Realtime publishers

The Essentials Series

Architecting the Right Solution for Strong Authentication

sponsored by

imprivata®

by Jeffery Hicks

Copyright Statement

Article 1: The Perils of Weak Authentication

In today's corporate IT environment, insufficient security (both data and physical), weak authentication, and silos of compliance reporting are hidden currents, much like an undertow at the beach, that can lead to data breaches and compromised systems. Your IT environment remains vulnerable to pervasive threats both internal and external. These limitations drive up the cost of compliance reporting, promote ad hoc solutions to security challenges, can hinder employee productivity, and decrease the company's ability to deliver competitively appropriate levels of customer service.

Fortunately, the right strong authentication solution (or strategy) can address these issues. With a combination of consolidated identity management, single sign-on services, and comprehensive compliance reporting, these systems can reduce compliance costs, improve security, and remove significant drags on productivity. Collectively, I'll refer to this as a strong authentication solution. However, it may be comprised of different elements from a variety of vendors depending on your business and sector requirements. Before you can realize the benefits of strong authentication, you must first understand ways in which weak authentication can hamper business operations and productivity.

What Is Weak Authentication?

To understand the need for strong authentication, it makes sense to understand and define its opposite. *Weak authentication* is generally the system we have had in IT for decades. A user attempts access to a resource and is challenged to identify themselves. As long as the user supplies the expected answer, such as a password, authentication is approved and access granted. I'm sure you can see the inherent weakness.

Imagine a user, Alice, approaching a locked door with a small slot in the center. Alice comes to the door and knocks. A voice from behind the door asks, "Who goes there?" Alice replies, "Alice" and takes a piece of paper from her purse, which she slides through the slot. After a moment, the door opens admitting Alice. Bob, being a curious and particularly nosy fellow, also wants to see what is behind the door. He knocks and announces himself. Bob scribbles something on a piece of paper and slides it through the slot since he observed Alice. The voice behind the door says, "Go away. You are not allowed." Bob repeats the process but announces himself as Alice and slides another piece of paper through the slot. The voice says, "Go away. You are not Alice." Later that day Bob sneaks into Alice's purse and makes a copy of her paper slips, or perhaps looks over her shoulder when she is creating them. Bob returns to the door, announces himself as Alice and slips in his purloined slip of paper. The door opens admitting Bob. Bob has effectively fooled the doorman into thinking he is Alice.

I'm sure you would agree that this authentication system is inherently weak. Bob can say he is anyone and the only proof is a slip of paper that confirms the identity. The problem is that there any number of ways Bob can obtain that very important slip of paper.

How Weak Authentication Affects Your Business

Weak authentication, as I've just illustrated, can have a negative impact on your company or organization. The most devastating impact is loss of data or services. Let's go back to Bob who has gained access to a room he's not supposed to be in. He may stumble around in the room breaking things or interfering with the operations within the room. It doesn't necessarily matter if his intentions are malicious or not, the consequences are the same.

> **Authorization vs. Authentication**
>
> Even though Bob has been authenticated and granted access to the room, he can only do things in the room for which he has proper authorization. Because he has been authenticated as Alice, he can do all the things that Alice can do; if Alice can turn off the lights, so can Bob. The problem with many IT organizations is that they neglect to look at authorization and focus solely on authentication. If Alice has no job requirement to be able to turn off the lights, then she shouldn't be authorized. However, if she is authorized, then protecting authentication becomes even more important.

To make it harder for Bob to pretend to be Alice, the company may ask Alice to use a very complicated password. She complies but because she has trouble remembering it, she keeps a copy taped to her monitor.

Some companies might ask Alice to frequently change her password, which she does by recycling old passwords that may or not have already been discovered by Bob. Or Alice may be in the middle of a major project only to be interrupted with a need to change her password.

Weak Authentication and the Bottom Line

Imposing password management responsibilities on Alice adds to her workload and reduces her productivity. If Alice is forced to come up with her own shortcuts to circumvent these responsibilities, this increases the likelihood of Bob stepping in—and who knows what Bob will do. The company could suffer a loss of data, which has a number of consequences from financial to regulatory and compliance failures to loss of goodwill.

