ADUCID Architecture

Version 3.0.4

Release date	February 1, 2016

Antala Staška 2027/79, 140 00 Prague 4 | T +420 271 100 100 | F +420 271 100 101
Vídeňská 125, 619 00 Brno | T +420 547 100 100 | F +420 547 100 101
Sady 5. května 59, 301 00 Pilsen | T +420 271 100 100 | F +420 271 100 101
Teslova 30, 821 02 Bratislava | T +421 (2) 4821 3111 | F +421 (2) 4821 3199

ISO 9001 ISO 14001 ISO/IEC 27001 ISO/IEC 20000

CZ > Corp. ID 25313029 | Registration Court RC Brno, File no. B2113
SK > Corp. ID 35787546 | Commercial Register DC Bratislava, Section Sa file 2431/B

Table of Contents

1. Purpose of this document

This document describes ADUCID® at the system level necessary for integrating with target application.

To understand this document, the reader is required to have knowledge of web technologies, programming and integration of web applications.

2. Basic components

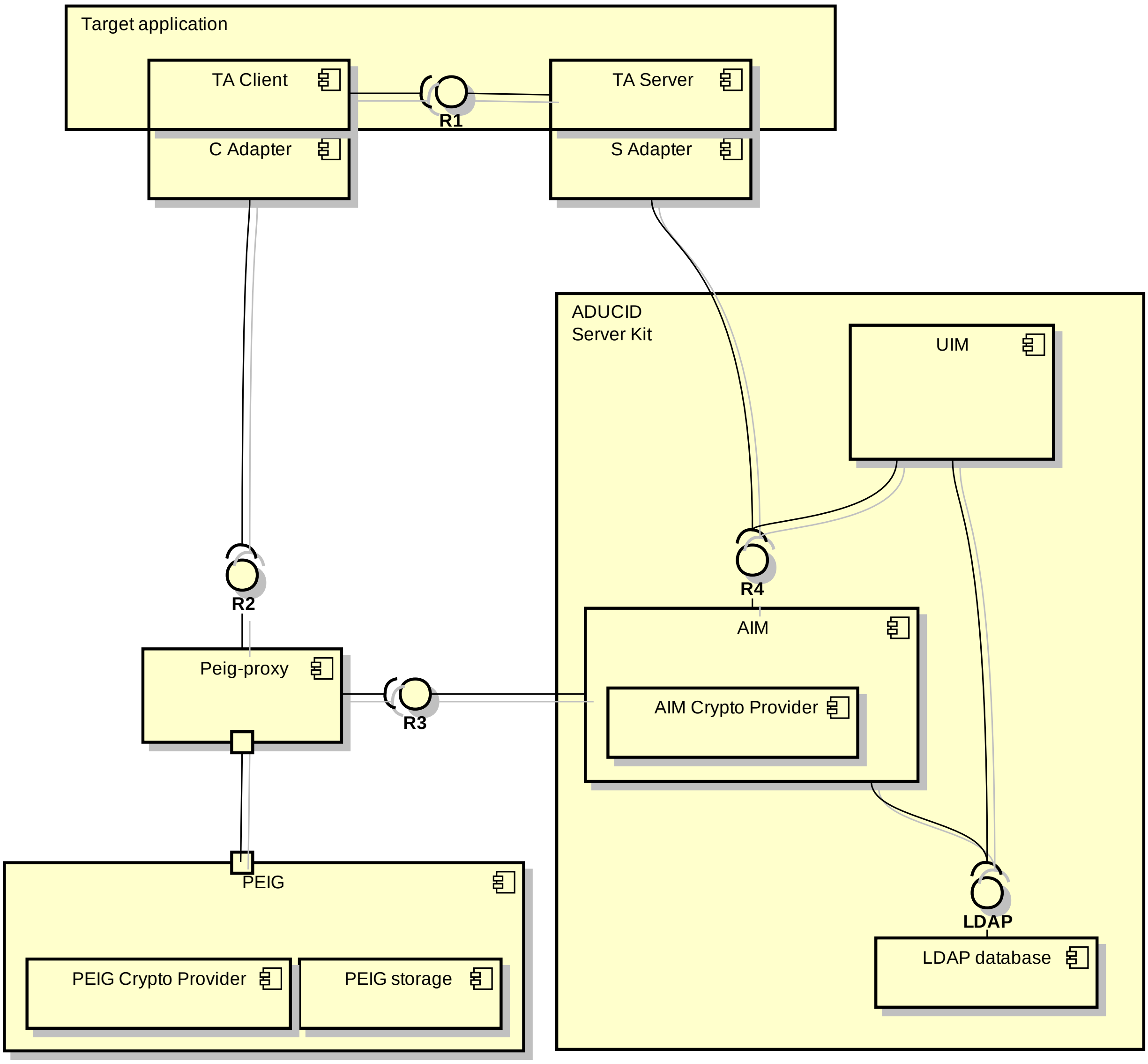


Figure 2-1 ADUCID® system diagram for integration

2.1. Target application

Target application is any application that uses ADUCID® services. Examples of such applications include web applications with standard thin client (standard browser), classic client-server applications, or even universal system tools which are not normally viewed as applications, e.g. a VPN system for remote access, Wi-Fi connection, terminal access (e.g. X terminal), etc.

From the system point of view, the application consists of a client part and a server part (TA Client and TA Server), which communicate with each other in their own manner via an R1 interface.

2.2. Server part of ADUCID®

The server part of ADUCID® consists of following parts:

- AIM – ADUCID® Identity Machine – delivers ADUCID® server functionality, performs all ADUCID® operations and provides access to user data stored along with electronic identities in the LDAP database.
  AIM is controlled by the target application using the R4 interface. Using this interface, it also provides services for working with user data.
  Using the R3 interface, it communicates with the client part of ADUCID®.
  Another part of AIM is the provider of cryptographic services (AIM Crypto Provider) that can be implemented through different manners - e.g. as a software library or hardware device (HSM, etc.).
- Data for electronic identities and user data along with other operational data is stored in the standard LDAP database.
