"My digital keys" Version 4.0 – 02/03/2021

CSAM

"MY DIGITAL KEYS - Log on to online public services" - TERMS AND CONDITIONS OF USE

Article 1 - Scope of these Terms and Conditions of use

These Terms and Conditions of Use govern the procedure provided by the federal administration for the electronic registration, identification, and authentication of end users, whether or not citizens of Belgium. End users are able to use this procedure to gain secure access to electronic services of the federal administration and for the purpose of secure electronic communication with the federal administration.

Nevertheless, it may be the case that some public bodies make use of other systems for electronic end-user management.

Article 2 - Access to the procedure

The end user shall have access to the procedure, but without any guarantee of being assured access to the procedure and offered services at all times nor any guarantee that the procedure is free of errors or technical faults.
Access to the procedure may be closed completely or partially at any time (including for, but not limited to, maintenance purposes). In so far as reasonably possible, the end user will be notified of any such interruption in advance.
The end user shall only have access to particular services provided by the federal administration once he/she has completed the applicable procedure for registration, identification, and authentication.
In doing so, the end user shall:

- declare his/her agreement to the present Terms and Conditions of Use;
- shall provide a correct e-mail address.

The end user is obliged to amend the data that concern him/her in order to ensure they are up to date and accurate at all times.

Article 3 - Use of digital keys

The end user's access to certain services provided electronically requires the use of digital keys (eID, security code via mobile app/SMS/e-mail and user name and password, etc.).

Some digital keys are provided entirely by FPS Policy and Support − DG Digital Transformation, while some digital keys are provided by other parties accredited by FPS Policy and Support − DG Digital Transformation. These parties can only be accredited once compliance with strict security and privacy requirements provided for in the Belgian Royal Decree of 22 October 2017 establishing the conditions, the procedure and the effects of the accreditation of services for electronic identification for government applications, as well as other requirements, has been confirmed.

These digital keys and the associated data are strictly personal and non-transferable.
All end users shall be responsible for the proper safekeeping, security, confidentiality and management of their digital keys and the data associated with them.
The end user shall be responsible for choosing a secure password or other secret code.

Should the end user become aware of the loss of his/her user name, password or other digital key, or of any unauthorised use thereof by third parties, or suspects such loss or unauthorised use, he/she must take all necessary measures without delay to deactivate the digital key as stipulated in Article 6 and elsewhere.
In the event that his/her digital key is locked, the end user must request a new one.

Article 4 - Use of the e-mail address

The end user shall be responsible for the choice of e-mail address that he/she has provided. He/she declares that this e-mail address belongs to him/her and that third parties cannot use it without his/her permission.

The end user confirms that he/she uses this address regularly.

Article 5 - Use of the procedure

All end users are obliged to:
1. provide complete, accurate, truthful, and non-misleading information;
2. to comply with the provisions stipulated by a law, regulation, decree, ordinance or decision by the federal administration, or a regional, local or international authority;
3. to refrain from tampering with the information provided in any way whatsoever or using any kind of technique whatsoever.

Article 6 - Procedure in the event of loss or change of a digital key or a part of a digital key

In the event of loss or theft of an identity card, the holder is required to report this to his/her local municipal administration office or nearest police station as soon as possible, or to contact the DocStop service of FPS Interior.

In the event that an end user loses his/her smartphone/mobile phone or this has been stolen, he/she is required to report this to his/her service provider as soon as possible. He/she must also delete the relevant keys (security code via the mobile app and/or security code via SMS, and/or security code via email) under "My digital keys".

If an end user wishes to use a new mobile number, he/she is required to delete the key "security code via SMS" for the old number first.

If an end user loses his/her token, he/she must deactivate it. The old token will be deactivated immediately and can no longer be used from that point.

Article 7 - Protection of privacy

The federal administration shall take responsibility for your privacy and act in accordance with the provisions of Belgian and EU data protection legislation at all times.
You can view our Privacy Notice here.

Article 8 - Definitions

For the purposes of these Terms and Conditions, the terms below are understood to have the following meanings:

- **Registration** - The process by which a person requests to be added to a list by following a prescribed procedure, and therefore indicates that he/she wishes to use a particular service.

- **Identification** -A process that is used to establish the identity of a particular person.
- **Authentication** - A process that is used to confirm the identity of a particular person. For example, a person can confirm that they are indeed the person he/she claims to be by providing certain confidential data that are known only to him/her (e.g. a password he/she has chosen him/herself).