AIRLOCK®
SECURE ACCESS HUB

WHITEPAPER

Strong authentication. Easy.

Airlock 2FA

Contents

1 Basics of a secure login

Why is two-factor authentication necessary?

One piece of everyday wisdom is: two is better than one. The two-factor authentication (2FA, MFA or SCA for short) in the area of IT security offers double the security. 2FA is thus the optimal solution for the rising complexity of access management. The second factor undisputedly offers more security than simply requesting a username and password. However, it must be user friendly and cost efficient as well as complying with currently valid legal requirements.

The main reason for strong authentication is largely password vulnerabilities:

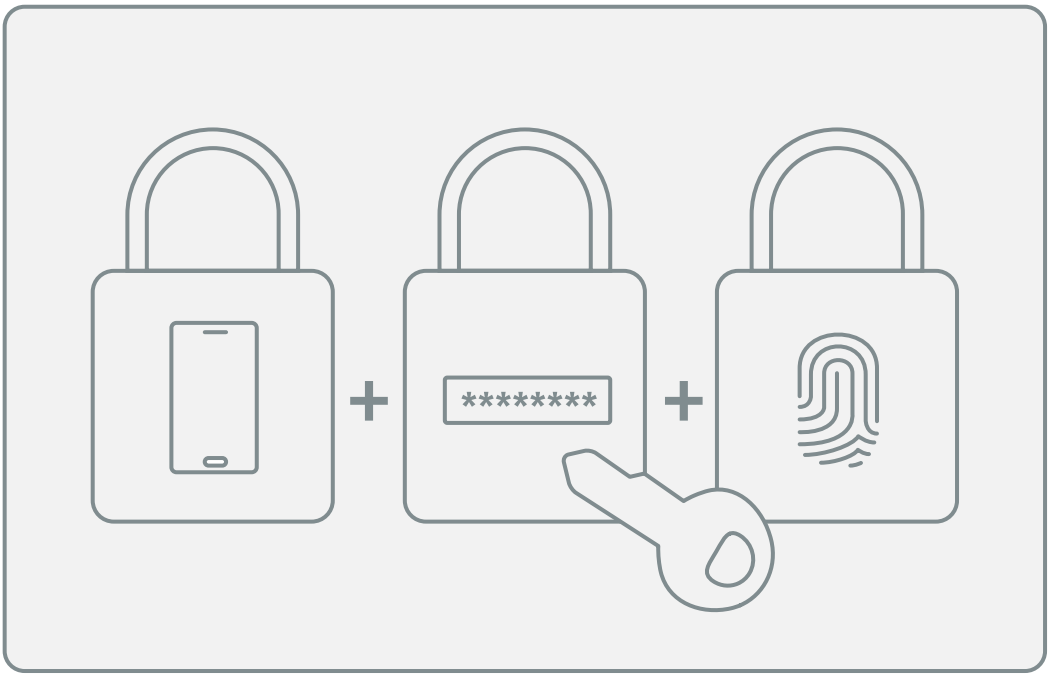
- **90% of passwords are cracked in under six seconds.**
- **2/3 of users use the same password for different web services.**
- **passwords suggest a convenient security to users which doesn't actually exist.**

Legal requirements such as PSD2 have significantly increased complexity. Requirements for verifying identities have also changed considerably. Many regulators and laws stipulate strong authentication.

In addition to the security and legal requirements, there is another aspect which plays a key role in the implementation of a 2FA solution: user friendliness. In combination with efficient customer identity & access management (cIAM), numerous processes are significantly simplified. This increases user friendliness via self services, user flows or single sign-on as well as simplifying internal processes and efforts.

Strong authentication – what even is it?

“Knowing”, “having”, “being” – these are the three principles on which multifactor authentication is based. The specific details related to implementing these can vary greatly. To achieve strong authentication, at least two of the three principles must be fulfilled.



Something that only the user has:

e.g. a bank or credit card, key, smartphone or token.

Something that only the user knows:

e.g. the username, passwords, PINs or answers to security questions.

