AUTHENTICATION AND PCI DSS

Next Generation Authentication and MFA

February 2021

PREPARED FOR

Acceptto®

ALPINE
Security Consulting

EXECUTIVE SUMMARY

If you use a password, you should read this paper. If you hate using passwords, you should finish this paper. If you haven't developed a strategy to implement and benefit from passwordless authentication and Intelligent Multi-Factor Authentication (MFA), you are behind the curve and need a solution yesterday. This paper will help ensure you make an educated decision and not simply implement either an old and expensive solution or the cheapest and quickest solution that does not scale. We will use the Payment Card Industry Data Security Standard (PCI DSS) framework to look at one of many ways that good authentication strategies with MFA can be leveraged to meet an existing standard, as well as how it can go beyond such baselines and offer much more.

Quality authentication and MFA solutions are on the rise, but distinguishing the best of the breed and the best fit for your specific business needs can be a difficult challenge to work through. Even the most popular solutions may only offer the minimum functionality, and cost is always a concern for any solution. Understanding the value and impact on various compliance standards from an MFA solution can also be a daunting task for an enterprise. To use PCI DSS as an example, some have said that it is simply a baseline, not true security – and the same thing can be true for MFA solutions.

This paper will provide a good framework with which to review an MFA solution and highlight some of the most important areas so that you can make an informed decision that will help future-proof your MFA investment. We will review some critical aspects of what to look for to help you to understand your own specific needs better.

Finally, we will take these concepts and explore how Acceptto offers more than just a baseline authentication solution. Leveraging a model of continuous authentication and the ability to remove passwords, while still offering MFA, is where both small and enterprise businesses are headed sooner rather than later.

HIGHEST RISKS | PEOPLE OR PASSWORDS

When the average executive is asked about the highest risk in their cybersecurity posture, it's not surprising that many identify "people" or "an employee" fairly quickly. You can invest in all kinds of education programs, expensive security technology and security solutions, and possibly even implement them effectively, into an enterprise program and within a hardened environment. However, getting people and employees to consistently behave in a secure manner is more difficult.

If you then ask the average employee in that company, including their executives, what they struggle with the most, or what they dislike while meeting their responsibilities in the company's cybersecurity practices and policies, invariably the answer is "managing passwords!" If you look at the number of compromised passwords on the internet, the only people left who have not had one or more of their own passwords stolen are those that don't use technology.

You may wonder about the following question: Why are passwords still so commonly used when most cybersecurity experts would agree that they are inherently one of the riskiest parts of any cybersecurity system? There are certainly no easy answers to this question, and removing passwords may seem like an impossible task in itself. After all, passwords have been the authentication technique of choice for over 50 years. Most standards and regulations contain some level of minimum requirements for passwords to meet. As an example, PCI DSS 3.2.1 currently says a password must have a minimum of 7 characters and use an alpha-numeric character. So, "password1" is ok – not exactly an ideal baseline. Most organizations go far beyond this minimum, but what if there was no password at all—would it then fail a PCI DSS assessment? What if there was the possibility to meet PCI DSS's MFA requirements, and do so with no passwords? Imagine the ability to remove one of the weakest cybersecurity links and improve authentication at the same time! Put another way, consider protecting your most critical data and limiting what cyber criminals can do in your environment, in a way that both reduces your cyber risk and meets whatever compliance standards your organization needs to meet. This is what passwordless MFA and continuous authentication can offer.

The ability to let people authenticate continuously without passwords is now possible.

Which then is the larger risk, people, or passwords? When it comes to authentication, it's both – people using passwords. The ability to let people authenticate continuously without passwords is now possible and doing so correctly will increase security while meeting the intent of today's standards and compliance requirements.

LEVERAGE MFA FOR COMPLIANCE

MFA SIMPLIFIED

MFA itself offers clear security advantages and even consumers are getting used to dealing with the hassles of providing something other than an annoying password in order to do everyday tasks, such as making a purchase online or logging into a healthcare system. However, few understand what MFA really is; most think it's a password, plus a phone. The National Institute of Standards and Technology (NIST), one of the nation's oldest physical science laboratories and now part of the U.S. Department of Commerce, has posted this MFA basics article. While it is helpful to see the technical definition of MFA from NIST, this article's example promotes the assumption that a password plus another factor is all that exists in everyday practice. While password plus a second factor is the most common scenario, it is not the most secure option, and certainly not the only option.

