ADUCID Binding

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 Content

1. System Design

Binding is a mode of communication among components of ADUCID authentication scheme.

There are several binding types derived from the use scenarios of the target application, ADUCID devices (PEIG types) and technological limits.

The following binding types are currently designed:

- A—application binding using PEIG on the same host that the application client is running. App-PEIG communication uses RA (Redirect Adapter—ADUCID 2.20) and A1R (application, one device, redirect).
- B—application binding using PEIG on the same host that the application client is running. App-PEIG communication uses URI schema (Android) and A1U (application, one device, URI).
- C—application binding using PEIG on a different host than the application client is running. App-PEIG communication uses QR code and A2Q (application, two devices, QR).
- D1—application binding using PEIG on a different host than the application client is running (two devices). App-PEIG communication uses a QR code displayed by PP (new design— from ADUCID 2.50). The host with the target application includes ADUCID client software (PP—PEIG-proxy). App-PP communication uses RA, PP-PEIG communication uses QR code and A2RQ (application, two devices, redirect, QR).
- D2—application binding using PEIG on a different host than the application client is running (two devices). App-PEIG communication uses a QR code displayed by PP (new design— from ADUCID 2.50). The host with target application includes ADUCID client software (PP—PEIG-proxy). App-PP communication uses URI schema, PP-PEIG communication uses QR code—A2UQ (application, two devices, URI, QR).
- E—TLS binding using PEIG on the same host as the application client is running. TLS-PEIG communication uses URI schema (new unverified design—not included in current version) —T1U (TLS, one device, URI).
- F—TLS binding using PEIG on a different host than the application client is running. TLS-PEIG communication uses QR code (new unverified design—not included in current version) —T2Q (TLS, two devices, QR).

PEIG (PP) evaluates information about the communication path used (input from the application), and then transfers the information to AIM by specific binding communication over the R3 interface.

AIM controls communication during the operation start, based on the information received from PEIG (PP). AIM evaluates the information about binding communication, about PEIG activity and controls binding (with respect to the binding settings). AIM transfers information about the binding used to the target application, as a part of the PSL attributes.