- UIM is a web application used to administer ADUCID® and can also be used to administer users for a target application or multiple target applications. In addition to this, administration of users can also be provided through a certain target application.

The entire server part of ADUCID® along with the operating system and all third-party systems required to operate the server part of ADUCID® are supplied as complete virtual appliances (Orange Box).

2.3. Client part of ADUCID®

PEIG® is the fundamental client element of ADUCID® that fully manages electronic identities of its user.

PEIG documentation is located at http://www.aducid.com/support

Currently, PEIG is supported on Windows 7, Windows 8, Mac OS X, Android (4.0+) and iOS 7+ devices

Windows machines also support PEIG located on a USB token.

2.3.1. Windows PEIG PC, OSX PEIG

PEIG can run on the same computer as the target application client. PEIG communicates with the target application by using the internal communication of the host operating system. A separate PEIG-proxy is used.

PEIG®-proxy functions as a communications module for the client part that connects the client part of the target application to PEIG®, and also as an application firewall that protects PEIG®. PEIG®-proxy must be run on the same computer as the client part of the target application (in contrast to PEIG®, which may be on a different device carried by the user).

PEIG®-proxy contains no user data.

PEIG®-proxy provides ADUCID® services via the R2 interface. This is used to initiate the activity of PEIG® and transmit outputs of the client part of the target application.

2.3.2. Windows PEIG USB

PEIG can be also used from USB storage. This type is supported only on Windows platform.

2.3.3. iOS PEIG and Android PEIG

PEIG can run on a mobile phone (Android 4.0+ or iOS). Two communication options exist in the case:

- QR code
- aducid:// URI schema

The mobile phone presents an authentication token in the case of QR code usage. A user can log in into the target application by taking a QR code snapshot. It is possible to do this in the case of a remote desktop, as well. It is possible even if no ADUCID software is installed on the client computer.

The mobile phone runs the client part of target application, together with PEIG in the case of aducid:// URI schema usage. The applications communicate with each other as expected in mobile phone operating systems.