SIMPLY PUT

NIST identifies 3 possible factors for MFA:

- SOMETHING YOU *KNOW* (such as a password)
- SOMETHING YOU *ARE* (such as a fingerprint)
- SOMETHING YOU *HAVE* (such as a smart card)

Using 2 or 3 of these 3 possible factors means you are using MFA.
Using 1 of these factors twice (such as two different passwords) is not MFA.

For any of these 3 factors there are multiple options that qualify as meeting that factor. An extensive list is beyond the scope of this paper, but as an example, something you **are** includes several possible biometric options, fingerprints, facial recognition, voice recognition, eye print, etc. Also worth noting is that NIST does not include such concepts for other possible valuable factors such as a behavioral factor. An example of this would be the location, time and devices someone authenticates with.

Now that MFA has been defined in a simple manner, let's review how the example of PCI DSS defines the use of MFA to meet the PCI DSS itself. PCI leverages NIST in various ways and the two have had their respective requirements mapped to each other in order to highlight some of the intersections and differences.

LEVERAGE MFA FOR COMPLIANCE

ADDRESSING PCI DSS

Here we will briefly examine the PCI DSS to see how MFA and authentication are addressed within this particular standard. Other standards take similar approaches, and a review of how PCI DSS applies can be leveraged across many different standards.

The most obvious example is Requirement 8: Identify and authenticate access to system components. The PCI DSS lays out how actions need to be tied to specific users and be trackable—or logged. It then describes the importance of passwords related to authentication. The goal here is to protect cardholder data through secure authentication.

Sub-requirement 8.3 has two aspects that define when and where MFA is required:

1. All human administrative access to the Cardholder Data Environment (CDE) when going over a network interface – rather than a direct connection to a system in the CDE
2. All remote access into the CDE

Any authentication solution that can meet the above definition around MFA can easily meet this particular requirement.

There are many other PCI DSS requirements that can be met and supported by most authentication solutions as well:

> *Implement Strong Access Control Measures – Requirements 7, 8 and 9 all focus on this:*

- *Limit access to CHD by business need to know*
- *Identify and authenticate access to system components*
- *Restrict Physical access to CHD*

> *Regularly Monitor and Test Networks – Requirements 10 and 11:*

- *Track and monitor all access to network resources and CHD*
- *Regularly test security systems and processes*

Beyond these obvious requirements, the ability to properly leverage an authentication solution that can continuously monitor access to sensitive data, in this case, CHD, is critical to meet the intent of the entire standard. It doesn't matter how well CHD is encrypted or handled if the authentication credentials to decrypt or access the actual CHD are compromised.

LEVERAGE MFA FOR COMPLIANCE

BEYOND PCI DSS

Traditional authentication methods can meet these basic PCI DSS requirements fairly easily, but most of these solutions rely on passwords and then stop with basic MFA and logging support. The current version of the PCI DSS, 3.2.1, is a great baseline to have a password focus and has been leveraged by many organizations to get much-needed MFA practices in place. The new 4.0 (expected to be released in 2021) version of PCI DSS has the potential to enable organizations to take a new approach on how to execute authentication and meet the PCI DSS requirements in a manner that is both specific to the organization and with a stronger security perspective.

Many authentication and MFA solutions have the potential to go slightly beyond these baselines if implemented well, but few can offer a forward-looking approach that can go significantly beyond these baseline standards. Keeping in mind the above definitions of MFA and the example of PCI DSS (as one of many standards) should provide some good context on what else to look for in your authentication options.

Here are a few key technical points you can look for in a modern authentication and MFA solution, either your existing one, or one you might migrate to in the future, in order to ensure it will not only provide the return on investment you are looking for but also some level of future-proofing for this important security investment:

- *Are passwords required to be one of the three factors?*
- *For any one of the three MFA factors, how many options does your solution offer?*
- *How often is your authentication getting validated, only upon initial authentication, or before and after?*
- *Are other factors beyond the three MFA options part of the solution? For example, behavioral factors such as time of day or location?*
- *What actions are logged, and how accessible are the logs for these actions?*

There are many other considerations, however starting with these often overlooked questions can help you make an informed business decision for your authentication and MFA investments.

LEVERAGE MFA FOR COMPLIANCE

FUTURE PCI DSS

With PCI DSS 4.0 on the horizon, there is also the opportunity to approach authentication with a more risk-based approach. Rather than the traditional 7 characters with an alpha-numeric, it will offer the opportunity to implement strong authentication, enabling a solution with passwordless MFA and continuous authentication offer even more advantage. With the many iterations of PCI DSS before the 4.0 standard, IT professionals have learned to view authentication as a point in time event with a binary outcome – at this exact time, the user either got access or was denied access. It's time to move into the future to let go of this old approach and move to viewing authentication as an on-going or continuous process with consistent validation of an identity. There are significant and compelling business benefits for those willing to make this transition toward a continuous authentication experience.

