27. Juni 2018

Benutzerordnung betreffend den Zugriff auf das Informationssystem der Föderalbehörde und der öffentlichen Einrichtungen der sozialen Sicherheit und die Benutzung dieses Systems durch Bürger und ihre Bevollmächtigten

Artikel 1 − Anwendungsbereich

Diese Benutzerordnung regelt den Zugriff auf das Informationssystem des föderalen Dienstes und der öffentlichen Einrichtungen der sozialen Sicherheit (hiernach Informationssystem genannt) und zu den dadurch angebotenen Diensten und die Benutzung dieses Systems durch Bürger und ihre Bevollmächtigten.

Artikel 2 − Begriffsbestimmung

Mit „elektronischem Personalausweis“ im Sinne dieser Benutzerordnung ist der elektronische Personalausweis im Sinne der Artikel 6 ff. des Gesetzes vom 19. Juli 1991 über die Bevölkerungsregister und die Personalausweise und zur Abänderung des Gesetzes vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen gemeint, auf dem die Identitäts- und Signaturzertifikate aktiviert wurden.

Artikel 3 – Angebotene Dienste und zur Verfügung stehende Kanäle

Die angebotenen Dienste sind über verschiedene Kanäle zugänglich.

1. Über das Internetportal der sozialen Sicherheit (www.sociale-zekerheid.be):

a) jeder Benutzer hat Zugriff auf die in der Tabelle in „ANLAGE 1 − Anwendungen über das Internetportal der sozialen Sicherheit“ aufgeführten Anwendungen;
b) für den Zugriff auf diese Anwendungen kann ein digitaler Schlüssel erforderlich sein. Jeder dieser digitalen Schlüssel hat eine bestimmte Zuverlässigkeit. Wenn diese für den Zugriff auf eine Anwendung ausreicht, so gilt dies auch für die anderen digitalen Schlüssel der gleichen oder einer höheren Ebene. Die Tabelle gibt pro Anwendung an, welche digitalen Schlüssel die entsprechende Zuverlässigkeit besitzen. Zukünftige neue digitale Schlüssel können entsprechend ihrer Zuverlässigkeit sofort verwendet werden.

2. Über das Internetportal des föderalen Dienstes (www.belgium.be):

a) jeder Benutzer hat Zugriff auf die in der Tabelle in „ANLAGE 2 − Anwendungen über das Internetportal des föderalen Dienstes“ aufgeführten Anwendungen;
b) für den Zugriff auf diese Anwendungen kann ein digitaler Schlüssel erforderlich sein. Jeder dieser digitalen Schlüssel hat eine bestimmte Zuverlässigkeit. Wenn diese für den Zugriff auf eine Anwendung ausreicht, so gilt dies auch für die anderen digitalen Schlüssel der gleichen oder einer höheren Ebene. Die Tabelle gibt pro Anwendung an, welche digitalen Schlüssel die entsprechende Zuverlässigkeit besitzen. Zukünftige neue digitale Schlüssel können entsprechend ihrer Zuverlässigkeit sofort verwendet werden.

3. Über das Internetportal von eHealth (www.ehealth.fgov.be)

   a) jeder Benutzer hat Zugriff auf die in der Tabelle in „ANLAGE 3 − Anwendungen über das Internetportal eHealth“ aufgeführten Anwendungen;
   b) für den Zugriff auf diese Anwendungen kann ein digitaler Schlüssel erforderlich sein. Jeder dieser digitalen Schlüssel hat eine bestimmte Zuverlässigkeit. Wenn diese für den Zugriff auf eine Anwendung ausreicht, so gilt dies auch für die anderen digitalen Schlüssel der gleichen oder einer höheren Ebene. Die Tabelle gibt pro Anwendung an, welche digitalen Schlüssel die entsprechende Zuverlässigkeit besitzen. Zukünftige neue digitale Schlüssel können entsprechend ihrer Zuverlässigkeit sofort verwendet werden.

Der Inhalt der Dienstleistungen und der Zugriff auf diese Dienstleistungen können jederzeit geändert werden.

Artikel 4 − Zugriff auf das Informationssystem

Der Benutzer hat Zugriff auf das Informationssystem, ohne dass jedoch gewährleistet ist, dass der Zugriff auf dieses System und die angebotenen Dienste jederzeit gesichert oder frei von Fehlern oder technischen Störungen ist.

Der Zugriff auf das Informationssystem und die angebotenen Dienste kann jederzeit ganz oder teilweise (u. a. zu Wartungszwecken) gesperrt werden. Im Rahmen des Möglichen wird der Benutzer über eine derartige Unterbrechung im Voraus informiert.

Der Benutzer ist für die Bereitstellung und Wartung des Terminals verantwortlich, das zur Benutzung des Informationssystems erforderlich ist. Die Anbieter des Informationssystems sind nicht für das Terminal und dessen Benutzung verantwortlich und sind nicht verpflichtet, diesbezüglich irgendeine Unterstützung zu bieten.

Artikel 5 − Verwendung des digitalen Schlüssels

Der Zugriff des Benutzers auf bestimmte auf elektronischem Weg angebotene Dienste erfordert die Verwendung eines digitalen Schlüssels (wie das eID-Kartenlesegerät, ein auf TOTP (Time-based One-time Password) basierender Sicherheitscode per mobiler App oder SMS, ein Bürgertoken und Benutzername plus Passwort, (mobile) Schlüssel, die im Rahmen der durch den K. E. vom 22. Oktober 2017 zur Festlegung der Bedingungen, des Verfahrens und der Folgen der Anerkennung von Diensten zur elektronischen Identifizierung für Regierungsanwendungen anerkannt sind).

