UC-001: Authentication using the mechanism of eHealth IDP (using FAS)

/!\ the columns 'mobile application' of all use-case must be changed to application

Acronyms

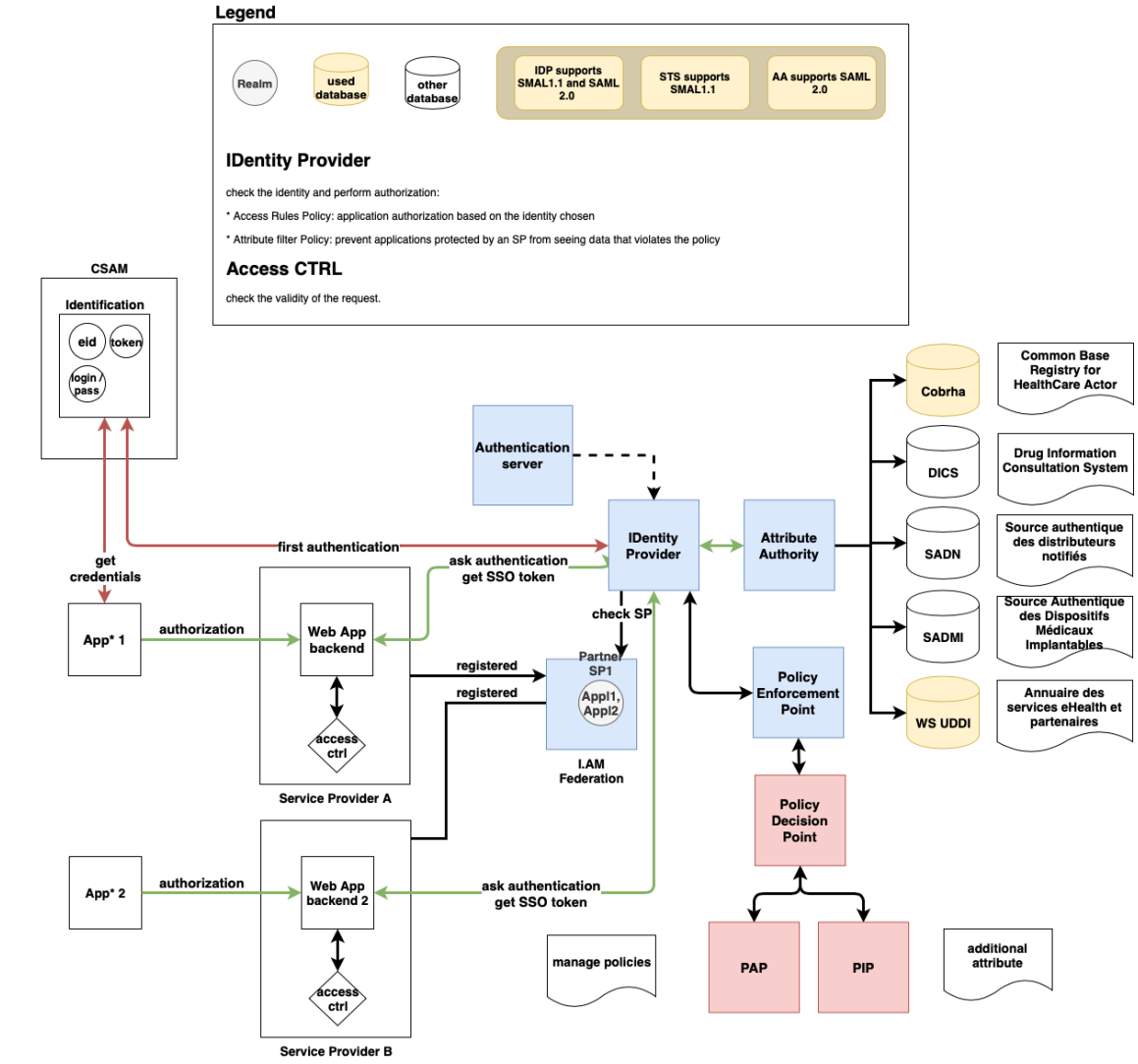
Acronyms	Meaning
FAS	Federal Authentication Service (aka CSAM)

