Introduction

1. 1. My physical working place was in ...., ... and I was working in the ....From Oct. 20/// to Oct. 20// I worked in this company and this project was defined within this period of time. I worked mainly in the position of telecommunications technical officer.

Background

1. 2. The nature of project is preparing infrastructure of country public key. The objective of project was implementation of digital certificate in different system digital certificate has various application that the most important of them is digital signature. Digital signature in fact is replacement of manual signature in the virtual world. This project started at the time that there was no proper reference for implementation of digital signature in /////// and each company did some implementations according to its own style and methods and this had resulted in lack of interaction between systems that digital signature was implemented in them. The project physical address was ///////////////. The client of project was ///////////////// and contractor was a combination of IT companies such ///////////////

1. 3. Total duration of the project two years starting on and completing on. My responsibilities and duties in this project and in this company as a telecommunication technical officer were mainly revolving around the following:

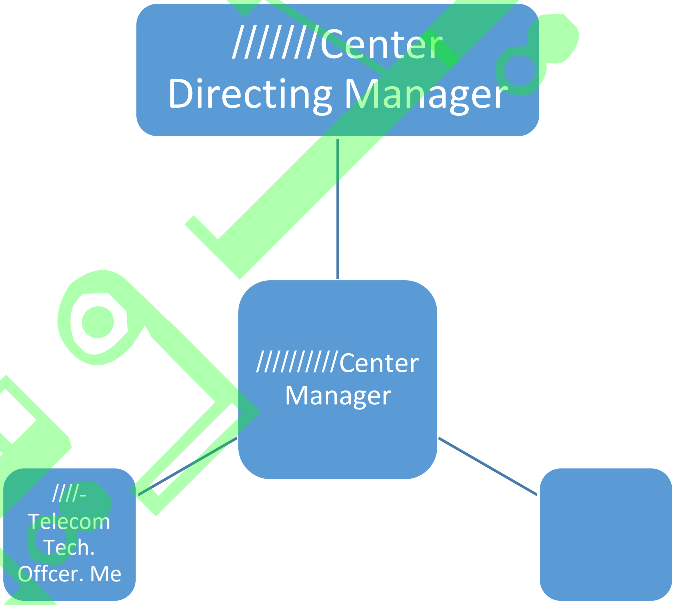
- Studying the matching process of documents with overall policies of ///////. I should add here that //////////, //////////// is classified as trust point in higher hierarchies of the infrastructure and below it there are median certificate issuance centers such as ///////////////
- Installing, commissioning and maintenance of telecommunications equipment
- Monitoring telecommunications equipment and networks efficiency
- Preparing infrastructure development design for telecommunications network used by users
- Analysis and assessment of communication traffic and servicing level
- Preparing process documents, instructions, rules and communication policies
- Reviewing and improving the national PKI standards
- Being a part of technical committee for approval of standards
- Compliance Auditing of several systems with PKI standards
- Designing models for trade facilitation between ECO countries
- Preparing reports about global incidents related to SSL security

1. 4. I divided the project into phases including first phase outsourcing, second as receiving documentaries and studying them, third phase as approval in the /////////// organization. I was in full communication in contractor companies as abovementioned and also I sent work report to the related expert. My purpose from unit is /////////////////.

1.5. As ////////////////// expert, my responsibility was review, inspection, and studying of matching documents to the policies of ////////////////////. My work was in this manner that I studied existing foreign references and also policies of //////////////////////// that were decided to be transformed into ////////////////. By policies, I mean certificate policy. Every center for certificate issuance in every part of the world should have a CP or policies document in which mentioned related regulations with digital certificate and its application. Moreover, other than technical issues, processes and legal issues are also mentioned in CP. To observe this document, you can refer ///////////////. Therefore, my role was mainly technical and except my personal activities management, I did not manage human resources or any team.

1.6. This project was on ///////// scale and first includes all ///////////// and then some organizations and ///////////////// of /////////////// office. The project objectives were development of public key infrastructure in the country and integration of country public key infrastructure to facilitate interoperation; and finally reliability of the business and electronic commerce in the country.

