The world's most advanced authentication system

ON AUTHENTICATION

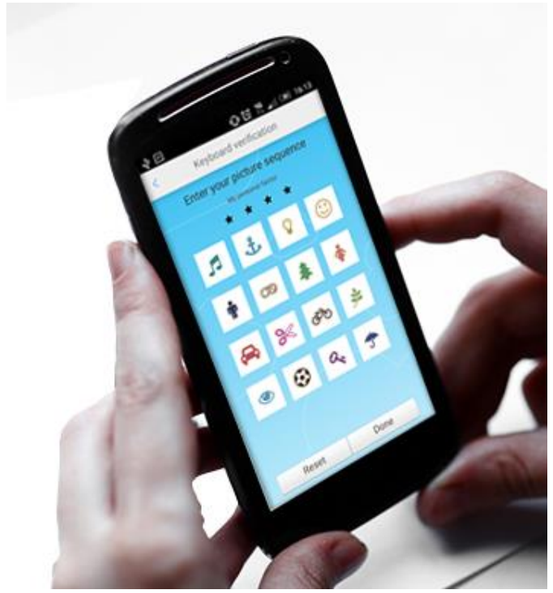
A large and ever-growing part of our work and personal lives has moved online… and so have criminals. When stealing your sensitive information assets or money, attackers no longer steal your wallet, PC or phone. Nowadays, in most cases, they steal your identity online. It is much easier for them and you won´t even notice until it´s too late.

To increase your protection online it is essential to have strong authentication – if you cannot distinguish an attacker from a rightful user, all other security measures are at risk, if not totally useless.

In today's online world, around 90 % of all authentication transactions are still based on login & password, a method more than 50 years old. This method is increasingly insecure – serious security breaches occur every day due to compromised passwords.

At the same time, it is inconvenient: users have 30 online accounts on average. Who can remember all the passwords for numerous online accounts? Average users can't, and so they use weak passwords and/or re-use the same password for several accounts, which again results in more security breaches.

Many online services started to add other security factors to the conventional password login, such as OTP, SMS or digital certificates. This is, however, more costly, inconvenient for users and often still not secure enough to protect them from attacks. www.aducid.com



ADUCID

The patented ADUCID authentication technology is the right answer to all of these pressing issues.

ADUCID introduces a novel concept of authentication which protects users from all types of authentication attacks known today, completely eliminates phishing, and on top of that requires no passwords at all.

ADUCID offers you a tool which will take care of authentication of users for them and simply protect their accounts from attacks better than any solution before.

No more passwords to remember, no more renewals, no more additional hardware, no more retyping of SMS or OTPs – and you can still enjoy the highest level of security when accessing online accounts from any preferred device.

DESCRIPTION

ADUCID was primarily designed to secure the access to online services which work with valuable information assets. ADUCID consists of two components.

Users have their PEIGs, software for secure authentication, which is basically a set of software boxes for cyber identities of end users. PEIG can be stored on their smart phone, PC, Mac, tablet or USB.

Each user can have several PEIGs on different devices, which are simultaneously pointing to the same user (real identity) – the loss of user´s PEIG thus does not stop the user from continuing their work. Each PEIG can guard an unlimited number of unique private key sets to an unlimited number of services/online applications.

On the provider´s side, there is AIM – a virtual authentication server integrated with the target application(s). AIM can hold on to an unlimited number of unique private keys sets for an unlimited number of users; ADUCID acts as a transparent authentication layer used by the target application – either using the supplied adapter, or through the provided API.

FEATURES

MAXIMUM USER COMFORT

- No passwords - just simple clicks and taps

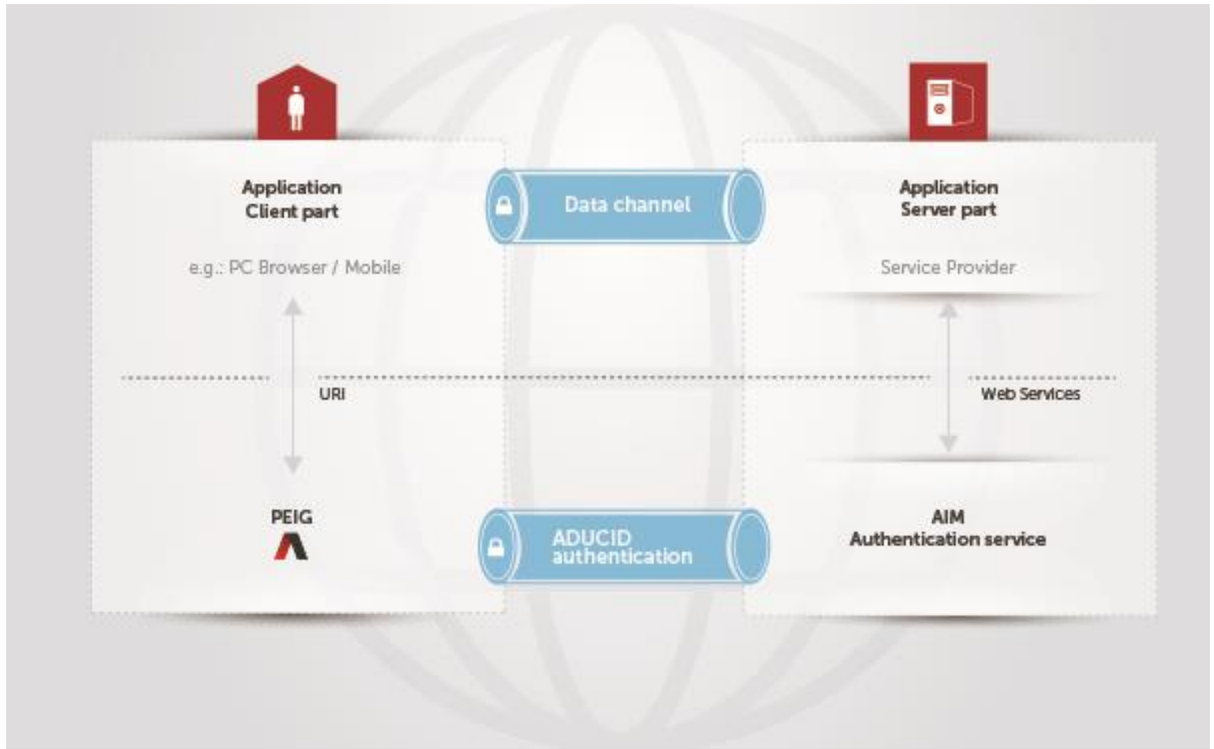
- No passwords – just simple clicks and taps
- No renewals of credentials
- No additional HW – nothing to retype (no SMS, no OTPs)
- Device freedom
- Self-service backup and recovery

SUPERIOR LEVEL OF SECURITY

- Strong asymmetric cryptography
- Multiple-factor local protection (incl. NFC and Bluetooth)
- Native mutual authentication against phishing
- No personal-related information go through public networks
- Anti-copy & anti-attack
- Authentication traceable – accountability

OPERATIONAL EFFICIENCY

- Identity management can be
  - In house
  - Outsourced by third party
  - Shared with an entrusted partner
- Identity life cycle is fully automated
- Several ID proofing methods are incorporated
- No costly additional channels (HW or SMS, etc.)



PLATFORM & OPERATING SYSTEMS

SDK & adapters included:
Tomcat, Spring Security, Java SDK, PHP SDK, C SDK (Windows/Linux)

End user platforms:
Windows, Android, iOS, OS X

YOU WILL BENEFIT FROM:

Improved protection of your online assets
Simpler access to online accounts for your clients
No additional costs (SMS or tokens)
Platform independence

IMPLEMENTATION SCENARIO

ADUCID is an independent authentication service, taking care of all security matters for you, incl. encryption, authentication, security policies, breach detection, recovery and others.

Once switching to ADUCID authentication, the service provider receives an AIM, a virtual appliance (VMware) which can be installed in a private IT environment. Another option is to use AIM in a public cloud under the AaaS model.

The integration of AIM with the target application(s) is just a matter of days – basically, it means embedding only a few authentication code lines whereas the particular SDKs are provided. The communication between AIM and the application server is based on a few web service calls.

The ADUCID team and its partners offer consulting as well as active assistance throughout the implementation phase.

The next step after integrating AIM with the target application(s) is to redesign the connected identity management processes, such as administration of user rights or log management, and to define distribution of PEIGs among the clients of the service.

IDENTITY PROOFING

It is important during the implementation phase to define how to migrate the existing clients to ADUCID and how to handle the identity proofing of new clients. ADUCID supports several identity proofing methods which are already incorporated in the solution by design.

- EXISTING CLIENTS

Migration of the existing clients to ADUCID is simple: the clients log into their accounts using their prior authentication (the existing credentials), and confirm the upgrade to ADUCID using the PEIG installed on one of their devices with just 1 click or 1 QR code scan.

- NEW CLIENTS

New clients of each particular service go through a certain procedure when opening an account. The registration process can remain unchanged; however, ADUCID supports multi-factor identity verification at registration (using pairing keys) or ID verification (using entrusted 3rd party services).

USER EXPERIENCE

GETTING STARTED

After being notified that their service provider has upgraded the authentication to ADUCID, the user downloads PEIG to their smart phone or other preferred device. PEIG is freely distributed on App Store, Google Play, the website of the service provider or it can be even embedded in the native app of the service provider (in this case, switching to ADUCID is nearly invisible to the user). After downloading PEIG to the device, PEIG is still an empty “box” to user´s future unique electronic credentials.

ADUCID LOGIN

When logging into a user account with ADUCID, the user can access the account directly on the device with PEIG by simply entering the desired web page and going to login without typing any name or password. Then ADUCID takes care of the dual-channel authentication for the user.

However, authentication via ADUCID doesn’t require PEIG to be installed locally. Users may use their phone/tablet with ADUCID PEIG to scan a QR code from any public PC, ATM, TV or other screen in order to login to these devices effortlessly.

1-click login – PC & PEIG

1-click login – smart phone & PEIG

1-click login – smart phone & PEIG

ESTABLISHING CYBER CREDENTIALS

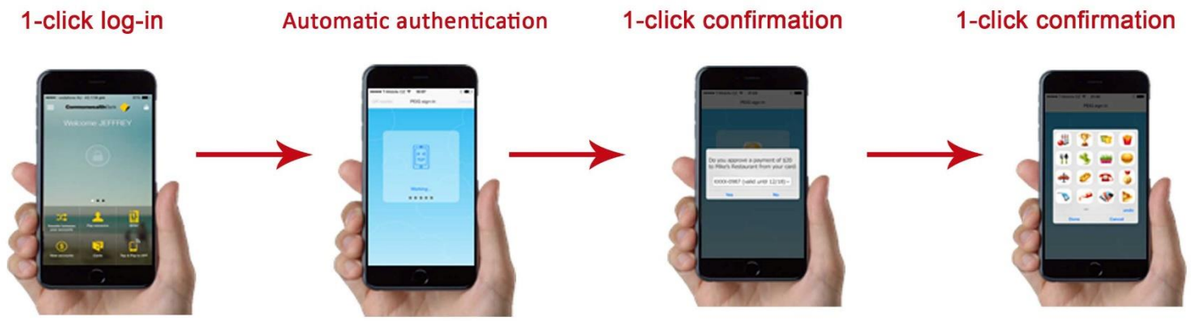
After installing PEIG, users enter the desired web application for the first time, and AIM automatically recognizes a new user. Once the users confirm that they are entitled to access their user account, ADUCID automatically generates a unique key set for the particular user, their cyber credentials, and since that moment AIM will always recognize the particular PEIG. Again, this requires only 1-click confirmation or 1 QR scan instead of creating e.g. a new username & password.

IDENTITY PROOFING

The final step is to confirm user´s real identity through one of the above-mentioned identity proofing methods. Since that moment, the user can safely access their account with just one click or simply by reading a QR code (on an unfamiliar device), and make even the most sensitive transactions online.

To ensure the highest level of security, ADUCID employs an adaptive multi-factor protection (see later) in addition to other security attributes.

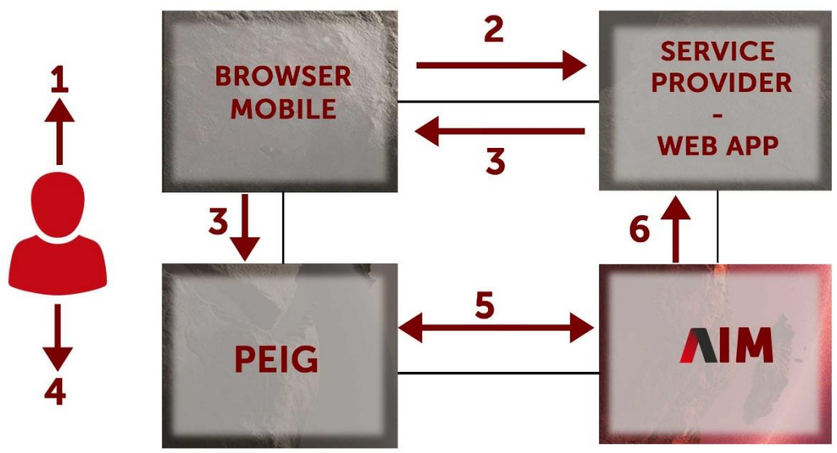
LOGIN & TRANSACTION CONFIRMATION



AUTHENTICATION PROCESS

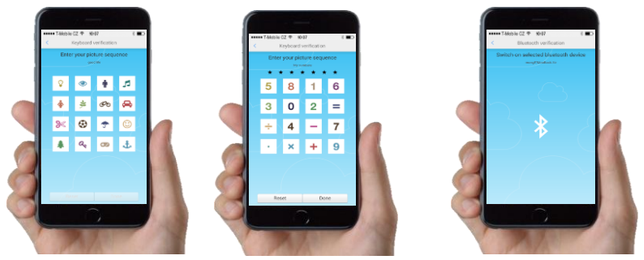
The process that is behind ADUCID login:

1. User enters the web page/application of the service provider
2. The web application ”asks” AIM to authenticate the user
3. AIM issues a session number to the web application and a URL of AIM which is passed to the user through the original data channel (see the scheme above)
4. The user reads the generated QR code with PEIG on their smart phone or the authentication happens automatically when the users are logging in on a device with PEIG
5. PEIG approaches AIM, and they authenticate each other using a separate ADUCID authentication channel
6. AIM provides the application with information about the authenticated user



ADAPTIVE MULTI-FACTOR

ADUCID incorporates several additional factors that strengthen the security of user authentication. The first security factor is the ownership of PEIG itself. In addition to that, ADUCID offers other factors – PIN, picture secret (higher entropy than with a classic PIN), NFC or Bluetooth (not only) wearables. In the coming versions, biometrics will be supported as well.



NFC in alpha on Android

Any biometrics or other factors can be added within weeks

What sets ADUCID apart from other authentication methods is using the second factor only locally – therefore, no secret travels online or is held by the server on the back-end, and thus it cannot be compromised online. More specifically, ADUCID converts all users´ local factors into discrete pseudorandomly generated dynamically changing identifiers that are never stored and can be evaluated only by AIM. This means that ADUCID users never have their biometrics, PINs or other factors compromised, even when users´ devices, communication channels or user databases themselves do get compromised.

The multi-factor protection by ADUCID is adaptive. In other words, the service provider decides if and when the additional security factor is to be used – during login, during certain transactions or not at all.

DISTINGUISHING SECURITY FEATURES – SUMMARY

ADUCID has been developed by world's leading experts in authentication, cryptography and other security areas and the novel concept of ADUCID technology has been patented worldwide.

ADUCID eliminates all security problems in authentication such as phishing, man-in-the-middle, eavesdropping or hacks on identity servers, and securely handles authentication even if the communication channel or the network security is compromised.

This is because ADUCID opens a separate secured authentication channel during the authentication process between the user´s device and the target application which doesn´t rely on the security of the original data channel nor any other authentication (such as TLS) or file system encryption.

BACK UP

With ADUCID each user can back up their ADUCID credentials (PEIG) on an unlimited number of devices – another smart phone, tablet, PC, etc.

Service providers can limit or enable users to have multiple PEIG devices in order to find the right balance between control and recovery when losing a device. Users can be provided with self-care functions, which will enable them to deactivate and re-activate any of their devices without interacting with customer support.

The process of creating security back-up credentials is very simple and consists of only a few steps. When creating security back-up credentials on a different device, the same additional local factor from the original PEIG becomes automatically active with the new PEIG too (e.g. the same picture secret).

ADUCID security backup is not a copied PEIG. It is a new PEIG with a new set of unique credentials pointing to the same user.

By design, ADUCID uses an active anti-copy mechanism, which reliably detects an unauthorized copy of user´s PEIG.

Security attributes of ADUCID authentication

- Strong **modular asymmetric cryptography**

- **Mutual authentication eliminating phishing** attacks
  - The logic of ADUCID technology is based on a corresponding pair of unique keys (2 opposite pairs of public and private keys) on both the provider´s and end user´s side

- ADUCID enables adaptive incorporation of **local multi-factor protection** (picture sequence, PIN, NFC, Bluetooth)
  - No shared secret which could be compromised (such as password) is transmitted online during the authentication session

- Own UACP – **Universal Authentication Cryptographic Protocol** – resistant to all known authentication attacks
  - Uses a separate cryptography layer (no need to code in the target application)
  - Open to different types of key-material (encryption)
  - Open to different cryptographic algorithms & parameters, even the future cryptography algorithms
  - Unlike others, ADUCID:
    - can upgrade cryptography & security parameters “on the fly” (e.g. automated re-encryption of the unique keys)

- ADUCID is based on distributed topology – unlike other PKI authentication mechanisms, ADUCID has **no Single-point-of-failure** and is not threatened by compromised certification authority

- Active **Anti-Attack** mechanism – recognition of an active attacker

- Active **Anti-Copy** mechanism – protection against the copy of user´s credentials

- **Security Replicas** – no loss of credentials in case there is an incident (self-service)

- Active **protection of the data channel** – “binding” – ADUCID can detect an attacker on the data channel

- ADUCID enables collection of relevant authentication data, such as users device ID, GPS, time, etc. to be used **to support today´s sophisticated Fraud Detection Systems**

OTHER USE CASES

- ADUCID ELECTRONIC SIGNATURE & DOCUMENT ENCRYPTION

Unprecedented protection of ADUCID unique keys for electronic signatures and document encryption

- INTERNET OF THINGS

Secure access and communication of M2M or server-to-server. ADUCID “machine-oriented” authentication solution enables fully automated and remotely manageable authentication and secure communication

- ADUCID VPN – TLS AUTHENTICATION

100% end-to-end security of communication – ADUCID VPN and ADUCID TLS authentication

- WI-FI AUTHENTICATION

Secure access to internal WI-FI – ADUCID Authentication proxy server for guest as well as employee WI-FI networks

BEYOND ONLINE AUTHENTICATION

Touch-free ATM withdrawals

POS purchases

P2P payments

ADUCID