1 april 2026

Gebruikersreglement voor de toegang en het gebruik van het informatiesysteem van de federale overheid en de openbare instellingen van sociale zekerheid door burgers en hun lasthebbers

Artikel 1. - Toepassingsgebied

Dit gebruikersreglement regelt de toegang tot en het gebruik van het informatiesysteem van de federale overheid en de openbare instellingen van sociale zekerheid (hierna informatiesysteem genoemd) en de daardoor aangeboden diensten door burgers en hun lasthebbers.

Artikel 2 - Definitie

Onder "elektronische identiteitskaart" in de zin van dit gebruikersreglement wordt verstaan de elektronische identiteitskaart bedoeld in de artikelen 6 en volgende van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten waarop de identiteits- en de handtekeningscertificaten zijn geactiveerd.

Artikel 3. – Aangeboden diensten en beschikbare kanalen

De aangeboden diensten zijn toegankelijk via verschillende kanalen.

1. Via de portaalsite van de sociale zekerheid (www.socialezekerheid.be):

a) elke gebruiker heeft toegang tot de toepassingen opgenomen in de tabel in "BIJLAGE 1 – Toepassingen via de portaalsite van de sociale zekerheid", voor zover hij de nodige toegangsrechten heeft;
b) voor de toegang tot deze toepassingen kan een digitale sleutel vereist zijn. Elk van deze digitale sleutels is voorzien van een betrouwbaarheidsniveau. Wanneer dit niveau voldoende is voor toegang tot een toepassing, dan geldt dit eveneens voor de andere digitale sleutels behorend tot hetzelfde niveau of tot een hoger niveau. De tabel geeft per toepassing weer welke digitale sleutels van voldoende niveau zijn. Toekomstige nieuwe digitale sleutels zullen onmiddellijk kunnen aangewend worden in overeenstemming met hun betrouwbaarheidsniveau.

2. Via de portaalsite van de federale overheid (www.belgium.be):

a) elke gebruiker heeft toegang tot de toepassingen opgenomen in de tabel in "BIJLAGE 2 – Toepassingen via de portaalsite van de federale overheid", voor zover hij de nodige toegangsrechten heeft;
b) voor de toegang tot deze toepassingen kan een digitale sleutel vereist zijn. Elk van deze digitale sleutels is voorzien van een betrouwbaarheidsniveau. Wanneer dit niveau voldoende is voor toegang tot een toepassing, dan geldt dit eveneens voor de andere digitale sleutels behorend tot hetzelfde niveau of tot een hoger niveau. De tabel geeft per toepassing weer welke digitale sleutels van voldoende niveau zijn. Toekomstige nieuwe digitale sleutels zullen onmiddellijk kunnen aangewend worden in overeenstemming met hun betrouwbaarheidsniveau.

3. Via de portaalsite eGezondheid (www.ehealth.fgov.be):

   a) elke gebruiker heeft toegang tot de toepassingen opgenomen in de tabel in "BIJLAGE 3 – Toepassingen via de portaalsite eGezondheid", voor zover hij de nodige toegangsrechten heeft;
   b) voor de toegang tot deze toepassingen kan een digitale sleutel vereist zijn. Elk van deze digitale sleutels is voorzien van een betrouwbaarheidsniveau. Wanneer dit niveau voldoende is voor toegang tot een toepassing, dan geldt dit eveneens voor de andere digitale sleutels behorend tot hetzelfde niveau of tot een hoger niveau. De tabel geeft per toepassing weer welke digitale sleutels van voldoende niveau zijn. Toekomstige nieuwe digitale sleutels zullen onmiddellijk kunnen aangewend worden in overeenstemming met hun betrouwbaarheidsniveau.

De inhoud van de diensten en de toegang tot deze diensten kunnen te allen tijde worden gewijzigd.

Artikel 4. - Toegang tot het informatiesysteem

De gebruiker heeft toegang tot het informatiesysteem zonder dat evenwel gewaarborgd wordt dat de toegang tot het informatiesysteem en de geboden diensten te allen tijde verzekerd is en vrij is van fouten of technische storingen.

De toegang tot het informatiesysteem en de diensten die via het systeem worden geleverd kan te allen tijde geheel of gedeeltelijk worden afgesloten (o.m. voor onderhoudsdoeleinden). In de mate van het mogelijke zal de gebruiker op voorhand op de hoogte worden gebracht van dergelijke onderbreking.