Another problem with authentication is that most modern companies have multiple systems that require some sort of authentication. Here's a small sample. How many apply to your organization:

- Physical access to the building or a room
- Local Area Network (LAN) authentication
- Wireless network authentication
- Remote access and virtual private network (VPN) authentication
- Intranet authentication
- Internet-access authentication and control such as a proxy server
- Database authentication

- Internal application authentication
- Third-party or vendor authentication
- Extranet, vendor, or partner authentication

More than likely, poor Alice has to manage multiple passwords, all of which take time out of her day. Most likely, Alice will use the same password repeatedly, which means if Bob acquires her password for one silo, he has access to all of them.

Managing multiple passwords is not only a burden for the user but also for the IT administrators who must manage these siloed systems. More than likely, each system has its own requirements—not to mention the increasing number of regulatory and compliance requirements that often include some sort of auditing. The IT administrator cannot be efficient and productive when forced to manage these diverse and typically weak authenticated systems.

What Is Strong Authentication?

The answer to many of the issues raised is *strong authentication*. Let's return to Alice, Bob, and the locked room. Alice approaches the door and announces herself. She inserts her slip of paper through the door slot. However, now she also inserts her hand. The doorman on the other side checks the piece of paper *and* measures Alice's hand and compares it with her hand measurement on file. Since the measurements match, Alice is admitted. Bob approaches the door and announces himself as Alice. He inserts his copy of Alice's paper and then puts his hand in the slot. However, since his hand is different than Alice's, Bob is refused admittance. Short of lopping off Alice's hand, there is no way Bob can pretend to be Alice. Weak authentication is often referred to as *something you know* and strong authentication is *something you possess*. Strong authentication is often referred to as *two-factor authentication*. As in this example, Alice must not only present her password but also a second factor, her hand.

Strong Authentication Is Not Perfect Authentication

There is one potential flaw to strong authentication as presented in this scenario. Alice's hand, her strong authentication factor, must be initially measured so that future comparisons can be made. If Bob shows up in Alice's place and has his hand measured, he has effectively become Alice. To prevent this, Alice's company must have secure enrollment procedures that verify Alice's identity. In addition, great care must be taken to protect Alice's hand measurements lest Bob acquire them and construct an artificial hand built to Alice's precise specifications. There are many types of strong authentication systems, many of which might overcome these challenges, but most likely will introduce challenges of their own. Don't be complacent and assume that once you have a strong authentication solution all your problems disappear.

Today, strong authentication mechanisms typically fall into these categories:

- One-time passwords or tokens
- Smartcards
- Proximity detectors
- Biometrics such as fingerprint, voice, or retinal scans

Strong authentication isn't limited to only one item from this list. In fact, the United States government defines strong authentication as a *layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.* The challenge is to find the right balance of security and authentication that meets business, regulatory, compliance, end-user, and systems administrator needs without placing an undue burden on any individual requirement.

Regulatory and Compliance Requirements

In today's IT environment, one area of responsibility that seems to increase on a weekly basis is regulatory and compliance requirements. More and more organizations are facing industry-specific requirements and regulations. From the Sarbanes-Oxley (SOX) Act to the Health Insurance Portability and Accountability Act (HIPAA) and everything in between, companies face greater challenges to maintain data security. The penalties for failure can be devastating. A healthcare organization that exposes confidential patient information can be hit with civil complaints or even lawsuits. Strong authentication decreases the likelihood of these types of problems.

Many compliance requirements include some sort of auditing provision. Can you prove who accessed what, when, where, and why? If you have siloed systems each with a different reporting or auditing mechanism (assuming one exists to begin with), can you easily prepare a comprehensive and complete report?

Although it is not impossible to meet regulatory and compliance requirements with weak authentication, historically, these solutions provide limited auditing information. You might be able to capture who accessed a critical piece of data and when, but that's about it. And of course, we've already seen that you can't even be sure who really accessed the data. Was it really Alice or was it Bob in disguise?

