

SecureAuth IdP

Authentication Mechanisms

SMS OTP

A one-time password delivered via Short Message Service to the phone number recorded in the user's profile.

Telephony OTP

A one-time password delivered telephonically to the phone number recorded in the user's profile.

E-mail OTP

A one-time password delivered via e-mail to the address recorded in the user's profile.

Static PIN

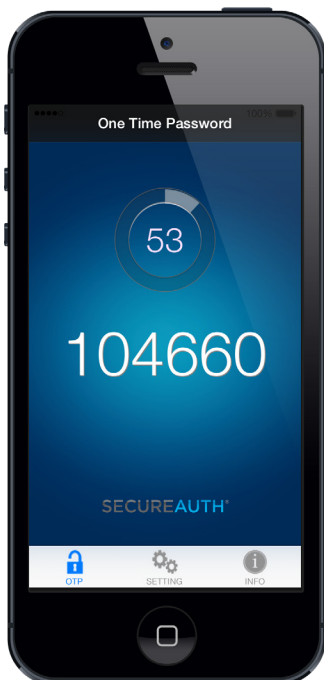
A personal, unchanging PIN code.

Yubikey (USB)

A USB that plugs into a user's device and generates a one-time password that is instantly inputted on the screen.

Password

A user's known password.



KBA/KBQ

Knowledge-based answers/questions that are stored in the user's profile.

Kerberos (IWA)

Microsoft's Active Directory desktop SSO system of logon.

X.509 Native

An X.509 certificate that is placed in a device's built-in OS certificate store.

X.509 Java

An X.509 certificate that is placed in a browser's java certificate store.

Help Desk

A one-time password delivered by the help desk after verifying the user's identity.

PUSH Notification

A one-time password delivered to a user's pre-registered mobile device (smartphone, tablet) immediately as a notification.

Device Fingerprinting

The patent-pending process in which SecureAuth IdP *pulls* unique characteristics from a device and then maps that identifying value to the user's profile. This enables frictionless subsequent authentications for mobile or desktop users.

Social IDs

Identities from social websites, such as Facebook, LinkedIn, Twitter, or Google.

Federated IDs

A token that is issued in a trusted language (SAML, WS-Fed, OAuth) that validates the user's identity without transferring password information.

NFC Proximity Card

Any object that utilizes Near Field Communication for information regarding the object's identity.

CAC / PIV Card

A smart card with an X.509 certificate used by the U.S. government and its agencies.

Mobile OATH Token

A time-based one-time OATH password generated on a user's iOS, Android, Windows, or Blackberry mobile device.

Browser OATH Token

A time-based one-time OATH password generated on a user's browser interface.

Windows Desktop OATH Token

A time-based one-time OATH password generated on a user's Windows desktop.

Third-party OATH Token

A time-based one-time OATH password generated from a provider other than SecureAuth that can be hardware- or software-based.

Symantec VIP

Symantec's cloud-based VIP service used for authentication into a SecureAuth-protected resource.



2-Factor Access Control for the Mobile Enterprise

8965 Research Drive
Irvine, CA 92618

1.949.777.6959
secureauth.com