BUSINESS IMPACTS

It is critical to understand the technical, security and compliance capabilities for any authentication and MFA solution. Once this is established, then there are additional factors to consider before a solid business decision can be made. Ask any CEO or CFO what they are looking for in any investment, and these are the top things you are likely to hear:

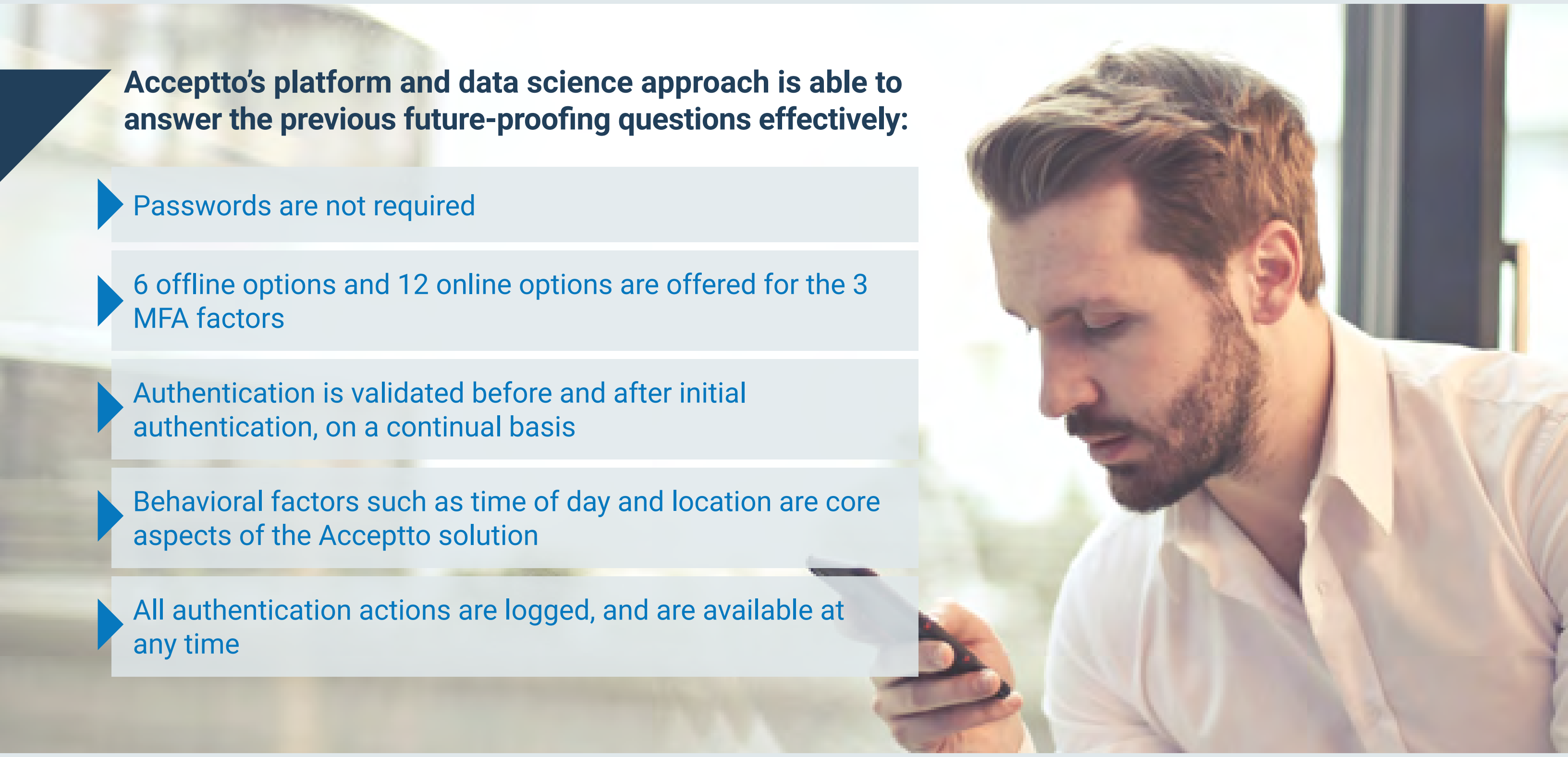
- *Will this make our organization more profitable?*
- *Will this save time for important resources?*
- *How much will this cost?*
- *How will this keep me from negative publicity?*

Note that you rarely hear the question, "will it make our organization more secure?" That would be the CIO or CISO's job. A question like "will it meet our compliance requirements" typically comes from the GRC executive. All of these are valid and important questions, so how well any authentication or MFA solution can answer these questions is a requirement to make the final business decision to invest in that solution.