Strong Authentication and the Bottom Line

Without a doubt, a strong authentication solution can have a positive impact on the bottom line. Strong authentication reduces the password management tasks on end users and administrators alike. End users can spend more time working and servicing customers instead of managing authentication to required resources. Whereas weak authentication is often an obstacle to efficient workflow, a well-planned strong authentication solution should be practically invisible to the user.

In addition, the systems administrators face fewer password-related calls to the Help desk. Security is increased, which also means less time spent investigating unauthorized incidents. Ideally, a single strong authentication solution can be implemented across a variety of systems, which reduces the number of management tools and licenses. Consolidation also makes the administrator more efficient by offering a single management interface instead of several. Strong authentication typically meets most compliance requirements and definitely reduces the chance of data or security breaches. This saves the company money in remediation efforts, not to mention possible civil consequences.

In the next article, I'll discuss what to look for in a strong authentication solution and how to select one.

Article 2: Selecting a Strong Authentication Solution

Strong authentication solutions address many complex and difficult situations in today's corporate IT environment. But if these solutions are so terrific, why aren't they more widespread? If you want a solution, where do you begin?

Let me begin by expanding my definition of a strong authentication solution. This is more than simply installing a fingerprint scanner at every desktop, although that may be one part of it. Strong authentication solutions should interface with every system or resource that an employee or user interacts with, and it should do so with a minimal profile. I have a few other details for an ideal solution which I'll cover a little bit later.

Strong Authentication Myths and Misconceptions

If you ask any number of IT managers and systems administrators, you will likely discover a short list of excuses for not implementing a strong authentication solution. Oftentimes these excuses are really misconceptions, so let me clear away the clouds of confusion.

Strong Authentication Is Too Expensive

By far the number one myth and misconception is that strong authentication solutions are too expensive. I suppose if you are looking only at your shopping cart's total price, you might think so. However, you aren't simply buying a loaf of bread; you are making an investment in your IT infrastructure. You have to look at the full picture.

Let's start with security. With weak authentication, the risk of data loss or exposure is quite high. Depending on your industry, the consequences could be severe—from regulatory fines to civil actions to loss of customer goodwill. How much would a single data breach cost your company in hard dollars? I'm not even talking about the internal time and resources you will have to expend to deal with the situation. Oh, and don't forget about lost opportunity. While your company and employees are dealing with a security incident, they can't attend to other work, which means potential lost earnings.

Another hidden cost to weak authentication is the impact on user productivity. End users have to expend time managing passwords, calling the Help desk for password resets, or simply taking an extra few minutes to securely access a network resource. It may not seem like much but these minutes of lost productivity add up.

Let's say you have 100 employees and they spend 10 non-productive minutes a week dealing with the consequences of weak authentication. That's 1000 minutes a week of lost productivity. Multiply that by an average hourly rate of say $20 hour, which comes out to 33 cents a minute, and weak authentication is costing you $330 a week or over $17,000 a year! I haven't even factored in your IT costs to support all of this.

If you still aren't convinced, consider your auditing and reporting requirements to meet compliance or regulatory obligations. How much time are systems administrators or analysts spending collecting and compiling this information? How much time is spent formatting the data into an appropriate format? Are you confident that you haven't missed anything? What are the consequences if you have? The cost of IT goods and services should obviously never be ignored. However, don't neglect the "big picture," especially for an item that has the potential to affect every aspect of your organization's operation.

Strong Authentication Is Too Difficult to Manage

Often, companies believe that strong authentication solutions are too difficult to implement and manage. Although I won't say that there aren't solutions that might be more difficult compared with others, such a blanket generalization is self-defeating. One of your goals when selecting a solution is to identify one with a simple, easy-to-use management interface. You also want a solution that is seamless and unobtrusive. Perhaps in the past, early strong authentication solutions were complex and difficult to use, but they don't have to be.

If anything, a strong authentication solution should simplify the administrator's workload. Instead of a hodgepodge of management tools and procedures, s/he only has to learn how to use a single, comprehensive tool. Granted, some individual components of your strong authentication system may have their own management interface, but you should seek out products that allow you to consolidate and integrate.

