ATHENA

WHERE IDEAS BECOME REALITY

Athena User Authentication

Presented by:
Athena Consulting

2023

Contents

Introduction and Background

Authentication is the process of verifying one's identity. Any unique identification of a person or object that can not be replicated by another source is known as authentication. In a social setting, authentication could be providing an ID or social security number, or it could be answering a set of personal questions that only the person in question could answer. With the rise of computing and the internet, authentication has come to be known as passwords, fingerprints, two-factor authentication, and other sorts of authentication.

When computers were first made public in the 1960s, they were huge and expensive, meaning that not anyone could afford owning a personal computer, and rather a whole community or university were meant to share resources in using a very limited number of computers. This meant that all users would have to share the same resources in the computer. Now that first created the issue of each user wanting to store their data and access it at a later date directly rather than basically everyone having access to everything. Therefore, the most rudimentary phase of authentication was created: plaintext passwords.

In the early 1970s, everyone realized that storing passwords in plaintext in storage was a huge mistake, it was easy to search and find all the passwords of all users and access any one of them at any time. Therefore, passwords and authentication started to get more sophisticated over time. First, hashing was introduced so that the passwords stored could not be directly read by humans who opened the file. Then, static hashes turned out to be easily decrypted and salts were introduced to randomize hashes and significantly increase the time to decrypt the passwords. Passwords kept on getting more secure, with the rise of the internet, to be stored on private "secure" databases, the creation of one-time passwords etc....

In the 2010s, biometric authentication finally became a reality outside of movies. Although this is outside the scope of this report as although it is one of the most reliable ways of user authentication, it is not scalable for user authentication on websites as the cost and security of sharing this data is still not worth it. In the future though, it definitely will change.

What our authentication relies on, is a method created and worked on in the 1980s, which is asymmetric cryptography which is the use of private and public keys for fast, reliable, and secure authentication. With the rise of blockchain technology, which focuses on the use of asymmetric cryptography as a method of access to wallets that contain cryptocurrencies and a digital identity of the blockchain, Athena decided to work on a revolutionary prepackaged method of authentication that is more secure, faster, and more reliable than traditional password-based authentication methods. In this product report, we state our findings and development and introduce Athena User Authentication.

The Issue With Passwords

The first question we need to answer is: What is wrong with passwords and why is there a need for a change? The ethos behind passwords on websites and applications we use is that we need to trust the website or application to store our passwords securely, hashed and hidden away from any malicious intent.

Back in august 2022 a password management company suffered a data breach, where the hackers were able to gain access to certain elements of our customer's information. The company stated that after the incident that the stolen information was encrypted making their customer safe from hackers accessing their data without the user's master password. Unfortunately making a strong password isn't as straightforward as people think. Only truly randomized passwords are secure from brute force attacks–when hackers make multiple password attempts using thousands or millions of possibilities. Typically, these types of attacks are thwarted by limited password attempts. But when hackers have unlimited tries (like with the case of a data breach), it's only a matter of time before they can break any password.

From a shallow point of view, this shows not to be such a problem with all the implementations set in place to avoid such breaches. Deeper down, we can see that since the ethos of forced trust is bound to create issues, which have happened thousands of times. In the last decade, thousands of websites have been hacked and personal authentication information has been shared and exploited. Whether the website was on it is a different subject outside of the scope of this report, but the conclusion lies the same. Trusting a third party with data that does not inherently belong to it is a disaster ready to happen. This is why blockchain was created, as a decentralized database that does not rely on a third party to store it and overlook it from malicious attacks but distributes the responsibility on code and decentralized nodes that create a much safer environment by removing the idea of "forced trust".

The second issue with passwords is that it relies on improper storage, which can manifest in three ways:

1. The user uses the same password for all their websites, and therefore any breach in one website will cause all the user's websites to have the same fate.
2. The user chooses one password for each website and memorizes them, but with the need for highly complex passwords, this idea is definitely not scalable and human memory is too unreliable to depend on in that case.
3. Users store their different passwords on their local machines or written or using a third party storage which is highly insecure due to most users just keeping them plaintext, and adds a degree of insecurity to the password being stored.

Athena User Authentication

Passwords have never been an ideal solution to access your accounts, but it’s the best we’ve come up with since the 1960s. We’re well into the 21st century. It’s time to move on. Athena User Authentication (AUA) focuses on creating a product to authenticate websites and applications using a blockchain wallet. This product is a seamless API and server that any client can set up and run cheaply and in no time. AUA uses asymmetric cryptography of blockchain wallets to authenticate users on a website. This removes the need for the client to store any passwords on their side and gives users the responsibility of handling their authentication power.