De gebruiker is verantwoordelijk voor het voorzien in en het onderhoud van de terminal die nodig is voor het gebruik van het informatiesysteem. De aanbieders van het informatiesysteem zijn niet verantwoordelijk voor de terminal en het gebruik dat ervan wordt gemaakt en zijn niet gehouden tot het bieden van enige ondersteuning dienaangaande.

Artikel 5. - Het gebruik van de digitale sleutels

De toegang van de Gebruiker tot bepaalde langs elektronische weg aangeboden diensten vereist het gebruik van digitale sleutels (zoals eID kaartlezer, beveiligingscode op basis van TOTP (Time-based One-time password) via mobiele app, SMS of email, en gebruikersnaam en wachtwoord, (mobiele) sleutels aangeboden in het kader van diensten erkend conform het KB van 22 oktober 2017 tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor overheidstoepassingen, en digitale sleutels erkend overeenkomstig artikel 6 van de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, hierna "eIDAS-middel" genoemd (zie https://sma-help.bosa.belgium.be/nl/eidas#7258).

Deze digitale sleutels en de gegevens eraan verbonden zijn strikt persoonlijk en niet overdraagbaar.

Elke eindgebruiker is verantwoordelijk voor de goede bewaring, beveiliging, geheimhouding en beheer van zijn digitale sleutels en gegevens eraan verbonden.

De eindgebruiker is verantwoordelijk voor de keuze van een veilig wachtwoord of andere geheime code.

Indien een eindgebruiker kennis heeft van het verlies van zijn gebruikersnaam, wachtwoord of ander digitale sleutel, of van elk ongeoorloofd gebruik ervan door derden, of een dergelijk verlies of ongeoorloofd gebruik vermoedt, dient hij onmiddellijk alle nodige maatregelen te treffen om de digitale sleutel te deactiveren.

In geval van vergrendeling van zijn digitale sleutel, dient de eindgebruiker een nieuwe aan te vragen.

De digitale sleutels worden aangewend in het kader van CSAM (zie https://www.csam.be). Het aanmaken en gebruik daarvan worden ook geregeld in de gebruikersovereenkomst van CSAM. Sommige digitale sleutels zijn niet beschikbaar gesteld voor elke toepassing.

Artikel 6. - Gebruik van het informatiesysteem

Met betrekking tot het gebruik van het informatiesysteem en de via dit systeem verleende diensten, is elke gebruiker ertoe gehouden:

1. volledige, accurate, waarachtige en niet-misleidende informatie te verstrekken;
2. de door wet, reglement, decreet, ordonnantie of besluit van de federale, regionale, lokale of internationale overheid voorgeschreven bepalingen na te leven;
3. zich te onthouden van het manipuleren van de geleverde informatie, op welke wijze dan ook of met gebruik van eender welke techniek;
4. via het informatiesysteem geen gegevens, berichten of documenten te versturen op eender welke wijze, hetzij gegevens of documenten via het informatiesysteem op te laden:
    a) waarbij de rechten (waaronder persoonlijkheidsrechten of intellectuele eigendomsrechten) van derden of van de aanbieders van het informatiesysteem worden geschonden;
    b) waarvan de inhoud onwettig, schadeberokkenend, lasterlijk, gewelddadig, obsceen of onterend is of waarbij de privacy van derden wordt geschonden;
    c) waarvan het gebruik of het bezit door de gebruiker bij wet of bij overeenkomst verboden is;
    d) die virussen of instructies bevatten die schade kunnen toebrengen aan de aanbieders van het informatiesysteem en/of het informatiesysteem en/of de via het informatiesysteem verleende diensten in het gedrang zouden kunnen brengen of verstoren.

Artikel 7. - Gebruik van het certificaat van de elektronische identiteitskaart

De toegang van de gebruiker tot bepaalde diensten vereist het gebruik van een elektronische identiteitskaart.

Indien de toegang tot de aangeboden diensten via een elektronische identiteitskaart gebeurt, wordt de authenticatie gerealiseerd door het identiteitscertificaat van de kaart en wordt de elektronische handtekening aangebracht via het handtekeningscertificaat van de kaart.

Zodra de private sleutel aangemaakt is, is de certificaathouder alleen verantwoordelijk voor de vertrouwelijkheid ervan. Wanneer er twijfel bestaat over het behoud van de vertrouwelijkheid

van de private sleutel of wanneer de in het certificaat opgenomen gegevens niet meer met de werkelijkheid overeenstemmen, dient de houder het certificaat te laten herroepen. Wanneer een certificaat vervalt of herroepen wordt, mag de houder na de vervaldatum van het certificaat of na herroeping geen gebruik meer maken van de overeenkomstige private sleutel om zich aan te melden of om gegevens te ondertekenen of om zijn gegevens te laten certificeren door een andere certificatiedienstverlener.