Strong Authentication Impedes User Workflows

Another common misconception is that a strong authentication solution impedes user workflow. That is, it is merely an obstacle that prevents a user from getting his or her job done. IT professionals are concerned that end users will be confused by new security requirements and that having to authenticate, perhaps with biometrics, will take too long and disrupt productivity. Or suppose a company has adopted two-factor authentication with smart cards and the user leaves the card at home?

I'm not naïve enough to suggest that strong authentication will never impede a user's daily routine. However, proper user education and well-documented policies and practices should more than mitigate any losses. Don't forget that one of the downsides of weak authentication is the amount of time a user has to spend dealing with passwords and clumsy security implementations. If anything, weaker authentication is more of a hindrance, which the proper strong authentication solution can address.

Strong Authentication Has a Low User Adoption Rate

One final misconception is that users, and to some extent organizations, have been slow to adopt strong authentication solutions. In my opinion, this situation is a self-fulfilling prophecy. Companies are faced with many myths and misunderstandings surrounding strong authentication and consequently are slow to implement a solution, if they ever do. So yes, there may be a slow adoption rate, but that's only because of misinformation that dissuades many people.

The other contributing factor to this misperception is security itself. For many organizations, their security infrastructure remains confidential, and rightfully so, for many reasons. You can never truly know how many strong authentication solutions have been implemented in your area or industry sector, but working with the right vendor can help alleviate this worry.

Solution Requirements

Hopefully, I've convinced you by now regarding the viability and benefits of a strong authentication solution. Of course, like any product, not every solution is equal. The following sections explore key elements I think you should consider as requirements for any strong authentication solution.

Multi-Protocol Support

Consider your environment. How many different authentication systems and protocols are currently deployed? Do you have a physical access control system (PACS)? If you are in the healthcare sector, you might have a vertical application such as Siemens Medical. Do you employ a user provisioning system such as IBM's Tivoli Provisioning Manager? Or perhaps you are in the financial sector and rely heavily on a Fiserv solution? You need an authentication solution that can easily incorporate such an application. These are simply a few major technologies that come to mind; I'm sure you can identify many more in your company.

Your requirement for a strong authentication solution is to integrate all user access activities across multiple and disparate systems from physical access to network security. This has the effect of providing a comprehensive security infrastructure by integrating physical access with IT and data access. *Comprehensive* is definitely the key word here, followed closely by *seamless*. You require a solution that does not force you to cram it into your network with 20-page implementation checklists. You should be able to point the solution in the right direction and it does the rest.

Easy Deployment and Management

Which brings us to the next requirement you should seek: Any strong authentication you consider should be easy to deploy and shouldn't require an army of consultants or vendor technicians. Remember, you are looking for a solution that can fit seamlessly into your existing network and support multiple protocols and platforms.

One sure-fire test is to investigate what it takes to *remove* the solution. If uninstalling requires massive server reconfigurations, driver uninstalls, service account deletions, or system reboots, it more than likely is not a seamless solution and is far from unobtrusive.

Some solutions may require agent installation around your network. I've always felt the use of agents is personal preference. There is not anything inherently wrong in using agents, but they should be extremely easy to deploy and configure, consume a low amount of system resources, and otherwise maintain a low profile.

One of the end results from implementing strong authentication is that you want to make it easier to manage and control who gets access to corporate networks, applications, resources, and data. Very often, this includes password policy management.

Your preferred solution should have an easy-to-use management interface that consolidates all your disparate platforms. I'm personally fond of Web-based dashboards that I can securely access from anywhere. But a reasonable desktop application that doesn't require dedicated resources or hardware is acceptable as well.

Consolidated Reporting and Auditing

One of the primary reporting purposes for a strong authentication solution is to provide insight into all user access activities across the entire enterprise. This includes physical as well as IT services. The key word here is *comprehensive*. You need to be able to reliably report what resources a user accessed, where those resources were accessed, and when they were accessed. Reporting should be easy without requiring extensive work on your part to develop complex database queries or reporting templates.

> **Note**
>
> I hope it goes without saying that all of this data must remain secure and that access to this data is also monitored.

