DATA SHEET

CA Strong Authentication

At a Glance

CA Strong Authentication allows you to deploy a wide range of authentication methods in an efficient and centralized manner. It also provides a flexible set of easy-to-use, multi-factor credentials that can increase security and improve compliance without burdening your users or your help desk. CA Strong Authentication works with CA Risk Authentication to further enhance authentication security and improve user convenience. It also integrates with the entire CA Identity and Access Management portfolio.

Key Benefits/Results

- Reduces the risk of inappropriate access, data breaches and attacks
- Increases security without altering end users' login experience
- Eliminates the risk of stolen passwords
- Scales with your organization's needs

Key Features

- Supports wide variety of credentials– from passwords and knowledge-based authentication (KBA) methods to two-factor software and hardware tokens
- Provides out-of-band (OOB) authentication using one-time passwords (OTPs) delivered via text, voice or email
- Eliminates the risk of stolen password files because passwords are never stored
- Converts workstations, smartphones or tablets into a second-factor token
- Offers a wide variety of integration options such as SAML, API and RADIUS
- Protects millions of users without degrading your web application or network performance.
- Available as a cloud service, MSP-hosted service or on-premise solution.

Business Challenges

Improve security for online logins/sensitive transactions. Passwords can be easily compromised. Organizations need an adaptable way to identify users and protect confidential data and sensitive online transactions without inconveniencing their users.

Support the mobile economy. Mobile applications and devices are becoming the preferred method for users to interact with an organization. Organizations need a consistent authentication strategy that accommodates a full range of devices.

Meet regulatory compliance directives. Numerous regulations are recommending or requiring stronger authentication for sensitive transactions. Implementing the proper forms of authentication in a cost-effective manner is an ongoing challenge for many organizations.

Simplify user experience. Users are fickle and many enterprises are struggling with mobile app adoption. Increasing security without impacting the user experience is critical.

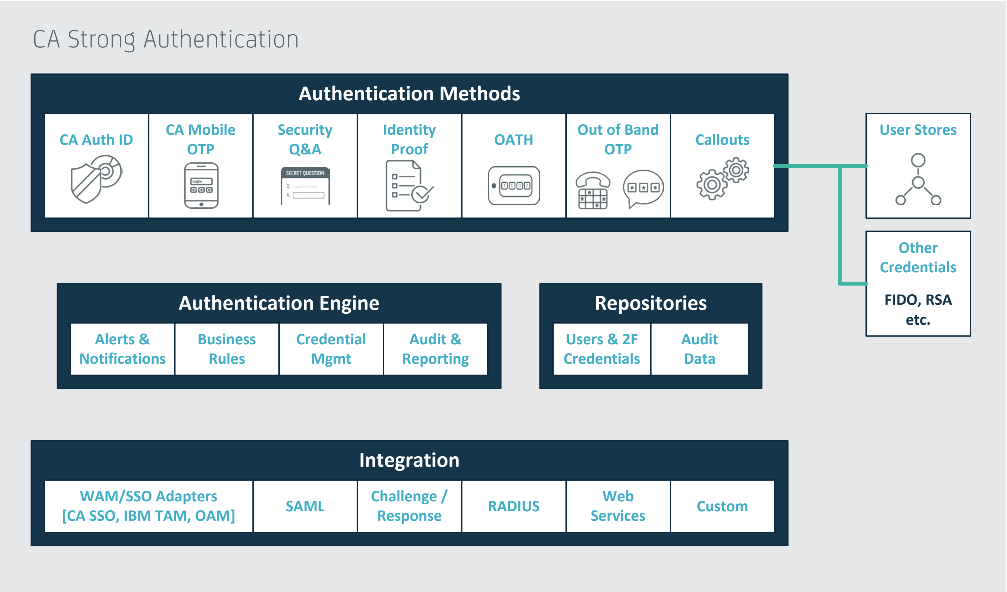
Solution Overview

CA Strong Authentication provides multi-factor authentication for web applications, portals, and mobile apps with a wide range of credentials. You can deploy the right credential with the right level of security based on the application being accessed. You can provide easy to use multi-factor authentication in a cost-effective and centralized manner based on your business policies without causing unnecessary friction in the authentication process. This can result in better security, an improved compliance profile, lower operational costs and increased customer retention. Our software-only approach gives you the right balance of cost, convenience and strength for enhancing the protection of your web resources and the identities of your web users. The solution works with CA Risk Authentication to provide multi-layered authentication security.

Critical Differentiators

For over a decade CA Strong Authentication has been a leader in multi-factor authentication, addressing the critical need for identifying online and mobile users and managing access to applications and cloud services.

- **Unbreachable passwords.** Customers can continue to use passwords. But the password is never transmitted over the Internet and never stored on the user's device, or within any backend system, so it remains a true secret that is only carried in the user's head.
- **Bring your own credential**. You can use the wide range of authentication methods and credentials available or incorporate your existing credentials as part of your centralized authentication strategy.
- **Cryptographic camouflage.** Patented key concealment technology is used to protect the unique multifactor CA Auth ID and CA Mobile OTP credentials from brute force and dictionary attacks.
- **Total cost of ownership.** The solution is licensed on a per-user basis, not per credential, so organizations can issue unlimited credentials to support an unlimited number of users and devices.



Related Products/Solutions

CA Risk Authentication. Risk-based authentication with behavioral profiling, mobile device risk assessment, DeviceDNA™ and dynamic rules.

CA Single Sign-On. Web single sign-on across on-premise, hosted or cloud-based applications for your employees, customers and partners.

CA Privileged Identity Manager. Privileged account management, protecting servers, applications and devices across platforms and operating systems.

Supported Environments

Devices – Android, iOS, PC, Win8 Mobile

Browsers - Apple Safari, Google Chrome, Microsoft® Internet Explorer®, Mozilla Firefox

Single Sign-On – CA Single Sign-On, IBM® Tivoli® Access Manager, Oracle Access Manager

Standards and protocols – EMV CAP/DPA, HOTP/TOTP, HTTP/HTTPS, RADIUS, SAML, SOAP

For more information, please visit ca.com/us/multifactor-authentication

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

Copyright © 2015 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.