Something that only the user is:

e.g. their fingerprint, face or iris pattern.

2 Selecting the optimal second factor – the key considerations

Depending on the application, the second factor can be implemented in very different ways. The market offers a variety of different types of authentication including certificates, TAN lists, mTAN via SMS, own hardware or using a smartphone.
An overview of the currently common variants can be accessed using the following link:
https://www.airlock.com/en/secure-access-hub/components/customer-identity-access-management-ciam/2-factor-authentication/authentication-methods/

It is therefore important to make a careful selection which takes into account aspects relating to the user, IT security and the business. The following must be considered:

Focus on the user

- **Target groups**
  Who will be using the second factor? Customers in a B2C or B2B context, partners or even employees? Digital natives or older users?
- **The context**
  What is the user's perception of security in the specific application? Will they have a positive view of a more complex authentication process? For example, when it comes to large financial transactions. Or should the process be as simple as possible – e.g. when making a till payment?
- **The device used**
  Does the user accept an app on their smartphone as a second factor? Or is an additional hardware token required? Do users require several devices for the authentication process?
- **The usage situations**
  In which situations do the users authenticate themselves? Does this perhaps even require continuous verification? Can the user always be online? Should the authentication also work in areas without network coverage?

Focus on IT security and compliance

- **Types of authorisation**
  Is the second factor only used to login to an online service or will it also approve transactions or release sensitive data?
- **Security-related scenarios**
  How high should the security level be? Is SMS/mTAN sufficient or is a modern authentication solution with increased security and user friendliness required?
- **Legal requirements**
  Which applications require strong authentication for regulatory reasons? Does the company need to comply with e.g. the Swiss federal law on electronic health records (EPDG) or the European Payment Services Directive (PSD2)? Do requirements need to be met in accordance with PCI-DSS or MAS?
- **Expertise of the application developers**
  According to a study conducted by the NoSQL developer, MongoDB, less than a third of developers say that they assume responsibility for security. Should the developers make the decision about authentication methods and thus security themselves for every new application? Or should a centralised, generally applicable overall solution be chosen?

Focus on business aspects

- **Involvement of partners and digital ecosystems**
  Should additional services from third-party providers be involved and should APIs be available for future external partners? Is strong authentication required here too?
- **Market situations**
  Is agility and a quick time to market important? Do many digital services already exist? Will this number increase due to digitisation?
- **Brand context**
  To what extent should the brand as well as the corporate identity and the corporate design be taken into consideration?
  Should non-branded solutions be implemented?
- **App integration**
  Should the 2FA technology also be integrated in company apps?

Answers must be available in the selected two-factor authentication for all these questions. A sound evaluation thus protects against future problems in the implementation.

The key advantages and disadvantages of the most common methods are summarised at a glance in the following table.

Method	Security	User friendliness	Management	Costs
Certificate	⊕⊕	⊖⊖	⊖	⊖
Cross-off lists	⊖	⊖	⊖	≈
Matrix card	≈	⊖	⊖	≈
mTAN via SMS	⊖	≈	≈	≈
Hardware OTP	⊕	≈	⊖	⊖
Software OTP	⊕	≈	≈	⊕⊕
Push	⊕⊕	⊕⊕	≈	⊕
QR Code				
– with OTP	⊕⊕	≈	≈	≈
– without OTP	⊕	⊕	⊖	⊖⊖
Biometric	≈	≈	≈	≈
– with hardware	⊕⊕	≈	⊖	⊖⊖
– with smartphone	⊕	⊕⊕	≈	≈
FIDO-2	⊕⊕	⊕	≈	≈
FIDO-1	⊕	≈	⊖	⊖⊖
OTP via e-Mail	≈	≈	≈	⊕

The term clarifications are available in more detail in the glossary.

3 Six success criteria for successful 2FA integration

There are certain particularities which must be considered for every implementation of a strong authentication. The most important ones are listed below.

Integrating 2FA in existing systems

A two-factor authentication is the only way to verify an identity more strictly. It is thus not a standalone solution, but should rather be integrated as efficiently as possible in existing systems which manage identities and regulate access. In which form, in which processes and with which access rights the second factor is implemented must first be defined.

1. **Identities**
   To which user directories should 2FA be connected? To an internal database, to Microsoft Active Directory (AD), LDAP and/or to a customer IAM (cIAM)?
2. **Accesses**
   Which applications should be protected specifically? Which APIs, web portals or mobile applications? Is a 2FA solution already being used for certain applications?
3. **Authentication**
   Which components does the user already have? Smartphones, hardware tokens, etc.? These can be involved as supports for the second factor in order to achieve cost savings as well as higher user convenience.

Upstream authentication

Upstream authentication means: Every individual application is no longer protected separately, but rather the entire application landscape is protected as a whole. The first advantage is a significant increase in security for the whole IT infrastructure. The second is a long-lasting efficiency increase. With upstream authentication, every security update, every compliance change and every implementation of a new authentication medium is controlled and managed centrally – this saves a lot of time and increases cost effectiveness. The development costs and time for new applications are thus significantly reduced.

Developing risk scenarios

Every customer group is different. Every company-specific risk scenario is too. This is why a sound evaluation is key. The first step involves the question of whether and for which applications and services a strong authentication is required. The desired security level should then be defined for every application (or for the entire application architecture) and the type of registration should be determined. The users must then also be analysed more closely: are they tech-savvy and do they trust digital identities?

Enable a consistent customer journey

User-friendly processes are essential for new customer acquisition. The logical consequence: the customer journey must be well thought out and logically structured. Devices used must be given just as much thought as the specific design of the onboarding process. It can be designed gradually via social registration and social login for low entry barriers up to a strongly authenticated user account for top security. Functionalities such as user self services or single sign-on (SSO) also further optimise the user friendliness. If the second factor itself can be chosen and a reliable replacement is available in an emergency, these are prized added values for customers which will also take a load off of support staff.

Optimising rollout and replacement processes

An integrated security solution with cIAM and integrated two-factor authentication minimises business outlays and simplifies workflows. This applies not only to ongoing operations, but also to rollouts. When integrating new 2FA methods, modern cIAM systems thus automatically adopt all customer information thanks to clever communication through various channels. Particularly when it comes to the initial registration, intuitive user self services provide permanent relief for the helpdesk, as well as in cases where the user loses or wishes to replace their device for the second factor.

Facilitating migrations

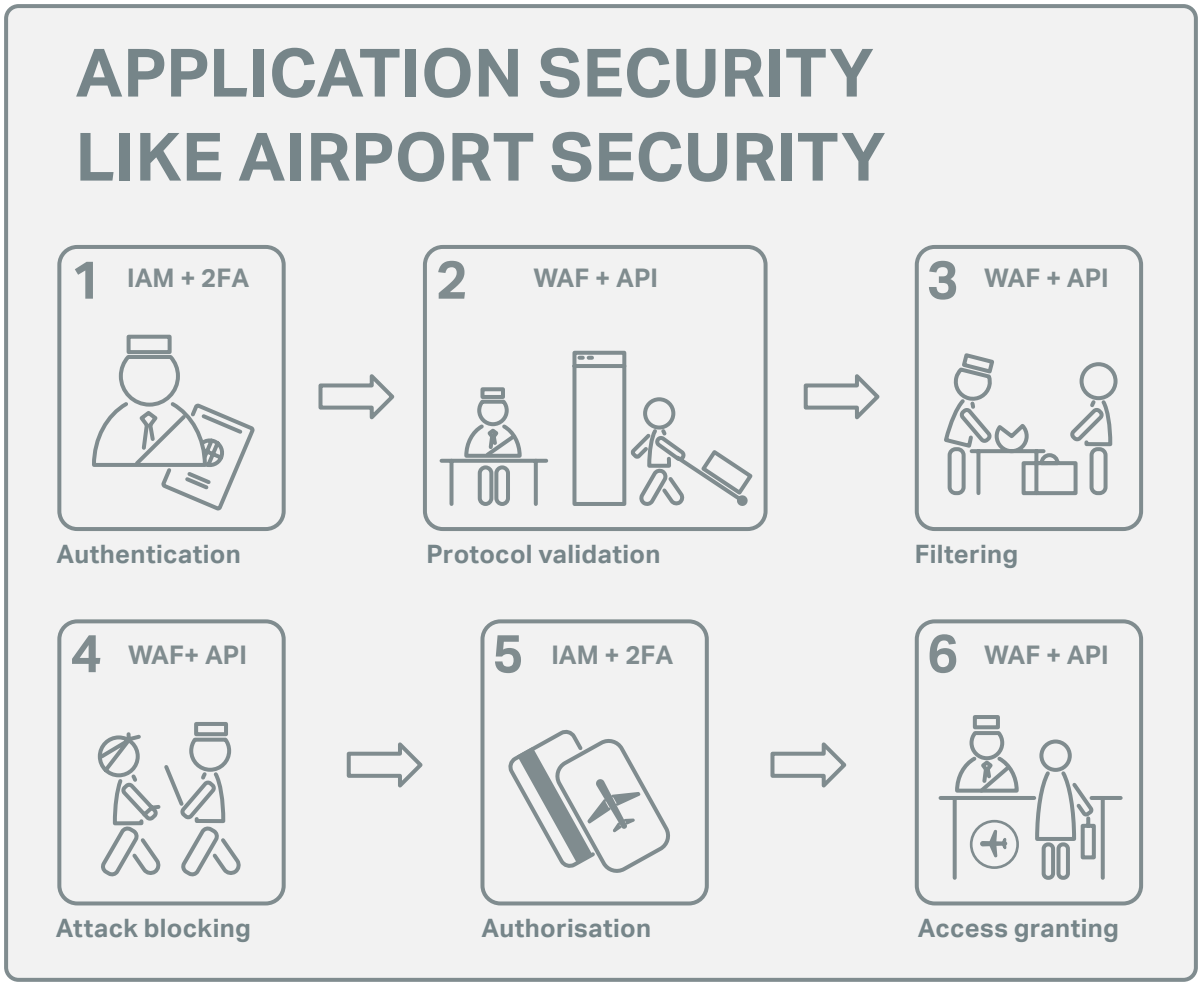
All new things are associated with extra work – not only for businesses but also for customers. It is therefore important to make the migration processes of existing two-factor solutions as easy and user friendly as possible. The new two-factor authentication should thus be introduced gradually and allow for mixed operation during the transition phase, whereby both the old and the new authentication methods can be used.

4 Ensuring coordinated security with cIAM and 2FA

Two-factor authentication is a singular technology for verifying identity properties. However, if you verify identities, you must also manage these and their access rights. Customer Identity & Access Management (cIAM) is responsible for this.

What applies in real life also applies to IT security: airport checks form the perfect analogy for this. They are more complex than you'd think. Boundaries must be established, checking procedures must be determined and identities must be defined with their authorisations. Content must also be checked. Precisely here is where the challenge lies. A passenger first appears as a person without identity or connection to a flight. It's only the various checks which qualify them to board the respective plane and find the right seat.

2FA corresponds to the ID check in this airport analogy. But how are the ticket issue and checks, the luggage scans, boarding, etc. covered in IT security? The web applications and APIs must also be more widely protected. A coordinated organisation of identity management and checks in an integrated overall solution is thus the future-proof approach. With 2FA in combination with cIAM, an upstream web application firewall and an API security gateway.



Five reasons why the combination is important:

- **Full integration**

  A modern cIAM is compatible with various different authentication processes and offers an efficient user and access management option which is easy to integrate. A connection to a second authentication factor is thus particularly simple, especially if it is already fully integrated.

- **Optimal authentication processes**

  In combination with 2FA, a cIAM can control user access in various waysand offer different access options based on the risks and users – e.g. taking into account the access history or the device currently in use. For customers, this means that they experience a consistent authentication process which is ideal for their respective situation. Their identity can thus be checked at home, for example, without additional interaction and a risk-based authentication, while using a user-friendly authentication on the go with just one touch via smartphone.

- **Practical single sign-on**

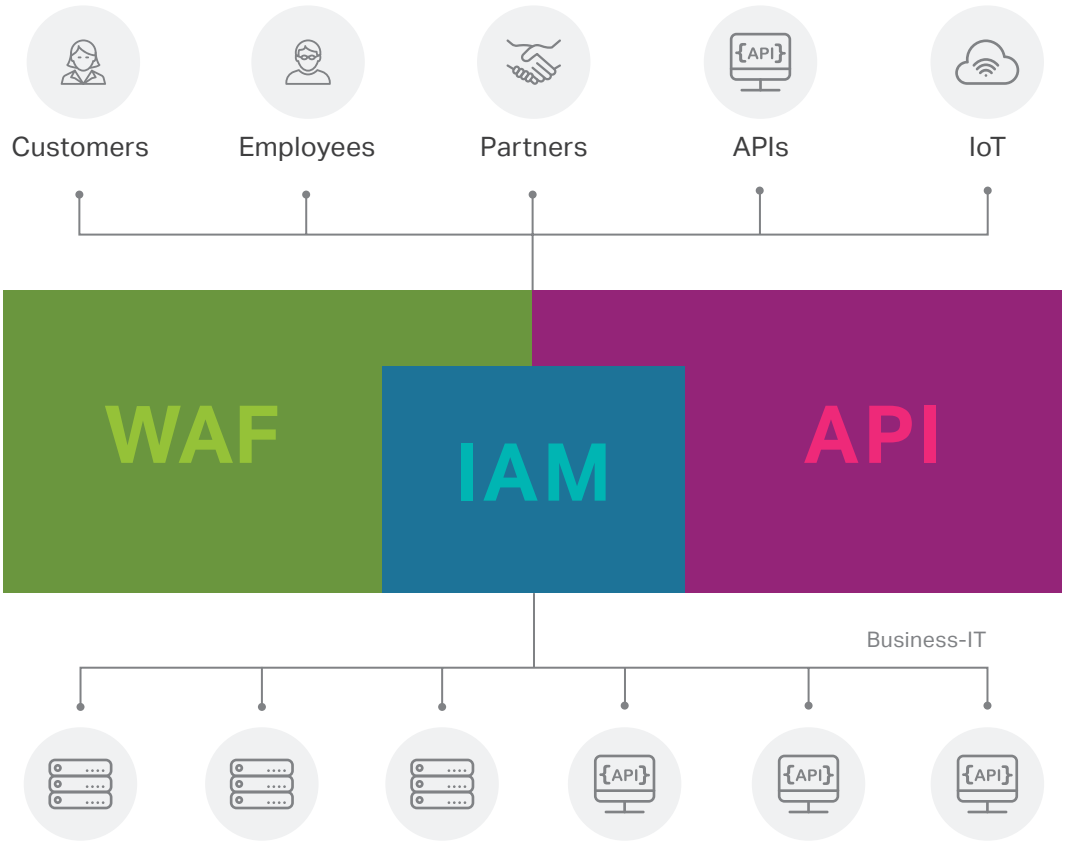
  Individual access to applications is unlinked and the identity of an authenticated user is used several times. This makes a transparent single sign-on possible which combines high security with high user acceptance.

- **Modern user self services**

  So that not only the registration is user friendly, comprehensible userself management is important – e.g. for managing their own data, consent declarations (GDPR) and selecting the second factor for using new services. In addition, user self services carried out via cIAM also relieve the business helpdesk, thereby leading to huge cost savings.

- **Efficient out-of-the-box solution**

  The question arises while selecting a 2FA solution: Should I select an integrated overall solution? Or use existing components but set up an extra server and adapt everything to the authentication process individually? This question is not only important during the system selection but also when it comes to system management. The individual components mean that every update and every regulatory change must be implemented at every point. It is thus worthwhile at this point to carry out a full cost calculation which will often result in favour of the holistic out-of-the-box solution.



Web applications and APIs

Three central advantages for businesses

An organised security solution also brings with it big economic advantages. Integrated overall solutions are particularly persuasive where it really matters today: when optimising internal and external processes.

1st advantage: Increasing user friendliness

There is much to be said for the following assertion: the high user friendliness and intuitive user guidance are key success factors for digital champions such as Amazon, Apple, Google, Netflix and Uber.

The clear figures support this determination: according to a CEI survey, 86 percent of buyers are willing to pay more for better user friendliness. That's the good news. But here's the bad news: only 1 percent of customers had the impression that providers consistently meet their expectations in this regard.

According to a further study by PWC, 73% of buyers report that the customer experiences is a key purchasing criterion. The gap between the desired, positive user experience and the actual user experience, however, is huge – between 10% and 33% depending on the industry.

On the other hand, our everyday experience alone shows us why simple onboarding and authentication processes are useful. After all, if you confirm a flight ticket purchase with a fingerprint, make online purchases using an app and the login for online banking can only be carried out via ambient noises, then this is not just secure but also a lot of fun.

2nd advantage: Reducing costs

Security is expensive. This is also the case when implementing 2FA. However, certain costs can also be saved when it comes to security – depending on how intelligent the selected solution is. This relates to both expenditures during implementation as well as during the ongoing operation.

Many businesses still use SMS and mTAN as a 2FA method. This is dubious not only in the context of security. SMS also performs poorly in terms of cost efficiency. Businesses that switch to another second factor quickly save five to six-figure amounts in telecommunication costs alone.

Another cost driver is the volume of enquiries sent to a company's helpdesk. Research shows that on average, 40% of a Swiss financial services provider's support calls relate to login and onboarding issues. This results in huge financial expenditures for something that users could implement themselves through 2FA and thought-out user self services – user self-services which are quicker and more convenient for customers.

And when implementing 2FA? Here, the combination of 2FA and cIAM can show off its full potential, as a high level of standardisation means there are virtually no initial expenditures. A further advantage is that in combination with cIAM, communication with customers is fully automated, so technical work when migrating and rolling out new second factors tends to approach nil.

3rd advantage: Increasing security

Double-checked means doubly secure – this is the fundamental logic of 2FA. In addition to this significant advantage, the use of a multi-factor authentication, as in the airport analogy above, boasts numerous other security advantages.

Fundamentally, it can be observed that a single factor is simply no longer enough for the secure authentication of users and identities. Reverting to SMS and mTAN as a second factor is also seen as outdated. Smishing (SMS phishing attempts) has become a real problem, and many mobile operators want to block sending SMS abroad. Mobile apps with personal keys on your own smartphone are thus the better alternative.

In addition, 2FA combined with cIAM offers added values which are becoming increasingly important. Transaction approvals (also known as transaction signing) are a good example in this regard. Approval for a transaction is requested through an individual interaction with the customer.

5 Airlock 2FA

How does one achieve the ideal combination of user friendliness, cost reduction and higher security levels? This question is key when selecting the second factor. Dynamic solutions are now available so you can respond to different application cases according to the risk. The advantage of risk-based authentication is a seamless authentication process which meets both requirements – security and user friendliness.

Zero touch

It couldn't be easier: a unique 2FA which enables a secure login without any user interaction. Zero touch uses information about your surroundings, making logging in easier than ever before.

UX: ⊕⊕⊕ Security: ⊕⊕ Costs: ⊕⊕⊕ Online

One touch

With the aid of **push notifications** via Airlock 2FA, users simply need to touch the display once to confirm a login or approve a transaction. This is also additionally secured via fingerprint or facial recognition.

UX: ⊕⊕ Security: ⊕⊕⊕ Costs: ⊕⊕⊕ Online

(Offline) QR code

Users can scan a QR code with Airlock 2FA to log in or authorise a transaction within seconds, even if they're offline.