Meets Sector, Regulatory, or Compliance Requirements

Much of what we face in IT today, especially when it comes to regulatory requirements or compliance is *accountability*. Have you taken prudent and reasonable measures to protect data and network resources and can you prove it? I can only assume that you are aware of regulations and requirements that pertain to your sector or industry. You need to seek out a strong authentication solution that meets, or ideally exceeds, those requirements.

For example, in a healthcare setting, it is not uncommon for multiple users to share a common desktop. Often, these computers are in publicly accessible areas. Thus, the first step is to prevent unauthorized access without adding unnecessary steps for doctors, nurses, and technicians who legitimately need access. One solution might be a proximity card reader that authenticates the user who needs only enter a PIN.

However, even within this scenario, there is another layer. We've controlled access to the network but what about data? A lab technician needs access to specific parts of a patient's record. A physician waiting to use the same desktop needs access to the full patient record. Your strong authentication system should seamlessly authenticate the doctor's access to the data with minimal effort on her part. Of course, all of this is logged and easily reported.

Finding a Solution

Once you have identified your requirements for a strong authentication solution, it's time to go shopping. I have some advice that should streamline this process.

Consult with Peers

I can't think of a better recommendation than from a professional colleague whose opinion I trust. The first step I would take would be to contact my peers and discover what solutions they are using or even have considered. Granted, their environments will have different requirements, but you should still be able to narrow your list.

Consult Industry-Trusted Publications and Resources

Does your industry or sector publish trade-related journals or magazines? While there's nothing wrong with considering a vendor based on a trade advertisement, use caution. Typically, you only see the big players who have an advertising budget. There is no guarantee they have the expertise or experience to meet your needs. To compensate for this fact are there sector-related web sites that offer unbiased product information and reviews? This type of information is very valuable because these resources will be evaluating solutions based on your specific sector needs. A financial services organization will have different strong authentication requirements than a manufacturing company.

Find a Vendor with Clients and Case Studies in Your Industry

I think it is vital that you identify a vendor with clients similar to your own company. Or at the very least, they should offer related case studies. You wouldn't use a mechanic that specializes in brake repairs when you need transmission work. You must find a vendor with the experience and expertise to meet your requirements. The solution you are looking for has business-critical and enterprise-wide implications, so you can't afford a vendor who doesn't "get" your industry and requirements.

Evaluate and Test in *Your* Environment

Finally, the most important recommendation I can make is to evaluate and test in *your* environment. You need to understand what impact the solution has on your network, resources, and users. The right solution should be unobtrusive and easy to install as well as remove. Pilot test the solution with a representative cross-section of users and administrators. Provide the proper level of training and then evaluate the impact on their daily routines. Does the solution interfere with or enhance their daily routines? Can administrators easily manage everything? Do the reporting features meet your requirements? How responsive is the vendor when things go wrong?

This is not a process that you can complete in a few days or even a week. If I was the IT manager, I would be planning at least a 30-day trial and evaluation, especially if the company has end-of-month activities. You want to ensure that all business operations are supported. It is also critical to dedicate sufficient resources to properly manage and test everything during the trial period.

If all goes well, that is, users and administrators report a positive experience, you should be able to scale out the implementation and deploy enterprise-wide. In the final article of this series, I'll discuss concepts surrounding deployment and management of your strong authentication solution.

Article 3: Deployment and Management of Strong Authentication Solutions

Congratulations. You've recognized the need and value in a strong authentication solution. Of course, it has no value if it remains in the box. In this article, I'll discuss ways to take advantage of your new solution and pitfalls to avoid. I also believe that you should use this information as part of your planning and selection process. A solution that you can't easily deploy and manage is not a solution worth having.

Control Deployment Risks

I'm sure you are aware of the adage about reading the manual, and this most definitely applies here. This is not the time to "wing it" and think you know what steps to take. Although, hopefully, implementation and deployment steps are simple, you should not ignore the documentation. You can't afford to miss any critical step.

Once you know what steps to take, it is very important, in my opinion, to start small. Don't introduce an enterprise-wide solution to the entire enterprise on Monday morning. You can control deployment risks by starting small. Identify a core group of users and administrators that represent a cross-section of your employees. These individuals should have some technical savvy and be willing to deal with an occasional problem.

