



WHITE PAPER

You're either in or you're out: The challenges with Authentication

Understanding today's challenge with authentication

The concept of authentication has been around long before computers. In human history, there often existed the need to verify someone's credentials. The Roman military used what was called a tessera militaris - a codeword written on a small square of wood or bone and passed among soldiers so if they met another soldier and weren't sure if they were a friend or foe, they could ask for the codeword. If they didn't get the correct answer, swords would be drawn.

Now, things are much more complicated and for good reason. Technology has advanced the ability to authenticate someone with multiple options, but has also removed the restriction of geography.

Secondly, today's workforce and customer base are scattered across the globe and have a heightened awareness of privacy. The person being asked to prove who they are can actually be using a device anywhere in the world. Ironically, these factors have anonymized authentication.

The challenge with authentication is that at its core it is designed to provide a positive or negative response. But the world's complexities mean simply authenticating someone with such a black or white response is no longer sufficient. If someone is granted full access and it's a mistake, it can result in a public breach, which can have a financial and brand impact. A more prudent move would be to slow things down and take the time to confirm proper authentication before providing access.

The challenge with authentication is that at its core it is designed to provide a positive or negative response. But the world's complexities mean simply authenticating someone with such a black or white response is no longer sufficient.



However, be it commerce, healthcare, manufacturing, almost any task done on a network today requires speed. Organizations can't afford to slow down because in the best case scenario, delaying access to a customer attempting to authenticate into their system to complete a purchase could result in a loss of sale/revenue.

Yet, if they ignore that risk and focus more on speed and convenience via an overly simplified method of authentication alone, a more deadly scenario is a bad actor successfully authenticated into a network ends up shutting down all systems within, say, a healthcare system, demanding a ransom. That has happened and can have deadly consequences with surgeries canceled and patients turned away.

Authorization is the next step following authentication and its purpose is determining what someone can do once their credentials are verified. Depending on the situation, what one can do with their access may vary wildly from person to person. Just because someone has full read and write access in one situation doesn't mean they should have it in every situation.



Scenario 1

As an example, consider an employee who is authorized to review and process online orders above a certain amount. In one situation, that employee is sitting in their secure office building in a private area.



Scenario 2

In another situation, that employee is on their laptop on a commuter train sitting next to a complete stranger. Should that employee have the same access and visibility in both those situations?

Balancing the need for speed and convenience with the need for security is a struggle in almost every organization, and this is particularly true when it comes to authentication. As the title of this white paper says, with authentication you're either in or you're out.

Therein lies the problem. The "yes or no" question, while still important, doesn't address the real life scenarios enterprise security teams currently face. There needs to be a way to deliver a balance between speed and security.

Enter authorization: Authentication's sibling in the quest for properly governed access management

However, be it commerce, healthcare, manufacturing, almost any task done on a network today requires speed. Organizations can't afford to slow down because in the best case scenario, delaying access to a customer attempting to authenticate into their system to complete a purchase could result in a loss of sale/revenue.

Yet, if they ignore that risk and focus more on speed and convenience via an overly simplified method of authentication alone, a more deadly scenario is a bad actor successfully authenticated into a network ends up shutting down all systems within, say, a healthcare system, demanding a ransom. That has happened and can have deadly consequences with surgeries canceled and patients turned away.

Authorization is the next step following authentication and its purpose is determining what someone can do once their credentials are verified. Depending on the situation, what one can do with their access may vary wildly from person to person. Just because someone has full read and write access in one situation doesn't mean they should have it in every situation. As an example, consider an employee who is authorized to review and process online orders above a certain amount. In one situation, that employee is sitting in their secure office building in a private area.



Scenario 3

In another situation, that employee is on their laptop on a commuter train sitting next to a complete stranger.

Should that employee have the same access and visibility in both of those situations?

Because of the complexities mentioned above, access isn't a simple thing to manage. Who decides when someone should have full access in one scenario and not in another? How do you determine the scenario every time they request access? Does this need to be done manually? How will that affect the speed element? Does this need to be done for everyone who may require access to every application and data access point?

To address the challenges faced with access management, we need to break down the key aspects separately into digestible pieces. Quite simply, access management boils down to these two aspects: security and speed.

Let's look at security first.

How do you secure access in real life situations?

To simplify, let's break the security aspect down into scenarios.

“Yes, BUT” scenarios

The first scenario we will review is the “Yes, but” scenario when a requestor has successfully passed authentication and you want to enable access, but perhaps with a caveat. Honestly, this makes up the majority of the grey areas of today's challenges around access. These are critical to the success of your business as they enable access so the requestor can complete a task, but they do so in a manner that still protects your sensitive data and processes.

Example: Working remotely

This scenario should hit home for almost every organization over the last couple years. You have an important worker who for whatever reason must work away from the office. When the worker conducts business from their office, they are in your building and on your network and you have confidence there are necessary protections in place to ensure the information they access is not exposed to risk.

However, when they are working remotely, you no longer have control over where they are, who can see their screen, whether they are on a public Wi-Fi or even if their home Wi-Fi network has been compromised. At the same time, as we have all seen as a result of the pandemic, this is a new reality organizations are forced to accept, knowing they cannot simply eliminate access if an employee is no longer consistently on-site.



In these cases, the user will successfully authenticate into their network or application, creating a need for authorization as organizations take extra steps to secure their data and processes. When authorization is added into the access management strategy after authentication, specific attributes are evaluated to determine the most appropriate access outcome. For example, one of the attributes that can be examined is whether the user is on the company network or connecting from an external network.