From the user's blockchain wallet, a specific message is signed that is sent for verification to the client's server to verify authenticity and identity of the user on the website in a non-custodial way.

The power is now in the hands of the user, who has the ability to sign with a wallet seamlessly to any website of choice, alternate between addresses for each website they decide to sign in to, and sleep sound knowing that their accounts are now more secure.

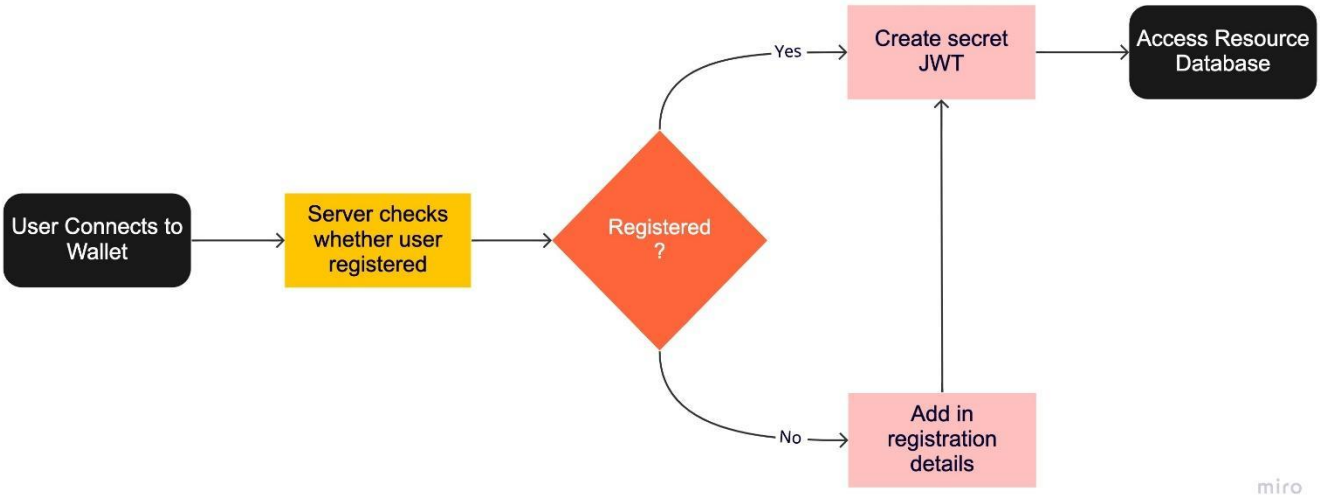
The rest of the report focuses on the AUA product with detailed metrics, possible concerns, and technical details.

Technical Description

AUA is an API that can be integrated with any website or application that needs user authentication. AUA uses asymmetric cryptography (public/private key pair) and JWT standard to create a seamless integration with any website. The client will have access to GET and POST requests from a server that they will run personally on a cloud (that Athena will provide the source code to).

GET requests	**userauthv1/nonce/{publickey}**	This checks whether the user has already registered to the platform, it returns a nonce which is an unsigned integer. If the nonce is -1, then the user did not register yet, then the platform should show the registration page. If the nonce is positive, then the user is registered.
	userauthv1/generate_jwt/{nonce}/{public_key}	Generates a JWT object that is integrated into the resource database to verify the user primary to access read/write data.
POST requests	**userauthv1/nonce_set/{public_key}/{nonce}**	This adds to the database a mapping of a public key to a nonce to verify next time that the user has already registered. This nonce is harmless and although securely stored, any breach will not release any sensitive user data.

Table 1. GET & POST requests of AUA API



Resource Database

The resource database is the database used by the website to store user information to be shown on the website or any other resource needed. We need to create a customized API that works with the specific resource database to be able to read a user primary key with a different method than the password using our JWT.

SWOT Analysis

Strengths

- AUA removes the need of storing usernames and passwords (sensitive data) on the server side and taking responsibility for thousands of passwords.
- Reduce the incentive of attacks since the sensitive data is not there anymore.
- Better and faster User Experience for authentication to the website.
- User freedom to login with any address, and be able to have different wallets for different websites for increased security and anonymity.
- Increased trust from users. Users would prefer websites that are easy to trust than websites that are harder to trust.

Weaknesses

- Connection of wallet to different devices may not be optimal for users as they would have to add their private key to different devices. This is not a big problem however since with mobile wallets, they could sign it by a QR code solution.

Opportunities

- Adoption of blockchain technology is increasing day by day and more and more computer users have a blockchain wallet that they use for their day-to-day usage.
- Recent password breaches in different applications and websites have shown that the “forced trust” issue with password storage is just not logical or sustainable.
- Methods that have been trying to make access more secure such as 2FA are a user experience obstacle and users would prefer a more seamless experience.