The PEIG Mobile supports internal data saving in mobile phone internal storage only.

2.4. Adapters

Special adapters are developed and supplied to simplify the integration of target applications. The client adapter (C Adapter) communicates with the client part of the target application; the server adapter (S Adapter) communicates with the server part of the target application.

The interface between the adapter and target application is the specific interface of that particular application.

For example, for standard web applications, the client interface is either an HTTP interface for a redirect adapter, or an internal interface of the respective browser for a plug-in adapter.

Adapters communicate with the rest of ADUCID® using standard interfaces (R2 and R4).

The target application can, but is not required to, use the adapters. It can communicate with ADUCID® directly using the R2 and R4 interfaces.

3. Communication between components

A fundamental unit of activity in ADUCID® is an operation. Such operation can be an authentication, creation (initialization) of an electronic identity, a change in electronic identity, etc. Operations can have their own parameters.

The server part of the target application first requests the required operation via the R4 control interface and specifies its AIM parameters.

The result is a unique, one-time authId operation identifier that can be initiated either by the target application or AIM.

The client part of the target application transmits the PEIG®-proxy startup event through the R2 interface. The startup event includes authId and the R3 interface URL.

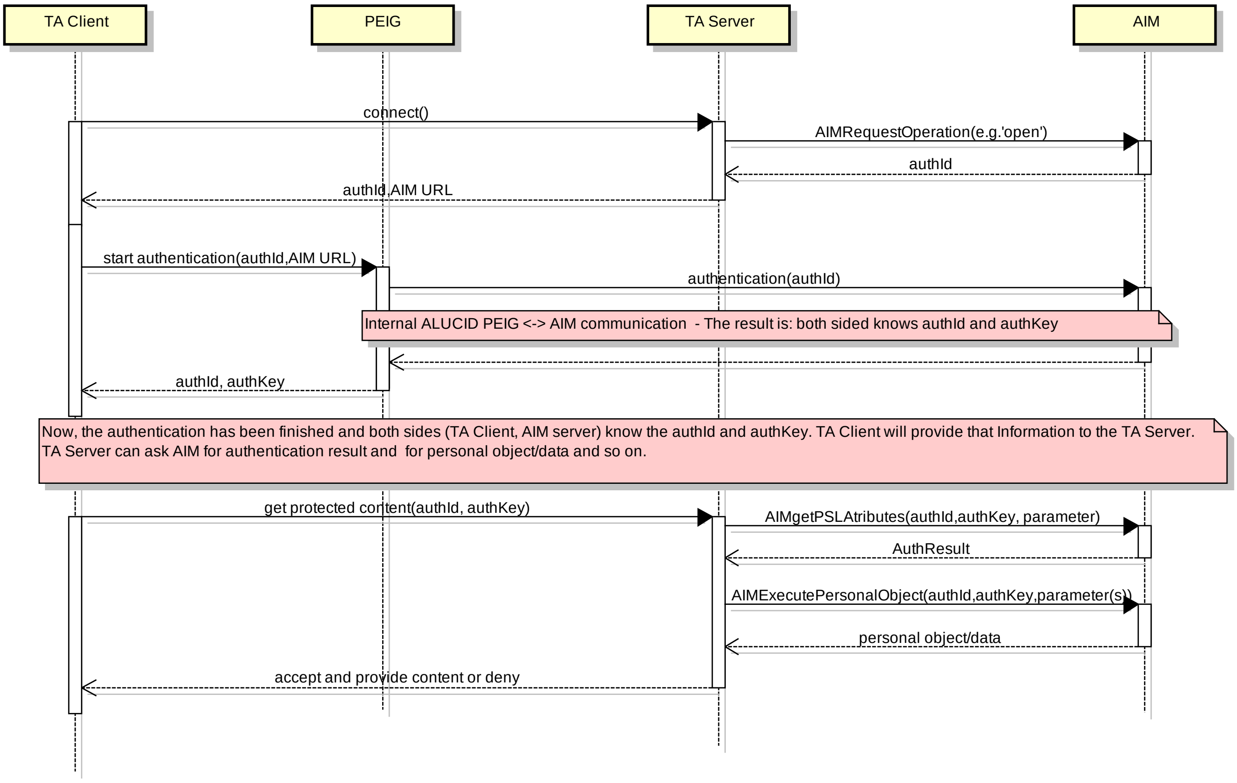
Communication between the client part and the server part of the target application via the R1 interface is handled internally by the target application.