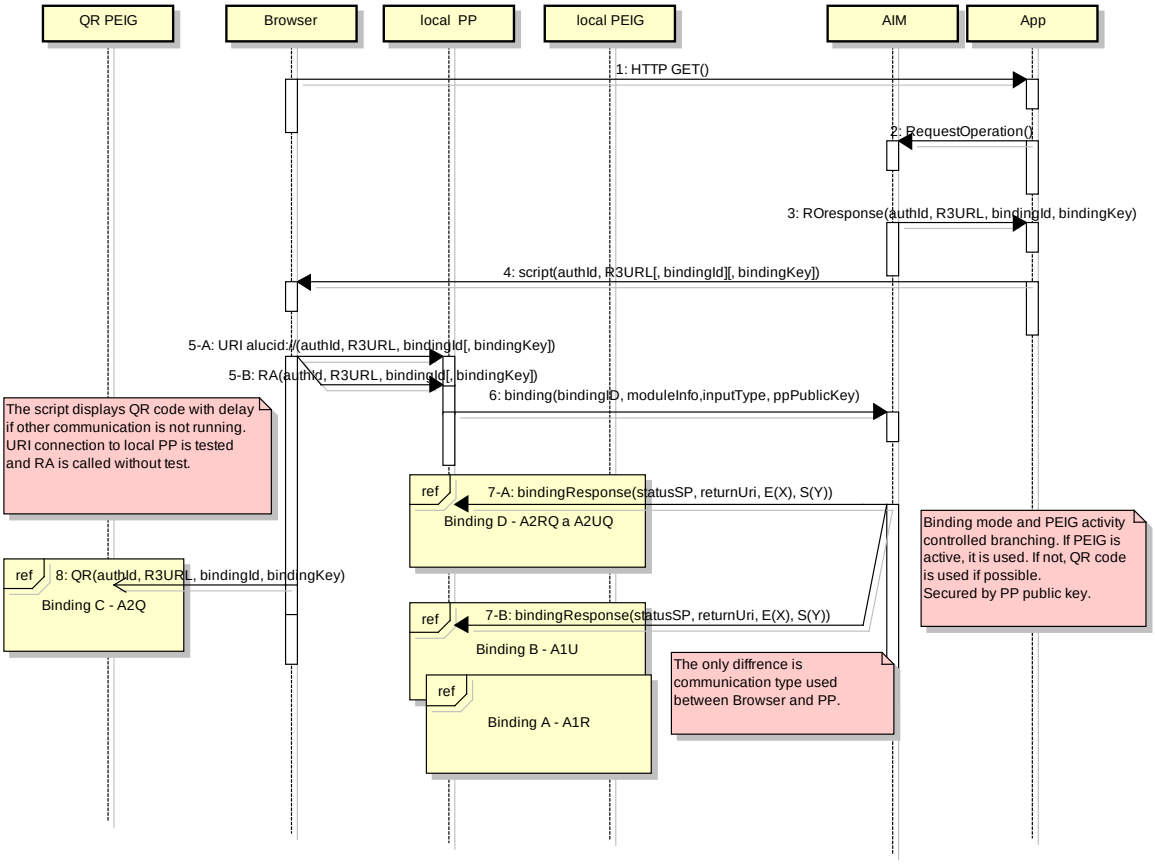

Figure 1—Application binding global schema

1.1. Binding design A—A1R

“Classical” binding used in older ADUCID versions. It uses Redirect Adapter and PEIG on the same personal computer as the target client part of the application.

It is extended by using **bindingId** and **bindingKey** to control binding, and to support compatibility with other binding scenarios.

