ADUCID

Simple login.
Secure authentication.

We provide strong customer authentication for eID solutions in eGovernment and eBanking that enables **user login, virtual transactions and online digital signatures** with NIST, eIDAS, PSD2 and EBA compliancy.

CONTENTS

ON AUTHENTICATION

May it be your clients' emails, photos, important documents or bank accounts, a large and ever-growing part of our work and personal lives has moved online. 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 it is not possible to 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.

This method is increasingly insecure – serious security breaches occur every day due to compromised passwords.

At the same time, it is inconvenient – users have 100 online accounts on average and in 2020 the average number will be around 200 accounts per internet user. Who can remember all the passwords for numerous online accounts? 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.

All of this is not news and 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 and their data from attacks.

INTRODUCING ADUCID

The patented authentication technology is the right answer to all of the pressing issues mentioned above.

It 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 user names or passwords at all.

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

It is an external authentication solution with focus on fast and flexible integration into existing applications and it is ready for use in securing online payments or electronic signatures. It can also be provided "as a service". Our protocol uses a dedicated channel for authentication.

No passwords to remember, no renewals, no additional hardware, no retyping of SMS or OTPs. Just simple login for the users and secure authentication for the providers. Everything automatically.

DESCRIPTION

ADUCID was primarily designed to secure the access to online services which work with valuable information assets. It achieves this by using two components:

Users have their PEIGs (*Personal Electronic Identity Guardian*) – 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 practically unlimited number of unique private key sets to any number of services/online applications.

Providers manage their AIMs (*ADUCID Identity Machine*) – a virtual authentication server integrated with the target application(s). An 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. It can also be operated/provided "as a service".

FEATURES

MAXIMUM USER COMFORT

- No passwords
- No renewals of credentials
- No additional HW
- Nothing to retype (no SMS, no OTPs)
- Device freedom

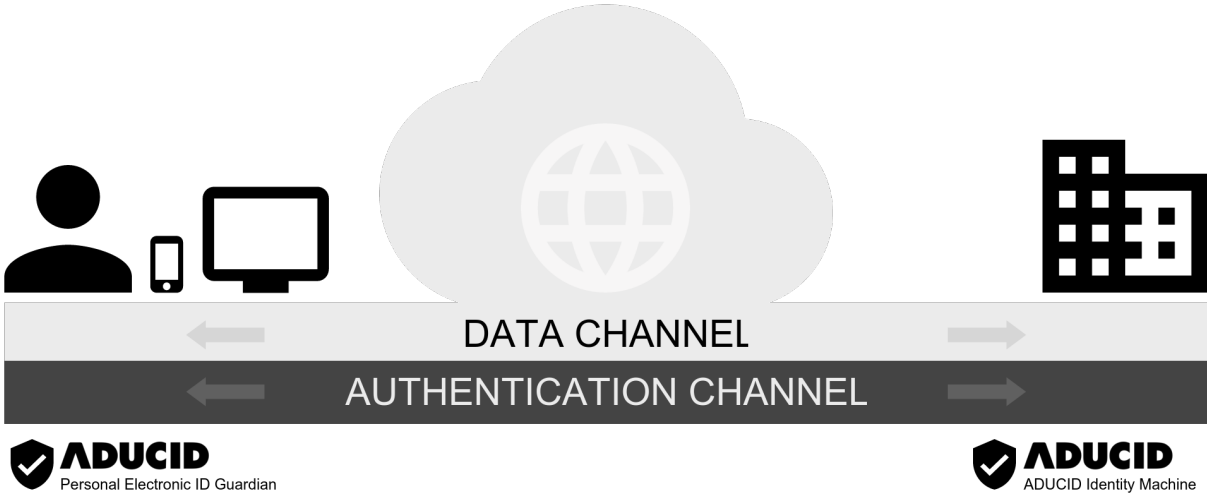
SUPERIOR LEVEL OF SECURITY

- Strong asymmetric cryptography
- Multiple-factor local protection (incl. NFC, Touch ID and other local biometric auth.)
- Mutual authentication protects against phishing
- No personal-related information go through public networks
- Authentication traceable – accountability
- Anti-copy & anti-attack

OPERATIONAL EFFICIENCY

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

ARCHITECTURE



Authentication flow

STEP 1: User (left) initiates communication with the web server by opening a new window in a web browser. Provider's web server detects the presence of client app (PEIG) and provides the web address of the authentication server (AIM).

STEP 2: Provider's web server detects the presence of client app (PEIG) and provides the web address of the authentication server (AIM) through the web browser.

STEP 3: PEIG (client app) receives the address of the authentication server and initiates communication with AIM (auth server) via independent authentication channel.

STEP 4: Once the authentication channel is opened, authentication protocols are initiated and mutual authentication of both devices is attempted.

STEP 5: Successful mutual authentication is passed on to the application web server which then provides the user with access to his account and/or other valuable assets.

