

Architecture for Scalable, Self-*, human-centric,
Intelligent, Secure, and Tactile next generation IoT

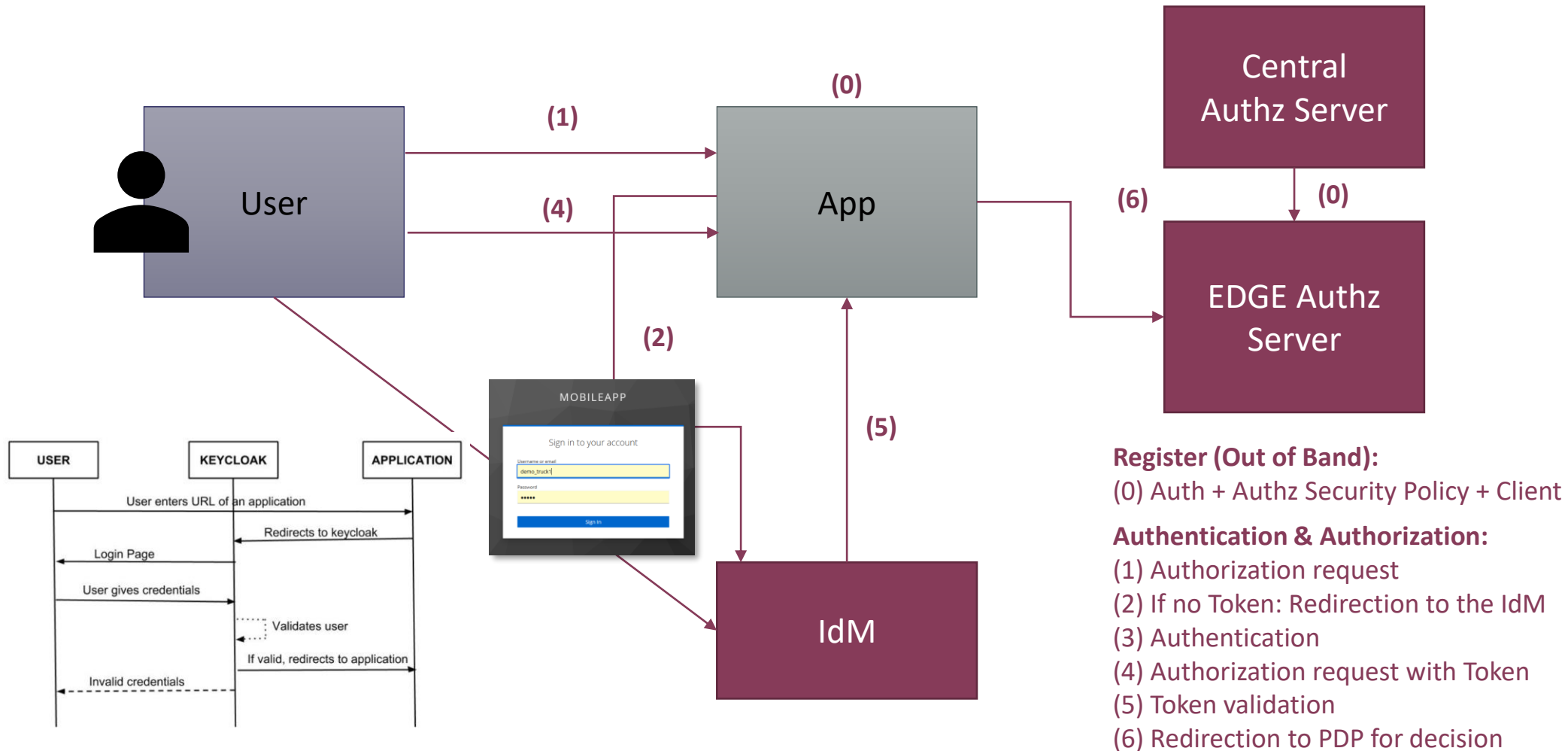
assist-iot

**AuthServer Step by Step
Configuration manual**

S21Sec



T5.3 E1-E2 Authz + IdM



T5.3 E1Authz Configuration

Step 1: Organizations

- Setup Organizations
 - Go to the menu
 - Add Organization



A screenshot of the 'Add Organization' form. The form has a title 'Add Organization' and a single input field labeled 'Name'. The input field contains the text 'Auth_Org' and is highlighted with a blue rectangular box. A blue arrow points from the 'Add Organization' instruction in the list to this box. To the right of the input field is an 'Add' button.