The startup event from the R2 interface of PEIG®-proxy is transmitted to PEIG®. PEIG® then starts processing the operation by transmitting the authId to R3 URL (via PEIG®-proxy). AIM manages the entire operation process that consists of transmitting and processing several messages between PEIG® and AIM.

In terms of communication, PEIG® is a client, or more precisely, a PEIG®-proxy client and an AIM server. In terms of control, the operation is managed by the AIM (based on target application request submission).

When the operation is concluded, a random, one-time secret authKey is generated on PEIG® (if successful), which is then transmitted to the client part of the target application along with authId via PEIG®-proxy and R2.

The server part uses authId and authKey for further communication with AIM via the R4 interface in order to obtain electronic identity attributes and to work with user data (personal objects). In order for these requests to be carried out successfully, correct values for authId and authKey (one-time secret that was transmitted at the end of a successful operation at the client part of the target application) must be transmitted.


TA Client
PEIG
TA Server
AIM
connect()
AIMRequestOperation(e.g.'open')
authId
authId,AIM URL
start authentication(authId,AIM URL)
authentication(authId)
authId, authKey
get protected content(authId, authKey)
AIMgetPSLAtributes(authId,authKey, parameter)
AuthResult
AIMExecutePersonalObject(authId,authKey,parameter(s))
personal object/data
accept and provide content or deny

Internal ALUCID PEIG <-> AIM communication - The result is: both sided knows authId and authKey

Now, the authentication has been finished and both sides (TA Client, AIM server) know the authId and authKey. TA Client will provide that Information to the TA Server. TA Server can ask AIM for authentication result and for personal object/data and so on.

Figure 3-1 ADUCID® communications diagram

The R2, R3 and R4 interfaces are standard web services. R3 and R4 are transmitted via HTTP; R2 uses an internal transport layer of the host operating system.

Communication is simpler in the case of PEIG for a mobile phone. The PEIG proxy is internally integrated with PEIG in one application and the mobile phone operating system internally supports inter-application communication.

PEIG is registered with aducid:// URI in an operating system. The R2 interface starting event is transferred as an aducid:// URI to an operating system. The operating system activates PEIG by using the URI parameters.

PEIG finishes its activity by using a return URI. The return URI is transferred from AIM to PEIG during PEIG activity. The return URI is typically https://, to activate a registered web browser.

C Adapter is an internal part of operating system, in this case.

4. Integration with web applications

Adapters (both client and server) are used to simplify the integration with target applications.

Integration of web applications supports two different types of communication between the client (web browser) and the server: redirect and HTTP authentication.

4.1. Redirect

Redirect facilitates the communication between the client and the server adapter via standard HTTP redirect functionality.

No adjustments or plug-ins for standard browsers are required. It’s sufficient that the browser allows redirect to localhost.

A client redirect adapter is installed at the client station and expects an HTTP redirect to the ADUCID® port (44240) that initiates authentication.

The server part may use the server adapter to create and manage this communication redirect (AIM-proxy).

From the system’s perspective, the option to use a standard browser is considered an advantage, while the use of the HTTP redirect to a TCP/IP port is considered a disadvantage.

4.2. URI schema

The current operating system (including mobile phone operating systems and workstation operating systems) brings a new way of secure communication between applications in a protected user space. It is the registered, specific URI schema.

If the supporting application is registered in the operation system with the URI schema during installation, the operating system ensures activation of the registered application and transfer of the URI parameters to the application.

This option is used by PEIG for mobile phones.

4.3. Other adapters

Other adapters also exist that simplify the integration of web applications with ADUCID®. One of them is an API for working with user attributes (after authentication) that allows read/write without the need to program a web service for the R4 interface. There are also specialized adapters for relevant specialized frameworks or environments used by web application designers (Spring, PHP).

