What is the Effect of Product Attributes on Public-Key Infrastructure adoption?

Mattila, Anssi; and Mattila, Minna

Abstract — ***the arguments for adopting Public-Key Infrastructure (PKI) are strong and yet PKI products have suffered from relatively low adoption rates. The results presented in this paper help managers to better understand the effect of product attributes on PKI adoption. In this paper product attributes are defined as features, quality and design. When implementing the technological developments, the knowledge on security products, organizational IT assets and organizational culture becomes of an outmost importance. Therefore, this paper further makes a significant methodological contribution when combining marketing instruments with product development processes to better capture the dynamic nature of the innovation adoption factors.***

Index Terms — innovation adoption, product attributes, technology, PKI

1. Introduction

FOR the time being companies are more and more concerned about the security of their information technology assets courtesy of the connection to the Internet. They invest money in various security products, and hope for the technology to provide the security. The repertoire of security products is and has been wide including both software and hardware. Firewalls, monitoring devices/software, security management tools etc. can easily comprise a myriad of non-compatible systems that require money, attention and endless patience. This has been realized and systems that can provide security for more and more complex network environments have been under way for some time. Public-Key Infrastructures (PKI) belong to this category of products and its prospects are interesting. Whether they will be fulfilled will be seen in the future.

So far PKI has been mostly applied to e-commerce and secure communications. E.g. the Bank of Canada Public-Key Infrastructure has been up and running since April 1999, and there are hundreds of banks around the world running their own PKIs [1]. Some businesses have been merging their PKI with Virtual Private Network (VPN) in order to safely open their IT resources to the outside world [6]. PKI has been claimed to be complex, difficult to install/implement, inadequately standardized and so forth. It seems that all the implemented PKIs are more or less pilot projects, so there is no long-term research and experience on the subject, except trying to achieve stable and sound standards.

The four most influencing factors affecting the success of a new product development process are high-quality new product process, a defined new product strategy for a business unit, adequate resources of people and money, and R&D spending for new product development [12].

When implementing the technological developments, the knowledge on security products, organizational IT assets and organizational culture becomes of an outmost importance. Therefore, this paper further makes a significant methodological contribution when combining marketing instruments with product development processes to better capture the dynamic nature of the innovation adoption factors.

2. PKI Product Attributes

Quality:

There are several kinds of quality: quality of inputs, processes and outputs. There is no simple uni-dimensional measure of quality. In our research the quality of PKI systems should be evaluated. A PKI system can be understood as an output, so what means do we have to evaluate the quality of a PKI product. One way to evaluate quality, is to measure product characteristics, which can be set an exact value, e.g. height, weight, volume, time etc. In other words variables can be formed from these characteristics to be able to make measurements and give exact values, which can be evaluated afterwards. The benefit of this is to be able to notice how much the product misses quality specifications if it doesn't pass the check. However, this requires special skills from the employees, special equipment, time and effort.

Features:

The main goal cannot be to include as many as possible features into software. If features are meaningless to users it is the same if there are n or n+10 features. Therefore the number of features is not the most significant point. From the vendor, or from the producer of software point of view including features, which are not in the competitors' products, can be a competitive edge in case buyers value those features. Additional features cannot still increase the price of the product unless the increase is well founded and understood by the customers.

Design:

Another way to add customer value is through product design. Design is a broader concept than style. Design goes to the very heart of the product. A sensational style may grab attention and produce pleasing aesthetics, but does not necessarily make the product perform better. Good design contributes to a product's usefulness as well as to its looks. For example, a properly designed user interface in the case of a software product offers a significant tool for positioning. That investment in design pays off has been recognized by global companies, which have embraced design. Good design can attract attention, improve product performance, cut production costs and give the product a strong competitive advantage in the target market.

3. NEW TECHNOLOGY ADOPTION REASONS

Some kind of competitive advantage should be gained by adopting a new technology. Shapira et al. 1996 introduces several ways to ease and accelerate technology adoption process. Some of the proposals are hard to implement for small companies due to the lack of needed personnel or funds [8].

An increase in the value of a product or a reduction in the costs of bringing the product to market means competitive advantage. Using automated equipment and computer control, which affects the quality of a product, can minimize human errors. [4]

Information security technology, like a PKI, can be seen as an increase in the value of certain products. Product support, e.g. of paper machine, can utilize a PKI system in a way, that customers data remains secret all the time, as well as any communication with the customer. In inter-organizational communication it is not uncommon, that organizations make demands on information security level of peer organization, and in here a PKI system is of great assistance, though security could be achieved by other means or by other technology too.