ACCEPTTO'S PASSWORDLESS CONTINUOUS AUTHENTICATION

As an organization, you have already invested a lot of time and funds into your existing authentication strategies and solutions. If you have not included MFA, you likely have existing pressure to figure that aspect out. If you have not considered the risk of passwords before reading this paper, and have not considered how to remove them from your approach, this paper has touched on some valuable concepts to help you make informed decisions. With many authentication solutions available today, choosing the one that best fits your environment can seem like a difficult task. Here we will look at Acceptto's passwordless continuous authentication platform and consider what it offers in this space.

While the PCI DSS leverages NIST and offers one baseline to evaluate where you stand regarding authentication and MFA, it is essentially a cybersecurity standard or compliance-based perspective. With Artificial Intelligence (AI) and Machine Learning (ML) on the rise, there are some additional perspectives that can now be better considered with regards to many cybersecurity approaches, and certainly can be applied to specific critical areas such as authentication. This perspective can be called a "data science approach" to authentication. Taking a data science perspective can help move your approach beyond a standards-based approach and doing this can help protect your authentication investment for many years to come.



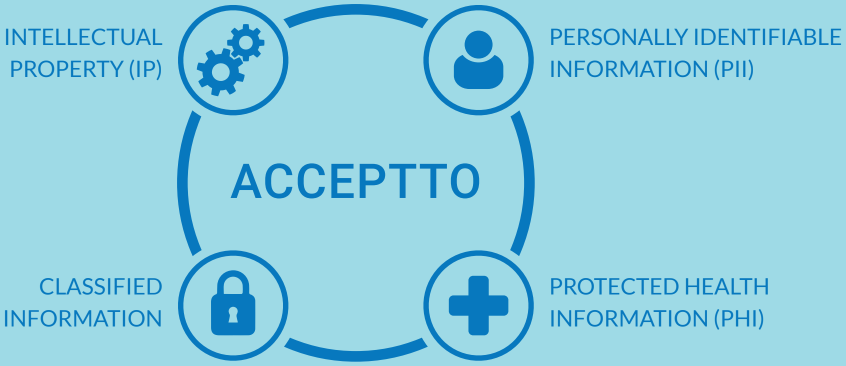
Acceptto's platform and data science approach is able to answer the previous future-proofing questions effectively:

- Passwords are not required
- 6 offline options and 12 online options are offered for the 3 MFA factors
- Authentication is validated before and after initial authentication, on a continual basis
- Behavioral factors such as time of day and location are core aspects of the Acceptto solution
- All authentication actions are logged, and are available at any time

ACCEPTTO'S PASSWORDLESS CONTINUOUS AUTHENTICATION

Acceptto's platform leverages more than a traditional standards-based approach to authentication and MFA: it leverages a data science approach in a way that goes beyond just meeting core PCI DSS compliance requirements, or any other common standard.

ACCEPTTO'S approach to authentication and MFA can protect not only CHD, but also protect access to all other kinds of sensitive data such as


INTELLECTUAL PROPERTY (IP)
PERSONALLY IDENTIFIABLE INFORMATION (PII)
ACCEPTTO
CLASSIFIED INFORMATION
PROTECTED HEALTH INFORMATION (PHI)

These and many other specific data types have dozens of potential standards to protect them, including: HIPAA/HITECH, GDPR, NIST, FedRamp, CMMC, FFIEC, CCPA, SOX, GLB, ADA, NERC-CIP, etc.

Meeting any of these standards is a great goal, but Acceptto's approach also advances ahead of these standards to actually provide ongoing continuous awareness of data access. This offers many additional security, functionality and usability benefits, some of which meet additional requirements, and many that are not even part of a standard. A few key things Acceptto's authentication approach supplies from a technical, security or compliance perspective:

- *With no passwords, attackers have reduced options to attack your organization's environment.*
- *With continuous monitoring of identity in real-time and behavioral AI, your threats can be reviewed and actions can be taken at run time to prevent the threat from becoming a breach.*
- *The ability to use risk to define your policy orchestration creates a dynamic approach to authentication and enables continuous automated enforcement.*

ACCEPTTO'S PASSWORDLESS CONTINUOUS AUTHENTICATION

From a business perspective here are a few considerations:

