FOD Beleid & Ondersteuning
SPF Stratégie & Appui

FAS Assurance Framework

FPS BOSA - DG Simplification & Digitalization
Domain Identification, Authentication and Authorisation (IAA)

Version 1.2

Table of Content

1. Document control

BOSA-SD IAA Governance mandates this section in order to provide enough track records for this document.

1.1 Document Copyright and Classification

1.2 Document history

Version	Date	Author	Description of changes/ Remarks
V.0.1	04/11/2019	BOSA-DG SD IAA	First draft version before IAA comments
V.0.7	16/06/2020	BOSA-DG SD IAA	Internal reviews
V.1.0	16/06/2020	BOSA-DG SD IAA	Internal review English
V.1.1	09/12/2020	BOSA-DG SD IAA	Minor corrections in figures
V.1.2	26/09/2022	BOSA-DG SD IAA	Addition of the digital key myID

1.3 Contact

For information on this document, contact : servicedesk.dto@bosa.fgov.be

2. Introduction

2.1 Scope and objectives of the FAS assurance framework

FAS, The Federal Authentication Service, is one of the services offered as part of Common Secure Access Management - CSAM.

The Gcloud service Identification CSAM (Fiche gCloud version 1.2 – 18/04/2018) contains the following functionalities :

- FAS – Federal Authentication Service
- SMA – Self Management Application / CSAM – My Digital Keys

FAS Definition :

FAS delivers a central standard identification and authentication service to be used by :

- Belgium's citizens and residents
- Foreigners who may request access to Belgian government services

FAS is the platform offering an authentication service, this service supports several digital keys associated with a Level of Assurance (LoA).

The FAS Assurance framework aims to :

- define the basic principles of the different processes and concepts (registration, authentication, identification,...) and set a common defined vocabulary
- define what are the different levels of assurance used
- refer to the guidelines that specify the technical, management and process requirements for the definition of assurance levels

This is an evolving document, it will serve as a basis for introducing new digital keys and methods (e.g. remote identification, biometrics,...) and to improve existing digital keys.

2.2 Not in scope of the FAS assurance framework

- The FAS only authenticates natural persons. The digital keys can be used to authenticate on behalf of an enterprise, through a system of roles and mandates of natural persons. This system of roles and mandates (authorization) is out of scope of the FAS Assurance Framework.
- Consent management - authorization of access
- Classification of data and documents according to a level of assurance

2.3 Audience

The target audience is the application providers (relying parties) and the (candidate) partners for recognition or integration of an electronic identification service into the FAS.

2.4 Definitions

		Examples
Identity Assurance framework	Practices and principles governing the development of the rules framing the FAS	
Assurance levels / Levels of assurance (LoAs)	The assurance level depends on the degree of confidence that electronic identification means provide in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented	eIDAS: Low/substantial/ High
Digital/Electronic identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person	
Authentication	An electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed	
Digital key / Authentication means	'Electronic identification means' is a material and/or immaterial unit containing person identification data and which is used for authentication for an online service	eID, Itsme, myID.be, userid/pwd/TOTP, Token

3. Definition of the FAS assurance framework

The FAS Assurance Framework is based on the eIDAS Assurance framework (COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014).

The eIDAS framework only defines criteria that should be met and is technology neutral. The FAS Assurance Framework implements these criteria with appropriate technologies to the Belgian context, without any deviation from the eIDAS framework.

The FAS Assurance framework only concerns natural persons. The digital keys can be used to authenticate on behalf of a enterprise, through a system of roles and mandates of natural persons (authorization). This system is out of scope of the FAS Assurance Framework.

3.1 Legal reference

Beside the European Regulation that plays an important role within the FAS framework (eIDAS, GDPR, Only Once) Belgian Regulation also frame that matter. Among those:

- Law (18/07/2017) on electronic identification
- Royal decree (22/10/2017) laying down the conditions, procedure and consequences of the approval of electronic identification services for public applications

3.2 Phases and Governance dimension

The FAS is operated by the domain Identification, Authentication and Authorisation (IAA).

Identification is the process of validating a person's attributes and characteristics — including uniqueness — in order to establish his or her digital identity, using person identification data in electronic form. It takes place through identity proofing, which verifies and validates attributes,

such as name, date of birth, fingerprints or iris scans, that the person provides. **It answers to the question : "Who are you ?"**

Authentication is the process of determining if the digital key used to claim a digital identity is valid – that it belongs to the same person who previously established the identity. **It answers to the question : « Are you who you claim to be ? »,** based on one or more identity credential (based on Something I Am, Something I Know, Something I have, and even Something I do).

Authorization: what are you entitled to do ?

The FAS Assurance Framework deals with two important concepts of this domain: Identification and Authentication and a crosscutting Governance dimension.

3.3 The eIDAS regulatory framework

All steps and dimensions considered to assess the LoA of Digital keys used by the FAS are regulated by the E.U. implementing act 2015/1502[1] on setting out minimum technical specifications and procedures for assurance levels for electronic identification means:

Enrolment & Identification

- Application & registration
- Identity proofing and verification

Electronic identity means management

- Electronic means characteristics and design
- Issuance, delivery and activation
- Suspension, revocation and reactivation
- Renewal and replacement

Authentication

- Authentication

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R1502

Governance

- Published notices and user information
- Information Security Management
- Record keeping
- Facilities and staff
- Technical controls
- Compliance and audit

3.4 Three Levels of Assurance

	Degree of confidence in the claimed identity of a person provided	**Use of technical specifications, standards and procedures, including technical controls for the purpose of**
Low	a limited degree	decreasing the risk of abuse or alteration of the identity
Substantial	a substantial degree	decreasing substantially the risk of abuse or alteration of the identity.
High	a higher degree	Preventing the abuse or alteration of the identity.