Au et al. (2000) conducted a study on attitudes towards adoption of new technology. The results indicated that the adoption process is related in several beliefs such as perceived difficulty, adoptive experiences, suppliers' commitment to the firm, perceived benefits, compatibility and enhanced value [9].

Deployment of a PKI system could be seen as improvement in quality of the product in the eyes of a customer. Customer can realize that its needs are better taken care of. Today it should be minimum requirement, that all customer data, and communication, is well taken care of by deploying encryption, authentication etc., and this is transparent when PKI technology is used. However, is it reasonable to make purchase decision of a PKI system based on estimation of a possible increase in the quality of a product, e.g. paper machine?

PKI technology doesn't belong to production or manufacturing technologies, instead it is a technology that can create more value to a product or it supports these aforementioned technologies. Therefore the downsides (possible financial risks, jeopardizing the market position etc. [4]) of deploying a technology among the first won't be much of a threat if PKI fails: it quite unlikely affects the manufacturing process.

In software business it is difficult to make masses buy. IT decision makers in companies tend to buy front-runner products. Once users learn how to use a certain product, become very familiar with it and so forth, then they are not that eager to switch to another product. Being a first-mover and trying to "set a standard" e.g. by marketing extensively, is a key element when trying to succeed in software business [11].

Evaluation of a new technology to be adopted should begin with financially analyzing all quantifiable factors that can be set a monetary value. In addition to this all qualitative and intangible factors are analyzed. Then results of these two analyses are summed up to facilitate the evaluation of all involved risks related to uncertain costs and revenues. [4]

4. A COGNITIVE MODEL OF THE PKI ADOPTION

Based on theoretical literature review the research framework (Figure 1) was formed, in which the relations of corporation's macro- and microenvironment, and product development are presented. In software business high-speed changes in technology are the normal course of business. Macro factors are presented to accomplish the overview of software ventures' environment.

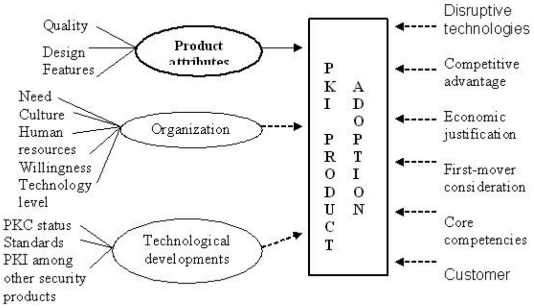


Figure 1: A cognitive model of the PKI adoption

Altogether the factors presented in figure 1, contribute toward success (or failure) to retain business customers in terms of creating added value. Some of the factors have more direct effect on the PKI adoption than others as can be seen from figure 1. In this study, however, the main focus lies within the two inner boxes; in other words the relation between the product attributes and PKI product adoption.

5. *Data Collection / Methodology*

The preliminary study was conducted to become familiar with empirical study's research field. Five test interviews were made with the key personnel of the case firms. In these preliminary open interviews the list of important issues was not used, and the interviews were recorded. The interviewed persons wanted to have the possibility to communicate freely about all issues they felt relevant to this research. During these interviews, the organizational views of future directions of technology adoption within an organization were clarified.

A qualitative, interpretive study approach was used to evaluate product attributes in the technology adoption context. The qualitative study approach is considered appropriate when little is known about the phenomenon under investigation, the concepts are immature due to the lack of theory and previous research and a need exists to explore and describe the phenomena [10].

Two organizations and three PKI products were included in the study. Metso Corporation is a globally leading supplier of processes, machinery and systems for the pulp and paper industry and a foremost expert in the key technologies of this sector. Sonera Ltd. is the leading mobile communications operator in Finland. Keon product family is a common product of RSA Data Security and Security Dynamics. Keon provides encryption of data, encryption of telecommunication, end-user authentication and encryption of application server data. Entrust/PKI is security application, which is intended for enterprise use. Its main goals are to enhance e-commerce security, encryption of files and e-mail and being able to digitally sign them. Certicom is a US located company specialized in security of wireless environments. Founders of the company are also related to invention of elliptic curve cryptography (ECC), which has partly made it possible to extend PKI to wireless environments.

