



Arcot SignFort™

Business-Enabling Digital Signatures without Additional Hardware or Software

DATA SHEET

Overview

Transition to fast, secure fully electronic business processes by replacing legacy “print and sign” requirements for electronic documents with an easy-to-use digital signature solution.

Delivers audit-quality digital signatures that will verify that the signature was valid at the time of signing.

THE DIGITAL SIGNING CHALLENGE

You want to enable fully electronic business processes and eliminate the “printing and signing” of your electronic documents to minimize approval time and reduce costs. You don’t want to install additional software or expensive hardware on your employees, partners, and customers’ desktops. You also want an audit-quality digital signature that will verify that the signature was valid at the time of signing. You don’t want a digital signature that you can’t verify in six months, making the signed document unenforceable. The challenge you face is how to provision your users quickly and inexpensively with the ability to create enforceable, business-enabling digital signatures.

THE SIGNFORT SOLUTION

Arcot SignFort gives you a fast, scalable, and cost-efficient way to enable digital signing. SignFort allows organizations to replace traditional ‘print and sign’ methods with a more secure, streamlined process for signing and approving documents. Arcot’s software-only approach eliminates the need for expensive hardware. SignFort verifies and protects your users’ identities with Arcot’s proven multi-factor authentication embedded in Adobe® Acrobat® and Reader®. It also delivers audit-quality signatures that will verify that a signature was valid at the time of signing, months or years after the signing event.

Arcot and Adobe: Practical Digital Signing

Adobe embedded Arcot signing and multi-factor authentication technology in Adobe® Acrobat® and Adobe Reader® to provide a seamless and secure digital signing experience for users, no matter where they are or what computer they are using. There is no additional hardware or software to install on your users’ desktops to enable digital signing of PDFs.

Roaming and Portability of Digital IDs

SignFort creates and stores digital IDs that always remain on a centralized server. This enables your employees, customers, or partners to use secure digital signatures from any network-connected PC.

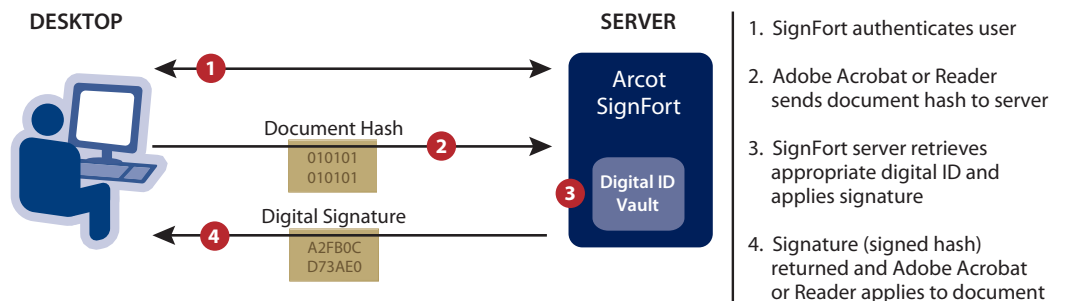
“Green” Business Processes

Becoming more environmentally friendly is a priority for many organizations, and moving to fully electronic business processes will reduce the impact your operations have on the environment. SignFort gives you the ability to measurably reduce your organization’s environmental footprint by reducing the amount of paper it consumes.

Reduce Cycle Time, Improve Customer Satisfaction

Arcot digital signing reduces your processing time, lowers your operational costs, and delays from waiting for signatures. Your customers benefit from faster turn-around time and fewer frustrations from having to manually process forms.

HOW ARCOT SIGNFORT WORKS: EASY DIGITAL SIGNATURE PROCESS INSIDE OR OUTSIDE THE FIREWALL



Desktop Platforms

Client OS Platforms

- Microsoft Windows
- Sun Solaris
- Mac OS
- Linux

Server Platforms

Server OS Platforms

- Microsoft Windows Server

Application Servers

- Tomcat

Security Modules

- nCipher
- SafeNet Luna

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.

SIGNFORT FEATURES AND BENEFITS

FEATURE	BENEFIT
Requires no security hardware or software installation by end users	Easy for organizations to deploy and enable digital signatures
Digital IDs held at secure central server on a hard drive or on a Hardware Security Module (HSM)	Removes burden from end user of protecting digital IDs against theft or unauthorized use. Allows seamless renewal of digital IDs, without any user action required.
Signing Policies	Restricts digital ID use to specific times of day, IP address, device ID, or other criteria to provide additional control or authentication requirements
PDF document and form support	Supports the most commonly signed electronic document format, providing a user-friendly, intuitive signing process. Includes support for secure submission of data in PDF forms by digital signing to defeat Man-in-the-Browser and Man-in-the-Middle attacks.
Vacation Mode	Prevents unauthorized usage during vacation or other specific periods via user-initiated disablement of their digital ID
RFC 3161 Time Stamp Support	Time stamps signatures from a trustworthy time source
Administrator controls signature quality	Ensures that the signature embeds signature validation responses (CRLs and OCSP) and Secure Time Stamps. This enables viewing the document to determine the validity of the signature based solely on information contained in the document--no external server access or existence required.
Log of all signing events	Provides detailed logging of each signature request, including the document hash for each signature, enabling more rapid identification of a security breach

Safe, Secure Signing

SignFort first authenticates users prior to signing by the Arcot WebFort Authentication Server. WebFort uses a configurable sliding scale for determining the appropriate authentication method, based on your organization's policies: a single-factor username/password scheme, or a multi-factor ArcotID.

Tamper-Evident Audit Logs

SignFort logs authentication and signing events for audit and non-repudiation purposes. It also tracks all changes to the document made after its creation.

Enforce Signing Policies

SignFort allows you to restrict digital ID use to specific times of day, IP address, device ID, or other criteria to provide additional control. SignFort logs authentication, management, and signing events for audit and non-repudiation purposes. It tracks all changes to the document, giving you an audit trail of any edits.

SignFort Applications

- **Financial institutions** can use Arcot SignFort to electronically manage all of the document approvals necessary for complex financial transactions. Digital signing will lower costs and accelerate the approval process.
- **Enterprises** can use Arcot SignFort to approve electronic documents with digital signatures to improve the speed of purchasing processes. The enterprise and its largest suppliers can handle requisition issuance, bid submission, purchase order approval, and orders against open POs, all electronically.
- **Hospitals and medical centers** can deploy Arcot SignFort so physicians can digitally sign when updating patient medical information and care instructions. Since SignFort's central digital ID repository eliminates the need for desktop security hardware such as smart cards or a USB tokens, physicians no longer need to worry about their digital IDs being lost or stolen. Additionally, the hospital can quickly enable a digital ID for a visiting physician, or disable it if a physician goes on vacation.

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.