

CA Mobile OTP



At a Glance

Consumers have embraced the fact that mobile devices are being utilized for so much more than the traditional call or text. Most consumers expect flawless access to online applications no matter where they are, making them highly susceptible to internet attacks. In this day and age, fraudulent online activity and relevant theft is commonplace.

As a result, financial institutions struggle to find a solution that invokes strong authentication for suspicious online transactions. With CA Mobile OTP, issuers have access to a solution that has a significantly lower cost of ownership with an improved user experience for authenticating multiple cards and accounts. CA Mobile OTP allows issuers to provide their customers a simple mobile authentication application that reduces fraud loss and provides a positive user experience.

Key Benefits/Results

Reduce fraud losses. Easily distinguish legitimate cardholders from fraudsters.

Simplify authentication. Customers no longer inconvenienced by having to remember passwords.

Utilize across multiple channels. Unified authentication enables a positive experience for customers.

Key Features

EMV-Compliant dynamic password generation. Uses industry standard EMV based algorithm for generation of dynamic password.

User keys protected by Cryptographic Camouflage. 2-factor authentication keys protected against brute force attacks.

Multi-channel support. Same authentication app can be used for multiple channels.

Deploy within existing mobile apps. Can be integrated into your branded mobile apps.

Configurable policies. Configure policies related to provisioning, reprovisioning and transaction processing for users not provisioned.

Over the air provisioning and enrollment. Can deploy the app from an app store or from a bank site.

Instant reporting on provisioning and transactions. Provide data transparency to satisfy customer inquiries immediately.

Delivered as a cloud service. Limit IT involvement with SaaS capability.

Business Challenges

3-D Secure cardholder authentication programs, like MasterCard SecureCode and Verified by Visa, provide the ability to authenticate a shopper at checkout for online transactions. Currently, the most common authentication method is a simple password. However, the adoption of stronger authentication methods for e-Payments is increasing due to the increase in internet fraud. Similar concerns apply to Internet account access and other online applications such as VPN access or web portal login.

With advancements in technology, fraudsters have begun gathering personal data from cardholders through phishing and harnessing social media data. Authentication using static forms of data, such as simple passwords, has become inadequate in the battle against fraud.

Furthermore, current hardware based authentication mechanisms introduce additional complexity and cost to financial institutions, such as costs of distribution and usability challenges for customers.

Solution Overview

CA Mobile OTP is a mobile authentication solution that allows financial institutions to provide a user-friendly mobile app that generates a dynamic one-time-password. It provides flexible and cost-effective options for implementing 2-factor authentication to help prevent fraud when customers access their accounts or complete payment transactions.

The solution uses the industry standard EMV algorithm for dynamic password generation, both CAP Certified and DPA compliant. It stores keys, protected by patented Cryptographic Camouflage, on the mobile device defending customers from brute force attacks while limiting the amount of information a customer must remember, ensuring maximum security and a positive user experience. The dynamic password can be generated without access to a mobile network or Internet connectivity during authentication, for example, when attempting to withdrawal money from an ATM.

CA Mobile OTP provides the ability to easily distinguish a legitimate cardholder from a fraudster, enabling financial institutions to dramatically reduce fraud loss. CA Mobile OTP is easy to provision and manage, thus avoiding the distribution costs of dedicated hardware password generators.

Critical Differentiators

Strong Cryptographic Camouflage-based key storage. Keys stored in the software using patented cryptographic camouflage technology providing resilience against brute force and other end point device centric attacks.

Single Authentication across multiple channels. Use the same mobile app for 2-factor authentication across multiple channels.

Integrate with existing mobile applications. Client Libraries can be used to integrate with existing mobile applications giving issuers control over branding and messaging.

Delivered as a cloud service. Deploy the solution with minimum IT involvement resulting in a faster time-to-market.

Related Products/Solutions

CA Transaction Manager. Offer a 3-D Secure security service in full compliance with Verified by Visa, MasterCard SecureCode, American Express SafeKey and Discover/Diners ProtectBuy cardholder authentication programs.

CA Risk Analytics. Provides real-time, intelligent risk assessment for 3-D Secure transactions using an advanced neural network fraud model and flexible rules to help minimize the risk and monetary loss from online payment fraud.

For more information, please visit ca.com/us/securecenter/ca-mobile-otp-for-payments

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.