



ArcotOTP – Secure Software Passcode Generator for Secure e-Payments and Internet Access



FACT SHEET

One Convenient Authentication Solution for Multiple Applications

The incidence of fraudulent online activity and related theft has driven the quest for better ways to authenticate Card Not Present (CNP) transactions and online access to applications such as online banking. In response, Visa developed the 3-D Secure protocol as a simple yet effective way to protect against fraudulent online transactions and provide secure online shopping. Today, all three major card brands use this protocol in their cardholder authentication programs: Verified by Visa™, MasterCard® SecureCode™, and JCB J/Secure™. Arcot participated in the development of the 3-D Secure protocol and has also developed patented technologies that protect online access.

The 3-D Secure e-Payment system provides various mechanisms to enhance authentication at purchase time for web 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. Arcot provides a wide range of fraud detection and multifactor authentication methods to reduce the risk of online fraud for e-Payments and internet access. These include password, risk-based authentication, EMV CAP/DPA chipcard support, the ArcotOTP secure software passcode generator, and the ArcotID secure two-factor software credential. The ArcotOTP is a software application that runs on mobile devices and personal computers and provides multiple OTP algorithms incorporating HOTP and EMV standards. The OTP algorithm can be selected based on application requirements. Both HOTP and EMV methodologies can be used on the same user device supporting multiple accounts. This fact sheet focuses on the EMV CAP/DPA authentication methodology used in the 3-D Secure environment.

MasterCard Chip Authentication Program EMV Authentication Standards

MasterCard's Chip Authentication Program (CAP) is an implementation of the EMV standard. CAP requires that a hardware device be distributed to users for authentication. The user receives an EMV Chipcard and a small "disconnected" reader that is carried with the user. During a web purchase the user inserts the card into the reader and types in a PIN. The Chipcard generates a one-time-passcode: a decimal string derived from an internally generated cryptogram. The user reads it and types it into a web form or speaks it aloud during a telephone purchase. However, the CAP solution has not solved the administrative or distribution problems associated with any hardware device or token. They are costly to deploy and use, and inconvenient for the user. Hardware solutions require the user to carry the device with them any time they want to shop online. But physical devices are easily forgotten or lost.

ArcotOTP – High Security, High User Convenience

ArcotOTP is an all purpose secure software passcode generator that supports standards including EMV and OATH. It implements MasterCard CAP without requiring a disconnected card reader. The user's mobile phone runs the ArcotOTP application that generates the dynamic passcode. The card reader image appears on the phone and depicts the card reader interface experience with the same buttons, options, and menu items. This provides a seamless transition for those customers that have previously used the disconnected reader and is easy for new users to learn. ArcotOTP allows users to easily generate an OTP to shop online or gain account access with a device that is already part of their everyday life.

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 which protects the keys from brute force and dictionary attacks.

When the user makes a web purchase or logs into an online account, the experience is identical to the conventional CAP solutions. The user gets out the mobile device, runs the ArcotOTP application, enters the PIN, and generates the dynamic passcode. Just as with the traditional disconnected reader, no wireless or other connectivity is needed. ArcotOTP can store and authenticate multiple cards at once. Users can easily select the card that they want to use. ArcotOTP will generate the



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

correct passcode for the selected card. In addition, the correct card brand will be displayed on the card reader image on the phone.

This results in a solution that has a significantly lower cost of ownership with improved user experience that can be used to authenticate multiple cards and accounts.

Support for Mobile Phones, PDAs, Desktops

ArcotOTP runs on all major mobile devices. In addition, ArcotOTP runs in JavaScript in a desktop web browser. In the latter case, the keys are stored in a browser cookie or Flash movie, accessible only by pages from the correct domain, and hidden from prying eyes by camouflage.

Fully Compatible with Existing Infrastructure

ArcotOTP is consistent with the hardware chipcard and disconnected reader. No changes need to be made to EMV CAP/DPA authenticating server-side operations.