Used documentation

Cookbook/ materials	Version	Location
Identity & Authorization Management (I.AM) - Overview	1.0	https://www.ehealth.fgov.be/ehealthplatform/file/view/c87f7d093e56ff1054c73d6aae09e0bb?filename=ehealth_i.am_-_overv
Identity & Authorization Management (I.AM) - Identity Provider (IDP)	1.0	https://www.ehealth.fgov.be/ehealthplatform/fr/data/file/view/d43784683d86392e68f1a95b860f721170f30c7b?name=ehealth_i.am_-_idp_v1.0.pdf
CSAM Youtube channel	-	https://www.youtube.com/channel/UCzMGudd9xdMeGjYpbpjsXFw

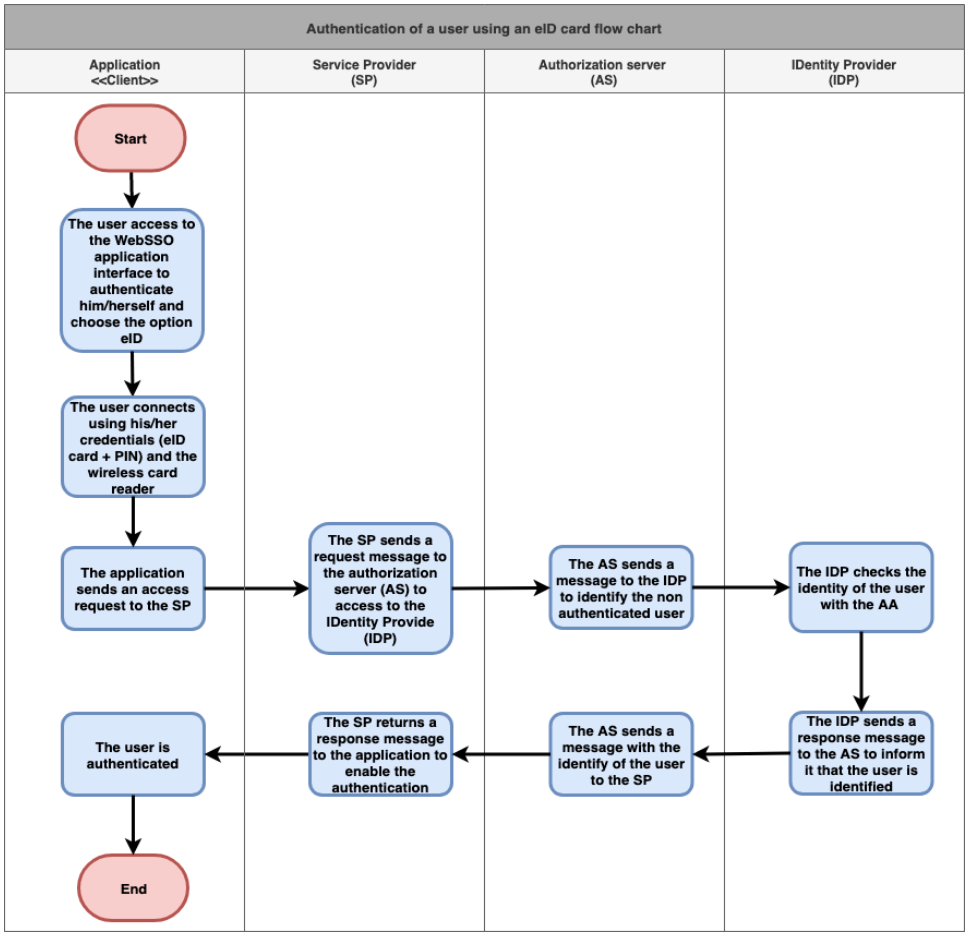
General information

In the figure below, we provide an overview about the interaction between the different services of the e-health platform involved in the IAM. It is noteworthy that the presented architecture is dedicated to the WebSSO solution.



