15/03/24

Unit-4

Remote-User Authentication

It is the fundamental building block and the primary line of defense. User authentication is the basis for most types of access control and for user accountability.

→ It is defined by RFC 4949 (Internet Secure Glossary version-2).

→ mainly consists of two steps.

* **Identification Step:**

Presenting an identifier to the security system.

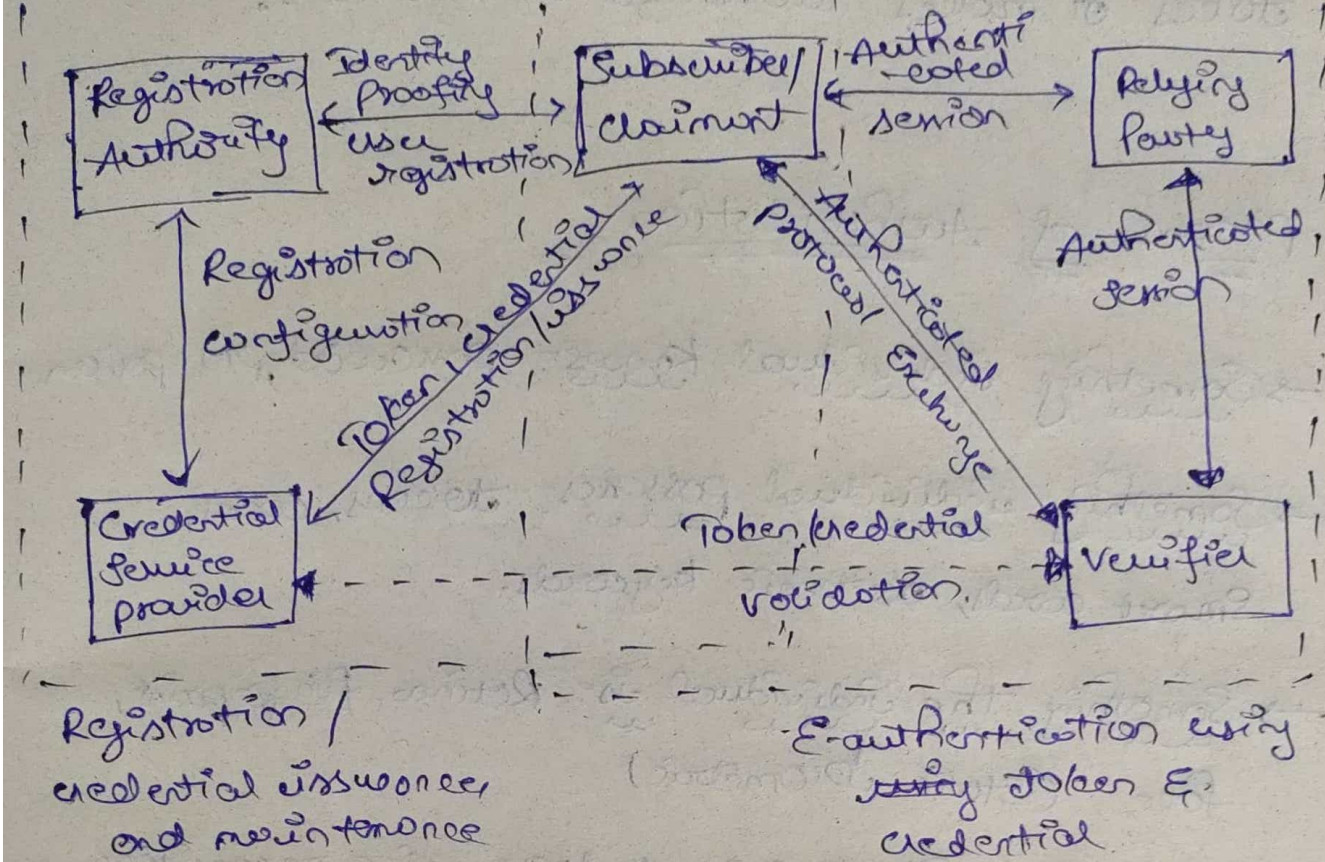
(Ex: Look up for the username in the server)

* **Verification Step:**

Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

(Ex: Look for the password given by the user is matched or not in the server).

