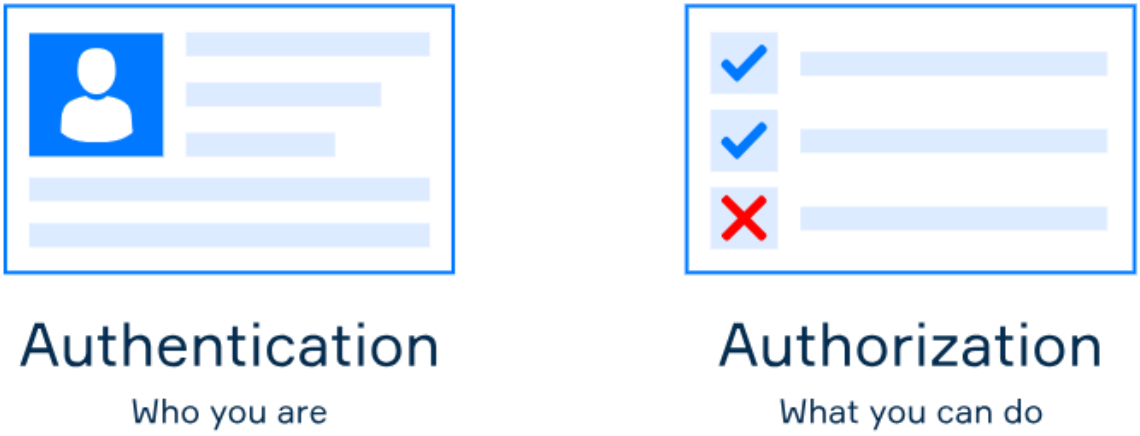
When working with data, it is important to think about protecting it to guard your privacy and avoid unauthorized access by intruders. The main tools that you can use for this are **authorization** and **authentication**. Let's take a closer look at what they are and how they work.



What is authentication?

Authentication is the first step in any security process. It stands for the act of validating that users are who they claim to be. Thus, the system will "know" who is going to work with it now. The main types of authentication are as follows:

- First of all, it is a **password.** If a person enters the correct username and password, the system grants them access.
- Secondly, there are **one-time pins** that grant access for only one session. If your bank account has a regular password that you never change, then to protect, for example, your account data, the bank may offer you one-time pins. This level of protection is more reliable than the first, but there is a chance that someone may intercept your one-time pin.
- The third type is **an authentication app.** They work as follows: first, the system fills in a password and username and then generates a long

one-time access code that changes every 30 seconds making it difficult to intercept.
- The last one is **biometrics.** A user presents a fingerprint or eye scan to gain access to the system. The advantage of biometric identification systems is that the characteristics used in these systems are an integral part of the personality, so it is impossible to lose, transfer, or forget them.

Authentication is always visible to the user so that they can pass it. Moreover, they can partially change it by replacing a password or their username, for example.

Often all the data during the authentication moves through an ID token, which is a formatted character string that contains information such as ID, username, account login time, ID Token expiration date.

Now you know what authentication is and what types of it exist. Let's move to the authorization then.

What is authorization?

Authorization often goes after authentication when the system successfully "recognized" you. Authorization checks if you have the right to access the content or resources to which you have requested access. For example, the permission to download a particular file on a server or to provide individual users with administrative access to an application.

Often all the data here moves through special access tokens, not ID ones, as during authentication.

Also, unlike authentication, authorization is not visible to the user and there is no option to change it. That is because only the data owner can provide the permissions. For example, one can not view and change a document until the document owner sends a certain invitation that permits editing it.

Having figured out what authentication and authorization are, let's talk about their fundamental differences.

Authentication vs. authorization

Let's use an analogy to outline their differences. Imagine someone asked their friend to pick up a parcel from the post office and take it to this person's house. The friend will need:

- a key (authentication). The lock on the door will grant them access to the house, it is like a password.
- permissions (authorization). Once inside, the friend has permission to access the living room and put the parcel on the table. But the friend may not have permission to go into the kitchen to take some food from the fridge.

Authentication and authorization work together in this example. The friend has the right to enter the house (authentication), and once there, there he gets access to certain areas of the house (authorization).

Let's put all the differences we have described into one table:

	Authentication	**Authorization**
What does it do?	Verifies credentials	Grants or denies permission

How does it work?	Through passwords, biometrics, one-time pins, or apps	Through settings maintained by security teams
Is it visible to the user?	Yes	No
Is it changeable by the user?	Partially	No
How does data move?	Through ID tokens	Through access tokens

Conclusion

To sum up,

- Authentication is the act of validating that users are who they claim to be;
- The authentication types are passwords, one-time pins, authentication apps, and biometrics;
- Authorization is the process of giving the user permission to access a specific resource or function.

A developer decided to create an authentication app for a new website. What steps should this system perform?

Select one or more options from the list

- [x] generate a long one-time access code
- [ ] generate password and username
- [x] accept the password and username
- [ ] it will only need a username

What is denied?

A writer gave a colleague access to a file with their new story and asked them to give their opinion on it. So, the writer's colleague can view the document. But what actions are denied to them?

Select one or more options from the list

- [x] changing the story
- [ ] reading the story
- [x] removing some parts from the story
- [x] downloading the story

What authentication type is it?

Imagine that you have a new phone and you do not want anyone else to be able to use it except you. So, you decide you will need to set up authentication. Since a regular password can be easily guessed, you want to use more secure data – a fingerprint. What type of authentication will it be then? Biometric

ID token contents

What should an ID token contain (in an encrypted form)?

Select one or more options from the list

- [ ] list of user permissions
- [x] token expiration date
- [x] user login
- [ ] user password