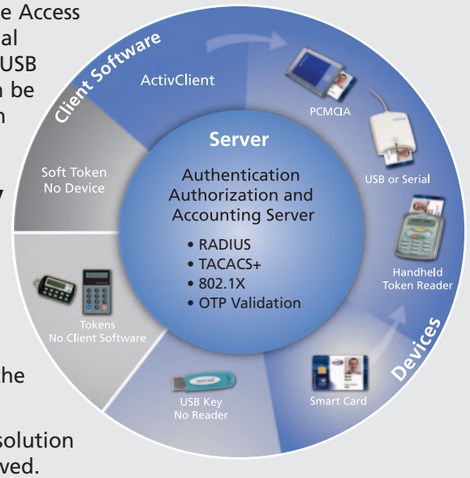
# Secure Remote Access At-A-Glance

The ActivIdentity Secure Remote Access Solution consists of four optional packages: Tokens, Soft Tokens, USB Keys, or Smart Cards, which can be deployed concurrently to match your company' specific requirements. All solutions are anchored with an **ActivIdentity AAA Server** that validates one time passwords and a device that generates them. More functional USB Key and Smart Card packages require **ActivClient™** software on the desktop to communicate with the smart card.




**Tokens** are a simple-to-deploy solution since no client software is involved. ActivIdentity AAA Server software and ActivIdentity Tokens are all you need for the most basic solution.

**Soft Tokens** are often a good, inexpensive solution for partners or customers to access your extranet.

**USB Keys** are a cost effective way of getting the benefits of a multi-function smart card without the cost of deploying smart card readers. ActivIdentity AAA Server software, ActivClient, and an ActivIdentity USB Key is what is takes for this economical smart card solution.

**Smart Cards** allow you to combine multiple forms of identity into a single Enterprise Access Card. Deploying remote access smart cards requires ActivIdentity AAA Server Software, ActivClient, your choice of serial, USB, or PCMCIA smart card reader, and a smart card.

## Other ActivIdentity Trusted Digital Identity Solutions

### Enterprise Access Card Solutions

ActivIdentity Enterprise Access Card allows organizations to dramatically improve IT security while reducing costs and increasing employee productivity. An Enterprise Access Card consolidates multiple identity credentials onto a single, secure smart card. The card can serve as a physical access badge and photo ID and enables secure network login, PC locking, secure VPN, secure-mail with digital signatures, and a variety of other desktop and network security applications. The solution leverages existing IT infrastructures via integration with enterprise directories, physical access systems and PKI services to streamline the issuance and administration of digital IDs.

### Single Sign-On Solution

AcivIdentity SecureLogin Single Sign-On (SSO) solves the challenge of too many passwords in the enterprise. With automated login and password management, users experience less frustration from using passwords eliminating a major source of help desk calls. In addition, ActivIdentity SSO protects the enterprise with support for a variety of multi-factor authentication options, providing both a stronger degree of security and end-user convenience.

## About ActivIdentity

ActivIdentity is a global provider of strong authentication and trusted digital identity solutions for secure remote access, single sign-on and enterprise access cards. Our scalable systems and strong authentication solutions are trusted by enterprise and government organizations around the world.

Actividentity™

www.actividentity.com

**ActivIdentity Americas**
Tel: +1 (510) 574.0100
Fax: +1 (510) 574.0101
info@actividentity.com

**ActivIdentity U.S. Federal**
Tel: +1 (571) 522.1000
Fax: +1 (703) 988.9636
info@actividentity.com

**ActivIdentity Europe**
Tel: +33 (0) 1.42.04.84.00
Fax: +33 (0) 1.42.04.84.84
info@actividentity.com

**ActivIdentity Asia Pacific**
Tel: +61 (0) 2.6208.4888
Fax: +61 (0) 2.6281.7460
info@actividentity.com

Copyright © 2005 ActivCard, Inc. All rights reserved.
SRA.SB.A4.10/05.3K.FR

ActivCard® is a registered trademarks of ActivCard Corp. ActivIdentity™, Mini™ and ActivClient™ are trademarks of ActivCard Corp. All other trademarks, tradenames, service marks, service names, and images mentioned and/or used herein belong to their respective owners.

### Remote Access Challenges

To reap the many benefits of moving your business processes online, you need a way to balance ubiquitous network access with the security required to create a trusted online environment.

