Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

NIST SP 800-63-3 (*Digital Authentication Guideline,* October 2016) defines digital user authentication as:

“The process of establishing confidence in user identities that are presented electronically to an information system.”

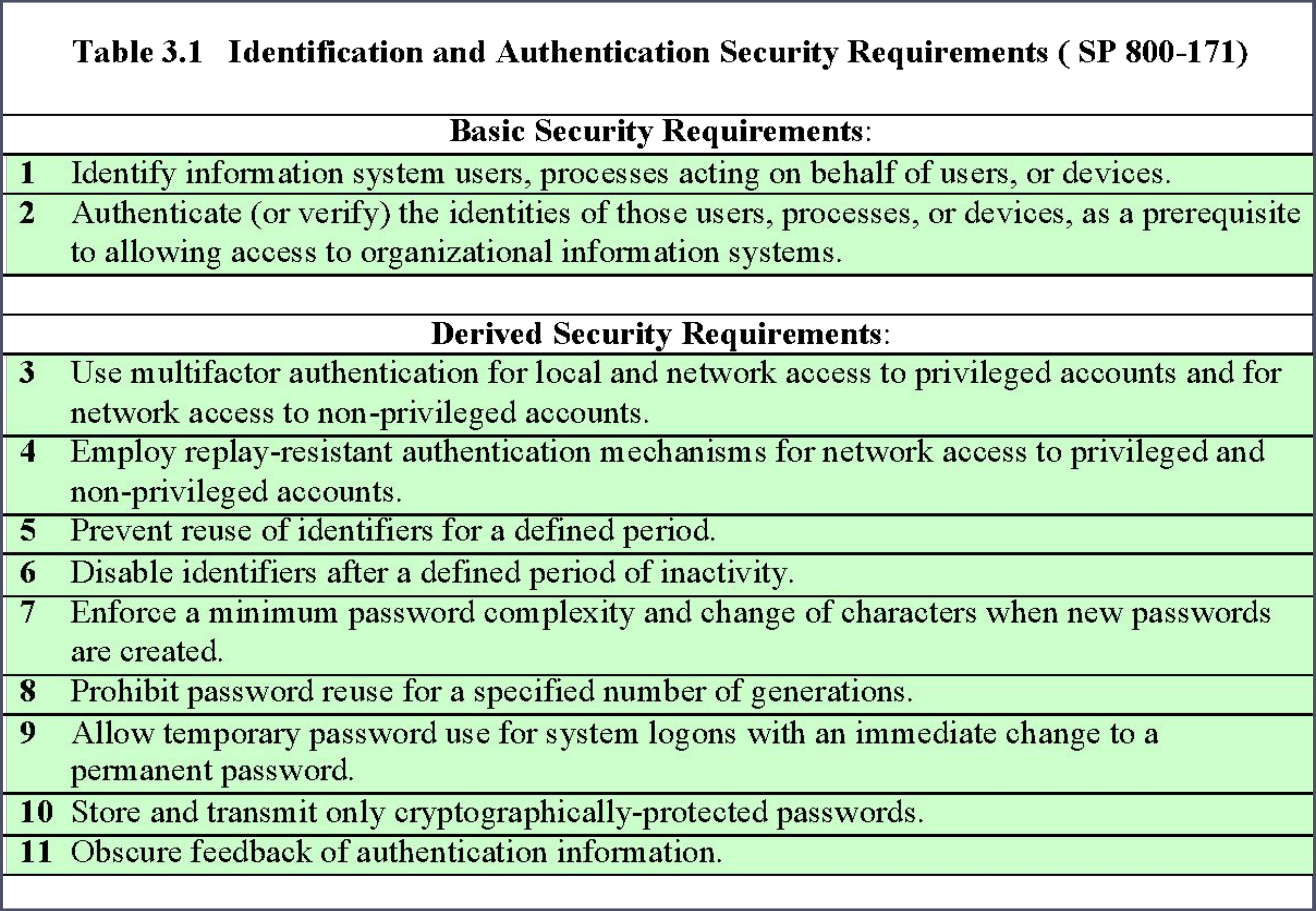

Table 3.1 Identification and Authentication Security Requirements (SP 800-171)

	Basic Security Requirements:
1	Identify information system users, processes acting on behalf of users, or devices.
2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
	Derived Security Requirements:
3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
5	Prevent reuse of identifiers for a defined period.
6	Disable identifiers after a defined period of inactivity.
7	Enforce a minimum password complexity and change of characters when new passwords are created.
8	Prohibit password reuse for a specified number of generations.
9	Allow temporary password use for system logons with an immediate change to a permanent password.
10	Store and transmit only cryptographically-protected passwords.
11	Obscure feedback of authentication information.

