

# Establishing Trust in Remote Access Transactions

## The Security Landscape

### Executive Summary

As of October, 2010, modern networks are getting more mobile, and attacks are increasing. Stolen credentials are the most common method of breaking into networks. Strong authentication reduces risk, and is getting easier to afford and own. Open standards for hard and soft OTP tokens meet a broad range of business needs. While some legacy tokens automatically expire after 3 years, ActivIdentity tokens last 2 to 3 times as long, dramatically reducing administrative and replacement costs. Innovative strong authentication products from ActivIdentity make migrating from legacy tokens easier, more flexible, and more secure. As laptop and smartphone populations continue to grow, IT executives should consider how best to meet their TCO and business flexibility needs by considering ActivIdentity's remote access solutions.



## Table of Contents

Executive Summary . . . . .	1
Ask first who's accessing your network? . . . . .	3
The Security Landscape . . . . .	3
Migration from a Legacy System . . . . .	4
What Product is Most Usable? . . . . .	5
What Standards Need to be Followed? . . . . .	5
How Easy is the Solution to Administrate? . . . . .	5
What's My Total Cost of Ownership? . . . . .	6
Compare these Cost Advantages . . . . .	6
What Does the Migration Path Looks Like? . . . . .	7
Conclusion: Why ActivIdentity? . . . . .	7

---

The 2010 Verizon Data Breach Investigations Report cited stolen credentials as the most common way of gaining unauthorized access into organizations in 2009.

## Ask first who's accessing your network?

Who is accessing your network? This is one of the fundamental questions in information security. From providing access to information to conducting critical business transactions, you must be sure about who you are dealing with.

- Are you sharing your confidential corporate information with an employee, vendor, contractor, customer – or worst case, a competitor or criminal?
- Is the individual changing the system parameters on your firewalls really the authorized administrator?
- Similarly, your employees, partners and customers wonder if they are the only ones who can access the resources they keep on your network.

You need to be confident in your answers to each of these questions, and as the world is becoming aware, static passwords are no longer sufficient.

## The Security Landscape

Security threats didn't go away with the recession. In fact, network intrusion attacks are increasing. Information Week cites a June 2010 survey where 80% of IT managers expect network-borne threats to increase throughout 2010 and 2011. An April 2010 Price Waterhouse Coopers' Information Security Breaches Survey, found attacks on large corporations have more than doubled since 2008, and the damage costs more than tripled. The 2010 Verizon Data Breach Investigations Report cited stolen credentials as the most common way of gaining unauthorized access into organizations in 2009. Simply put, there are more and more "bad guys" out there hoping to make a profit by attacking your organization. The "bad guys" job is getting easier because the workplace has had no choice but to become even more virtual.

Most organizations are dramatically increasing network exposure points. There is more off shoring with partners, contractors, and suppliers from all over the globe who need access to your network in order to support your operations. Your employee base is likely increasingly mobile as well. According to Frost & Sullivan, 2008 was the first year ever that laptop sales exceeded desktop sales to corporations. This trend is accelerating. Forrester Research predicts that by 2015 desktops will account for only 18% of the market. Add in the explosion of smart phones used for business-critical activity, and many organizations have, on average, more than one mobile device per employee, all requiring 24x7 access to the network. Security risks are quickly multiplying across the enterprise.

These security risks may also keep you up at night because regulations and data protection requirements didn't go away with the recession, either. It is clear that any organization which handles customer payment card information, medical records, or social security numbers has explicit and increasingly stringent data security regulations and requirements to follow. However, there is a growing consensus that all public companies have a fiduciary responsibility to their shareholders to diligently employ robust authentication practices to avoid "Wall Street Journal" level exposure.

You need a solution that can:

- Improve security while providing options to make security more usable
- Keep administration tasks simple and efficient
- Provide the industry's lowest total cost of ownership
- Simplify migration from a legacy remote access authentication system

At the most basic level, you need to secure a more mobile workforce with a stronger level of security. At the same time, you need to manage your costs more effectively, and ensure your security solution is usable. As your needs change, solutions should adapt and grow to meet those needs. If you are trying to do more with less, you are facing new hard choices about what you can really afford in today's economic climate.

## Migration from a Legacy System

Some of you may already have a strong authentication solution in place. Ask yourself the question, "Have my needs changed since I first purchased this solution? Am I getting all the value I'm looking for? Am I paying too much?"

If your current token solution forces you to replace all of your tokens every three years, replacing your legacy tokens with standards-based second-generation tokens will save you money immediately. These savings alone may be enough to offset the costs of swapping out the legacy token infrastructure for a second-generation standards-based system. AAA Server makes migration easy in two key ways.