Basic flow (EID)

Flow	Specification	
	Use case ID	UC-001-EID
	Use case name	Authentication using an eID card
	Actors	• Citizen • Healthcare giver • Representative of an institution
	Short Description	This use case denotes the authentication of a user via an eID card.



Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.	

Pre-Conditions	• The user has already an account
	• The user has:
	  ○ an eID card
	  ○ a PIN code of his/her eID card
	  ○ a card reader	

Post-Conditions	• The user is authenticated • The user has access to the services of the mobile application	
Steps (basic flow)	0	The user access to the WebSSO application interface to authenticate him /herself and choose the option eID
	1	The user connects using his/her credentials (eID card + PIN) and the card reader
	2	The application sends an access request to the SP
	3	The SP sends a request message to the AS to access to the IDP
	4	The AS sends a message to the IDP to identify the non authenticated user
	5	The IDP checks the identity of the user with the AA
	6	The IDP sends a response message to the AA to inform it that the user is identified
	7	The AS sends a message with the identify of the user to the SP
	8	The SP returns a response message to the application to enable the authentication

	9	The user is authenticated and can use the the services of the mobile application
Exceptions (exception flows)	• The PIN of the eID card is not correct • The creation is aborted (e.g. loss of connection, problem with the card reader, the session is expired)	
Frequency	• Every time the user needs to authenticate to the mobile application	

Exception flow 1

Specification		
Use case ID	UC-001-EID-EF-01	
Use case name	The PIN of the eID card is not correct	
Actors	• Citizen • Representative of an institution • Healthcare giver	
Short Description	It denotes the use case when the user tries to authenticate with his/her eID card and fails in entering the PIN.	
Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.	

Pre-Conditions	• The user has already an account
	• The user has:
	  ○ an eID card
	  • a PIN code of his/her eID card
	  • a card reader	

Post-Conditions	• The authentication is interrupted • An error message should be displayed	
Steps (basic flow)	0	The user access to the WebSSO application interface to authenticate him/herself and choose the option eID
	1	The user tries to connect using a wrong PIN code
	2	The authentication is interrupted
Frequency	• Every time for a user needs to authenticate him/herself and enter a wrong PIN code	