(Table can be found on page 65 in the textbook)

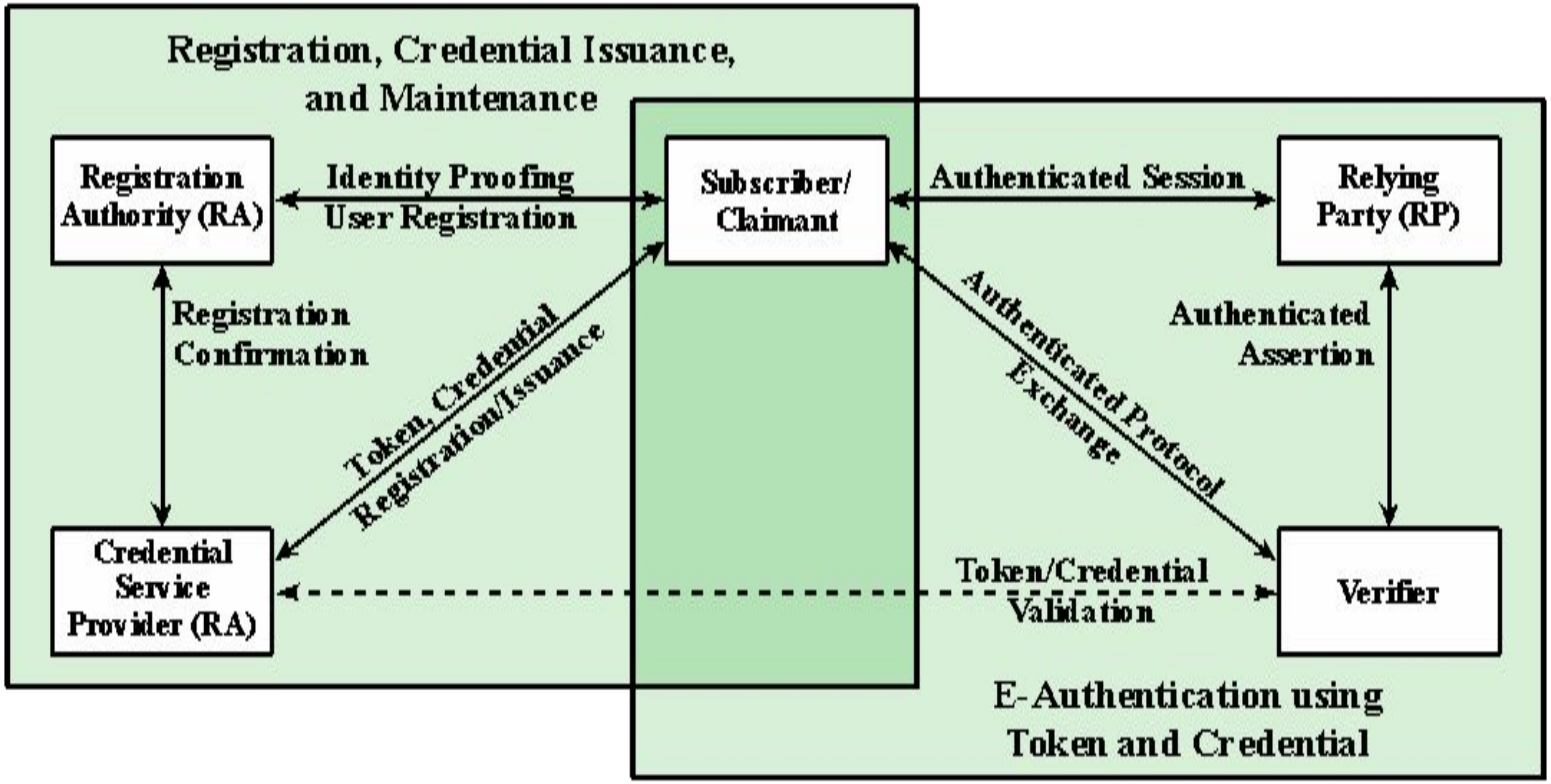
Registration, Credential Issuance, and Maintenance
Registration Authority (RA)
Identity Proofing User Registration
Subscriber/ Claimant
Authenticated Session
Relying Party (RP)
Registration Confirmation
Token, Credential Registration/Issuance
Authenticated Protocol Exchange
Authenticated Assertion
Credential Service Provider (RA)
Token/Credential Validation
Verifier
E-Authentication using Token and Credential

Figure 3.1 The NIST SP 800-63-2 E-Authentication Architectural Model

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm