Week 6 case study 2 submission gross salary 30 pages (7500 words) case study

Technology, Information Technology

Week 6 Case Study 2 Submission

Cryptography Number: Lecturer: Introduction With the current trends in technology, there is the emergence of complex systems, automated business transactions, and e-commerce applications that need the installation of complex and rigorous security measures. Public key cryptography is a security technology that is known for the support of security mechanisms like confidentiality, integrity, non-repudiation, and authentication. For the Software Company to achieve this security assurance there must be careful planning for the infrastructure. A public key infrastructure (PKI) is a foundation whereby other applications, systems and components of security are built. A PKI is a foundation where it acts as an overall security whereby all the other components and features must work. This paper will not look into the underlying structure of cryptography. PKI is a very wide cryptographic technique. This paper will offer the real opportunities that can be adopted, by the Software Company, to remove their fears, and misconceptions on the use of this technology. In addition to this, paper will also look into the rationale as to why this technology is suitable for various business applications.

There are components which are available in a PKI framework. These components include operational policies, security services, and interoperability protocols which are all geared to support the use of public-key cryptography. The generation and management of public keys occurs through the use of Certificate Authorities (CAs), Registration Authorities (RAs) and directory services which can be used to establish a list of trust. At the national level, the use of PKI can be very instrumental when dealing with security. One of the principles of PKI is to establish a trust hierarchy (U. S General Services Administration Government Smart Card handbook, 2004). In e-commerce, when dealing with trust mechanisms, there must be the provision of management control. There must be a management control at the Ministry of Information. In the e-commerce environment, entities, which are not known to each other, do not have enough trust that has been established to perform business, contractual, legal, or other types of transactions. For this trust to be achieved, the implementation of PKI should be done by using CA.

In summary, the working of CA is as follows. For entities which are unknown to each other, they will each establish a trust relationship with a CA. The CA will perform some form of entity authentication according to the rules that have been established as has been noted by the Certificate Practices Statement (CPS). After this process, each entity is then issued with a digital certificate. The beauty of this is the fact that the certificate is signed by CA and thus the identity of the entities is vouched (Stalling, 1999). With this, individuals who are unknown to each other can then establish trust between them because they have trust with the CA that it has performed some form of authentication on both of the entities. What is more, the signing of the CA is an attestation to this fact. One of the benefits of PKI is the establishment of a trust hierarchy which works well with networks which are of different environments and platforms.

Positive features of in-house CA

With the use of in-house CAs, there is easy management of the certificates. With this aspect, there is no need to have third parties to manage the certificates that have been created. With the Windows Server Active Directory that is present in the company, it is easy to manage the certificates as the CA can be integrated into the active directory of the server. In addition to this, there is no addition of costs when one is managing a certificate internally. They are also simpler when they are being configured as when compared to public keys (General Accounting Office (USA), 2004).

Negative features

With the use of in-house CA, the security and accountability of PKI rests with the organization that is hosting the PKI. If an organization goes for the option of in-house CA, the external parties will not sign any contract with organizations which have signed internal CAs. The management overhead of a certificate that is signed internally is higher than that of an eternal certificate (Kapilia, 2003).

Advantages of public CA

With the use of a public CA, the external third parties are responsible for the infrastructure of PKI in the company. Other parties who work with the company have confidence with certificate authorities, which have been signed by third parties like VeriZon. The management overhead of an external certificate is lower when compared to the in-house certificate.

Disadvantage of public CA

The integration of the certificate with the internal security infrastructure becomes hard as there are limitations. There is also a need to pay the certificates that will be used by the organization. This will be expensive for the organization. The expanding and the flexibility of the certificates will be limited.

Recommendation

I would recommend in-house certificate for the organization. This is because it will be managed well with the windows active directory. In e-commerce, when dealing with trust mechanisms, there must be the provision of management control (General Accounting Office (USA), 2001). There must be a management control at the Ministry of Information. In the e-commerce environment, entities which are not known to each other, do not have enough trust to perform business, contractual, legal, or other types of transactions. For this trust to be achieved, the implementation of PKI should be done by using CA.

In summary, the working of CA is as follows. For entities which are unknown to each other, they will each establish a trust relationship with a CA. The CA will perform some form of entity authentication according to the rules that have been established as has been noted by the Certificate Practices Statement (CPS). After this process, each entity is then issued with a digital certificate. The beauty of this is the fact that the certificate is signed by a CA and thus the identity of the entities is vouched. With this, individuals who are unknown to each other can then establish trust between them because they have trust with the CA that it has performed some form of authentication on both of the entities. What is more, the signing of the CA is an attestation to this fact. One of the benefits of PKI is the establishment of a trust hierarchy which works well with networks which are of different environments and platforms (Stalling, 1999).

References

General Accounting Office (USA) (2001). Advances and remaining challenges to adoption of PKI technology. New York: Cengage Learning.

General Accounting Office (USA) (2004). Authentication handbook for federal and government agencies. New York: Cengage Learning.

Kapilia, R. (2003). PKI security solutions for the enterprise, Wiley Publishing Inc.

Stalling, W. (1999). Cryptography and network security, principles and practice. New York: Prince Hall.