Authentication, 2FA, and MFA

A Plurilock Rapid Reference

Overview
Two-Factor and Multi-factor Authentication

2FA and MFA protected systems check a user's identity in more than one way. The first check is usually a password prompt.

On 2FA and MFA protected systems, after the password is entered, additional checks are then performed, often using one of the following technologies:

- Hardware authenticators
- One-time passwords
- Biometric scans
- Behavioral biometrics

Hardware Authenticators

Hardware authenticators are flash-drive-sized devices that are uniquely identifiable. Each authenticator is intended to be carried and used by one and only one user. Examples include YubiKey and RSA SecurID tokens.

Benefits

- Difficult to hack or crack
- No memorization required

Drawbacks

- When stolen, no longer secure
- Easy to steal, easy to lose
- Requires extra step to log in
- Can be difficult to configure
- Can be expensive to purchase

One-time Passwords (OTP)

One-time passwords change with each login (hence "one-time"). Users don't remember them—instead, they're sent to the user on a "trusted" communications channel. Examples include SMS codes and authenticator apps.

Benefits

- No new hardware required
- Often less expensive

Drawbacks

- Easily stolen at a glance
- Cumbersome manual entry
- Costly if phones are issued
- SMS codes highly insecure

Biometric Scans

Biometric scans are detailed scans of part of a user's body that are stored for identification purposes. To log in, they must demonstrate that they "possess" the right body by allowing the body part in question to be scanned again for comparison. Examples include fingerprint and face scans.

Benefits

- Simpler than OTP or hardware MFA
- Not easily stolen

Drawbacks

- Impersonation possible if stolen
- Can't easily be changed if stolen
- Requires dedicated hardware

Behavioral Biometrics

Behavioral biometric systems check identity by recognizing the ways in which a user's fingers move as they type or use a pointing device. These movement patterns are as unique as fingerprints, but are privacy-safe. Plurilock products offer behavioral-biometric MFA.

Benefits

- No extra steps required to log in
- No change in user experience
- More secure than other MFA tools
- No new or special hardware required

Quick Look
Invisible Authentication

Invisible authentication is a Plurilock MFA technology that leverages behavioral biometrics, geolocation, device fingerprinting, and machine learning technology to enable invisible authentication that:

- Requires no new hardware
- Requires no memorization
- Adds no new steps to user logins
- Is not visible to the user unless authentication fails

To see an invisible authentication solution in action, contact Plurilock for information about **Plurilock ADAPT.**

Quick Look
Continuous Authentication

Continuous authentication is a Plurilock technology that is both invisible to the user and that operates in the background, as they work. Continuous authentication:

- Confirms a user's identity every 3-5 seconds all day
- Operates invisibly, as regular everyday work happens
- Recognizes and locks strangers out in seconds
- Supports NIST 800-207 Zero Trust compliance

To see a continuous authentication solution in action, contact Plurilock for information about **Plurilock DEFEND.**

Quick Look
Passwords and Password Security

Password policies vary between organizations. Today they frequently include requirements that are no longer considered to be best practices. Current password policy best practices include:

- No periodic password refresh or reset requirements
- No special symbol requirements
- Extended (>10) length requirement
- Use of multiple memorable but unrelated words

Examples of good passwords include:

- SprinkleTacos4December
- I8AFunnyPlantFishPappy
- TwoMegaFractalBodegaJeeps
- 3ForestsAreMyBicycleTwig

Plurilock

Glossary

Common Authentication Terms and Meanings

Behavioral Biometrics

Behavioral biometrics is an identity verification strategy and matching set of technologies able to authenticate users' identities based on micro-patterns in everyday bodily movements.

Biometrics

Biometrics is an identity verification strategy and matching set of technologies that authenticate users based on measured physiological attributes, such as the spacing of ridges on a finger or facial features.

Brute Force Attack

A brute force attack is an attack in which every possible combination of letters, numbers, or words is tried in response to a shared secret authentication prompt.

Continuous Authentication

Continuous authentication is an authentication technology that uses other compatible authentication strategies (such as Plurilock's behavioral-biometric authentication) to verify users' identities on an ongoing, real-time basis, as they do everyday computing work.

Credential Stuffing

Credential stuffing refers to the automated attempt to access a protected system by trying a large number of stolen username and password combinations, usually obtained from data breaches.

Dictionary Attack

A dictionary attack is an attack in which many possible combinations of common words and phrases are tried in response to a shared secret authentication prompt.

False Acceptance Rate (FAR)

False acceptance rate, or FAR, is a measure of how often a biometric authentication system incorrectly authenticates an unauthorized user.

False Rejection Rate (FRR)

False rejection rate, or FRR, is a measure of how often a biometric authentication system incorrectly rejects an authorized user.

Identity Factor

An identity factor is one of several general categories of identity signals that can be used to validate a user's identity.

Identity Signal

An identity signal is a form of data that can be used to uniquely identify an individual.

In Band

In-band authentication factors are identity signals that rely on their identity check on the same system that is requesting user authentication.

Knowledge-based Authentication (KBA)

Knowledge-based authentication, or KBA, is a method of authentication in which a user proves his or her identity by providing information that only they should know.

Multi-factor Authentication (MFA)

Multi-factor authentication, or MFA, is a form of authentication requiring that a user prove their identity using two or more identity factors at once.

Passive Authentication

Passive authentication is a form of authentication in which the identity of the user is checked and confirmed without requiring specific additional actions for the purpose of authentication.

Password Hygiene

Password hygiene refers to the degree to which a user's passwords are selected and managed according to secure best practices.

Step-up Authentication

Step-up Authentication is an additional step in a login or authentication workflow in which a user is asked to provide additional confirmation of their identity.

One-time Password (OTP)

A one-time password is a password, supplied to the user through a trusted communications channel, that can be used to confirm identity only once before it expires.

Out of Band (OOB)

Out-of-band authentication factors are identity signals that do not rely for their veracity on the same system requesting user authentication.

Shared Secret

A Shared Secret is a static word, phrase, or string of characters agreed upon by two parties in order to confirm identity as a form of knowledge-based authentication.

Single Sign-on (SSO)

Single Sign-On, or SSO, refers to a user experience in which users who successfully authenticate their identities once are then able to use a variety of applications and resources without having to authenticate again for each of them.

Two-factor Authentication (2FA)

Two-factor authentication, or 2FA, is a form of authentication requiring that a user prove their identity using an additional identity factor beyond their username and password.

Plurilock