First, the ActivIdentity AAA Server can operate in parallel to your legacy token infrastructure allowing a graceful phased migration thereby reducing operational risk and cost. AAA Server does this by operating as a transparent RADIUS proxy and passing legacy tokens to the legacy infrastructure as needed. Any ratio of legacy and second-generation tokens can be used indefinitely in this way. For example, if your legacy tokens do not all expire at the same time, you can still start reaping savings immediately, while continuing to fully amortize the remainder of your legacy tokens. Since AAA Server pricing is based on number of users, rather than servers, you will only pay for what you actually use.

Second, AAA Server makes migration easy by largely leveraging your existing network infrastructure. AAA Server leverages Active Directory, LDAP, RADIUS, TACACS PKCS as well as wireless authentication protocols like EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to provide the easiest migration to a solution with all the scalability, high availability, and manageability of your existing network infrastructure. No LDAP schema extensions are required, greatly simplifying integration. This accelerates deployment and reduces hardware and platform software costs of the second-generation system as well. These capabilities bring a host of new operational and security benefits as well.

---

ActivIdentity offers the widest range of token designs in the industry, and because we are OATH compatible, customers can choose from any other design provided by other OATH compatible vendors.

## What Product is Most Usable?

Over time, it has become clear that usability must be considered as “table stakes” for any security solution. If a solution isn’t easy, users will work against it or even outright reject it. This lesson has come at the high price of lost confidence, lost data, and lost productivity. Yet, simple and usable are not always congruent with every strong user authentication solution in the market. Some solutions are just too cumbersome for some use cases and users. An important driver of usability is choice. Giving customers choices in how they interact electronically allows them to determine what method best fits their needs. Moreover, choice drives acceptance.

ActivIdentity offers a multitude of user choice options. From standalone tokens, smart cards, and USB dongles to software tokens that run on your users’ favorite smart phones or devices, we offer the industry’s widest range of options. These choices include SMS One Time Passwords (OTP) delivery to your end user’s cell phone, providing an easy-to-manage solution that secures your network while leaving nothing to lose or forget. ActivIdentity offers the widest range of token designs in the industry, and because we are OATH compatible, customers can choose from any other design provided by other OATH compatible vendors.

## What Standards Need to be Followed?

ActivIdentity can ensure freedom of choice without sacrificing security. In the token environment, there are several choices of algorithms and implementations. Proprietary vendor solutions have value and security, but may present interoperability challenges, which make implementation more difficult and limit how your users interact with authentication. ActivIdentity maintains the broadest range of algorithm choices and is a strong supporter of the OATH industry standard.

OATH is an algorithm base that was formed as an industry wide standard by a consortium of companies cooperating under the Initiative for Open Authentication. The value of this standard is that it allows for choice. Additional values are clear in the large number of users the algorithm enjoys, allowing for strong testing and support, not to mention the options of federated security that has increasingly become valuable as organizations begin to interact in a more seamless manner. ActivIdentity supports the OATH standard because it believes customers have a right to open, non-proprietary solutions.

## How Easy is the Solution to Administrate?

As the pace of strong authentication needs has increased, some solutions have pieced together acquired capabilities and are hindered by poorly integrated administration consoles. Our solution was built with customer usability in mind and our integration proves this out. ActivIdentity’s solution is one of the fastest and easiest to install. In minutes, your software is installed and you can begin your testing and pre-deployment processes. We’ve focused on our administration platform to make it user friendly, integrated, and simple to understand. Not only does this help you, but it also helps reduce our support costs. As a result, our costs and support needs are lower and we are able to pass on our cost savings to you in quality and

---

Some legacy vendors force their tokens to expire after only three years.

cost. Additionally we latch into existing LDAP and RADIUS infrastructure, allowing us to scale as much as your environment does.

Administration and management of many security systems is where the hidden costs are found. This can be particularly true for remote access because of the complexity of deploying and managing tokens to many users. The elements of those costs are in system complexity, deployment logistics, and renewal and recertification processes.

The most compelling factor that addresses both ease of administration and total cost of ownership is our paradigm shifting approach to the token lifecycle and renewal. Some legacy vendors force their tokens to expire after only three years, suggesting this ensures reliability and an orderly token replacement process. We believe this is a false dichotomy. It is much like programming a luxury car to stop working at exactly three years old, but with the promise that the car will never break down "unexpectedly." Modern token electronics and batteries are robust and typically last 2 to 3 times longer than that.