PLATFORMS & OS

SDK & ADAPTERS INCLUDED

Tomcat, Spring Security, Java SDK, PHP SDK, C SDK (Windows/Linux)

END-USER PLATFORMS

Windows, Android, iOS, OS X

TECHNOLOGY COMPARISON

	PASSWORD	SMS OTP	SMART CARD	ADUCID
No Weak Credentials		✓	✓	✓
No Reuse of Credentials		✓	✓	✓
ID Database Hack Protection			✓	✓
Malware Protection			✓	✓
Eavesdropping Protection				✓
Phishing & MITM Protection				✓
Anti-copy Protection				✓
Simple Integration	✓			✓
Inexpensive Infrastructure	✓			✓
Inexpensive Maintenance				✓

TECHNICAL SUMMARY

IMPLEMENTATION SCENARIO

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

ADUCID can serve as a unique authentication for your online services as well as a complementary authentication next to other existing authentication methods.

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

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.

It is also 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.

MIGRATING 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.

IDENTITY PROOFING OF NEW CLIENTS

Registration processes of new clients to your service can remain unchanged. Whether it be registration at a branch office or submitting a form online - ADUCID technology does not restrict how your business registers new clients.

With ADUCID you can also adopt a registered client from a 3rd party provider your company trusts. The new client simply registers online; an identity is created for her at your services and it is paired with an already existing identity from another service where the client is already registered.

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.

ESTABLISHING CYBER CREDENTIALS

After installing PEIG, users enter the desired web application for the first time, and AIM automatically recognises 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 recognise the particular PEIG. This requires only one click confirmation or one QR code scan instead of creating a new username and& password e.g.

IDENTITY PROOFING

In use cases where it is needed the final step is to confirm user´s real identity through one of the above-mentioned identity proofing methods (see section IMPLEMENTATION SCENARIO).

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.

There are also scenarios supported where the users use the service without any identity proofing and work in a semi-anonymous mode. The online service then recognises the particular users, however, does not require their real identity or private data.

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 automatically takes care of the dual-channel authentication for the user.

However, authentication via ADUCID doesn't require PEIG to be installed on every device. Users may use the PEIG on their smart phone or tablet to scan an authentication QR code to login using any public PC, ATM, TV or other device with a display and an internet connection.

TRANSACTION CONFIRMATION

When completing an on-line transaction, the user is notified about transaction details on their device with PEIG and a confirmation is requested. The transaction notifications are delivered to users device via a secure ADUCID channel. Optionally, the user may be asked to enter a security factor such as PIN or NFC (see section ADAPTIVE MULTI-FACTOR below).

ADAPTIVE MULTI-FACTOR

ADUCID incorporates several additional factors that strengthen the security of user authentication.

The first security factor is the ownership of the PEIG itself. In addition to that, ADUCID offers other factors – PIN, picture PIN (higher entropy than classic PIN), NFC and Apple Touch ID (other biometrics are in development).

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. It cannot be compromised online.

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 operations or not at all.

IDENTITY REPLICA

With ADUCID each user can replicate their ADUCID credentials (PEIG) on other devices – another smart phone, tablet, PC, etc. This replica can be used as a separate authentication device or serve as a "back-up" in case of an emergency.

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 fully functional 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 the use of an unauthorised copy of user´s PEIG.

DISTINGUISHING SECURITY FEATURES – SUMMARY

ADUCID has been developed by world's leading experts in authentication, cryptography and other security fields.

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.

SECURITY ATTRIBUTES OF ADUCID AUTHENTICATION

- Strong modular asymmetric cryptography (using elliptical curves)
- 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, Apple TouchID)
    - 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 cryptomaterial
    - Open to different cryptographic algorithms & parameters, even 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 based 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

BEYOND ONLINE AUTHENTICATION

Touch-free ATM withdrawals

POS purchases

P2P payments

OTHER USE CASES

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 – VPN and TLS authentication.

WI-FI AUTHENTICATION

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

ADUCID ELECTRONIC SIGNATURE & DOCUMENT ENCRYPTION

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

WHAT'S NEW IN VERSION 3.1

Substantial improvements to integration capabilities

- PEIG API – new interface for integrating PEIG with other mobile apps
- Embedding of PEIG directly into another mobile app
- SDK now enables embedding authentication QR code directly into a web page
- Improvements to server-side integration – Web Service WSA, Web SDK, Advanced SDK

Support of identity proofing processes

- QR proofing – fastest identity proofing
- Pre-configured identity proofing operations included – SDK, Web Service
- Sample identity proofing apps

Improvements to Personal Factor

- Apple Touch ID as a Personal Factor
- Removal of cryptographic weaknesses of the Personal Factor

Improvements to management of AIM server

- 3 new management apps – UserAdmin, SecurityAdmin, RoleAdmin
- Improved access statistics – based on type of PEIG, OS, type of operation e.g.
- New logs

New demo apps (launched together with version 3.1)

- demo e-commerce site with digital products
- companion mobile app for our online banking demo "DemoBank" on Android and iOS
- improvements to DemoBank

Other improvements

- Elliptical curves support (as part of new UACP2 protocol)
- Code optimisation, new tests
- Preparation for M2M deployment