Creating a high level of trust hinges on authenticating identity with methods that go beyond static passwords. However, reliance on reusable passwords to authenticate users remains the weakest link and underscores the need for two-factor authentication in securing a digital corporate environment.

Further, the multiple systems and networks remote users have to traverse in order to access enterprise applications and services is onerous, pointing to the value of consolidating remote access identity credentials on one simple secure platform with distributed authentication and central administration.

That's why a Secure Remote Access solution is the crucial first step for companies that are serious about securing the foundation of their network and Internet-based services and applications

# Secure Remote Access Solution

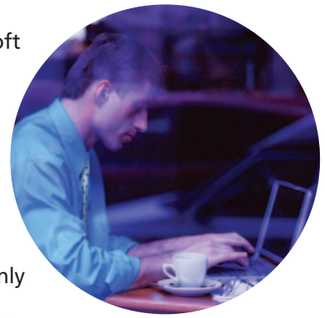
The ActivIdentity™ Secure Remote Access Solution provides everything you need to identify users with certainty and confirm network privileges, enabling you to:

- Increase productivity by allowing your remote employees to access information from anywhere, anytime
- Save time and money by deploying cost-effective devices with no expiration and streamlining administrative processes
- Improve efficiency by allowing partners, customers, and suppliers to securely access the critical information that they need to do business
- Increase security and address compliance issues by deploying strong authentication for remote and wireless access to critical corporate resources

## Streamlined Secure Access to Privileged Information, Services and Applications

The ActivIdentity Secure Remote Access Solution enhances mobility for secure remote access users while broadening the choice of authentication form-factors for secure dial-up, VPN, web access, terminal services, and wireless LAN access.

Based on industry standard RADIUS, TACACS+ and 802.1x authentication plus the ActivIdentity two-factor authentication technology, this comprehensive solution uses tokens, soft tokens, USB keys, and smart card devices to protect your network perimeter. User identities can be positively confirmed via the use of PIN-protected authentication devices that generate one-time passwords, synchronous, or challenge/response authentication. The ActivIdentity Secure Remote Access Solution is the only two-factor authentication solution on the market that delivers integrated WiFi Protected Access (WPA) security and leverages the existing enterprise LDAP directory structures to manage users and their rights.
In addition, the ActivIdentity solution lowers your total cost of ownership and provides a significantly higher ROI than competitive offerings.



Actividentity™

# ActivIdentity provides strong authentication, authorization and accounting services to secure:

Ensuring secure remote access to enterprise information is essential as companies continue to move their business processes online and extend the enterprise boundary beyond the corporate firewalls. Unfortunately, many organizations today still rely on static, reusable passwords, thereby exposing enterprise information through remote access by unauthorized users.

### Dial-Up

Most organizations still provide dial-up access to their traveling employees, as broadband connections are expensive and not yet ubiquitous. ActivIdentity provides an easy to use interface by integrating with Microsoft® Dialer.

### VPN

VPN's are quickly becoming the most popular form of remote access service for employees in the field or from home. ActivIdentity has a seamless integration with Check Point™ and supports all market leading VPN vendors including emerging SSL VPNs.

### Web Access

Many organizations are improving efficiencies by moving applications to the web. Providing not only employees, but partners, customers and vendors access to privileged information on-line. ActivIdentity provides strong one-time password authentication for any website running on IIS, Sun™ ONE, or Apache™ web servers as well as Microsoft's Outlook® Web Access.

### Wireless LAN

The fastest growing remote network access service is 802.11-based wireless LAN access. The deficiencies of 802.11-based security have been well documented. ActivIdentity helps secure wireless LAN access by offering integrated 802.1x authentication meeting the Wireless Protected Access (WPA) standard - supporting Microsoft and Cisco® clients.

### Secure Virtual Desktop

Take advantage of the growing server-based computing trend and secure login to Citrix® MetaFrame® (ICA® or Secure Access Manager) or Microsoft Terminal Services (RDP) with two-factor authentication.

## Why Two-Factor Authentication?

In our everyday lives, one-factor authentication is typically enough: a driver's license to write a check or a fingerprint to notarize a document. However, in the online world, relying on a single factor – such as static passwords – as a way to protect critical corporate systems, services and applications is fraught with risk. At a minimum, private access to privileged information should be protected with two factors of authentication: something you know such as a password or PIN, as well as something you have like a smart card or token. An example is a bank ATM card. It protects your account by requiring the physical ATM card (something you have) and your PIN (something you know). So just as financial institutions are concerned about private access to privileged information, the same safeguards need to be taken for secure remote access to your enterprise network.