Threats

- Lack of worldwide adoption of blockchain wallets as of now. Therefore, it is not the best strategy to offer ONLY AUA as a login option. But offering it as one of the options is one step in the right direction (explained below).
- Issues with regulated websites. If the client is a bank or other regulated entity, it may be difficult to integrate a blockchain wallet as there are regulations and laws that need to be followed and any change may need board approval to be possible.

Concerns and Issues

There are multiple concerns that clients may have concerning the product since it is a pretty new idea and different to traditional more known methods. In this section we will go over these concerns and the solutions for them.

Adoption

The first worry that users have is that blockchain wallets are still not mainstream and therefore not everyone will have access to the platform. That is true (as of today) but won't affect Web-3 platforms since all its users already have wallets that they use to interact with the platform. For Web-2 companies, it is different though since a percentage of their users won't have a wallet to authenticate with, therefore they should follow a different approach. Our recommendation would be to start gradually adopting AUA and introducing both options. The goal would be to decrease the number of passwords stored on a website and increase the number of authentications using the blockchain wallet. With the increase in adoption over time, the numbers will scale, and companies will be able to leave password authentication behind and become scalable and more secure.

Multi-accounts for Same User

Another concern is that users could create multiple accounts from different addresses which could be an issue on some websites. Although that may be true, the same thing could be said about password authentication with different usernames. As in password authentication, we can use email or OTP authentication to verify users cannot create multiple accounts. There are multiple ways that could be a solution to limiting multi-accounts which is necessary.

Tech Stack

Nonce Database and API

The nonce database is a database that stores user addresses mapped to a specific nonce. The Nonce Database would be accessed with an Express.JS API and is built using MongoDB.

Why The Change?

Now the greatest question that comes up, is why to change? Why should a platform move from a password-based authentication system to a blockchain based authentication system? Let us go through the reasons one by one:

Responsibility

Holding passwords in a secure database is just too much unneeded responsibility for a platform to hold. First of all, the platform is holding an object that is inherently not theirs in order to verify the identity of a user. Although the platform will not ALWAYS be legally liable for any platform exploit or attack towards user passwords, the platform will still be morally liable and will definitely get backlash. Now as a platform, what is there to gain from holding these passwords while asymmetric cryptography creates a non-custodial way of identifying users?

Financially Sound

Assume a platform is a business with a gross revenue of 1 million USD. This platform has 10,000 monthly users that the platform is responsible for holding the passwords for. Therefore revenue per client is 100 USD.

Now to understand the magnitude of attacks on the web, you must know that a website is hacked every 39 seconds online! The number is way more than you can imagine and exploits exist on every part and code of a website. Go to https://haveibeenpwned.com/ and check your email to see how many websites gave your password away.

Therefore if you have a business that is grossing over 1 million USD that is generated by clients visiting or using the platform, over the lifetime of the website, there is a significant probability that the website will be exploited. Suddenly, after an exploit, there is a very high probability that the revenue of the website due to fear and spreading of news can lead to a 40-50% drop in the gross revenue of the company. Not to mention that in some parts of the world, the platform could be liable for civil action and get a stiff fine. Therefore, in the long run, the expected value of storing passwords, and actually increasing the number of passwords that the platform stores is completely negative. A negative expected value means that there is no value for the platform to store those passwords and create a “forced trust” with the user, when in reality that does not need to exist.

User Utility

As a general rule, users will tend where there is the most positive utility and value for the user to be. User Utility can be calculated in a number of ways depending on the exact use case. In a free market, utility difference between platforms tends to drop significantly since there are always competitors with a very close use case and quality to another platform, and therefore the utility is usually pretty close.

In a free market:

$$\lim_{market \to free} u_1 - u_2 \approx 0$$

Therefore more reputable and safer platforms tend to succeed more than new unheard of platforms, and this is why social media and marketing are really focused upon since it creates credibility. Credibility comes from security and trustworthiness. If a company has been known to sell data for malicious purposes, users flock to competitors. If a company is known for its security breaches, users flock to competitors.

Since it is becoming harder and harder to actually create a platform with a strong competitive advantage (for a long time) in a free market, building credibility and trust could be the differentiation between platforms and where users will flock to next.

Conclusion

In conclusion, Athena Consulting believes that the password authentication system that websites use is becoming a security risk overall for the platforms and users. This is why we built Athena User Authentication to remove this necessity for websites and bring the responsibility of security on the users that make data breaches less relevant and less incentivized overall.