4.3.4.4 Authenticity

Return to Securability

About

Authenticity is a property indicating the source and origin of the information[1]. The process of authenticating a source starts when an entity (i.e., user, remote process, intelligent agent, etc.) attempts to access resources on a Computing Platform. The entity proves their identity in order to gain access rights. For example, traditionally when logging into a computer, users use a Single-Factor Authentication (SFA) by providing a `usernames` and `passwords` to confirm their identity to allow future authentication for access to resources. However, this `usernames` and `passwords` login combination is no longer considered secure enough, especially if there are poor CyberSecurity Culture (CSC). As a consequence, many systems have added Two-Factor Authentication (2FA) that require Biometrics (i.e., facial recognition, fingerprints, etc) or One-Time PIN (OTP). These 2FA methods generally require the user to be physically present to successfully login.

Public Key Infrastructure (PKI) is generally used to connect servers and clients or even nodes that have no user present to perform the SFA or the 2FA methods of authentication. It is often incorrectly used as a synonym for Encryption. Encryption is an algorithm used to encrypt and decrypt data. PKI is an infrastructure built around asymmetric encryption with two keys: public and private. PKI is used extensively to securely transfer data between Network Nodes. In the PKI infrastructure, entities (i.e., AAA and BBB) exchange public keys. To exchange information, one entity (i.e., AAA) encrypt a document using the other entities (i.e., BBB) public key. Anyone can receive the document encrypted by AAA using BBB's public key, but it remains encrypted until BBB uses the private key in the PKI to decrypt the document.

PKI is the backbone of most of the major secure document exchange sites. Some examples are[2]:

- Securing emails - Email Security (S/MIME Protocol)
- Securing web communications - Website Security
  - Hypertext Transport Protocol Secure (HTTPS)
  - Secure Sockets Layer (SSL)
  - Transport layer security (TLS)
- Secure Shell Protocol (SSH)
- Digitally signing software, applications or data
- Encrypting and decrypting data
- smartcard authentication
- Subscriber Identity Module (SIM)
- ISO/IEC 7816 Integrated Circuit Card Family of Specificaions

DIDO Specifics

Return to Top

To be added/expanded in future revisions of the DIDO RA

=-
=-

1) Authenticity, Computer Security Resource Center (CSRC) Accessed 14 August 2020, https://csrc.nist.gov/glossary/term/authenticity

2) How Does PKI Work ?, Venafi, Accessed 14 August 2020, https://www.venafi.com/education-center/pki/how-does-pki-work