- *The best user experience imaginable: With no passwords, and behavioral AI/ML, your users will authenticate effortlessly. Not only does the user base get to focus on real work and save time, it's actually more secure.*
- *Operational costs will reduce. Yes, it will save money in various ways, one of which is to reduce help desk costs with not needing to do password resets.*
- *Out of the box effortless implementation, customization and integration to existing authentication systems. Acceptto can work with whatever you have in place, and take it to a new level, or it can be leveraged to replace aging technology.*

Here is another way to view the business value you should explore with Acceptto:

- *Implemented correctly, your organization can be more profitable. For example, if you have a user base that you are required to move from traditional authentication to MFA, migrations can lose a significant percentage of users. With Acceptto, this loss can be avoided.*
- *Acceptto can save time for existing resources, including employees and users, by decreasing the time needed to authenticate and reset passwords. Additionally, the time needed for support desks to do password resets can drop to nothing – saving both time and operational costs.*
- *How much will this cost? If you can save more money than the cost of the solution, the answer to this question makes you money. Comparing the investment to other traditional authentication and MFA solutions is also worth your time.*
- *The best way to avoid negative publicity is to avoid a breach of any kind. Leveraging Acceptto to monitor authentication on an ongoing basis can provide information on a potential breach before it happens.*

Used correctly and tailored to your environment, Acceptto's passwordless continuous authentication has the potential to save you time and money, move beyond compliance, and future-proof your authentication needs as well as enhancing many of the security technology investments you have made or need to make soon.

CONCLUSION

As technology rapidly advances, the challenge of selecting the best solutions for your organization increases. When it comes to protecting your organization's most critical assets and data, your choice of the best authentication solution becomes a critical business decision. Which solutions will stay relevant and provide good long-term return on investment, while also offering the latest security for your digital environment, on-prem or in the cloud?

Understanding how authentication and MFA work together and the impacts on various compliance standards is core knowledge to answer the above and make these important business decisions. Having key questions to ask assists in distinguishing between different options for authentication solutions, and also supports your quest to choose the best solution and investment for your organization.

Acceptto's Passwordless Continuous Authentication fulfills many of these questions in innovative and forward-looking ways. Acceptto's platform has the potential to help your organization move beyond basic compliance standards and into a more secure approach to authentication. Saving money, saving time and offering the best digital experience can result in a more secure solution when using Acceptto's platform.

Jim Routh, Board member and former CISO at MassMutual, CVS, Aetna, JPMC, KPMG, DTCC & American Express, agrees: "Acceptto's approach delivers a more secure solution at a lower cost with a significantly improved digital consumer experience."

The ability to customize Acceptto's solutions to fit your organization means that any organization can obtain these security and usability benefits in ways that will integrate with nearly all existing or planned environments, while returning the most out of your authentication investments.

ABOUT ALPINE: www.alpineconsults.com

Alpine was founded to fulfill a passion to help businesses, and the people that work in them, overcome today's cybersecurity challenges and succeed in new ways by leveraging the untapped value that an innovative approach to security can provide. With a background of over 20 years in technology, security and compliance, Alpine's skill set can help virtually any business learn how to leverage innovative security technologies with the result of translating security investments into tangible business value.

ABOUT ACCEPTTO: www.acceptto.com

Acceptto is a transformative cybersecurity company driving a paradigm shift in identity access management by treating authentication not as a single event, but rather a continuum. Our AI/ML powered Passwordless Continuous AuthenticationTM technology analyzes and verifies user identity, inferring behavioral data to detect anomalies and eliminate dependence on vulnerable binary authentications. We deliver the smartest, most resilient and breach-proof identity validation technology commercially available today for web, mobile, cloud and IoT platforms.

ABOUT THE AUTHOR: Dan Fritsche, CISSP

Dan Fritsche, CISSP, is Founder and CEO of Alpine Security Consulting. Dan's specialty is in security innovation, helping companies of all kinds turn security from a hurdle into a strategic investment that has a positive return on investment. Dan started out with a security focus for 10 years at IBM, actively supporting penetration testing, vulnerability scanning, application security and business intelligence across multiple security disciplines. This led to 10 years at Coalfire helping hundreds of companies improve their security posture in application security, encryption, tokenization and many other security specialties. For over a year Dan was able to help Global Payments drive the value and involvement of innovative security approaches as early into applications lifecycles as possible. Dan is a Former QSA, PA-QSA, P2PE QSA and P2PE PA-QSA of 5-10 years each.

CREATED BY: HAMMER & CHISEL DESIGN COMPANY, LLC | www.hammerandchiseldesign.com HCD003-21