When I have been involved in pilot programs in the past, very often, a core group of IT administrators is first targeted. I think of this as the pilot's alpha stage. This provides an opportunity for you to work out enrollment procedures, troubleshooting experience, exposure to the management tools, and a first-hand understanding of what an end user might face.

The next part is the pilot's beta phase. This is the time to introduce end users to the process. You must understand and document their experiences. This provides Help desk knowledge as well as information that can be used to refine or revise policies and procedures. Some organizations may begin this phase with a very small set of users and, should all go well, extend the pilot to a slightly larger group.

When including end users in your pilot, don't forget to involve their management layer so that managers understand what is happening and can accept the potential for a temporary loss of productivity. Obviously, don't include users in mission-critical roles. Your pilot users should receive training in the product and tools they will be using. They should also have a mechanism to provide feedback and report problems.

The final way to control overall deployment risk is to break things. By that, I mean find ways to intentionally introduce problems or errors into the system. If using smart cards, what happens if the card reader is broken or missing? If using one-time use tokens, what happens if clocks are out of sync? What is the effect if a network switch goes belly up? Perform your own version of white-hat hacking. Attempt to circumvent the solutions and tools you are considering deploying. If a single sign-on platform is part of your overall solution, what happens if it is offline? Many administrators neglect to test for failure, which is just as important as testing for success. This sort of failure testing can have a bonus of revealing other deficiencies that need to be addressed.

Administrator Training

Any sort of IT management tool is only as good as the administrators who use it. You cannot neglect administrator training into all aspects of your authentication solution. If you are deploying smart cards, do your administrators know how to enroll a user? Do they know how to troubleshoot authentication and access problems? Do they know how to revoke authorization? When it comes to reporting, do your administrators know how to create the reports you need? If patches or updates are required for your solution, does your staff know how to deploy them with minimal interruption to your network and users?

This type of training does not necessarily have to be formal, classroom-led instruction; although, if your vendor offers it, I suggest you at least seriously consider it for a few key administrators. Very often, these types of security upgrades require a shift in corporate culture and paradigm. You need to make sure your IT staff is onboard from the very beginning, and proper training goes a long way toward that cooperation. Well-trained staff also mitigates deployment risks, as the staff should have the knowledge to handle problems and a thorough understanding of all aspects of your strong authentication solution.

End User Training

Training your IT staff is only one half of the equation for success. If your end user population is not properly trained on all the new technologies and tools that are part of your strong authentication solution, your odds of success are greatly diminished. It is well known that people fear what they don't understand, so you must educate them.

Not only do your end users need to understand the mechanics, they should be educated as to why all this change is occurring. Again, it is human nature to resist change, and the more you can get users to understand the benefits, the better off you will be.

I would venture that this level of understanding is even greater for all levels of management within the organization. If management doesn't recognize the value and benefits, their staff won't either. Any sort of IT-related project benefits when driven from the top down.

End user training can be delivered in a variety of ways from formal classroom training, perhaps vendor-provided, to informal hands-on training sessions led by your IT staff in your own test lab. If you have the expertise in house, there are plenty of tools for creating short video tutorials and training material that can be delivered via an intranet. In fact, ask your vendors if they have any end-user–oriented training material, especially material that can be centrally delivered.

If your authentication solutions will extend to external partners, vendors, and/or users, they too will need proper training not only on mechanics but also on Help desk procedures. Ideally, you should incorporate some of these users in the pilot deployments I mentioned earlier.

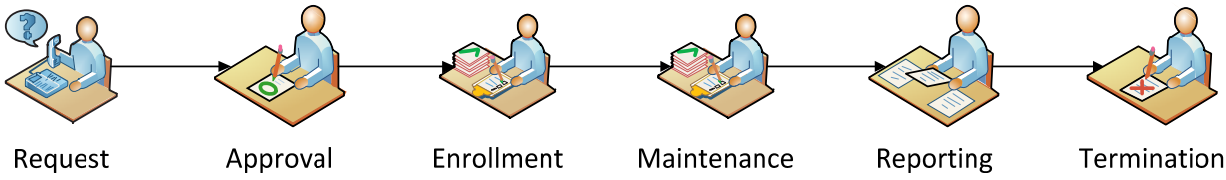
Documentation and Process

I'll admit, I'm like many of you and not a big fan of writing documentation. Unfortunately, a well-documented process is essential for maximizing your investment and achieving maximum efficiency. With a little planning, your documentation efforts can be manageable.