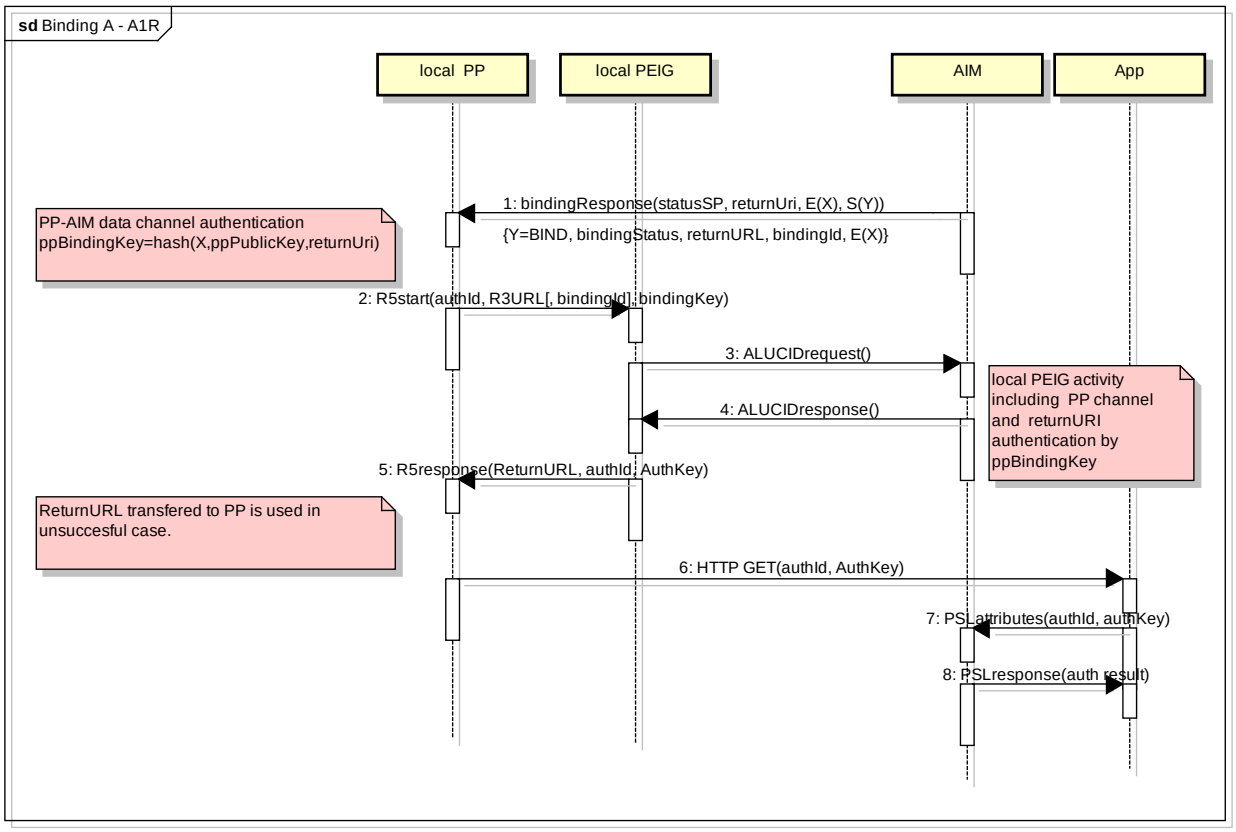

Figure 2—Binding A—A1R

1.2. Binding design B—A1U

A new binding mode using URI schema aducid:// enables communication between target application client, such as a Web browser, and ADUCID client (PP, PEIG). It is developed to be used in mobile phone operating systems, especially (Android, iOS). It can be used in modern workstations as well.

Compared to binding A—A1R, the B—A1U eliminates a risk of communication between different user contexts in multiuser systems based on use of shared TCP/IP Redirect Adapter port. It requires administrator rights for URI schema registration.