# The ActivIdentity Advantage

### Compelling ROI

For companies currently using two-factor authentication, the ActivIdentity Secure Remote Access Solution can be deployed without increasing your existing security budget. The result is a compelling total cost of ownership and return-on-investment advantage that is achieved by:

- **Lifetime replacement of tokens** – ActivIdentity tokens do not expire and come with a lifetime replacement policy - avoiding the cost of replacing token hardware and extending the time between re-deployment of new tokens.
- **Eliminating dual administration** – The ActivIdentity Secure Remote Access Solution leverages your existing corporate directory and does not require its own user database – saving time for a system administrator.
- **Substantially reducing help desk costs** Deploying an ActivIdentity smart card or USB key solution enables you to eliminate all re-synchronization calls by leveraging a challenge/response mechanism that enables the key or card to handle the complexity. In addition, you can reduce password reset calls by securely storing static passwords on your smart card, so users will only have to remember their self-managed PINs.
- **Consolidating credentials** – ActivIdentity smart card solutions enable the secure storage and management of all your static passwords, One-Time Password credentials as well as PKI private keys and associated certificates. The ActivIdentity device becomes equivalent to a key ring for all your corporate digital identity credentials – with the benefit of convenience for the user and cost-effective management consolidation for the organization.

### Familiar and Easy to Use

By consolidating multiple authentication credentials on a single smart card device, the ActivIdentity Secure Remote Access Solution enables a user experience that is as simple and familiar as using an ATM card. This ATM-like experience applies to VPN access as well. Users simply enter their PIN onto the keyboard of their terminal to access the credentials on their card. The ActivIdentity software then authenticates the user, configures the VPN session and makes a connection – all transparent to the user saving time and reducing complexity.

### Enhanced Security

WLAN attackers can access your network from the parking lot, making WLAN simply another form of remote access to the network. ActivIdentity AAA Server has integrated 802.1x authentication required by the WiFi Alliance as well as the upcoming 802.11i standard.

For security minded customers who want to guarantee personal control of their secret keys, the ActivIdentity Secure Remote Access Solution allows local initialization of devices and PIN management by the user. All private keys are generated and stored on the smart card providing strong storage and protection from hackers.

In addition, the ActivIdentity solution does not require a separate user store. ActivIdentity integrates with your corporate directory. This prevents an increasingly common security risk that occurs when employees are removed from the corporate directory, and mistakenly leave their record open in a separate remote access database.

### Smooth Bridge and Migration

The ActivIdentity Secure Remote Access Solution allows you to migrate smoothly from legacy single factor token devices to more advanced smart card and PKI-based technologies without having to replace your existing infrastructure.

If you are frustrated with your existing token solution that requires re-purchase of tokens every three years, the ActivIdentity SRA solution can smoothly migrate you from these high cost deployments to a lower total cost of ownership solution without disrupting your user population.

### Easy Implementation and Administration

The ActivIdentity Secure Remote Access Solution is designed from the ground up to be standards-based and to work with your existing network infrastructure:

- **Management with your existing infrastructure** – LDAP and SQL support. ActivIdentity AAA Server supports LDAP directories and SQL compatible databases. Thus, enabling users and their access rights to be managed centrally without the need to modify the existing corporate directory infrastructure. It natively supports both RADIUS and TACACS+ and does not require deployment of proprietary agents.
- **Centralized administration and distributed authentication** – ActivPack allows for central administration of users, roles, and policies while authentication occurs in the field, where you need it. The solution eliminates the need to deploy one-off, disparate authentication solutions for the various entry points into your network.
- **Deployability** – The ActivIdentity client software, is fully MSI compatible, supports custom setups, blind installs, and works with most market leading software push technologies. The ActivIdentity client gives the IT Administrator the ability to "push" the software to the user's desktop without interruption. It can be installed via a blind set-up – custom set-ups can be built to remove any undesired options for the user. In addition, ActivIdentity provides an auto-update solution so that patches, drivers, etc. can be loaded on a server. The product automatically requests these updates with minimal user intervention, just as you are used to with Microsoft AutoUpdate or Adobe® Acrobat® Reader.