Elke gebruiker dient derhalve zorgvuldig om te gaan met de private sleutel en het certificaat evenals met het eventuele paswoord dat nodig is om de private sleutel en het certificaat te gebruiken. De gebruiker is aansprakelijk voor elk al dan niet geoorloofd gebruik ervan, met inbegrip van elk gebruik door derden.

Artikel 8. - Gebruik van de elektronische handtekening en bewijs

De berichten die via het informatiesysteem door de gebruiker worden verstuurd met gebruik van het handtekeningscertificaat van de elektronische identiteitskaart, zijn voorzien van een elektronische handtekening, bedoeld in boek 8, artikel 8.1, 3° van het Burgerlijk Wetboek.

De gebruiker erkent uitdrukkelijk dat alle berichten die via het informatiesysteem worden verstuurd en die voorzien zijn van voornoemde elektronische handtekening dezelfde bewijskracht hebben als een onderhandse akte in de zin van het Burgerlijk Wetboek.

De gebruiker erkent uitdrukkelijk dat alle informatie betreffende berichten die door de aanbieders van het informatiesysteem op een duurzame en niet te wijzigen manier opgeslagen wordt, dezelfde bewijskracht heeft als een onderhandse akte in de zin van het Burgerlijk Wetboek, tot het tegendeel bewezen wordt.

De gebruiker erkent uitdrukkelijk als de zijne de handtekening die geplaatst is op basis van de elektronische identiteitskaart en, behalve in geval van misbruik, verlies, of diefstal, voor zover de daartoe voorziene procedure werd nageleefd.

Artikel 9. - Controleplicht van de gebruiker

De gebruiker is verantwoordelijk voor de controle van de inhoud van de door hem via het informatiesysteem verstuurde berichten en voor de opvolging daarvan naar aanleiding van berichten die door de aanbieders van het informatiesysteem aan de gebruiker worden verstuurd en die betrekking hebben op de (het) door de gebruiker verstuurde bericht(en).

De materiële fout(en) in een door de gebruiker verstuurd bericht, in een ontvangstmelding die daarop betrekking heeft of in eender welk ander bericht of document dat op de gebruiker betrekking heeft en dat toegankelijk is via het informatiesysteem, word(t)(en) op verzoek van de gebruiker via een daartoe voorziene rechtzettingsprocedure verbeterd.

Artikel 10. - Intellectuele eigendomsrechten

De gebruiker erkent en aanvaardt dat het informatiesysteem, de dienstverlening en de software die in verband met het informatiesysteem en de dienstverlening is ontwikkeld, beschermd worden door intellectuele eigendomsrechten (auteursrecht, merkenrecht, octrooirecht, enz.),

waarvan de aanbieders van het informatiesysteem (of haar licentieverstrekkers) de houder(s) zijn.

De gebruiker verkrijgt een niet-exclusief recht om het informatiesysteem te gebruiken voor de in het gebruikersreglement beschreven doeleinden. Behoudens uitdrukkelijke toestemming is het de gebruiker niet toegelaten om op welke wijze ook het informatiesysteem geheel of gedeeltelijk te kopiëren (op welke manier of op welke drager dan ook), aan te passen, te vertalen, te verkopen, te verhuren, uit te lenen, mede te delen aan het publiek, noch afgeleide werken van voormelde elementen te creëren.

Artikel 11 – Autenticatiemiddelen en zekerheidsniveaus

Authenticatiemiddelen worden gebruikt om de identiteit van een gebruiker betrouwbaar vast te stellen en zijn cruciaal voor digitale veiligheids- en toegangscontrole. De Federal Authentication Service (FAS) van de FOD BOSA biedt hiervoor verschillende middelen aan, die bijvoorbeeld door de KSZ en het eHealth-platform gebruikt worden om burgers en professionals veilig toegang te geven tot gevoelige toepassingen.

Het betrouwbaarheidsniveau (of zekerheidsniveau) van een authenticatiemiddel – hoe zeker het is dat iemand werkelijk is wie hij beweert te zijn – wordt volgens Europese regelgeving aangeduid als laag, substantieel of hoog. De FAS specificeert dit niveau ook met een cijfer (het FAS-authenticatieniveau) voor meer nauwkeurigheid.