The criteria sets for each of the three phases and the governance dimension are first assessed separately. Then, the final assurance level of the digital key is determined through the lowest score for the individual factors.

		Password
2,1	ENROLMENT	
2.1.1	Application and registration	high
2.1.2	Identity proofing and verification	high
2,2	ELECTRONIC IDENTIFICATION MEANS MANAGEMENT	
2.2.1	eID means characteristics and design	low
2.2.2	Issuance, delivery and activation	substantial
2.2.3	Suspension, revocation and reactivation	high
2.2.4	Renewal and replacement	high
2,3	AUTHENTICATION	
2.3.1	Authentication mechanism	low
2,4	MANAGEMENT AND ORGANISATION	
2.4.1	General provisions	*tbd*
		=low

Fig. 1 - LoA determination

According to the eIDAS guidance on LoA, the assessment of the strength of a digital key is done taking into account not only the factor(s) itself, but the whole mechanism to verify the factor(s).

4. FAS assurance framework in practice

4.1 Levels of assurance

Fig. 2 - supported EIM & their respective LoA

5. Life Cycle Management

5.1 Understanding the Identity Lifecycle

1. Registration (Identity Proofing)
2. Issuance (Credential Management)
3. Identity Authentication
4. Authorization
5. Identity Management (Identity Maintenance)

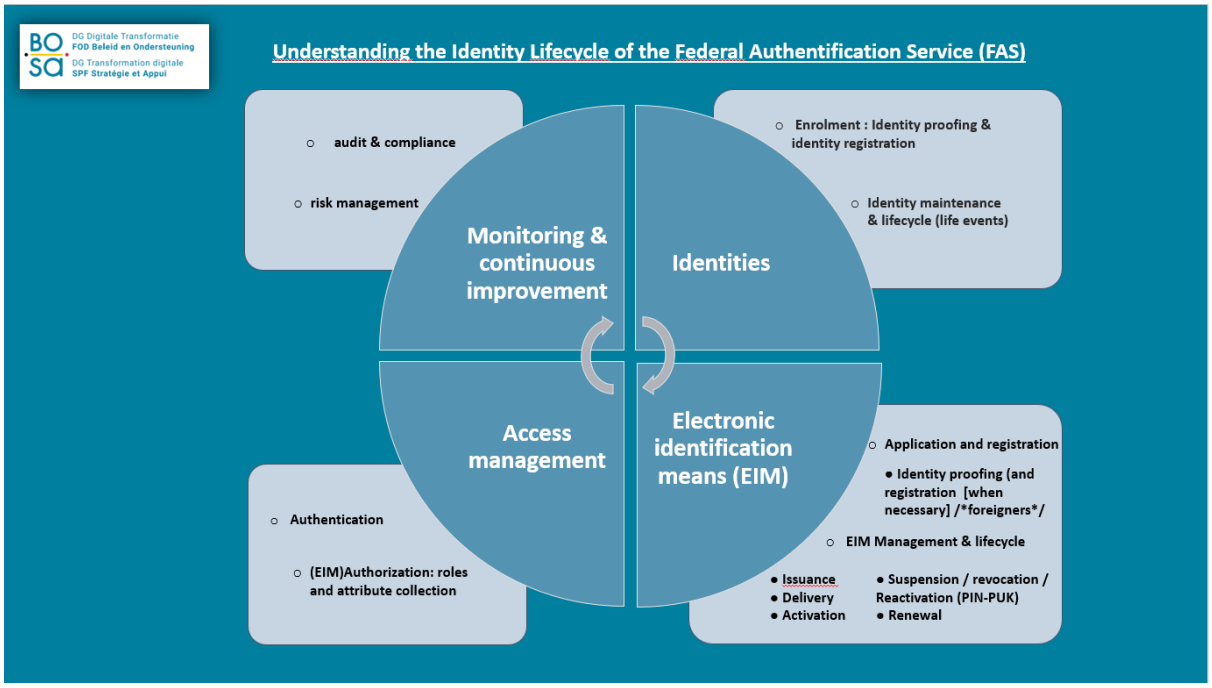

Fig. 3 - FAS & identity lifecycle

Throughout the lifecycle, the identity system (including facilities and staff, record keeping, compliance and auditing) is managed, with updates to the status and content of digital identities and authentications means if needed.

5.2 Person identification data

Person identification data used by the FAS :

- Unique identifier
- Other attributes depending of what is requested by the Relying party

5.3 Management and use of the Digital keys

Digital keys of the FAS Assurance Framework are either :

- Developed and supported in house by DG SD, or
- Developed and supported by a third party and recognized according to Royal Decree 22/10/2017, or
- Developed and supported by a third party and integrated in the FAS for a specific domain or set of applications

The FAS integrates the eIDAS node and mutually recognized notified schemes and digital keys.

Use for authentication in public organizations only.

Single Sign-On (SSO)

Single sign-on (SSO), is the option for users to gain access to various services part of the same circle of trust within the same browser session, performing only one authentication. The user logs in once at the first service and does not have to confirm his/her identity again for other services. There are possible measures required if the user switches from a service by one provider to a service by another provider. Currently, SSO does not allow access to both public and private services.

6. Sources of information

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Gcloud Service fiche CSAM Identification (https://www.gcloud.belgium.be/fr/service/detail/csam)
- Onboarding document