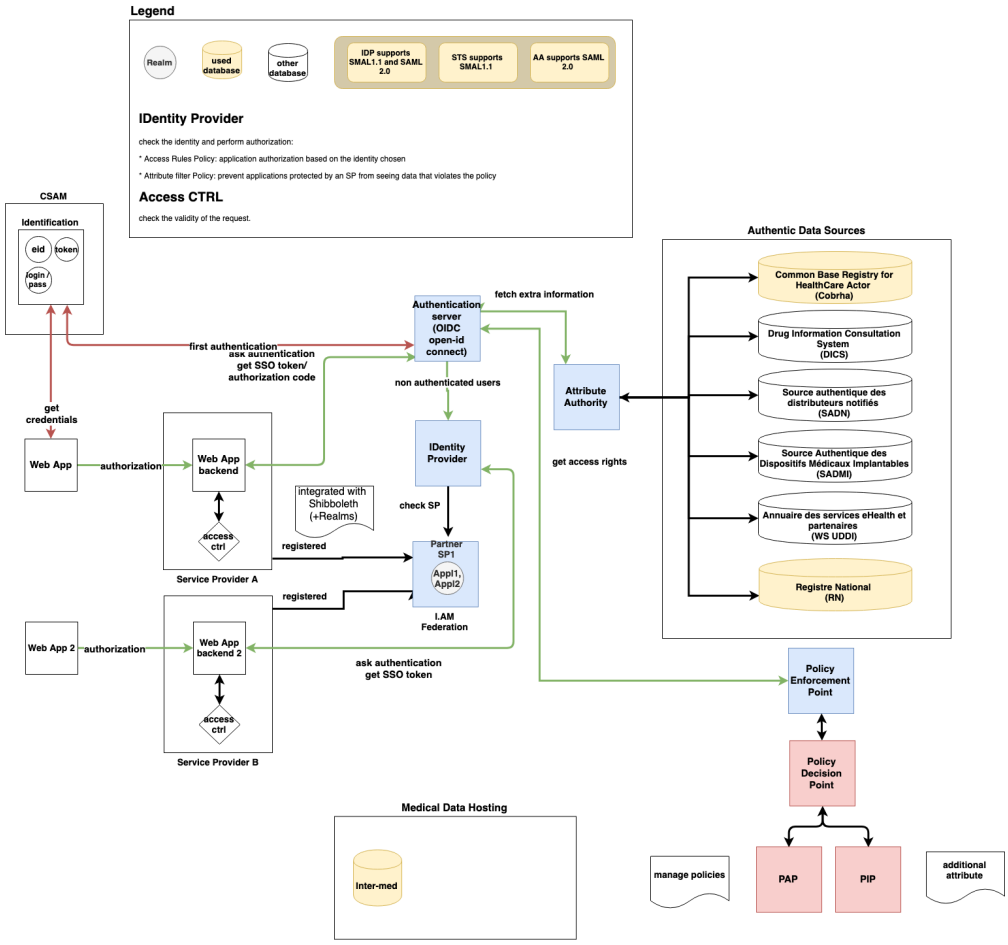
deprecated-UC-001 (ATH-UC-07): Authentication via TOTP

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
Gestion de clés numériques sur CSAM	-	https://iamapps.belgium.be/sma/generalinfo?redirectUrl=%2Fsma
S'identifier sur un smartphone ou une tablette avec un code de sécurité via une application	-	
itsme video	-	
Gestion de clés numériques sur CSAM	-	https://iamapps.belgium.be/sma/generalinfo?redirectUrl=%2Fsma

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.