Exception flow 2

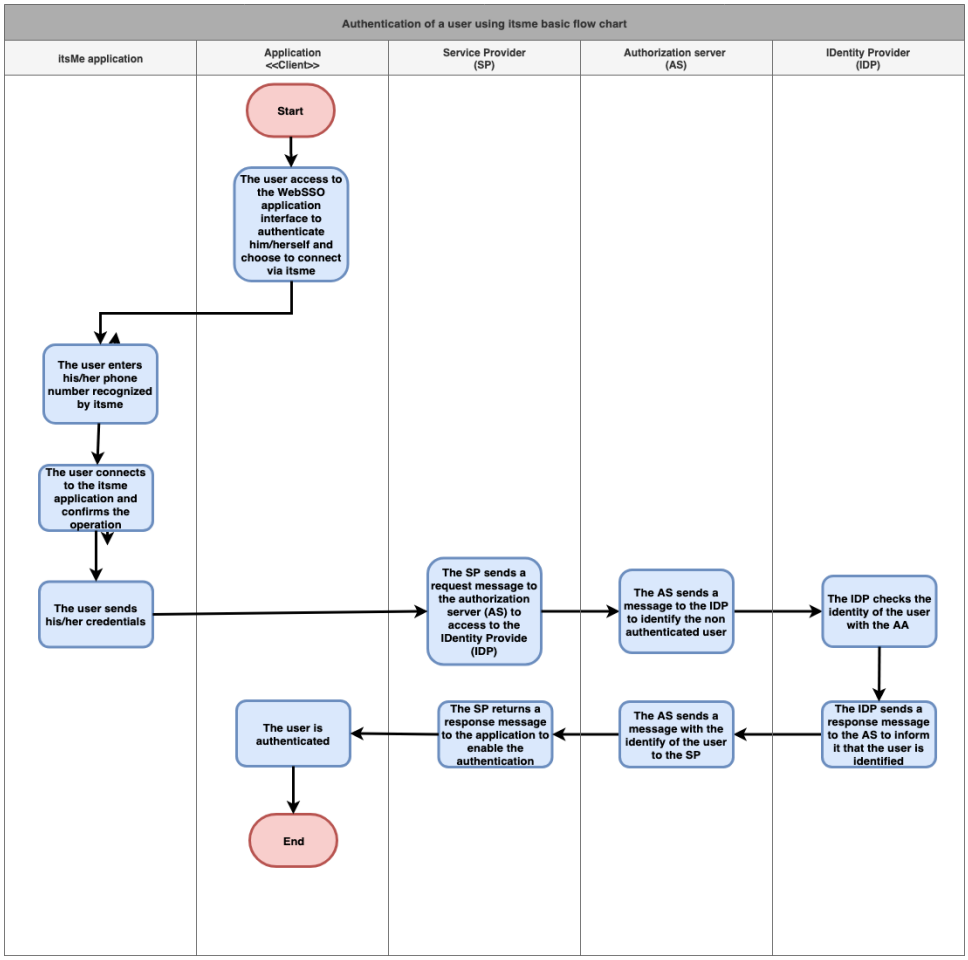
Specification	
Use case ID	UC-001-EID-EF-02
Use case name	The creation is aborted (e.g. loss of connection, problem with the card reader, the session is expired)
Actors	• Citizen • Representative of an institution • Healthcare giver
Short Description	It denotes the exception use case when the user loses the connection and he/she will not be able to finish the authentication. It may happens at any step of the basic and alternative flows.
Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.

Pre-Conditions	• The user has already an account
	• The user has:
	  • an eID card
	  • a PIN code of his/her eID card
	  • a card reader

Post-Conditions	• The authentication is interrupted • An error message should be displayed
Steps (basic flow)	
Frequency	• Every time for a user needs to authenticate him/herself and loses the connection

Alternative flow 1 (itsMe):

Flow	Specification	
	Use case ID	UC-001-ITSME
	Use case name	Authentication using itsme
	Actors	• Citizen • Healthcare giver • Representative of an institution
	Short Description	This use case denotes the authentication of a user via itsme.



	1 (High) Must have: The system must implement this goal/ assumption to be accepted.	

Pre-Conditions	• The user has an account
	• The user has:
	  • a phone number
	  • an account in itsme
	  • a smartphone with the application itsme
	  • a five secure code to confirm the operation on itsme	

Post-Conditions	• The user is authenticated • The user has access to the services of the mobile application	
Steps (basic flow)	0	The user accesses to the WebSSO application interface to authenticate him /herself
	1	The user chooses to connect via itsme
	2	The userenters his /her phone number recognized by itsme
	3	The userconnects to the itsme application and confirms the operation
	4	The user sends his /her credentials
	5	The application sends an access request to the SP
	6	The SP sends a request message to the AS to access to the IDP
	7	The AS sends a message to the IDP to identify the non authenticated user
	8	The IDP checks the identity of the user with the AA

	9	The IDP sends a response message to the AS to inform it that the user is identified
	10	The AS sends a message with the identity of the user to the SP
	11	The SP returns a response message to the application to enable the authentication
	12	The user is authenticated and can use the the services of the mobile application
Exceptions (exception flows)	• The user makes an error when editing his /her credentials (e. g. The phone number of the user is not recognized by itsme) • The creation is aborted (e.g. loss of connection, the session is expired)	
Frequency	• Every time the user needs to authenticate to the mobile application	

Exception flow 1

Specification	
Use case ID	UC-001-ITSME-EF-01
Use case name	The user makes an error when editing his/her credentials
Actors	• Citizen • Representative of an institution • Healthcare giver
Short Description	This use case represents the situation when the user is trying to connect with the itsme and he/she make an error when entering his /her credentials (e.g. The phone number of the user is not recognized by itsme). This exception flow may be triggered by the basic flow and any alternative one.
Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.