1.7. The organizational chart is as following:


///////Center Directing Manager
//////////Center Manager
////- Telecom Tech. Offcer. Me

Personal Engineering Activity

1.8. My entrance to //////////////////////// was simultaneous with definition of country public key infrastructure standards project. Before I entered the project, projects IDs were defined and international references were identified, therefore, I studied international standards such as FIPS and

NIST as well as different RFCs and I collected information that I required as an expert telecommunication technical officer. Since these standards are accepted worldwide, I trusted them as well, however in some cases there were contradictions between these standards and overall policies of our country, in which I prioritized our own policies.

1. 9. Our main problem in this project was mismatch of some international standards with CP //////////////// Center certificate policies (CP). Since public key infrastructure PKI is different in different countries. For example, in America, CA Bridge structure is used having several /////////////// centers in it, however in our country there is only one ///////////// Center for government sectors which ////////////////////// Center, therefore inevitably I had to eliminate some of the standards or add to them.

1. 10. PKI structures include bridge, mesh and hierarchy in which in our country only hierarchy is used which is a hierarchical structure and in it there is only one government Electronics Certificate Issue digital certificate issuance center and there are several median certificate issuance centers below it. The second problem I challenged was that there was not a definite method for inspection of matching software with these standards, by software here I mean software that country's public key is implemented in the, namely PKE (Public Key Enabled). To solve this problem, I prepared a series of indexes and started studying them in the ///////////////// lab in which my role as Electronics Certificate Issue Center inspector at this time of the project was inspecting accuracy of this lab performance by observing the test procedure and its outputs in the ///////////////

1. 11. In fact, definition of our problem in this project was mismatch of country electronic certificate policies and PKE software with international standards. My solution as an expert telecommunications technical officer was that I applied several different references and compared the method applied in them and in some cases, I applied a combination as well and for the purpose of matching software also, I prepared assessment indexes and matched the software output with expected output.

1. 12. Standards text was really hard and unintelligible. I applied my good English language competencies as well as my competencies in digital certificate technical issues; having these pre-requisites, I progressed the work. For example, I knew the different between shall and should in standard text so that accurately I could determine their requirement type in the standard text. I performed several tests considering the prepared indexes by ////////////////////// in ////////////////which did matching software with prepared standards by ///////////////////// Center. Some of them items that I tested included inspecting safe connection between different indexes of systems such as SSL, inspecting possibility of giving permit to different roles of issue or update of certificate, inspecting of existence of two factor authentication in systems and studying repository existence, LDAP or HTTP for CRLs and certificates maintenance as well as inspecting event logging as well as accuracy maintenance mechanism of these events by signing them. I also did inspecting feasibility of proof of possession operations in certificate systems as well as CA certificate management and studies observation of certificate profiles during the issue of certificate according to RFC5280 and etc.

1. 13. Majority of resources are available in the internet, though I used existing books and standards and RFCs. I used MS Office Word software and prepared indexes and standards used, however in ///////////////, for the purpose of inspecting of software, their output is matched to the expected

output and normally there is no need to use any other software. However, SQL is used to study related indexes to the software database, Ldap brower for connection to the server and inspecting server status, XCA for generation of certificate issuance on a case by case manner and P7s viewer for inspecting messages matching to the defined format in PKCS#7 standard.

1. 14. Large part of this project was research work, therefore as an expert telecommunication technical officer in no part of the work I hindered from researching on the internet, studying papers, books, standards and other references and manuals. I studied many references and in fact most of the time I was residing in R&D unit. I applied from consultation of contractors and also international standards in the filed.

1. 15. The main connection of my work was social and cultural issues and considering the fact that in virtual space, there is no proper way for determining accuracy of documents, therefore using digital signature for integrity seemed essential, however, lack of proper national standards and monotonous implementation of digital signature in different software systems would result in imbalance of these software and as a result lack of public trust to these type of software, therefore, I kept in mind that I need to make this digital signature work as a tool of security for the people using it.