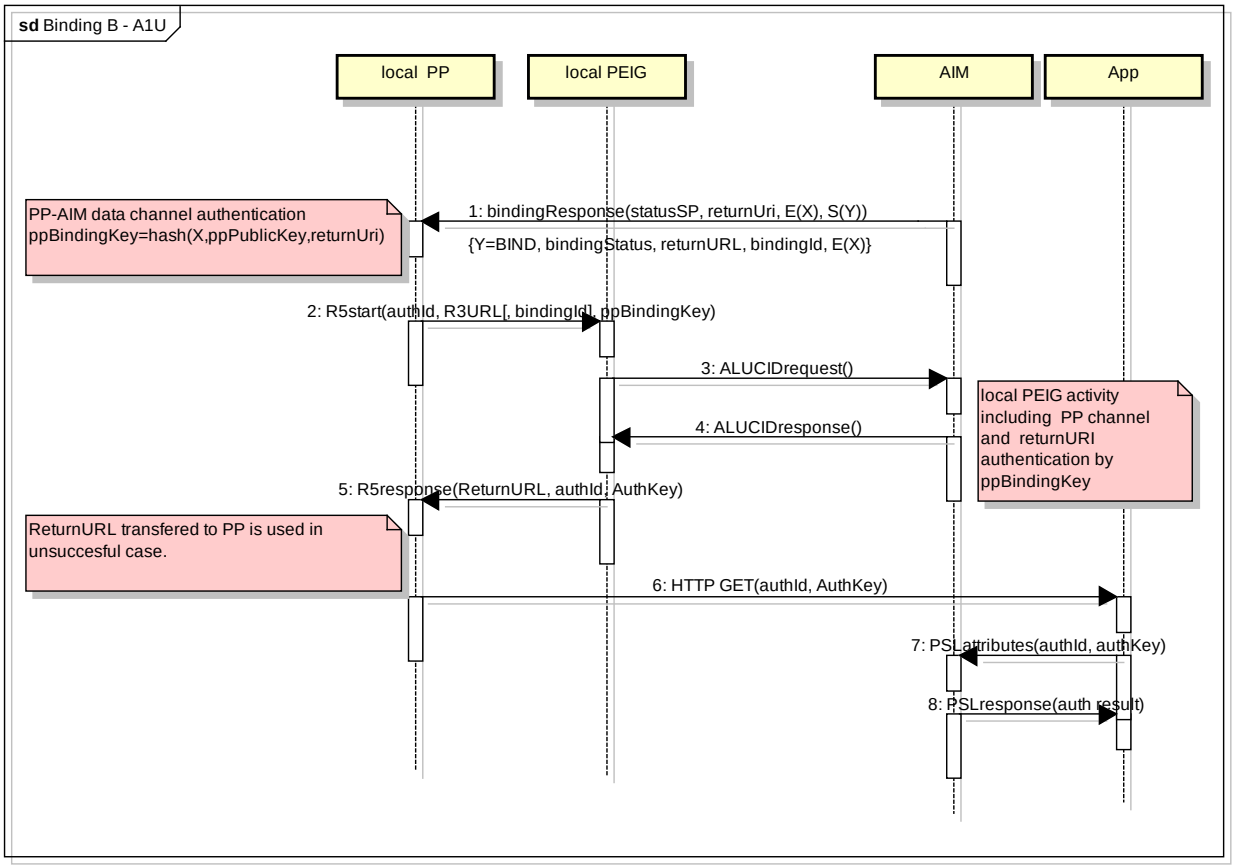

Figure 3—Binding B—A1U

1.3. Binding design C—A2Q

This new binding uses a QR code without the need to install any specific ADUCID client software on a client workstation. The QR code is displayed directly by the target client application (web browser). Therefore, security threats exist reflecting the scenario.

Note: These security threats can be solved by using secure transaction confirmation (use of ADUCID personal objects).

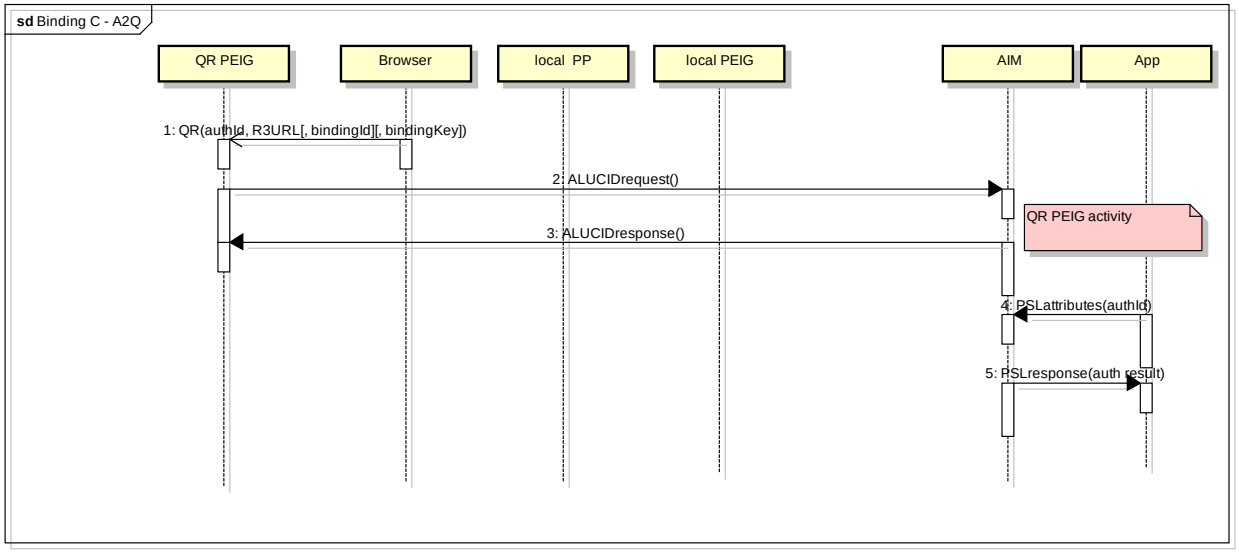

Figure 4—Binding C—A2Q

1.4. Binding design D—A2RQ and A2UQ

This is new specific solution of QR code use.