Pre-Conditions	• The user has an account
	• The user has:
	  • a phone number
	  • an account in itsme
	  • a smartphone with the application itsme
	  • a five secure code to confirm the operation on itsme	

Post-Conditions	• The creation of the account falls • An error message should be displayed	
Steps	0	The user accesses to the WebSSO application interface to authenticate him/herself
	1	The user tries to connect to the application via itsme
	2	The user makes an error when entering his/her credentials
Frequency	• Every time for a user needs to authenticate him/herself and makes an error when entering his/her credentials	

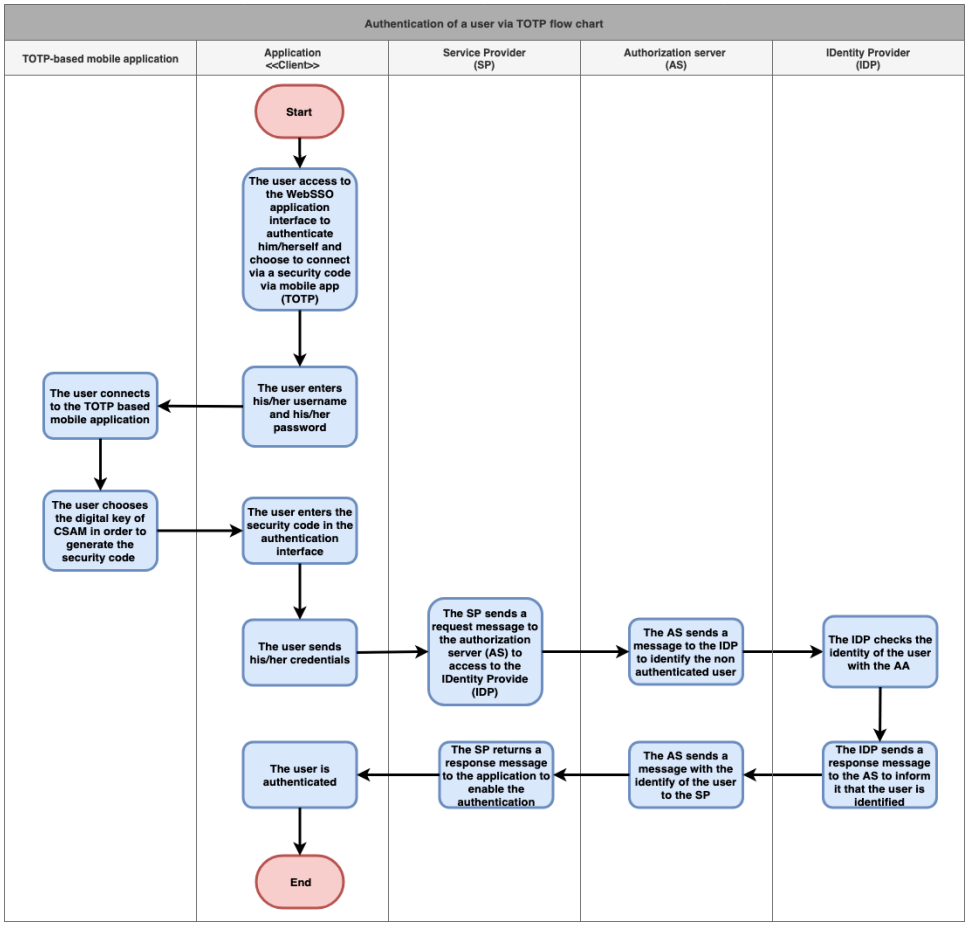
Exception flow 2

Specification		
Use case ID	UC-001-ITSME-EF-02	
Use case name	The creation is aborted (e.g. loss of connection, problem with the wireless card reader, the session is expired)	
Actors	• Citizen • Representative of an institution • Healthcare giver	
Short Description	It denotes the exception use case when the user loses the connection and he/she will not be able to finish the authentication. It may happens at any step of the basic and alternative flows.	
Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.	