During your development and testing phase, you should have written procedures for setting up your solution, enrolling users, troubleshooting, revoking users, maintenance, and reporting. You need this information so that you know what to test and how to test. There's no reason this information can't rollover into your final documentation. As you are working through the pilot phase, continually update the documentation. If you can use a collaborative tool such as a wiki or even Microsoft SharePoint services, so much the better.

Ideally, your security vendors have their own product documentation that you can integrate into your own. You don't want to have to search half-dozen locations looking for information. This also applies to end-user documentation. You must offer a central location for any information or services a user might require.

In my opinion, well-defined processes and workflow are critical to a successful strong authentication implementation. By this point, you should have identified all the systems you are integrating and how they are used. I recommend defining a life cycle for each element. From a high level, you might have something like this:



Let's assume part of your strong authentication solution uses proximity detectors for physical access. Using the example workflow, you need to define how these events are accomplished:

- A new hire needs access. Who makes the request and how?
- What steps do you take to verify and approve the request? Is there an audit trail?
- Once approved, how is the user enrolled in the system? How is the card delivered to the end user?
- Is there a standard training routine for the new user?
- What is the process for a non-functioning card?
- What is the process for a non-functioning card reader?
- What is the process when the user forgets the card at home?
- What is the process for a lost card?
- What is the process when a user's job status changes and the user requires different access rights?
- What steps do you take to generate access reports? Who can request them? How is the information delivered? How long is it retained?
- What is the process when the user's employment terminates?

This level of detail, if not more, is required for every element of your strong authentication solution. Of course, you need vendor solutions that facilitate all these steps. These are also all the steps you need to define and test anyway before full-scale deployment, at which point your documentation is essentially complete. Although I'm sure you know process documentation is a continual process, which is why a centralized collaborative approach makes the most sense.

Define Reporting Requirements

The final task in your deployment and implementation plan should be to define your reporting requirements. If your organization is covered by regulatory or compliance requirements, you obviously need to meet them. If your strong authentication solution includes report "accelerators" or templates, so much the better. But this is just the beginning.

Because you have implemented an integrated and cohesive strong authentication solution across your environment, there is a wealth of information available. Different parts of your organization will have a vested interest in different parts of your data, so one of the first steps you need to define is the process of requesting information. Who can request reporting data? What data can they access? What form or forms can the data be presented? How long will it be retained? Your strong authentication solution should have a reporting facility that supports delegated permissions. You don't want your systems administrators to be a bottleneck when it comes to reporting. Ideally, you need to be able to assign appropriate reporting permissions to various users and groups as needed so that they can get the reporting they need. Here are some examples:

- The Human Resources department may need physical and file access records to document an employee termination.
- Your server administrators may want to track file access to document obsolete data that can be archived or deleted.
- Your data security team is investigating suspicious file activity and needs to determine who is accessing data, from where, and when.
- Your legal department is responding to a request to verify patient data confidentiality has not been breached.
- Management wants to trim application-licensing costs. They need to see how many people are using an application, when, and for how long.
- A manager with telecommuting employees wants to know when their staff is connecting to the office and for how long.

Once you have an integrated source of authentication and access information, you'll be amazed at how valuable the information is. As part of your search process for strong authentication, hopefully you've identified some critical reporting needs. The more flexible the reporting features, the better.

Conclusion

Putting the pieces together for a strong authentication solution is not something you will achieve in a short period of time. However, the need for strong authentication has never been greater and can actually become a business asset. The more time you take in defining your requirements, working with vendors who understand your needs and can contribute their knowledge, involving end users in your testing, and documenting processes thoroughly, the more successful your deployment and the greater the return on your investment.