It is a more secure option of C (A2Q). In this case, faked active MITM site displaying the QR code and mimicking client to a target application should be eliminated.

PP creates an encrypted, unauthenticated channel between PP and AIM during the first part of binding communication, by using a temporary asymmetric key pair—**ppPrivKey** and **ppPubKey**. The UCP tools are used to support a creation and transfer of shared session key X.

The channel is used to transfer all required information for binding control, including the return URI of the target application (**returnUrl**).

PP creates two keys (**ppBindingKey** = hash(X, **ppPubKey**, **returnUrl**) and **ppAuthKey** = hash(X, **ppPubKey**).

PP transfers **ppBindingKey** to PEIG as **bindingKey** in the QR code.

PP waits for authentication to end, by using binding wait communication with AIM.

When the QR code is scanned by PEIG, and PEIG starts its communication with AIM, the QR code is cleared by PP, to decrease risk of rescanning the QR code and related authentication failure caused by repeated use of **authId**. PEIG authenticates the user and secures the binding channel during its operation.

PP redirects the user to the return URL, including transfer of the **ppAuthKey** as **AuthKey** in the return message.

Security note:

Waiting communication between PP and AIM is not cryptographically protected (using S(Y) and S(Z)). The risks are acceptable and protection should bring additional issues. The risks have a Denial of Service (DoS) nature (e.g. early QR code clearing, early redirection to **returnUrl**). The possible attacks in cryptographically protected communications should cause events generating a DoS, as well.

