**Topic 1\_RA**

Digital certificate which is also called as public key certificate cryptographically links public key ownership with the unit who owns it. These digital certificates are used for the purpose of authentication and encryption (Rouse, 2020). Digital certificates have the public key, which is certified, and identifies the information about the organization who owns the public key, metadata which is related to the digital certificate and a digital signature of public key which is created by the person who issued the certificate (Rouse, 2020). All major web browsers and servers use digital certificates to give assurance that the content has not been altered by unauthorized people. The best way to improve company’s security is getting own digital certificates. Digital certificate is the best option for securing company’s data online (Publico, 2018).

* Digital certificates protect data from outsiders who try to steal the data.
* Businesses including small scale and large scale can use digital certificates with same quality of encryption.
* Today’s world email or website can be faked , but digital certificates assure that message will come from deliberate recipient.
* The reputation and privacy of clients will be protected (Publico, 2018).

 Digital certificates are used to provide cryptographic assurance and privacy of data. Big companies which are making IoT devices should be aware of how to secure them. Even cars have network stacks, and should be able to upgrade firmware. Even phones, iPads have digital certificates which require authentication. This results a surge in digital certificates and as a business it would be hard to control the volume. Its important for a security team to properly manage digital certificates (Kubach, 2016). Even if a single certificate is forgotten to place on a device or server entire network can be compromised. If a person in an organization is responsible for management of digital certificate and if he goes on a leave for the week that the certificate expires, entire business can be at stake. The organization should make sure that the certificates are up and running. Digital certificate management is very important to the security posture of an organization. There are two kinds of critical impacts to digital certificates

* Outage: Possible business impacts are loss of income and customer dissatisfaction.
* Breach: Possible business impacts are loss of data , damage to reputation ,Fines and legal fees (Kubach, 2016).

Companies can properly manage digital certificates by

* By knowing the number of digital certificates
* If there are large number of certificates, then automation and involving third party to carryout infrastructure management would help.
* Decide whether there is cost basis for each certificate when evaluating.
* Know if certificate lifecycles are properly defined (Kubach, 2016).

**References**

Kubach, M. (2016). The importance of digital certificate management. Retrieved from https://blog.keyfactor.com/the-importance-of-digital-certificate-management

Publico, R. (2018). Five beneficial features of digital certificates. Retrieved from https://www.globalsign.com/en-sg/blog/five-beneficial-features-of-digital-certificates

Rouse, M. (2020). Digital certificate. Retrieved from https://searchsecurity.techtarget.com/definition/digital-certificate#:~:text=Digital%20certificates%20are%20used%20in,and%20authentication%20of%20digital%20signatures.

**Topic 2\_SRP**

**Evaluate the role of a digital certificate in cryptography.  How does it impact the security posture of an organization?**

A digital certificate, also known as a public key certificate, is used to cryptographically link ownership of a public key with the entity that owns it. Digital certificates are for sharing public keys to be used for encryption and authentication (Tycksen & Jennings, 2001). Digital certificates include the public key being certified, identifying information about the entity that owns the public key, metadata relating to the digital certificate and a digital signature of the public key created by the issuer of the certificate (Tycksen & Jennings, 2001).

A digital certificate is an attachment to an electronic message used for security purposes by many organizations. The most common use of a digital certificate is to verify that the user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply (Maes & Sedivy, 2000).

The digital certificate enables organizations to share their public key in a way that can be authenticated. Digital certificates are used in public key cryptography functions; they are most commonly used for initializing secure SSL connections between web browsers and web servers (Maes & Sedivy, 2000).

Organizations uses digital certificates for merchant authentication, SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards. SET uses X.509v3 digital certificates with RSA signatures for this purpose (Stallings, 2017).

 References

Maes, S. H., & Sedivy, J. (2000). U.S. Patent No. 6,016,476. Washington, DC: U.S. Patent and Trademark Office.

Stallings, W. (2017). Cryptography & Network Security GE. Pearson Australia Pty Limited.

Tycksen Jr, F. A., & Jennings, C. W. (2001). U.S. Patent No. 6,189,097. Washington, DC: U.S. Patent and Trademark Office.