Pre-Conditions	• The user has already an account
	• The user has:
	  • an eID card
	  • a PIN code of his/her eID card
	  • a wireless card reader	

Post-Conditions	• The authentication is interrupted • An error message should be displayed	
Steps (basic flow)		
Frequency	• Every time for a user needs to authenticate him/herself and loses the connection	

Alternative flow 1 (TOTP):

Flow	Specification		
	**Use case ID**		UC-001-TOTP
	Use case name		Authentication via TOTP
	Actors		• Citizen • Healthcare giver • Representative of an institution
	Short Description		This use case denotes the authentication of a user via TOTP.
			1 (High) Must have: The system must implement this goal/ assumption to be accepted.

	Pre-Conditions		• The user has already an account
			• The user has:
			  • a username and a password
			  • a smartphone with a TOTP-based mobile application to get a security code

	Post-Conditions		• The user is authenticated • The user has access to the services of the mobile application
	Steps (basic flow)	0	The user access to the WebSSO application interface to authenticate him /herself and choose to connect via a security code via mobile app (TOTP)
		1	The user enters his/her username and his/her password
		2	The user connects to the TOTP based mobile application

	3	The user chooses the digital key of CSAM and enters it in the authentication interface
	4	The user sends his/her credentials
	5	The SP sends a request message to the authorization server (AS) to access to the IDentity Provide (IDP)
	6	The AS sends a message to the IDP to identify the non authenticated user
	7	The IDP checks the identity of the user with the AA
	8	The IDP sends a response message to the AS to inform it that the user is identified
	9	The AS sends a message with the identify of the user to the SP
	10	The SP returns a response message to the application to enable the authentication
	11	The user is authenticated
Exceptions (exception flows)	• The username or the password is not recognized • The creation is aborted (e.g. loss of connection, the session is expired)	
Frequency	• Every time the user needs to authenticate to the mobile application via TOTP	

Exception flow 1

Specification	
Use case ID	UC-001-TOTP-EF-01
Use case name	The username or the password is not recognized

Actors	• Citizen • Representative of an institution • Healthcare giver	
Short Description	It denotes the use case when the user tries to authenticate via a TOTP and fails in entering his credentials (username /password)	
Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.	

Pre-Conditions	• The user has already an account
	• The user has:
	  ◦ a username and a password
	  ◦ a smartphone with a TOTP-based mobile application to get a security code	

Post-Conditions	• The authentication is interrupted • An error message should be displayed	
Steps (basic flow)	0	The user access to the WebSSO application interface to authenticate him/herself and choose to connect via a security code via mobile app (TOTP)
	1	The user enters his/her username and his/her password
	2	The authentication is interrupted because the credentials are not recognized
Frequency	• Every time for a user needs to authenticate him/herself and enter wrong credentials	

Exception flow 2

Specification	
Use case ID	UC-001-TOTP-EF-02
Use case name	The creation is aborted (e.g. loss of connection, the session is expired)
Actors	• Citizen • Representative of an institution • Healthcare giver
Short Description	It denotes the exception use case when the user loses the connection and he/she will not be able to finish the authentication. It may happens at any step of the basic and alternative flows.
Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.

Pre-Conditions	• The user has already an account
	• The user has:
	  ◦ a username and a password
	  ◦ a smartphone with a TOTP-based mobile application to get a security code

Post-Conditions	• The authentication is interrupted • An error message should be displayed

Steps (basic flow)		
Frequency	• Every time for a user needs to authenticate him/herself and loses the connection	