De FOD BOSA publiceert een overzicht van de beschikbare middelen:

Betrouwbaarheidsniveau	FAS Authenticatieniveau	Authenticatiemiddel
Hoog	500	eID
		eIDAS4 Hoog
	490	MyGov.be Hoog (met PIN)
	450	Itsme Hoog (met PIN)
Substantieel	400	eIDAS Substantieel
		Itsme Substantieel (met vingerafdruk)
		MyGov.be Substantieel (met vingerafdruk)
		TOTP (via Authenticator App)
		TOTP (via mail)
		TOTP (via SMS)
Laag	200	Username / Password

BIJLAGE 1 – Toepassingen via de portaalsite van de sociale zekerheid

Toepassing	UID/PWD +toekomstige (laag)	TOTP ITSME MyGov.be eIDAS +toekomstige (substantieel)	eID ITSME MyGov.be X509 cert. eIDAS +toekomstige (hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
Berekening inkomensgarantie-uitkering	Voor deze toepassingen is geen digitale sleutel vereist		
Berekenen van de beroepsinschakelingstijd			
Coming2Belgium			
België verlaten			
Jobcalc			
Checkin at work	Ja	Ja	Ja
Controlekaart volledige werkloosheid (eC3)			
Controlekaart tijdelijke werkloosheid - eC32			
Fonds Sluiting Onderneming			
Loopbaanonderbreking en tijdskrediet			
Mijn vakantierekening (raadpleging)			
Horeca@work - 50 days			
Interim@work			
My e-box	Nee	Ja	Ja
Pensioen-aanvraag			
MyPension			
Mijn aanvullend pensioen			
MyCareer			
Mijn werkloosheidsdossier			
Mijn vakantierekening (wijziging)			
MyBenefits			
MyHandicap			
CEDRIC			
Student@work			
Vrijstelling sociale bijdragen zelfstandigen			
Werken in het buitenland - Zelfstandigen			
Verenigingswerk			
Working in the Arts – Kunstwerkattest	Nee	Ja	Ja
Working in the Arts – Amateurkunstenvergoeding	Nee	Ja	Ja
Check In and Out at Work	Nee	Ja	Ja
Sociaal internetaanbod	Nee	Nee	Ja
Burgermandaten	Nee	Ja	Ja
Toegangtotmijndata	Nee	Ja	Ja
CPAS Online[1]	Nee	Ja	Ja

[1] Er bestaat ook een niet beveiligde versie

Inzetbaarheidsbevorderende maatregelen	Nee	Ja	Ja

BIJLAGE 2 – Toepassingen via de portaalsite van de federale overheid

Toepassing	UID/PWD +toekomstige (laag)	TOTP ITSME MyGov.be eIDAS +toekomstige (substantieel)	eID ITSME MyGov.be X509 cert. eIDAS +toekomstige (hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
2003 – Verkiezingen	Voor deze toepassingen is geen digitale sleutel vereist		
2004 – verkiezingen			
2007 – Resultaten federale verkiezingen			
Gemeenschappelijke catalogus			
Betalen met dienstencheques			
Forfaitaire vermindering energietarieven (Energie-korting)	Ja	Ja	Ja
Police-on-web	Nee	Ja	Ja
my.belgium.be			
Tax-on-web -dienst			

BIJLAGE 3 – Toepassingen via de portaalsite eGezondheid

Toepassing	UID/PWD +toekomstige (laag)	TOTP ITSME MyGov.be eIDAS +toekomstige (substantieel)	eID ITSME MyGov.be X509 cert. eIDAS +toekomstige (hoog)
	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE	Voldoende niveau JA/NEE
eTCT - Feedback aan de ziekenhuizen over de door hen verstrekte zorg en de kost ervan	Voor deze toepassingen is geen digitale sleutel vereist		
Authentieke Bron Implanteerbare Medische Hulpmiddelen			
Healthdata.be Data Reporting			
Software Register - officieel en gedeeld kadaster van gezondheidssoftware			
CEBAM Digital library for Health / CDLH / EMBPRACTICENET	Ja	Ja	Ja
Orgadon - Donatie menselijk lichaamsmateriaal: wilsverklaring			
E-loket Zorg en Gezondheid	Nee	Ja	Ja
Accreditering			
Platform Welzijn en Gezondheid			
Mijn Gezondheid			
Web Application Metahub			
eHealthConsent			
Moduledata-bank Jeugdhulp Vlaanderen			
Centraal tracerings-register			
Belrai mobile			
Uniek Portaal			