Single sign-on, these are systems where there are no separate passwords to several different systems, but the user authenticates to a central authority who then verifies your authentication to other dependent services. This means that services have to be specifically adapted to allow any one of these models of cooperative authentication.

Note how single sign-on puts great demands on the security of the single authentication that gives us the right to access several diverse services. To propose one small example - Kerberos documentation is careful to never use the term password, preferring pass phrase, thereby encouraging users not to create the same kinds of problems one commonly sees in passwords for this one, critical authentication.

Federated ID is similar in function to single sign-on but where the identity may be trusted across several organisations. Things can become complex here, for example when different organisations have different policies on what are sufficient factors to identify an entity, and yet hope to collaborate on the authentication.

A completely different take on securing passwords is one-time passwords. As the name implies, this involves using a password once, but once used that password is invalidated.

Biometrics – automated measurements of biological and behavioural features that identify a person.

Because biometrics are measurements of the characteristics of the individual, people are tempted to believe that attackers cannot pose as authorized users on systems that use biometrics. Several assumptions underlie this belief.

A close-up of a document

Description automatically generated

Multifactor authentication uses 2 different forms of authentication to validate identity.

Ex – Asks for a password (what the entity knows) and then asks to enter a sequence of digits sent to a smartphone (what the entity has).