5. Operation

The fundamental element of ADUCID®’s activity is an operation. The target application requests AIM to perform an operation, AIM along with PEIG® then perform the operation and make the result available to the application. The application can then use the result of the operation (e.g. use a positive authentication result to grant access to information to a specific user in the scope of that user’s assigned rights, or use a negative result to deny access).

Standard applications only use the "open" operation, which performs user authentication.

Applications that manage identities (Identity Management) use other operations that support the execution of the entire lifecycle of the identity and other activities. For illustration, a list of supported operations of ADUCID® is provided with a brief description of each operation:

- Initialization of an identity (II – Identity Initialization – "init") - PEIG® and AIM together form a new unique electronic identity.
- Use of an identity (IU – Identity Use – "open") - PEIG® and AIM together validate the eID and provide a link to user information (authentication).
- Change in an identity (IC – Identity Change – "change") - PEIG® and AIM together change the existing internal values of the identity while preserving the entire context of personification (including all associated personal data).
- Termination of an identity (IE – Identity End – "delete") - PEIG® and AIM together invalidate the electronic identity and prevent anyone from performing any operation using this identity.

- Reparative change of an identity (RC – Reparative Identity Change – "rechange") - Change of an identity performed if the validity of previous identity has expired.
- Reparative initialization (RI – Reparative Identity Init – "reinit") – identical with II, performed if corresponding identity exists on PEIG® (this operation's purpose is to restore AIM).
- Confirmation of a link between identifiers (IL – Identity Link – "link") – PEIG® and two AIMs form a unique, one-time shared identity, and its connection to user information for both AIMs.
- Replica of an identity (IR – Identity Replica – "replica") – The second (backup) PEIG® creates a new identity tied to the identity at the primary PEIG®. The link between the PEIG®'s owner and the user information is preserved.

6. Binding

The issue of authentication results from linking the target application together with the protection of the data channel between the client and server part of the target application. This is called "binding".

Different user scenarios exist for how to link a target application to ADUCID authentication. They have different user and security features. It is possible to take snapshot of a QR code by using a mobile phone, when the QR code is displayed on a workstation screen to log in, or it is possible to use PEIG from hard disk of the same workstation where the web browser is running, or it is possible to use a web browser on a mobile phone or tablet.

The AIM security manager can select what binding scenarios will be supported by AIM and what scenarios will be disabled. This is possible through the AIM "binding mode" attribute configuration.

7. Abbreviations

Below is a summary of used abbreviations and their meaning:

ADUCID®

ADUCID® is a new authentication system that functions on the principle of providing services and infrastructures of electronic identities. It is an identification and authentication framework based on new ideas, rules, procedures and implementations for work and support of a unified method of authentication.

The main purpose of ADUCID® is to provide identification and authentication services in the cybernetic world of ICT systems using the ADUCID® secure authentication layer.

ADUCID® provides:

- Electronic identity services
- Secure authentication services
- Essential infrastructure for listed services

PEIG®

PEIG® (Personal Electronic Identity Guardian) is a device that provides full management capabilities for its user's electronic identities. Using the user identity, it also provides automatic authentication between the client application (used by the user) and the server part of the target application (that the user is accessing).

AIM

ADUCID® Identity Machine - Implements ADUCID® server functionality itself. It performs all ADUCID® operations and provides access to user data stored along with electronic identities in the LDAP database.

Through a standard network interface (web services), it provides target applications with services related to administration of the CyberID/eID. AIM contains an administrator and a user graphic interface (called UIM). AIM can also provide authorization services (including administration of authorization attributes to the relevant CyberID/eID).

AIM-proxy

Specialized module for web applications used to communicate with the client web browser upon authentication of HTML applications. This component enables ADUCID® to login into UIM without modifying the browser (redirect login).

PEIG-proxy

Specialized software communications module that connects PEIG® Core to the client target application and AIM. It also functions as an application firewall to protect PEIG® Core. It must be run on the same computer as the client part of the target application.