UX: ⊕ Security: ⊕⊕⊕ Costs: ⊕⊕⊕ Online

Passcode

Airlock 2FA automatically generates a new one-time password (OTP) every 30 seconds. Users can thus approve their activities without Internet access.

UX: ⊖ Security: ⊕⊕⊕ Costs: ⊕⊕⊕ Online

Airlock Secure Access Hub: everything from one source!

Of course, the more integrated a system is, the better it performs. This is why a Secure Access Hub which includes and connects WAF, API Gateway, cIAM and 2FA is the ideal solution. The key advantages of this solution are the top-level security with low costs in a comprehensive solution which enables efficient application development and a quick time to market, without having to laboriously coordinate the individual components of different manufacturers.

Option	User friendliness	Security	Desktop	Single device authentication (mobile only)	Offline
2-factor authentication					
Zero-Touch	⊕⊕⊕	⊕⊕	●	●	
One-Touch	⊕⊕	⊕⊕⊕	●	●	
Offline QR-Code	⊕	⊕⊕⊕	●		●
Passcode	⊕	⊕	●	●	●
Transaction approval					
One-Touch	⊕⊕	⊕⊕⊕	●	●	
Offline QR-Code	⊕	⊕⊕⊕	●		●
Password-free authentication					
One-Touch	⊕⊕	⊕⊕⊕	●	●	
Offline QR-Code	⊕	⊕⊕⊕	●	●	●

⊕⊕⊕ Outstanding ⊕⊕ Very good ⊕ Good ● Airlock 2FA

6 Glossary

- **Two-factor authentication (2FA):** describes the verification of a user's identity by means of the combination of two different and especially independent components from the variants knowledge, possession and being.

- **Multi-factor authentication (MFA):** describes a generalisation of two-factor authentication, in which access authorisation is checked based on several independent features (factors).

- **Strong customer authentication (SCA):** is another term for two-factor authentication.

- **3-D secure protocol**: also known as 3DS is used especially for online shopping. Buyers must authenticate themselves to their bank as legitimate cardholders. To complete the ordering process, 3-D Secure requires a code or sends a push message to the customer.

- **One touch:** refers to an authentication variant of Airlock 2FA that requires minimal user interaction.

- **Zero touch:** describes an authentication variant of Airlock 2FA that requires no user interaction.

- **Certificate authentication:** Strong authentication method based on electronic certificates (typically according to X.509 standard). The certificate respectively its private key is stored on a USB token, a smartcard or a soft token. Depending on the application, a PKI (public key infrastructure) may be required.

- **TAN lists:** The user receives a letter with a list of TAN codes (cross-off list), each of which can only be used once. Entering the code fulfils the second factor.

- **Token:** a hardware or software component for identification and authentication of users. It is usually used in combination with a password or pin.

- **mTAN:** To use this method, the user requires a mobile phone with SMS function and must register the mobile phone number with the supplier. A security code, valid once, is sent by SMS and typed in by the user.

- **OTP:** stands for "One-Time Password" and is used in different authentication variants such as mTAN. OTPs are often generated time-dependent in hardware tokens or apps.

- **Push:** The user receives either a message via push to a special smartphone app, which he can confirm or reject, or he receives a transaction code, also called pushTAN, which he enters. The procedure is often used to confirm transactions (transaction approval or transaction signing), as it is easy to transmit and display transaction data.

- **QR Code Authentication:** With a Smarphone App or a hardware token, a QR Code (two-dimensional barcode) is scanned and an OTP is calculated using cryptographic key material. This OTP is then entered by the user to confirm the proof of identity or a transaction.

- **Challenge Response:** The term “Challenge Response” covers all procedures in which a challenge – often a random value - is sent from the server to the authentication token, where it is offset against secret key material and sent back to the server (“Response”). Many authentication methods are based on this principle. Examples: Certificate authentication, QR code login, matrix cards, push.

- **Authentication:** is the process by which the user logs on to a service. (e.g. entering user name and password). It is therefore the login process from the user's perspective.

- **Authentification:** is the verification of the login of an identity. It is therefore the login process from the server's point of view.