



ArcotOTP Versatile Authentication Solution for Mobile Phones

DATA SHEET

Overview

Turns mobile phones into one-time-password authentication devices

Can use one mobile phone to generate OTP for multiple accounts, so no need to carry multiple hardware tokens

Supports multiple OTP algorithms including those specified by OATH (HOTP/TOTP) and EMV (CAP/DPA).

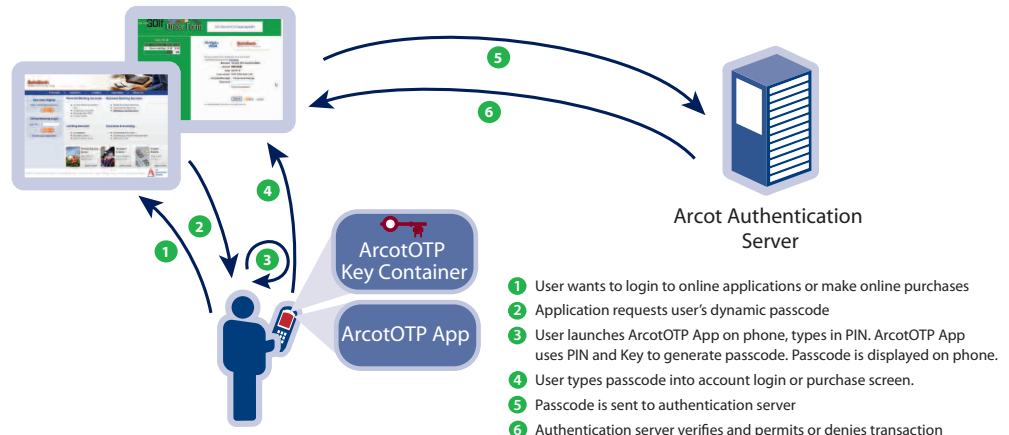
NEW ROLE FOR MOBILE PHONES Consumers have embraced their mobile phones as more than just calling or texting devices. They are demanding access to online applications no matter where they are, making them more vulnerable to internet attacks. The incidence of fraudulent online activity and related theft has driven the quest for better ways to authenticate access to applications such as online banking, e-commerce and Web portal access. Traditional security methods require a hardware device to authenticate to these applications. In most cases, a separate device is required for each account the user wants to access. The solution — use the mobile phone as an authentication device. Now, mobile phones are nearly ubiquitous and have become much more powerful. Why not take advantage of a device that is already part of a person's everyday life?

ArcotOTP TURNS MOBILE PHONES INTO AUTHENTICATION DEVICES Arcot provides a wide range of fraud detection and multifactor authentication methods to reduce the risk of online fraud for e-commerce, Web portal and remote access. We provide authentication methods that are strong, yet easy to use. Recognizing the expansion of the use of mobile phones worldwide, Arcot provides a mobile application, ArcotOTP, that allows you to use your phone as a secure authentication device.

ArcotOTP is a software application that runs on a mobile phone and generates a one-time-password that is used to authenticate to online applications and to verify valid credentials for online purchases. Organizations and their customers no longer need to settle for weak password authentication or carry a separate authentication token. ArcotOTP runs on virtually all mobile platforms and authenticates users with a choice of one-time-password (OTP) standards. ArcotOTP supports multiple OTP algorithms including those specified by OATH (HOTP/TOTP) and EMV (CAP/DPA). The OTP algorithm can be selected based on the application. All of the OTP methods can be used on the same mobile phone supporting multiple accounts. No wireless or other connectivity is needed to generate the one-time-password. ArcotOTP allows organizations to provide strong authentication at a lower cost of ownership while increasing the security and convenience for their customers.

ArcotOTP AUTHENTICATION PROCESS

Account Login or Online Purchase



Mobile Platforms

- Apple iPhone
- BlackBerry RIM
- Google Android
- Windows Mobile

Additional Mobile Devices equipped with Java, MIDP 2.0 and CLDC 1.1 including

- Nokia
- Samsung
- LG
- Motorola - Sony Ericson

Runs in JavaScript in desktop browser

About Arcot

Arcot is the cloud authentication leader. Our fraud prevention, strong authentication, and e-Document security solutions make Web transactions and online access safe for millions of consumer, enterprise, and e-Commerce users.

Organizations can transparently deploy stronger authentication and allow users to conveniently authenticate from any computer or mobile device. Arcot solutions deliver the right balance of cost, convenience and strength.

ArcotOTP – High Security, High User Convenience

Security is achieved by storing the associated keys in the ArcotOTP key container which resides on the user's phone. The ArcotOTP keys are protected by Arcot patented cryptographic camouflage key concealment technology, which protects the keys from brute force and dictionary attacks. No other mobile phone authentication technique offers this level of security.

ArcotOTP allows users to easily generate an OTP to authenticate to online applications with a device that is already part of their everyday life. When the user logs into an online account, the experience is identical to the conventional HOTP/TOTP solutions. The ArcotOTP application on the user's phone generates the one-time-password that is requested by the online application the user is trying to access. Similarly, ArcotOTP replicates the user experience for online shopping consistent with the MasterCard CAP and Visa DPA programs without requiring a disconnected card reader.

Supports mobile phones, PDAs, Desktops

ArcotOTP works on the world's leading mobile platforms including Apple iPhone, BlackBerry RIM, Google Android, and Windows mobile. The ArcotOTP solution also works on most Nokia phones, and with most feature phones by Samsung, LG, Motorola and Sony Ericson that are equipped with Java, MIDP 2.0 and CLDC 1.1. In addition, ArcotOTP runs in JavaScript in a desktop web browser.

Mobile Phone Authenticates Multiple Applications

ArcotOTP can manage and authenticate to multiple accounts from a user's mobile phone. Users can easily select the web portal, VPN, or online account they want to access and ArcotOTP will generate the correct single use password for the selected account.

Based on Open OTP Standards

ArcotOTP is based on open standards including EMV CAP/DPA, HOTP and TOTP. One-time- or single-use password (OTP) is a mechanism where a user provides a new password every time they access a site. The OTP is generated by a device carried by the user. If an attacker steals the password, it is useless because it won't be valid the next time the user accesses the site. The attacker cannot calculate the password because it must be generated based on a shared secret between the user and the validation site. In general, there are two types of OTP — event based and time based. Event based OTP (EMV, HOTP) generates a new password every time based on a counter. The counter must be synchronized between the client and the server. The server recognizes a valid OTP generated by a legitimate customer. Time based OTP (TOTP) is similar except that an OTP is valid only for a short amount of time.

Fully Compatible with Existing Infrastructure

ArcotOTP is consistent with EMV, HOTP, and TOTP standards. No changes need to be made to authenticating server-side operations.



The user can use their mobile phone to automatically generate the one-time-passcode to be entered to gain access to their account or to complete the payment transaction

For more information, please visit www.Arcot.com, or contact your nearest sales office

Corporate Headquarters, U.S.

Arcot Systems, Inc.
Ph: +1 408 969 6100

United Kingdom

Arcot International
Ph: +44 118 965 7998

Germany

Arcot Deutschland GmbH
Ph: +49 8157 997793

India

Arcot R&D Software Private Ltd
Ph: +91 80 6660 2745



www.arcot.com

Copyright © 2010 Arcot Systems, Inc. All rights reserved. Arcot, Arcot WebFort and ArcotID are registered trademarks of Arcot Systems, Inc. All other trademarks are the property of Arcot Systems, Inc. or their respective owners.