Public key infrastructure

Technology, Information Technology

Public Key Infrastructure Assignment Public Key Infrastructure (PKI) is a type of security architecture that offers a higher level of confidence when it comes to the exchange of information over the internet. The PKI allows for the integration of the various services connected to the concept of cryptography. The main aim behind PKI is to provide access control, integrity, confidentiality, authentication and non-repudiation (El-Ashqar, 2012). PKI is anchored on three main concepts. The first is authentication where strong authentication mechanisms help to verify the users of machines. Secondly, there is the idea of encryption where encryption algorithms ensure that the communications are secure and that data remain private as it is sent from one computer to another. Finally, through digital signatures, PKI helps to provide non-repudiation. The concept of non-repudiation helps prove that a particular individual performed a certain operation at a certain time (El-Ashqar, 2012). Therefore PKI can be of great benefit to the organization by guaranteeing the quality, source & destination, the timing and privacy of information.

The PKI could help in signing the company’s software by providing code signing certificates. This certification is done by the Certification Authority (CA) unit under the PKI which uses its private key to assign a certificate and signs it with the private key for that certificate authority (Zissis & Lekkas, 2013). The CA in this case refers to the company itself which will be involved in issuing and revoking of the digital signatures. In addition to the private key, the CA has its public key which is published. Therefore, the company may take advantage of this process and assign its software products digital certificates. The public key that is used in the authentication of the code

signature can be traced back to the root Certification Authority (Zissis & Lekkas, 2013). Clients make use of the root certificate generated by the CA to verify that the signatures have originated from that certificate authority. This will help the user know that a given software product is from the stated source or company. This will help show the user that the software is authentic and is from the trusted company.

Companies have to choose whether to use an external certification authority (CA) or an in-house CA that is controlled by the organization. Each of these approaches has its own merits and drawbacks. First, when it comes to internal CAs, it is easy for the organization to manage since there is no need to consult another party. Internal CAs has no cost per certificate fees and it's generally cheaper to configure (Spencer, 2013). However, the limitations of the internal CA are that its implementation can be complex, organizations are accountable for the PKI failures and the certificate management overhead cost is high in internal CAs (Spencer, 2013). Secondly, when external CA is considered, they are advantageous because the external CA is accountable in case of PKI failures. In addition, other organizations are likely to trust digital certificates from external CAs (Spencer, 2013). The certificate management overhead cost is lower compared to that of internal CAs. However, external CAs reduces the level of integration to the infrastructure of the organization. The fees associated with the cost per certificate can be very high, especially in large organizations. In addition, the level of flexibility in expanding and managing the certificates is reduced.

Based on the analysis above, I would recommend that the organization adopts the external CA instead of the internal CA. This is because external

organizations and clients will trust the CAs generated by external CA. this will help the organization grow and ensure that customers trust their products. In addition, since this is a relatively small organization, the cost per certificate fees will be small, and this will make the approach relatively cheap.

References

El-Ashqar, A., Mageed, T & Fahmy, A (2012). Taxonomy of Public Key Infrastructure. Journal of Applied Sciences Research, 8(7), pp. 3656-3663.

Spencer, W (2013). Understanding Certificate Authorities. Retrieved from http://www. tech-faq. com/understanding-certificate-authorities. html

Zissis, D. & Lekkas, D (2013). Trust coercion in the name of usable Public Key Infrastructure. Security And Communication Networks, John Wiley & Sons