T5.3 E1Authz Configuration

Step 1: Organizations

- Setup User

- Go to the menu
- Select your Organization
- Add username to the organization
- Click on Created username

The screenshot shows the S21 SEC web interface. At the top right is the 'S21 SEC' logo. Below it is a navigation bar with tabs: 'Home', 'Organizations', 'Security Domains', 'Data', and 'Security Policy'. The 'Organizations' tab is active, and a sub-menu is open showing 'Organizations' and 'Users'. The 'Users' option is highlighted with a red box. Below the navigation bar is a table titled 'Users of Organizations'. The table has columns for 'Organizations' and 'Users'. The 'Organizations' column lists several organizations: 's21sec', 'palrobotics', 'port_access', 'port1', 'transport_org', 'vehicle_dia_org', 'vehicle_ext_org', and 'auth_org'. The 'auth_org' entry is highlighted with a blue box. Below the table is a form to add a user to an organization. The 'Username' field is filled with 'auth_user1' and is highlighted with a green box. To the right of the form is a button labeled 'Add user to org: auth_org'.

- Add the Idm user and identification type

The screenshot shows the configuration form for the 'auth_org' user. The form has a table with columns 'Value' and 'Identification type'. The 'Value' column contains 'idm_user1' and the 'Identification type' column contains 'oauth2'. There is an 'Add' button next to the 'Identification type' dropdown. The entire form is highlighted with a purple box.

T5.3 E1Authz Configuration

Step 2: Security Domains

- Setup Security Domains
 - Go to the Menu
 - Add Security Domain
 - Add your Organization to your Security Domain

The screenshot shows the S21 SEC web interface. The top navigation bar includes links for Home, Organizations, Security Domains, Data, and Security Policy. The 'Security Domains' link is highlighted with a red box. Below the navigation bar, there is a table with one entry. The entry is labeled 'auth_sec_dom' and has an 'Add' button next to it. A red arrow points from the 'Go to the Menu' instruction to the 'Security Domains' link. A blue arrow points from the 'Add Security Domain' instruction to the 'auth_sec_dom' entry. A green arrow points from the 'Add your Organization to your Security Domain' instruction to the 'Add' button.

Security Domain	
auth_sec_dom	Add

The screenshot shows the 'auth_sec_dom' entry in the table. Below the entry, there is a form with two dropdown menus: 'Organization' and 'Role'. The 'Organization' dropdown is set to 'auth_org' and the 'Role' dropdown is set to 'owner'. There is an 'Add' button next to the 'Role' dropdown. A green arrow points from the 'Add your Organization to your Security Domain' instruction to the 'Add' button.

Organization	Role	
auth_org	owner	Add

T5.3 E1Authz Configuration

Step 2: Security Domains

- Setup Sources of identification
 - Go to the Menu
 - Select your Security Domain
 - Add your App Name

The screenshot shows the S21 SEC web interface. At the top right is the 'S21 SEC' logo. Below it is a navigation bar with tabs: 'Home', 'Organizations', 'Security Domains', 'Data', and 'Security Policy'. The 'Security Domains' tab is active. Below the navigation bar, there are three sub-menus: 'Security Domains', 'Identification types', and 'Sources of identification'. The 'Sources of identification' sub-menu is highlighted with a red box. Below this, the title 'Sources of identification' is displayed. A table with the header 'Domain' contains the following entries: 'trimekarea1', 'iotdomain1', 'port1', 'prodigi', 'assist_pilot1', 'assist_pilot3a', 'assist_pilot', and 'auth_sec_dom'. The 'auth_sec_dom' entry is highlighted with a blue box. A red arrow points from the 'Go to the Menu' step in the list to the 'Sources of identification' sub-menu. A blue arrow points from the 'Select your Security Domain' step to the 'auth_sec_dom' entry in the table.

