacks

Feedback was received from the following experts:

1. Paul Hines – Packetized Energy (solution provider)
2. Mark Norton – Smart Wires (solution provider)
3. Camille Hamon – RISE, former Svenska Kraftnät (research institute / transmission system operator)
4. Emil Hillberg – RISE (research institute)
5. Jan Segerstam – ENERIM (solution provider)
6. Paul Vinson – SuperGrid Institute (research institute)
7. Tim Schittekatte – Florence School of Regulation (research institute)
8. Sven Flake – OPTANO GmbH (solution provider)
9. Hendrik Natemeyer – Amprion (transmission system operator)
10. Evangelos Vrettos – Swissgrid (transmission system operator)
11. Michel Noussan – FEEM (research institute)
12. Qian Dai – China Electric Power Research Institute (research institute)

Question 1 – [State of Play]

Before going into more detailed questions: is your company already using cloud-based services (such as web applications)? Or do you exclusively use on-premise services? Are there some activities for which your company allows the use of cloud-based services and others for which it is forbidden? Are there some specific data which are not allowed to leave your premises? If you do use cloud-services, what are these services (name, functionality, provider…)?

Summary of received feedbacks:

The experts answering the consultation survey can be divided into three main activity segments: solution providers, research institutes and transmission system operators. The answers were quite different depending on the segment:

- Most of the service providers are preferring and using more often cloud-based services compared to on-premise services.
- Most of the research institutes are mainly using on-premise services while they have no policy for or against cloud-based services.
- For system operators, the situation is more nuanced. Cloud-based services are usually not the standard but for most of them it is however not forbidden. In all cases, the data is sensitive and so the service, its security and its privacy need to be evaluated. Additionally, the criticality of the application for the system operator must be taken into account. All of these may lead to imposed limitations.

Critical analysis:

The answers received strongly depend on the segment of the company of the respondent. For system operators, who is our target segment for the FlexPlan service, the use of cloud-based services seems not already standard but not forbidden. Security aspects are at the centre of their concerns, hence the relevance of this consultation survey.

Question 2 – [Benefits]

In the context of the project, developing the FlexPlan planning tool as a cloud-based service is bringing many benefits in terms of agility, scalability and ease of adoption (described above). If you had to use or participate in the development of the FlexPlan planning tool, would you consider these benefits as valuable? Have you encountered such benefits or additional ones when using/developing another cloud-based service?

Summary of received feedbacks:

- Most of the respondents agree with the identified benefits and consider them as highly important, especially with a development perspective. They consider that cloud-based services are more user-friendly and scalable than on-premise services.
- However, from a user perspective, the answers are more balanced. Indeed, some of the respondents consider important for them to be able to look into the code in order to understand the model and to help identifying bugs at early stages of the developments.
- Additionally, one point of attention mentioned is that costs might be higher for the development of cloud-based services compared to on-premise services. This seems especially true to set-up the service but using continuous integration and continuous development pipelines seems a good way to quickly recover the initial investment.

Critical analysis:

There is a common agreement on the benefits that the FlexPlan team has identified to develop the FlexPlan tool as a cloud-based service. However, depending on the type of business, users can see it as a bottleneck in order to understand the model and to participate in the debugging of the service. This limitation is also true in the context of the FlexPlan project in which the users can detect bugs by using the software but cannot help the development team to solve them. However, for the understanding of the model, in the case of FlexPlan, it should not be a limitation as the model is fully described in one of the deliverables.

Question 3 – [Concerns]

However, from the point of view of the real usage (future exploitation), a System Operator could feel it unacceptable to use a cloud-based service due to security concerns or pose limitations. Then, we must be aware of the implementation of the FlexPlan planning tool in order to comply with security constraints. Would you have these concerns or other ones if you were using the FlexPlan planning tool? What is the current policy in your organization regarding data security?

Summary of received feedbacks:

Overall, there is no unique answer to this question. All respondents emphasized that there are real concerns about data confidentiality for such a critical system as a grid operator. The use of such a tool by a system/grid operator would therefore require a thorough and careful assessment in order to decide which security requirements have to be met and to get a greenlight on using the service.

However, system operators emphasized that it is not unfeasible but the service should have:

- excellent security measures and
- trust and good contracts.

Moreover, some respondents emphasized that some system/grid operators are moving more and more to the use of cloud-based services both in Europe and in the US. In particular, in Europe the concern of data confidentiality for network data should not apply anymore as it is now publicly available as part of the TYNDP network datasets.

Critical analysis:

Getting the green light of system operators in order to use the FlexPlan tool currently developed as a cloud-based service seems not an easy journey. However, system operators themselves do not consider it as unfeasible. We should however be aware that the security might be the biggest obstacle in the promotion and application of this service.

Question 4 – [Security]

To make the FlexPlan planning tool appropriately secured, HTTPS data transfer is used and the service is protected with IP whitelisting and basic authentication (username + password). Additionally, no data is persisted to drives after processing ("stateless"). Would these security mechanisms bring you confidence to use the FlexPlan planning tool? Do you consider some of them as unneeded? Would you require other security mechanisms to use the FlexPlan planning tool? A foreseen alternative to IP whitelisting was to implement a Web Application Firewall (WAF). Would your answers be different in that case?

Summary of received feedbacks:

- Most of the respondents think that the implemented security measures are already a good basis which will give confidence in the service but that these measures shouldn't be decreased. Encryption for data in transit is definitely mandatory.
- In addition, two-factors authentication seems to be a must-have for a production service. This is considered by the respondents as not complicated to be implemented. Another security layer which would be welcomed is encryption at rest for the database (see next question). Also, using side-to-side VPN could increase the security.
- In any case, network topology data is very sensitive and the respondents therefore believe the concerns will never be fully eliminated. Therefore, each end-user company would require to perform a full security assessment and would ask for a clear data policy on how data is handled and how it is protected.

Critical analysis:

The already implemented security measures of the FlexPlan cloud-based service seems sufficient for the current development stage. However, if we want to go to production with this cloud-based service, at least two-factors authentication would be needed as extra security layer.

Question 5 – [Challenges]

The "stateless" operation of the FlexPlan planning tool prevents us to adopt a database which would simplify a lot the input data management. One of the main challenges that we are facing in the project is therefore the ability to transfer a large amount of data in a reasonable time to the cloud service. Have you already faced similar or different challenges when using/developing another cloud-based service? What workarounds did you use/implement to mitigate your challenges? Would you agree to use the FlexPlan planning tool if your data was saved in a database as long as your request is successfully acknowledged on your side? What would be the conditions?

Summary of received feedbacks:

- Generally, respondents believe that using a database is not out of question. Its security should be evaluated as the other building blocks of the service in order to see if it fits security requirements.
- However, if a database is used, all respondents believe that the data stored should be at least encrypted and even anonymized for some of the respondents.
- Furthermore, some of the respondents believe that generally having a real stateless service will be really complicated in view of the amount of data involved even though speed is not important for a planning tool.
- One respondent is suggesting to have a hybrid solution for which part of the data already publicly available in other platforms (e.g., ENTSOE) could be stored in a database and other part of data would be transferred only for the analysis.

Critical analysis:

Overall, the received feedbacks let us believe that using a database to store (part of) the data needed by the FlexPlan tool could be acceptable. Depending on the future needs and bottlenecks identified during the development of the service, this information could open the door to a revised architecture.