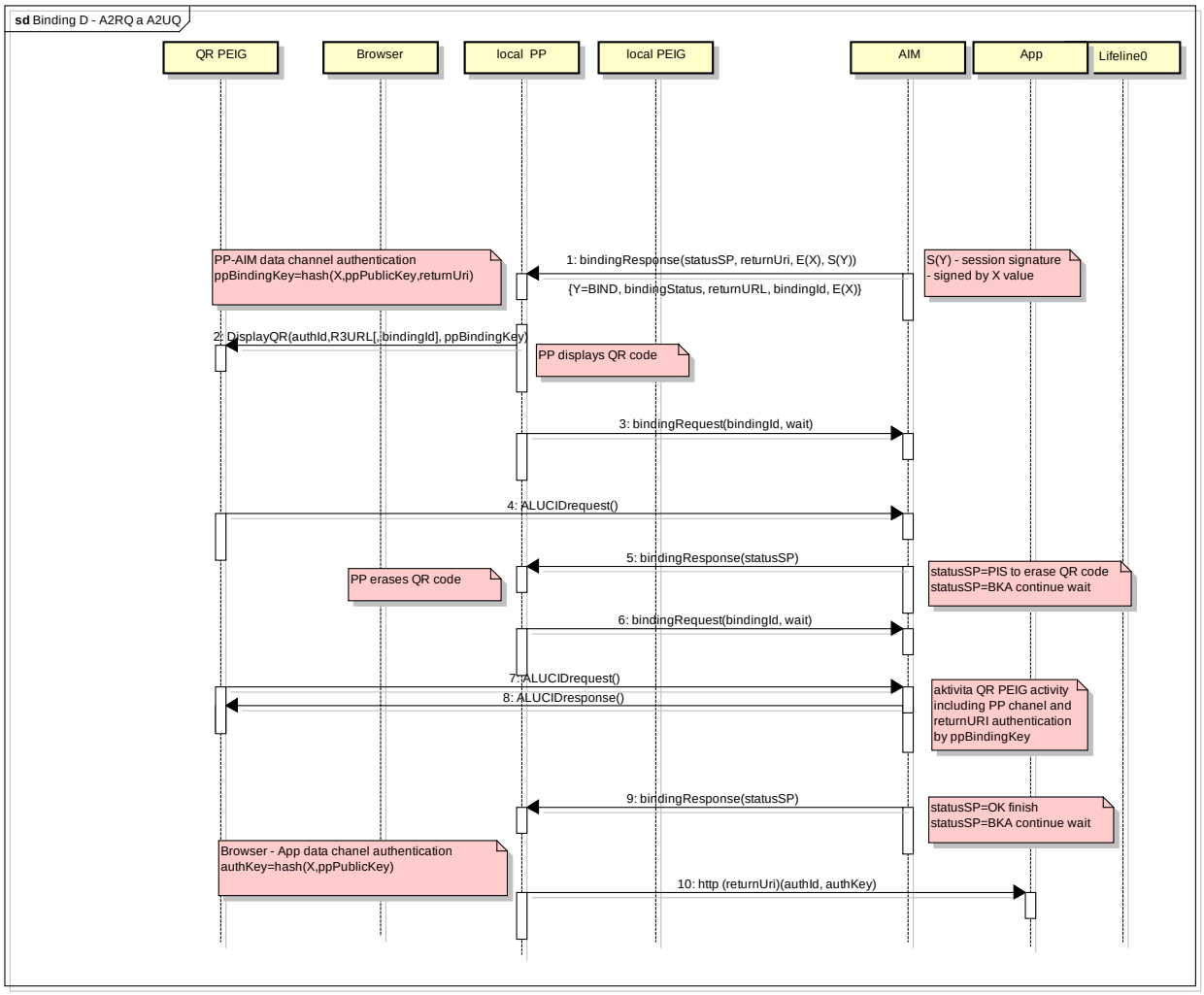

Figure 5—Binding D—A2RQ and A2UQ

2. Provider's scenarios

Different binding scenarios can be supported by a service provider and other scenarios can be disabled. The reasons can vary (e.g. security or business strategy).

Supported scenarios	Binding Mode	Description
ABCD	0	All possible options, weak and strong binding (A—A1R, B—A1U, C—A2Q, D—A2RQ, A2UQ)
ABD	1	One or two devices, strong binding (A—A1R, B—A1U, C—A2Q, D—A2RQ, A2UQ)
ACD	2	1+1 only (two devices or token and device), weak and strong binding, single user workstation (A—A1R, C—A2Q, D—A2RQ, A2UQ)
AB	3	One device only (A—A1R, B—A1U)
AC	4	1+1 only (two devices or token and device), no software installation on client workstation is required, weak binding, single user workstation (A—A1R, C—A2Q)
AD	5	1+1 only (two devices or token and device), strong binding, single user workstation (A—A1R, D—A2RQ, A2UQ)
BCD	6	All for a multiuser workstation, weak and strong binding (B—A1U, C—A2Q, D—A2UQ)
BD	7	All for a multiuser workstation, strong binding (B—A1U, D—A2UQ)
B	8	Only one mobile phone or tablet (B—A1U)
CD	9	Only two devices, weak and strong binding (C—A2Q, D—A2RQ, A2UQ)
C	10	Only two devices, without installation on a workstation (C—A2Q)
D	11	Two devices, with strong binding only (D—A2RQ, A2UQ)
Cs	12	Only two devices, without installation on workstation, simplified QR code – without bindingKey (C—A2sQ)

Figure 6 – Supported Binding Modes

Note: TLS scenarios (E – T1U and F – T2Q) are not included in this list. They are not supported in current version.

Binding B on personal computer and binding A are supported only for USB PEIG (without client software installation) and are not supported in current version.

ADUCID client software installation on a workstation is required for B and D scenarios. Scenario C does not require software installation. Scenario A does not require software installation if the USB token PEIG is used.

Excluded scenarios (mathematically possible):

- Nothing, A only, BC, ABC
- BC, ABC—client software installation is required; it has no sense to exclude strong binding.