The screenshot shows the configuration form for the 'auth_sec_dom' domain. The form has two main sections: 'Identifier' and 'Identification type'. The 'Identifier' field contains the text 'IDM_client' and is highlighted with a green box. The 'Identification type' field is a dropdown menu with 'oauth2' selected. An 'Add' button is located to the right of the 'Identification type' field. A green arrow points from the 'Add your App Name' step in the list to the 'IDM_client' text in the 'Identifier' field.

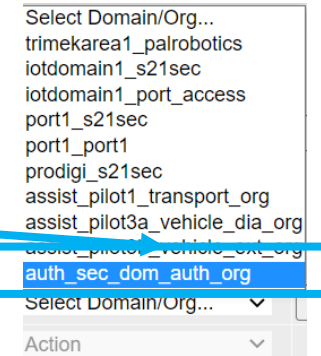
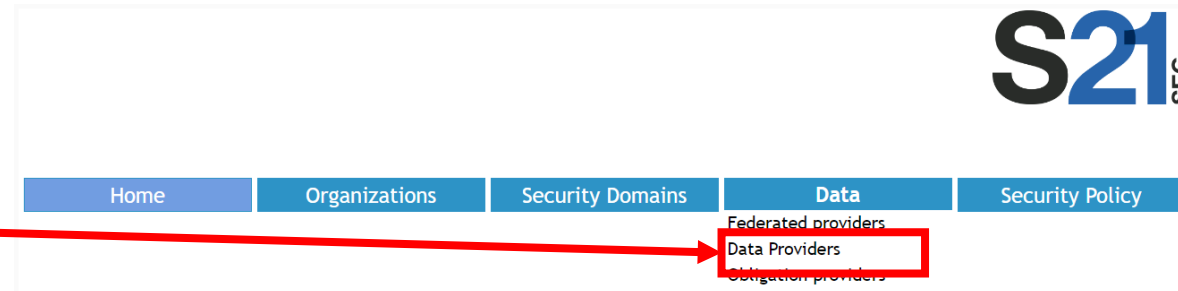
The same name configure in
the IDM, in Client's Menu

T5.3 E1Authz Configuration

Step 3: Data

• Setup Data Providers

- Go to the Menu
- Add new Data Provider
 - Select your Security Domain+Organization
 - Complete the PiP Url and the name of the Data Provider
 - Configure the Data Key, the name and data type of the variable



auth_sec_dom_auth_org

name_data_prov PIP URL: http://ipaddress:port/path Up Down Del

Method: GET Input value: action-id

Add Output values

PIP Data Key: Data_Key

Category: access-subject Data type: string

Variable name: MyVarName

Add Data provider

PIP URL	/<in_value>	Domain		Add
Name		Domain	auth_sec_dom_auth_org	Add
Rest Method	GET	Input value	Action	

Add Data provider

PIP URL: http://ipaddress:port/path

Name: Name_Data_Prov Domain: auth_sec_dom_auth_org Add

Rest Method: GET Input value: Action

T5.3 E1Authz Configuration

Step 4: Security Policy

- Setup Security Policy
 - Go to the Menu
 - Select Security Domain
 - Click on Edit

Security domain	Management policy	Status	Last deploy time			
auth_sec_dom						
	Domain auth_sec_dom_auth_org	Not initialized	Never	Edit	Clean	Deploy



T5.3 E1Authz Configuration

Step 4: Security Policy

- Setup Security Policy – Add Rule

- Add Rule => Permit + Add
- Click on Edit

Security Domain: auth_sec_dom Organization: auth_org

Rules

Add Rule:	Permit ▾	Add
Add Obligation:	Permit ▾	area1-inalert ▾ Add

Return

Security Domain: auth_sec_dom Organization: auth_org

Rules

Rule: 17	Effect: Permit	Edit	Delete
Add Rule:	Permit ▾	Add	
Add Obligation:	Permit ▾	area1-inalert ▾	Add