The NIST model for Electronic User Authentication



→ Applicant applies to "Registration Authority (RA)" to become a subscriber of CSP.

→ RA verifies the user identity to CSP.

→ CSP then gives electronic "credential" to the subscriber r.e. (stores the credential)

→ May be given by CSP, or third party.

→ @ Claimant (the website or the destination).

→ "Verifier" verifies the identity of the subscriber by checking the credentials in "CSP".

→ Sends the response to relying party (RP).

→ Then RP using the information provided by verifier takes or makes authorization decisions.

Means of Authentication

→ Something individual knows: password, pin, pattern

→ Something individual possesses: tokens, cards, smart cards, electronic keycards.

→ Something the individual is: Retina, fingerprint, face (Static biometric)

→ Something the individual does: voice recognition, handwriting & typing rhythm. (dynamic biometrics).

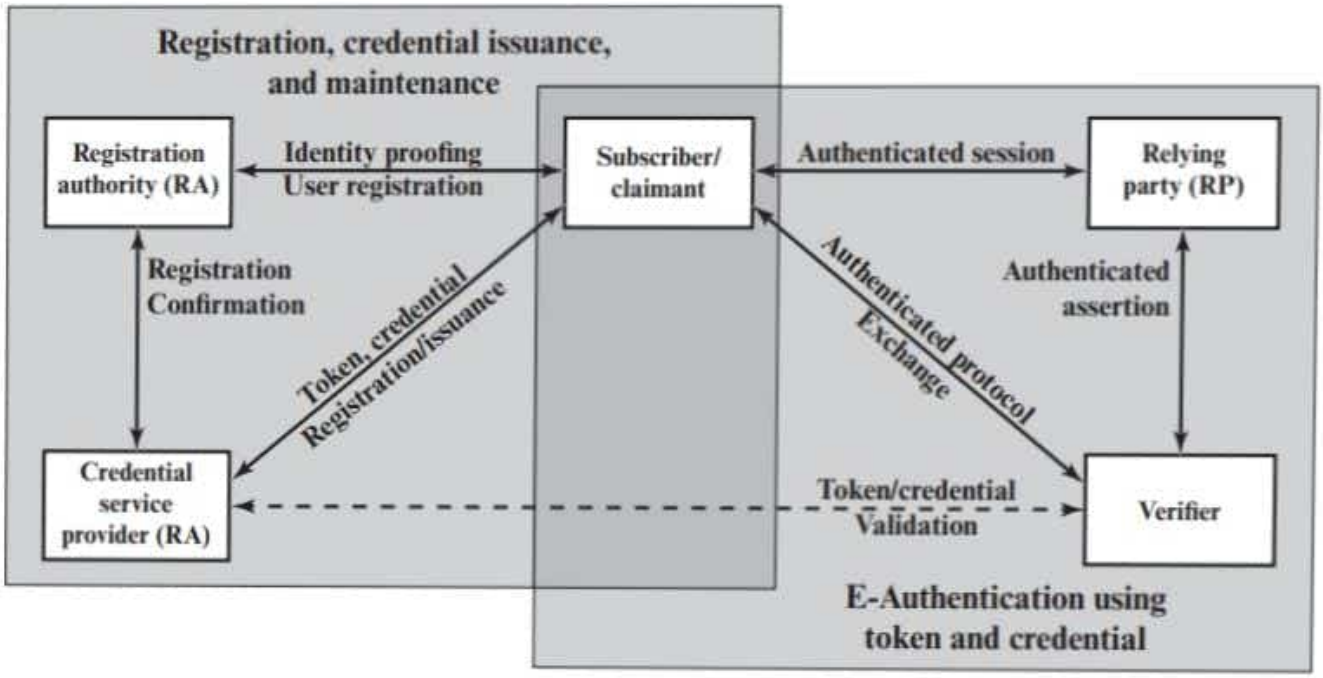


Figure 15.1 The NIST SP 800-63-2 E-Authentication Architectural Model