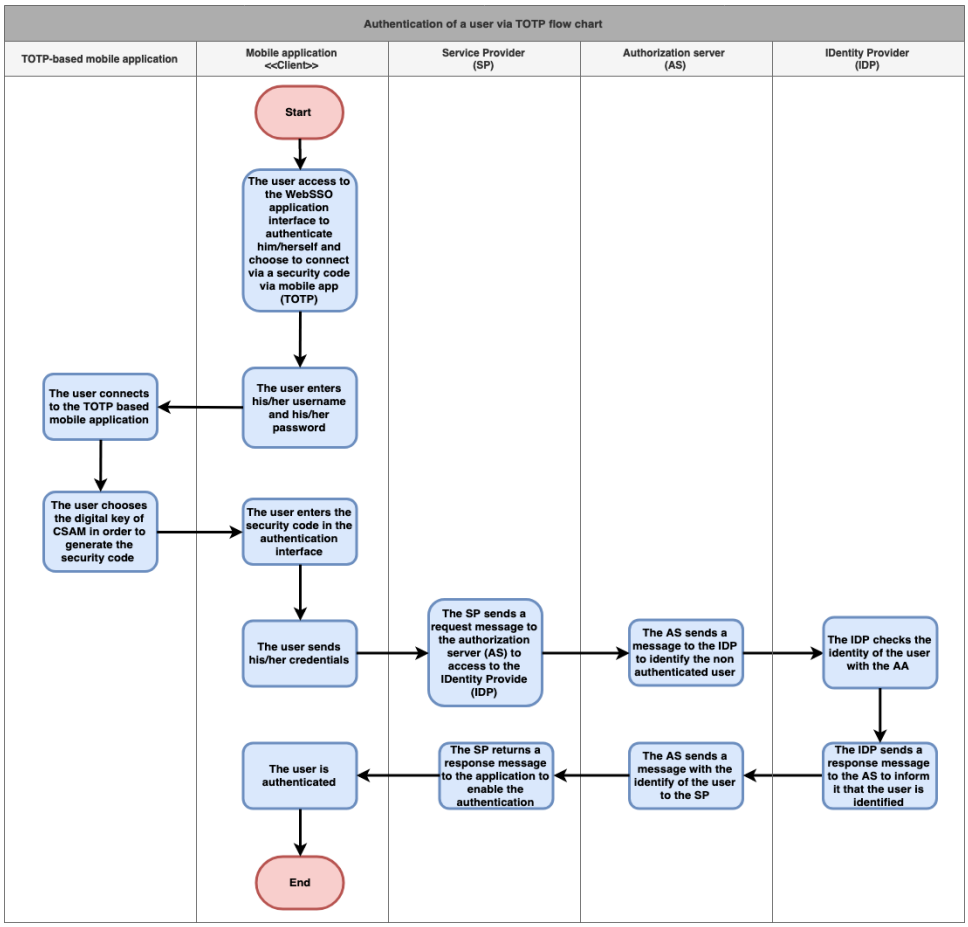
Mobile application supporting the TOTP protocols

There are several mobile applications available that generate a unique time-based security code with which the user can authenticate him /herself. For instance, the following applications support the TOTP protocol:

- Google Authenticator (Android/iPhone/BlackBerry)
- Duo Mobile (Android/iPhone)
- Authenticator (Windows Phone)

Basic flow

Flow	Specification	
	Use case ID	ATH-UC-07-BF
	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	

Alternative flow 1

Specification	
Use case ID	ATH-UC-07-AF-01
Use case name	First authentication via TOTP
Actors	• Citizen • Healthcare giver • Representative of an institution
Short Description	Depending on the profile of the actor, this alternative flow will be instantiated by one of the four use cases dedicated to the creation of a new account (refer to the basic flows): ATH-UC-01, ATH-UC-02, ATH-UC-03, ATH-UC-04. To implement this flow, the user should authenticate him/herself in the mobile application using a TOTP-based mobile application.
Priority	1 (High) Must have: The system must implement this goal/ assumption to be accepted.

Pre-Conditions	• The user has not 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 has an account • The user knows his credentials • The user is authenticated • The user has access to the services of the mobile application
Steps	For more details and depending on the type of the actor, see: • The citizen - ATH-UC-01 • The mandated citizen - ATH-UC-02 • The healthcare giver - ATH-UC-03 • The institution representative - ATH-UC-04
Exceptions (exception flows)	• The user makes an error when editing his/her credentials • 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 wants to authenticate him/herself via TOTP and he/she does not have an account.

Exception flow 1

Specification		
Use case ID	ATH-UC-07-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	ATH-UC-07-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	