Additional attributes might include geography, time of day, whether or not the information being requested falls under any sort of [compliance](#) regulation (as a result of the request origin), and so on. Multiple levels or attributes can be evaluated but also correlated should one impact the other as mentioned with geography.

Because all of those attributes are considered, a dynamic policy is applied separately to each request to ensure appropriate access. If the user is not on the company network, the policy may be that any data they access is anonymized or masked. To understand how this works, imagine an account manager visiting their client, John Smith.

As they wait in the lobby of Mr. Smith's building, they want to double check to see which version of the product the account uses. If the user is indeed who they say they are, as authentication is confirmed, and they know the customer ID number for the account, simply showing them an account screen with most of the information masked is really no risk to the customer, yet still enables the account representative to do their job. The key here is that security was maintained, while still enabling productivity.

“No, even though” scenarios

There are scenarios when to protect sensitive information, you will want your authorization component to still say “no, even though” the requestor passed authentication. These are important situations because if you solely rely on authentication, as many organizations do today, this shows how vulnerable you are to risks of which you are unaware.

Example: Multi-factor authentication

For sensitive access requests, many organizations now leverage multi-factor authentication to ensure the person requesting access really is who they say they are. The problem is that even in the case of good employees, there is a workaround used when accounts are shared.

A recent survey found 34 percent of respondents said they share passwords or accounts with co-workers. This isn't malicious - the majority do so simply to get work done and 38 percent said it's actually company policy to work this way. So if you have one account with multi-factor authentication turned on but it is used by multiple staff, how is that possible?

It's actually quite easy to work around. The key user/legitimate account owner simply approves the push on their phone or texts the other user with the authentication code they received. In this sadly common scenario, users can be in multiple locations worldwide, but as long as they are connected via a messaging application, it's an easy workaround. If this can be done by well-meaning employees, imagine how this is exploited by someone with malicious intent.

How does authorization address this gap in security?

One potential solution is to leverage the geo location as an attribute for review after authentication. Did the user sign in with their password in one location (i.e. New York) but their device is actually located in a completely different location (i.e. San Francisco)? If so, they are either in possession of some sort of transporter device, or they are not one person, but rather two different people sharing one login.

In that case, authorization can be denied and the user will not gain access. If this was a legitimate attempt, the employees can raise the issue to management and request separate accounts, in a practice that follows proper compliance guidelines and security practices. If it was not a legitimate attempt, then an attempted breach was just thwarted.

For more than twenty years, Axiomatics has worked with some of the world's largest and highly-regulated enterprises to deliver effective authorization as part of a successful access management strategy.



How do we ensure speed and convenience of access in real life situations?

If everything is locked down so securely that it is difficult to conduct business, going out of business becomes a moot point. The challenge is to ensure security while maintaining speed and convenience for employees, customers and partners. The solution lies in the ability to authorize and provide just-in-time access at the point of the request.

Consider that up until that point, no access existed, therefore reducing risk of exposure. When a request for access comes in (i.e. a user logs on to an application to perform tasks for the day), at that point the authorization solution examines various attributes to determine the scenario and then based on the policy, enables some form of access. All of this must happen extremely fast so the user isn't even aware these additional checks are happening.

Often, one of the concerns organizations have about adding an authorization step to the access process is how it will impact speed and user experience.

First, because this type of activity requires that it work at scale for large organizations with thousands of users all making multiple requests, the Axiomatics authorization platform has evolved over the last twenty years and has little effect on latency.

The second thing to consider when looking at speed is how much time an audit finding or even a breach will cost your organization. Adding authorization as an important part of your access management process won't even take as long as this.

An analogy that illustrates this point - people don't decide against wearing a seatbelt when they get in the car because it adds time to their drive. The risks are too high and conversely, the benefits are instrumental to ensure your organization can continue to operate at a speed you are accustomed to.

Already leveraging authentication?

As stated previously, the majority of organizations already leverage some technology to authenticate users into their applications and network. It is an important part of determining appropriate access, but as mentioned above, even with multi-factor authentication, relying on authentication alone opens your organization to risk.

The good news is that adding authorization to your access management strategy does not need to be a complex, time-intensive activity. Even if you start by simply adding an authorization policy to your most sensitive application, you can reap immediate benefits. As you establish access policies, you can continue to add or simply copy and modify them for more applications as your needs evolve.

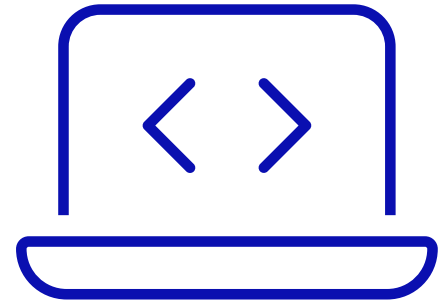
The key is you just need to start with one.



Take the next steps

Learn how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

[Meet with our solution experts for a demo](#) of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:



[Blog articles](#)



[Press releases and announcements](#)



[Resources, solution briefs, and tools](#)



[Join us on LinkedIn](#)



[Subscribe to our LinkedIn Newsletter](#)



[Subscribe to our YouTube channel](#)

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: <https://linkedin.com/company/axiomatics>

Join us on YouTube: <https://youtube.com/@axiomatics>

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240