The actual research was conducted during 1999-2001. In the two-year project we studied Public-Key Infrastructures and their applicability to industry and companies in general. This stage of research provided concrete data about the product attributes and their functions. After defining our requirements for the test PKI system we checked the supply and ordered the best fitting one. Our requirements, Single Sign-On -feature (SSO) and smart card authentication, made the supply scarce. We wanted to use SSO in an automation system, not only in logging to various web pages. Due to complexity and extent of PKI systems we required product support to be nearby.

Our first PKI system to be tested was Keon. Developing an agent for an automation system helped testing its SSO capabilities and smart cards features. SSO password saving problem (in clear) is avoided in Keon PKI by using special short lifetime certificates signed by security server. After Keon testing, we checked PKI-markets again and we chose Entrust PKI system. Entrust had a good reputation, possibility to use cross-certificates and generally seemed to be a versatile product. This constituted a good point of comparison for Keon.

At the time we finished testing Entrust, PKI wireless PKI product producers had tried to establish a firm foothold on the PKI market. Therefore we chose to explore wireless possibilities of PKI, like extending PKI to PDAs. Several companies used PDAs in different ways, though the applications were still not versatile and beneficial so that PDAs could be used in an efficient way.

The group discussions were used to further understand the observations, and especially actual product attributes' effect on the perceived willingness to adopt a PKI product within an organization. The first persons to participate in the group discussion were selected by using a purposive sampling to interview the personnel involved in business development. These experts further named some people working in the same area of operation, which could provide information from the field. This snowball method, in which the key person(s) name the next persons participating in the research, is suitable in situations, in which the other important people for the research are otherwise hard to identify [5]. Altogether 15 in-depth interviews were conducted among academics, managers from both seller and buyer side, and software development personal. The discussion themes covered topics from the theoretical framework presented in figure 1 including experiences from PKI product testing, development, and usage, organizational abilities to benefit from PKI products, and different kinds of indirect effects.

In qualitative research the aim is often to concentrate on small amount of cases and analyse them thoroughly; criteria of scientific research, when using qualitative methods, is not the quantity of the data but the quality of it. The amount of data or the number of persons interviewed does not have generally significant importance when evaluating the success of the study – the aim is not to make statistical generalizations but describe a phenomenon or understanding of some function [2].

6. *Results*

Quality:

Fast operation can be understood as part of the quality of a PKI system (Figure 2). It is important that system operates rightly, but it has to operate in due time. In software products the speed of operations of software greatly depends on hardware on which it is running, but high quality products can use underlying hardware better, thus being faster. Slow operation of software products might hinder the usage, and people might try to avoid the usage as they can.

The lack of support material and bad product support hampers e.g. ease of operation and repair. During the installation and piloting phase support material, as well as product support, is of great importance. These are the phases when people try to get the PKI environment function correctly and it is not uncommon that difficulties appear. As seen from the grid support material is highly valued, but not seen extensive and profound enough. Product support is seen better carried out.

Compatibility of software products is something to expect. Among the PKI products compatibility problems have risen and software houses are doing something to fix the problem. Large software products require compatibility with several hardware products and software products as well. Incompatibility of software products is the origin of several difficulties e.g. in installation, management, ease of operation and repair. According to definition ease of operation is part of quality, and compatibility is something that really facilitates ease of operation.

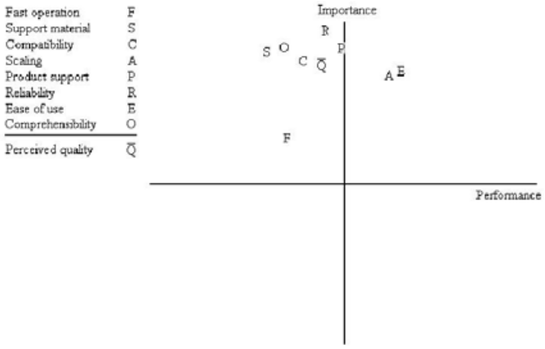


Figure 2: Perceived quality of the PKI products

Large number of users of PKI system makes scaling of PKIs highly significant. This comes up especially during the installation of PKI and PKI clients. The clients are installed on end users' PCs, which can be troublesome if scaling has not been taken properly into consideration (ease of operation).