1. 16. I received lots of advises from //////////////////////// expert considering his great experiences in PKI field and in some cases that there was need for decision making, he helped me out. For example, whenever there was mismatch of standards ////////////////// center certificate policies, I had a meeting with him and then we decided about changing the policies or standards. I had meetings for troubleshooting as well. I attended a meeting after preparing standard to form into ///////////////. According to the procedure, I attended the discussion group for this ////////// too.

1. 17. I challenged variety of problems during the project; for example, regarding the problem of sending certifying request one by one which required more time and cost, I suggested the method of group sending of certifying request or full request according to RFC5272 which can send several certificate issuance requests in the form of one single request. Up to that time no developer inside the country had done such development of structure. Moreover, in order to have cryptographic messages in the software system unique, I prepared cryptographic messages standard according to PKCS#7 standard which in fact introduces different messages notations according to ASN.1 structure. In addition, in the software on the client side or PKE, certificates used for signatures were not verified in which I using provision of creditability standard solved this problem and obliged software developers to this standard.

1. 18. I applied international standards such as PKCS#1-15, NIST (CAVP and CMVP standards) as well as RFC5280. I applied domestic standards as well. I followed a good communicative approach with IT engineers especially information security as we were policy makers in this area, I applied less consultation, however on case by case manner, regarding active companies in PKI, I applied form their expertise and knowledge.

1. 19. The project deadline was defined and for project time and cost management I followed predefined approach. Considering delivered outputs by contractor and phasing that was provided previously in RFPs, I studied standards. In some cases, that there was need for review, I performed several reviews. Regarding tests also, schedule table was provided by the /////////////// lab. Regarding project control, it was done using a web based system by managers.

1. 20. In this project I was not dealing with physical safety but with data security and I supplied this security via defining access level and encryption. Moreover, regarding confidential document such as under test software, I kept them in a safe in archiving section of maintenance center. I matched all received documents from contractors with reference documents such as international standards and in case there was any fault, I reported to contractor and even in some cases several time I corrected the documents.

1. 21. For the purpose of verifying documents and standards that contractors provided, I matched them to foreign standards that required English language competency which I not only improved mine but also I could progress the work and project using my English language competency. Moreover, considering the fact that standard language is different from regular text language, I also used my competency in literature of foreign standards so that I could recognize mismatch.

1. 22. Mainly I did not do management work in this project and I only as an expert worked in the project. Of course I as one of project telecommunications technical officers supervised on contractor activities process that were active in standard preparation; then I presented my report to my authorities in project. During this project I attended a ////////////////. Moreover, in order to elevate my knowledge in the filed and also monitor on the contractors' performance, on a permanent basis, I studied existing references and standards. Moreover, in order to get introduced to other software companies with written standards, I held several training workshops and with designing some PowerPoints, I described requirements for country public key requirements in which this training course and its teaching results in interaction with experts of this area adding in my general knowledge.

1. 23. As part of my activities in this project as an expert telecommunications technical officer, I prepared reports as well which I submitted to project manager. I interacted to project experts working in contractor companies. I monitored on lab reports as well and verified their accuracy and sent the reports from my inspections to ////////////// manager.

Summary

1. 24. Generally speaking, the project completed successfully since as the objective was standardization and it was achieved. Customers which in fact were software developers basically were not satisfied considering the fact that we had determined some requirements for them. However, ultimate customers were people that would be happy taking into account the fact of more security in their transactions. Considering the fact that there were bureaucratic procedures in standardization process and also lack of contractors' experience in this field in addition to the fact that this knowledge was high technology, we fell behind schedule in some part of the work.

1. 25. After this project not only improved my research work and experiences in the filed but also I improved my competencies in documentations and also digital certificate. I can dare to call myself a professional officer and expert in telecommunications considering the fact that I started policy making in a national scale and this work required professional competencies in the filed.