## What's My Total Cost of Ownership?

It's quite simple. You purchase tokens once, and we guarantee them for life. We don't make you take them out of circulation prematurely. We can do this because we've built with the customer in mind. We make tokens that last up to 10 years. If you prefer to methodically replace all tokens at a certain age, make it at the time and budget cycle of your choosing. If a token does expire, deploy a new one – while continuing operations using a seamless temporary access capability that ActivIdentity includes as part of the base solution. Your users don't suffer, and neither does your bottom line. With ActivIdentity, we let you buy your tokens, not force you into the appearance of a purchase only to find out you really only has a three-year lease.

Many customers are taking advantage of the fact that ActivIdentity also bundles the SMS OTP delivery capability with our servers, and use the SMS option exclusively for certain end user segments. So, the moment you implement an ActivIdentity token, your total cost of ownership has already started to decline.

When implementing, renewing, or just revisiting your remote access solution, it's easy to fall into the trap of a "quick renewal" cycle. Don't make the mistake of just renewing old hardware tokens and placing a new order for more without considering the security ramifications or cost justifications of such an action.

## Compare these Cost Advantages

- ActivIdentity tokens lasts 2 to 3 times as long as legacy solutions like RSA SecurID, providing 2 to 3 times the value of the more expensive token for less cost.
- Deployment costs are cut in half because you are eliminating at least every other deployment cycle, and these costs alone can equal the cost of the tokens themselves
- ActivIdentity's lifetime maintenance option means you never have to pay for a replacement token ever again.
- ActivIdentity secures emergency access via SMS OTP delivery, which reduces support costs and increases your employees' ability to Return To Operations (RTO).

---

ActivIdentity tokens last 2 to 3 times as long as legacy solutions like RSA SecurID, providing 2 to 3 times the value of the more expensive token for less cost.

- Implement and support a single authentication management solution that can handle all of the various authentication needs of your organization.
- By using tokens, you can eliminate passwords, which reduce support costs and increases security.

## What Does the Migration Path Look Like?

Let's take a quick moment to outline the migration path for your organization. You've recognized that managing your authentication lifecycle is proving more expensive and complex than you bargained for. Your number of laptops and smart phones needing tokens continues to grow. Credential Management has become a yearly nightmare as tokens come up for renewal on a 3-year cycle and the costs of the renewal and logistics are eating your operational budget alive. You decide to make a switch to ActivIdentity. Here an example of what migration might look like in your environment:

1. Implement the ActivIdentity AAA Remote Access Server, but leave your legacy infrastructure in place. The AAA server acts as a RADIUS proxy, allowing your legacy tokens to still be used until they are fully amortized.
2. Provision new end users with the ActivIdentity form factor of your choice. Recognize the convenience, security, and ease of management of the AAA service.
3. As legacy tokens come to term, do not renew and replace. Simply provision ActivIdentity tokens as the replacement for the dying legacy token and enjoy the benefits of having tokens that last twice as long and can be replaced over the course of their lifetime with no additional costs.
4. Repeat steps 3 and 4 until no more legacy tokens exist

Get the picture? Implementing ActivIdentity makes your ongoing operational remote authentication solution cheaper, more secure, and easier to manage.

## Conclusion: Why ActivIdentity?

Per recent research, network attacks are increasing. Most organizations are adding exposure points with growing laptop and smart phone populations seeking remote access. Static passwords are easily stolen. Strong authentication is needed. While the primary objective of remote access control is securing networks, applications, and data, it is clear that manageability, affordability and usability are requisite for success.

ActivIdentity offers a compelling remote access solution. Standards-based tokens provide economic and functional choice, lasting 2 to 3 times longer than legacy tokens and cutting replacement costs in half. Innovative remote access server technology provides user ease, simple administration and easy migration. Crucially, this ease of use increases user adoption which strengthens overall security.

### Footnotes:

<http://www.computerworlduk.com/news/security/20048/pwc-cost-of-security-breaches-triples-in-two-years-for-uk-firms/>

<http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=225701500>

[http://www.verizonbusiness.com/resources/reports/rp\\_2010-data-breach-report\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf) Page 28.

**Americas** +1 510.574.0100  
**US Federal** +1 571.522.1000  
**Europe** +33 (0) 1.42.04.84.00  
**Asia Pacific** +61 (0) 2.6208.4888  
**Email** [info@actividentity.com](mailto:info@actividentity.com)  
**Web** [www.actividentity.com](http://www.actividentity.com)

#### About ActivIdentity

For over twenty years and for thousands of customers, ActivIdentity has provided intelligent identity assurance solutions that offer a versatile approach to securing digital interactions and transactions. Our customers include many of the most security conscious organizations in the world, including Global 1000 companies, government agencies, and banks and growing businesses around the world. We provide usable security for organizations large and small. Now you can have security, convenience and choice all at a lower cost per token over its lifetime.