Return

T5.3 E1Authz Configuration

Step 4: Security Policy

- Setup Security Policy – Setup Rule (1)
 - Add Condition= Action
 - Add the Name of the Action
 - Add Condition (PiP)

Security Domain: auth_sec_dom Organization: auth_org

Rule:17 Effect: Permit

Condition ID	Description (All must be met)
Cond: 44	Evaluations: (At least one must be met) Action -- string-equal -- actionname(x) (Val:) [Add] [Del]

Add Evaluation to Condition 44:

Action [string] [string-equal] [Add]

Add Condition: [Var: name_data_prov->myvarname] [string] [string-equal] [Add]

Add Obligation: [Permit] [area1-inalert] [Add]

[Return]

Action
Identification Code
Authzserver Username
Identification User Role
Access Resource
Security Domain
Identification Type
Organization
Time
Date
Timestamp
Var: name_data_prov->myvarname
Action

Security Domain: auth_sec_dom Organization: auth_org

Rule:17 Effect: Permit

Condition ID	Description (All must be met)
Add Condition: [Action] [string] [string-equal] [Add]	
Add Obligation: [Permit] [area1-inalert] [Add]	

[Return]

Security Domain: auth_sec_dom Organization: auth_org

Rule:17 Effect: Permit

Condition ID	Description (All must be met)
Cond: 44	Evaluations: (At least one must be met) Action -- string-equal -- Value missing () [Del] [Delete Condition]

Add Evaluation to Condition 44:

[Action] [string] [string-equal] [Add]

Add Condition: [Action] [string] [string-equal] [Add]

Add Obligation: [Permit] [area1-inalert] [Add]

[Return]

T5.3 E1Authz Configuration

Step 4: Security Policy

- Setup Security Policy – Setup Rule (2)
 - Add the value of the PiP variable
 - Click on Return
 - Click on Return

Security Domain: auth_sec_dom Organization: auth_org

Rules	Effect: Permit	Edit	Delete
Rule: 17			
Add Rule:	Permit	Add	
Add Obligation:	Permit	area1-inalert	Add

Return

Security Domain: auth_sec_dom Organization: auth_org

Rule:17 Effect: Permit

Condition ID	Description (All must be met)	Delete Condition
Cond: 44	Evaluations: (At least one must be met) Action -- string-equal -- actionname(x) (Value) <input type="text"/> Add Del	Delete Condition
Add Evaluation to Condition 44:		
	Action <input type="text"/> string <input type="text"/> string-equal <input type="text"/> Add	
Cond: 45	Evaluations: (At least one must be met) Var: name_data_prov->myvarname -- string-equal -- Value missing () Del	Delete Condition
	Value <input type="text"/> value1 Action <input type="text"/> Add	
Add Evaluation to Condition 45:		
	Action <input type="text"/> string <input type="text"/> string-equal <input type="text"/> Add	
Add Condition:		
	Action <input type="text"/> string <input type="text"/> string-equal <input type="text"/> Add	
Add Obligation:		
	Permit <input type="text"/> area1-inalert <input type="text"/> Add	

Return

- Click on Deploy = If you DO NOT do this step the changes are not applied

Security domain	Management policy	Status	Last deploy time			
auth_sec_dom						
	Domain auth_sec_dom_auth_org	modified	Never	Edit	Clean	Deploy

Return

T5.3 E1Authz Configuration



Example

`http://192.168.15.189:9000/authzserver/rest/evaluate?resource=assist_pilot2@safety_health&action=check_health_info&code=health_technician_1@prevention_service`

```
{"retcode":"0","resource":"assist_pilot2@safety_health","action":"check_health_info","code":"health_technician_1@prevention_service","response":"Permit","msg":""}
```



This Communication is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N°957258

assist-IoT

S21sec