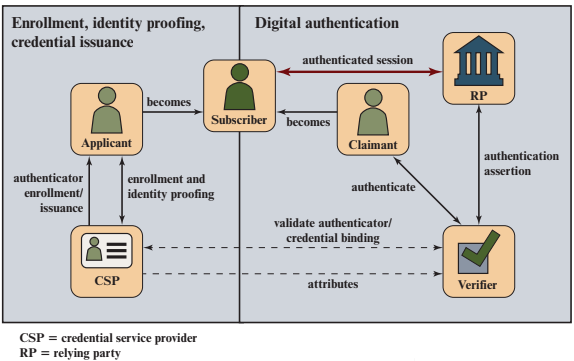
**CONTENTS**

**A - Remote User-Authentication Principles**

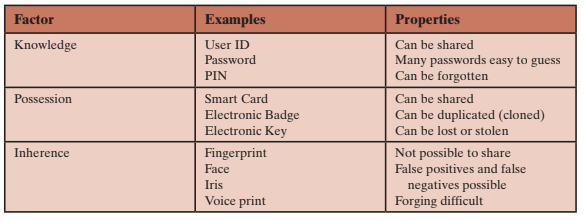
* **The NIST Model for Electronic User Authentication (**Mô hình xác thực người dùng trực tuyến của NIST - Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ National Institute of Standards and Technology - NIST)

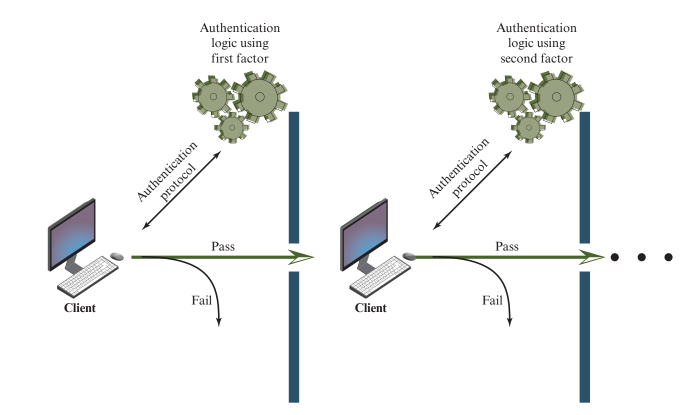
NIST SP 800-63 (tiêu chuẩn nhận dạng kỹ thuật số) xác định một mô hình chung cho việc xác thực người dùng.

**Giải thích mô hình:** Mô hình này mô tả quy trình xác thực số từ việc đăng ký, chứng minh danh tính và cấp phát thông tin xác thực cho đến việc xác thực số và thiết lập phiên làm việc đã xác thực. Các bước chính bao gồm:

* Đăng ký và Chứng thực danh tính: Người dùng (Applicant) trải qua quá trình đăng ký và chứng minh danh tính để trở thành Người Đăng Ký (Subscriber).
* Phát Hành Thông Tin Xác Thực: CSP (Credential Service Provider) cấp thông tin xác thực và quản lý việc đăng ký.
* Xác Thực Số: Người Đăng Ký trở thành Người Yêu Cầu (Claimant) và được Verifier kiểm tra thông tin xác thực và thuộc tính.
* Phiên Làm Việc Đã Xác Thực: Khi xác thực thành công, một phiên làm việc đã xác thực được thiết lập với RP (Relying Party).

Mô hình này giúp đảm bảo rằng chỉ những người dùng được xác thực mới có thể truy cập vào tài nguyên được bảo vệ trực tuyến.

* **Means Of Authentication** (các phương thức xác thực)
* **Multifactor Authentication** (xác thực đa yếu tố)
* **Mutual Authentication** (xác thực lẫn nhau)

Là một lĩnh vực ứng dụng quan trọng, nơi các giao thức cho phép các bên giao tiếp xác minh danh tính của nhau một cách đồng thời và trao đổi khóa phiên. Điều này đảm bảo rằng cả hai bên đều có thể tin tưởng vào danh tính của đối phương trước khi bắt đầu truyền thông tin hoặc dữ liệu. Đây là một bước quan trọng trong việc bảo mật giao tiếp và thường được sử dụng trong các kết nối mạng, như trong giao thức Bảo mật Lớp Vận chuyển (TLS) và các kết nối giữa các thiết bị Internet vạn vật (IoT).