Reliability and ease of use comes straight from the definition in the beginning. Comprehensibility has a link with reliability and ease of use. When you understand what you do (comprehensibility) and this requires only slight effort, and still everything (PKI, PKI services, etc.) works fine, then it feels that you can rely on PKI and using its services is no burden. Although some of the attributes mentioned above can be measured objectively, quality should be measured in terms of buyers' perceptions [7 kotler].

Features:

When looking at the performance-importance grid (Figure 3) elements in PKI, which could be a competitive edge as marketing PKI products, should be the ones that are in the leftmost upper corner. However, a PKI system is something that customers are rarely familiar with until they buy it. Therefore it is difficult for the customers to know which things in a PKI should be valued. Are we looking for a PKI system, which comes with very good support material, everything in it is easy to comprehend, it is very compatible and even highly reliable? As features of a PKI system was thought things with which users are in touch, and/or they can quite easily form an opinion.

Speed of operations of a PKI system and its clients is very tangible for end users. When a user logs in a system, the time it takes for the system to respond is easily noticed, and the longer it takes, the more it irritates. During log in periods the calculations different servers in PKIs have to go through are quite similar regardless of PKI product used. Therefore the time it takes to log in a system is quite the same.

Compatibility of different software products becomes evident at least during installation. However, this affects end users considerably less that people managing PKI. Similarly management (M) of the PKI system and GUIs don't concern end-users as much. Management and GUIs are features, which are noticeable for management people. Well implemented GUIs and management assist greatly in complicated system like a PKI.

Smart cards and tokens are mostly used during log in sessions. Smart cards and tokens are not an essential part of all PKIs. When they are deployed in a PKI both end-users and management people come into contact with them.

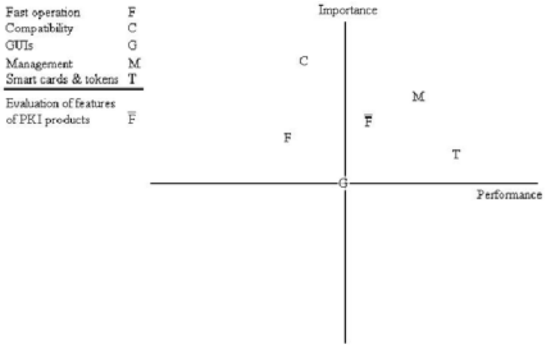


Figure 3: Features of a PKI system

Design:

Good design contributes to a product's usefulness as well as to its looks. For example, a properly designed user interface in the case of a software product offers a significant tool for positioning. Good design can attract attention, improve product performance, cut production costs and give the product a strong competitive advantage in the target market. Figure 4 represents the quality factor of a PKI.

Fast operation of software products depends greatly on hardware on which it is running. Errors in design of software can affect the speed of operations. However formal methods and libraries among others are deployed nowadays, which minimizes the chance of faults in design, and enhances the reliability of software as well.

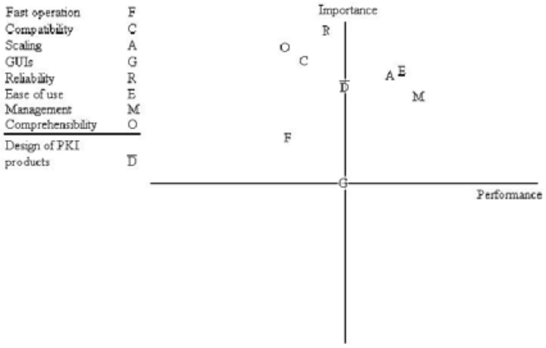


Figure 4: Design of the PKI products

Scaling of PKIs has to be considered carefully in the design. Large user base, client software on end users' PCs and so forth can make management personnel's work difficult unless scaling is well designed and implemented.

Different GUIs are a tool for the management personnel of a PKI. The GUIs (which has something to do with PKI and PKI services) that end users use don't require so much from the design. However, it is obvious that good design of the GUIs, which are used by the management personnel, facilitates ease of use and will assist in management of the PKI in general.

Comprehensibility is important for security. Especially the end users, who might not be very familiar with PKIs and e.g. certificates, should be taken into consideration. As designing GUIs and education (be it a guide book or education in general) for end users it might enhance the security if the end users would understand e.g. what all the messages are about.

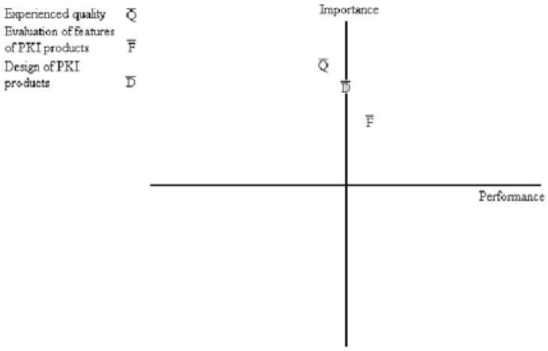


Figure 5: Summary of the product attributes

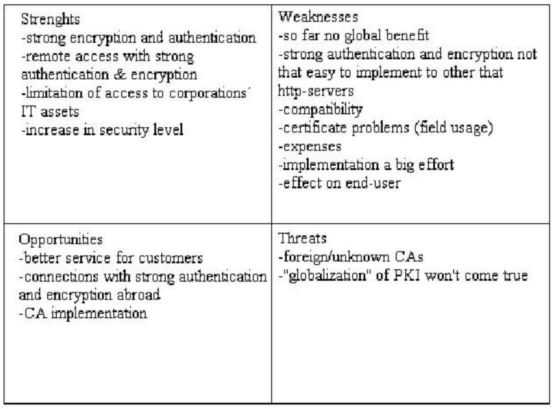
SWOT analysis of corporation PKI adoption:

Strengths of PKI adoption are closely related to asymmetric encryption and benefits created by it. A PKI is strongly based on security services, which are implemented using asymmetric cryptography. Usage of smart cards to carry personal certificates emphasizes strong authentication. However, the certainty of authentication process is comparable to identification procedure of CA issuing personal certificates. If you can't trust identification of ”subjects” done by a unknown CA, how much can you trust the bondage between the Public-Key on a certificate and the real person behind the ”subject-field” contained in a certificate? In here it is not that clear where to put strong authentication: it is obviously strength, but it can turn out to be a weakness.

Strong authentication can be applied to remote users as well. However, strong authentication of remote users is not possible only in PKI environment, but it comes in the package. Strong encryption possibility during remote connections is clearly a big plus for companies. Along the way from Brazil to Finland there are several places to eavesdrop telecommunication traffic. The best way to guarantee safety of your data is to take care of it by yourself with tools that can provide enough protection.

If a corporation really can trust the CA, which issues certificates, a PKI can be very useful in restricting access to corporate IT assets. Unfortunately these assets can too often include only http-servers, but there is always hope that situation will become better. Some PKI products offer authentication and encryption features to other application servers, combined with SSO too, but the implementation is not always effortless.

Using PKI to limit employees' access to resources, which they really need in their work, can be very beneficial. It is not uncommon that workers have access to places they should not have. According to statistics the threat quite frequently comes from inside the company. If workers have access to ”forbidden” places, they might be teased to try to do something bad. By creating a well limited working area a corporation sends a clear message and makes the abuse of its resources more difficult (Figure 6).



Strenghts -strong encryption and authentication -remote access with strong authentication & encryption -limitation of access to corporations´ IT assets -increase in security level	Weaknesses -so far no global benefit -strong authentication and encryption not that easy to implement to other that http-servers -compatibility -certificate problems (field usage) -expenses -implementation a big effort -effect on end-user
Opportunities -better service for customers -connections with strong authentication and encryption abroad -CA implementation	Threats -foreign/unknown CAs -"globalization" of PKI won't come true

Figure 6: SWOT analysis of corporation PKI adoption

SWOT-analysis describes PKI's benefits and disadvantages. Weaknesses of PKI include e.g.

the lack of confidence in certificates signed by unknown CA limits PKI usage. There is no guarantee that ”John Smith” is really the one you know is living in New York. It is impossible to now how the CA identified him when it issued him a certificate, which binds his name to this offered Public-Key. Like mentioned in the Strengths-chapter extending strong encryption to other than http-servers is not unambiguous. Some PKI products offer this possibility, but then come problems with e.g. firewalls when trying to access server from outside.

Compatibility of different PKI products is improving. Big software houses have noticed the problem and initiatives have been taken. Compatibility problem concerns also the usage of different certificate fields. Certificate standards or drafts, e.g. rfc 2459 [3], can be very extensive works covering lots of pages. Based on the open interviews, the researcher got an impression that the usage of different certificate fields might have been misunderstood by software producers, or they might have been thinking their own advantage in determining the meaning of a given field.

Implementation of a PKI affects end user at least in logging process. According to our experience the time logging takes is still quite long. Hopefully it is not required frequently during working days. The time that encryption and authentication processes takes from the processor will lose gradually importance in the future, because processing power will increase faster that complexity of mathematics in encryption/decryption (Figure 6).

Opportunities of PKI product adoption are to do with mainly with the privacy dimension they offer. Many companies have customers and business partners with whom it exchanges information, which should have better privacy. While implementing a PKI environment it is quite easy to take important people from customers and business partners into user base. So, this is a change to offer clients better service by enhancing security of their business interactions. And it is possible to offer this ”service” to foreign customers too.

Threats of PKI adoption are not yet so visible. One thing worth mentioning is of course the difficulty to trust certificates issued by unknown CA. This might be one of the weakest links in PKIs and has potential to create problems. If more trustful CAs won’t appear it might be difficult to make good use of possibilities of PKI (Figure 6).

7. Conclusion

PKI products are expensive but powerful tools in limiting access to own IT assets. Strong authentication, strong encryption, smart cards and SSO are details that really strengthen security when deployed correctly. However, PKI alone cannot make any company’s network secure without e.g. a firewall. Firewalls itself can be rather expensive investment due license expenses, software updates and so on. PKI is not a necessity, because encryption, authentication among others can be implemented without it. On the other hand, to implement strong authentication, strong encryption, and strong security in general, PKI can be very important part of it.

The effect of product attributes on adoption of PKI is not an unambiguous matter. According to performance-importance grid the emphasis in PKI products has been so far on features, and transition to more customer-centric product development might be desirable. Quality and design of the products are seen as more important factor than features, and maybe more intensive participation of customers in the product development would make the customers and product developers understand better each other’s, and thereby customers could be offered better, more suitable products. And maybe this would lower the adoption threshold of the customers in the future. For companies it is difficult to see a PKI system as a necessity, even if it is based on the latest security technology.

References

[1] Clarke, J., "Internet Security: PKI in pilot mode but expectations run sky high," *Medias Transcontinental Inc*, Computing Canada, 2000, pp. 67-82.

[2] Eskola, J. and Suoranta, J., “Johdatus laadulliseen tutkimukseen,” *Vastapaino*, Tampere, Finland, 1999, pp. 23-31.

[3] Housley, R., Ford, W., Polk, W. and Solo, D., “RFC 2459: Internet X.509 Public-Key Infrastructure Certificate and CRL Profile,” http:// www.ietf.org, 24.1.1999.

[4] Krajewski, J. and Ritzman, L., “Operations Management: Strategy and Analysis,” 5th edition, *Addison-Wesley Publishing Company*, London, UK, 1999, pp. 213-332.

[5] Malhotra, N. and Birks, D., ”Marketing Research: An Applied Approach”, *Prentice Hall,* Essex, UK, 2000, pp. 342-367.

[6] Salamone, S., “TimeStep Merges PKI With VPNs,” *United Business Media*, Internetweek, 1999, pp. 22-25.

[7] Kotler, P., Armstrong, G., Saunders, J., Wong, V., “Principles of Marketing,” 3rd European Edition, *Pearson Education Limited,* Essex, UK, 2001, pp. 453-489.

[8] Shapira, P., Rosenfeld, S., “An Overview of Technology Diffusion Policies and Programs to Enhance the Technological Absorptive Capabilities of Small and Medium Enterprises,” background paper prepared for the Organization for Economic Cooperation and Development Directorate for Science, Technology and Industry, August 1996.

[9] Au, A., Enderwick, P., “A cognitive model on attitude towards technology adoption, *Emerald Group Publishing Limited,* Journal of Managerial Psychology, 1996, pp. 266-282.

[10] Creswell, J., “Research design: Qualitative and quantitative approaches,” *Sage Publications*, Thousand Oaks, UK, 1994, pp. 146-147.

[11] Hoch, D., Roeding, C., Purkert, G., Lindner, S., Müller, R., ”Secrets of software success: Management insightsw from 100 software firms around the world,” *Harvard Business School Press*, Boston, US, 1999, pp. 122-124.

[12] Cooper, R., Kleinschmidt, E., “Winning businesses in product development: The critical success factors,” *Industrial Research Institute*, New York, US, 1996, pp. 18-29.