



Arcot RegFort

Digital ID LifeCycle Management

DATA SHEET

Product Overview

Enable an organization to easily manage digital IDs at any stage in their lifecycle from initial provisioning to revocation. Supports issuance from multiple Certificate Authority vendors to hardware smart cards, USB tokens, and software smart cards (ArcotIDs).

Value to Customers

User friendly, easily customizable, and vendor neutral solution allows organizations to easily deploy digital IDs from the Certificate Authorities to various security form factors to meet business requirements.

Applicable for pharmaceutical companies, healthcare entities, financial institutions, government agencies, enterprises, and other organizations that are transitioning to electronic processes that require strong two-factor authentication or digital signatures for approvals.

ENABLE STRONG AUTHENTICATION, DIGITAL SIGNING, AND ENCRYPTION CAPABILITIES:

Organizations worldwide have recognized the benefits of transitioning to electronic processes and documents to reduce costs, improve security, and reduce cycle times. With the growing legal, regulatory, and procedural acceptance of digital signatures, organizations are also increasingly replacing “print and sign” and other paper-based processes with electronic processes using digital signature for approvals. In addition, many organizations have established web portals to streamline their operations and customer interfaces, enabling, for example, e-commerce, banking, and insurance transactions, supply chain management and government procedures.

As more processes are conducted electronically, organizations need additional security to protect these processes, in particular to ensure that the user’s identification is adequately authenticated prior to initiating an electronic transaction. A fundamental enabler of strong authentication and digital signatures is the issuance of digital IDs, also known as certificates or private keys. Different users of an organization’s electronic processes – employees, partners, customers, and other constituents – may need digital IDs issued through different business processes.

Organizations wishing to provide their users with digital IDs are challenged to cost effectively and securely issue, deploy and cancel these digital IDs, particularly if potential users are geographically disbursed, or if users include partners or customers outside their IT infrastructures. From a user perspective, the process of requesting, gaining approval, and receiving a digital ID from the organization can have its own set of challenges.

Arcot RegFort: Versatile Digital ID Management System

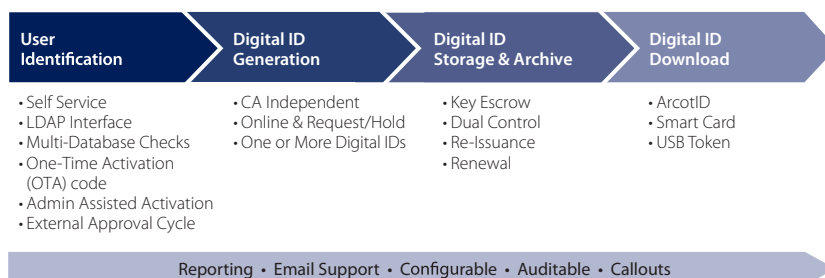
The Arcot® RegFort™ Digital ID Management System addresses these challenges by simplifying the processes and reducing the costs of digital ID issuance and management. RegFort offers an integrated web-based credential management system that supports a range of registration options, credential types, and interfaces with the different certificate authorities. Arcot’s RegFort is highly customizable, to meet the diverse organizational requirements for digital ID management. RegFort also enables a high degree of organizational control over the company’s digital ID management processes, to increase overall security. In addition, RegFort supports a variety of methods for issuing digital IDs – face-to-face, self-service, or with assistance from an administrator – which enables

the organization to match its geographic, security-level or department-specific digital ID requirements.

RegFort is highly versatile, it supports loading of digital IDs into the organization’s preferred hardware form factor, such as smart cards or USB security tokens. It will also load digital IDs into ArcotIDs, Arcot’s patented software technology that offers near hardware-strength security but without the loss, theft, or maintenance issues associated with hardware solutions (please refer to the ArcotID datasheet for details at www.arcot.com).

RegFort and the ArcotID also support user requirements for roaming – digital IDs can be securely downloadable to PCs enabling secure anytime, anywhere strong authentication or approval of electronic documents.

ARCOT REGFORT CREDENTIAL ISSUANCE PROCESS



Desktop Platforms

Browsers

- Mozilla
- Firefox
- Netscape Navigator
- Apple Safari

Client Platforms

- Microsoft Windows (2000, 2003, XP)
- Mac OS X

Server Platforms

Server OS Platforms

- Microsoft Windows Server 2003
- Sun Solaris

Application Servers

- IBM WebSphere
- BEA WebLogic
- Tomcat

User Identification Data Sources

- LDAP Directories
- SQL databases

Identity Provisioning

- Sun Java Systems Identity Manager

Certificate Authorities

- OpenSSL
- VeriSign OnSite
- MS Certificate Server
- Entrust/PKI
- RSA Keon CA
- CyberTrust Unicert

About Arcot Systems

Arcot makes Web transactions safe for millions of users worldwide by verifying and protecting users' identities. Its software-only solutions eliminate the need for expensive hardware or changes to user behavior. Arcot delivers risk authentication, strong authentication, digital signing, and cardholder authentication solutions. Arcot provides the right balance of cost, convenience and strength.

REGFORT FEATURES AND BENEFITS

FEATURE	BENEFIT
Complete digital ID lifecycle management	Single, customizable solution for management of digital IDs from provisioning, renewal, and retirement
Web-based system integrates various registration options and credential types	Single point solution handles multiple steps in the digital ID request, approval, provisioning, issuance, and revocation processes
Java-applet based desktop client	Easy to provision digital IDs to employees, partners and customers – no desktop software to install
Configurable policy rules for groups, roles, issuance model, and web page	Fine-grain control over digital ID management process to cover multiple models (e.g. high security, internal users, external users)
Multiple issuance processes: self-registration, face-to-face registration, proxy registration, pre-registration	Organization can customize issuance processes to meet its specific security, geographic or department needs
Supports storage of digital IDs in hardware smart cards, USB tokens, and ArcotID software smart cards	Accommodates the security solution(s) of the organization
Dual control function for administrative privileges	Two administrators must agree before executing critical actions, increasing security
Key escrow for encryption digital IDs	Multiple admins working together can retrieve encryption IDs if they are lost, or destroyed by terminated employees, to prevent data loss
Audit logs for all operations available through XML templates	Complete audit information can be quickly customized to any desired data set and layout

RegFort Issuance Models

Arcot's RegFort supports a number of models for issuing digital IDs to an organization. This flexibility enables organizations to map their digital ID issuance processes to their particular resource, geography, and security considerations:

- **Self registration:** Users can identify themselves, be registered, and have their digital IDs issued and remotely loaded, without the involvement of a system administrator
- **Face-to-face registration:** Users can be issued digital IDs in person, with the verification and registration of the user by the organization's registrar
- **Proxy-registration:** The registrar can complete the registration process and issue the digital ID on the user's behalf, then ensure the digital ID is sent securely to the end user

Groups of users can be pre-registered by the organization. The individual user then can remotely load the digital ID using a one-time activation code

RegFort in Action

- **A large pharmaceutical company** needed a self-service model to issue their employees digital IDs. The Arcot RegFort solution enabled the company to easily issue digital IDs, cutting months of their estimated deployment schedule.
- **A service provider** needed digital IDs issued from multiple certificate authority (CA) products. Arcot RegFort enabled them to centrally manage all the IDs across CAs from a consistent end user and administrator interface which required less training, enabled faster deployment cycle, and less complex lifecycle management.

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 9886 238 131



www.arcot.com

Copyright © 2008 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.