Defeats Internet Threats

ArcotOTP can protect against the growing internet threats such as phishing. The ArcotOTP desktop browser solution provides additional protection against real-time redirection attacks such as man-in-the-middle (MITM).

ArcotOTP Security — Cryptographic Camouflage

The crucial secrets of a hardware chipcard are two DES keys called UDKA and UDKB, and they cannot be used unless the user presents a valid PIN. The keys are “camouflaged” in the ArcotOTP key container with the user’s PIN. When the user types in the PIN, these keys are transformed into the correct key bytes, and the

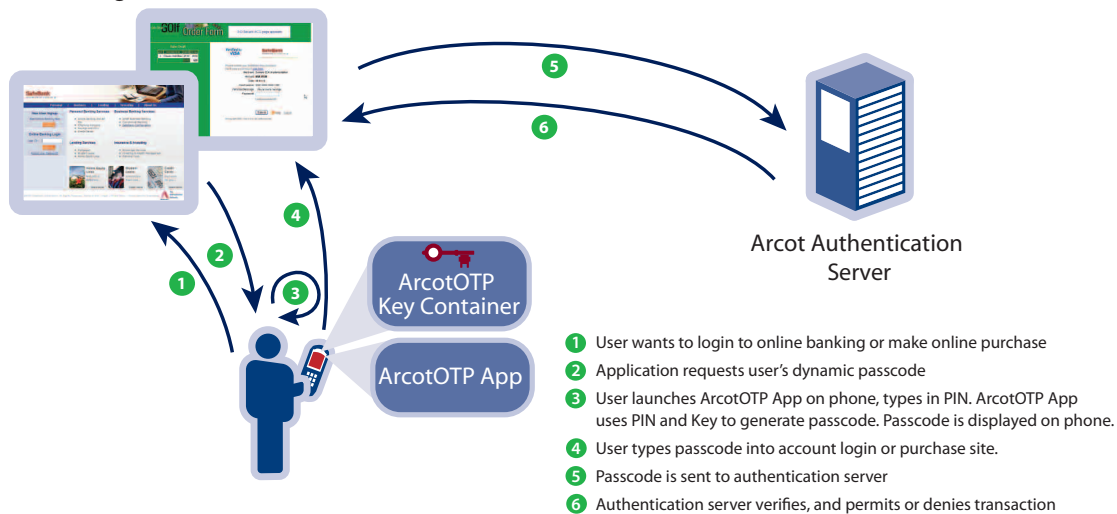
one-time-passcode is generated. But suppose an attacker has acquired the ArcotOTP key container. When any PIN, of any length, is applied to transform the keys, the result will always be perfectly valid keys—except that they will be the wrong ones unless the correct PIN was used. The attacker has no way to test the passcode other than submission to the authentication server. Just as multiple wrong dynamic passcodes generated by a card reader will lock a hardware chipcard, multiple wrong ArcotOTP-generated passcodes will lock the user’s account and the attacker will be defeated.

Information At-a-Glance

- Arcot co-invented the 3-D Secure protocol for online payment security with Visa. Three major card brands use the 3-D Secure protocol in their cardholder authentication programs: Verified by Visa, MasterCard SecureCode, and JCB J/Secure
- Arcot is the 3-D Secure market leader with over 13,000 financial institutions using Arcot solutions to protect the identities of millions of consumers worldwide
- Arcot patented technology prevents Man-in-the-Middle, Man-in-the-Browser, brute force and other internet attacks
- Arcot certifications include Federal Information Processing Standard (FIPS) 140-2, Level 1, from the U.S. National Institute of Standards and Technology (NIST). SAFE-Biopharma certified, SAS 70 certified, PCI DSS-Compliant.

WORKFLOW DIAGRAM FOR ARCOTOTP USER EXPERIENCE USING THE EMV CAP/DPA METHODOLOGY

Account Login or Online Purchase



For more information, please visit www.arcot.com, email sales@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.