Diese digitalen Schlüssel und die damit verbundenen Daten sind strikt personengebunden und nicht übertragbar.

Jeder Endbenutzer ist für die korrekte Aufbewahrung, Sicherheit, Geheimhaltung und Verwaltung seiner digitalen Schlüssel und der damit verbundenen Daten verantwortlich.

Der Endbenutzer ist für die Wahl eines sicheren Kennworts oder sonstigen geheimen Codes verantwortlich.

Falls der Endbenutzer sich des Verlustes seines Benutzernamens, Kennworts, Bürgertokens oder sonstigen digitalen Schlüssels bewusst ist, oder einer unerlaubten Nutzung derselben

durch Dritte, oder er einen solchen Verlust oder eine unerlaubte Nutzung vermutet, muss er unmittelbar sämtliche erforderlichen Maßnahmen ergreifen, um die digitalen Schlüssel zu deaktivieren.

Im Falle einer Verriegelung seines digitalen Schlüssels muss der Endbenutzer einen neuen beantragen.

Die digitalen Schlüssel werden im Rahmen von CSAM angewendet (siehe https://www.csam.be). Deren Erstellung und Benutzung unterliegen daher den Vorschriften der Benutzervereinbarung von CSAM. Einige digitale Schlüssel stehen nicht für jede Anwendung zur Verfügung.

Artikel 6 − Benutzung des Informationssystems

In Bezug auf die Benutzung des Informationssystems und der über dieses System angebotenen Dienstleistungen ist jeder Benutzer dazu verpflichtet:

1. vollständige, zutreffende, wahrheitsgemäße und nicht-irreführende Informationen zu erteilen;
2. die kraft Gesetz, Ordnung, Erlass, Verfügung oder Beschluss der föderalen, regionalen, lokalen oder internationalen Behörde vorgeschriebenen Bestimmungen zu respektieren;
3. die erteilten Informationen nicht zu manipulieren, auf welche Weise oder mit welcher Technik auch immer;
4. über das Informationssystem keine Daten, Meldungen oder Dokumente auf irgendwelche Weise zu versenden, bzw. Daten oder Dokumente über das Informationssystem zu senden:
   a) bei denen die Rechte (darunter Persönlichkeitsrechte oder geistige Eigentumsrechte) von Dritten oder der Anbieter des Informationssystems verletzt werden;
   b) deren Inhalt illegal, schädigend, verleumderisch, gewalttätig, obszön oder entwürdigend ist oder durch den die Privatsphäre Dritter verletzt wird;
   c) deren Benutzung oder Besitz durch den Benutzer kraft Gesetz oder durch Vertrag untersagt ist;
   d) die Viren oder Anweisungen enthalten, welche den Anbietern des Informationssystems und/oder dem Informationssystem Schaden zufügen könnten und/oder die die per Informationssystem angebotenen Dienste beeinträchtigen oder stören könnten.

Artikel 7 − Benutzung des Zertifikats des elektronischen Personalausweises

Der Zugriff des Benutzers auf bestimmte Dienstleistungen erfordert die Benutzung eines elektronischen Personalausweises. Wenn der Zugriff auf die angebotenen Dienste über einen elektronischen Personalausweis erfolgt, wird die Authentifizierung durch das Identitätszertifikat der Karte vorgenommen und die elektronische Signatur über das Signaturzertifikat der Karte angebracht.

Sobald der Privatschlüssel erstellt ist, ist nur der Zertifikatsinhaber für die Vertraulichkeit dieser Daten verantwortlich. Wenn Zweifel über den Erhalt der Vertraulichkeit des Privatschlüssels bestehen oder die im Zertifikat aufgenommenen Daten nicht mehr der Realität entsprechen, muss der Inhaber das Zertifikat widerrufen lassen. Wenn ein Zertifikat ungültig oder widerrufen wird, darf der Inhaber nach dem Fälligkeitsdatum des Zertifikats oder nach dem Widerruf den entsprechenden Privatschlüssel nicht mehr benutzen, um diese

Daten zu unterzeichnen oder durch einen anderen Zertifizierungsdiensteanbieter zertifizieren zu lassen.

Jeder Benutzer muss daher mit dem Privatschlüssel und dem Zertifikat sowie dem für die Benutzung des Privatschlüssels und des Zertifikats erforderlichen Kennworts sorgfältig umgehen. Der Benutzer ist haftbar für jede diesbezügliche erlaubte Benutzung, einschließlich jeder Benutzung durch Dritte.

Artikel 8 − Benutzung der elektronischen Signatur und Nachweis

Die Meldungen, die über das Informationssystem durch den Benutzer mittels Benutzung des Signaturzertifikats des elektronischen Personalausweises versandt werden, umfassen eine elektronische Signatur im Sinne von Art. 1322, Abs. 2 des Zivilgesetzbuchs.

Der Benutzer erkennt ausdrücklich an, dass alle Meldungen, die über das Informationssystem versandt werden und mit der oben genannten elektronischen Signatur versehen sind, die gleiche Beweiskraft wie eine Privaturkunde im Sinne des Zivilgesetzbuchs haben.

Der Benutzer erkennt ausdrücklich an, dass alle Informationen über Meldungen, die durch die Anbieter des Informationssystems auf dauerhafte und nicht zu ändernde Weise gespeichert werden, dieselbe Beweiskraft wie eine Privaturkunde im Sinne des Zivilgesetzbuchs haben, bis das Gegenteil nachgewiesen wurde.

Der Benutzer erkennt ausdrücklich die Signatur als die seinige an, die anhand des elektronischen Personalausweises unter Einhaltung des dazu vorgesehenen Verfahrens geleistet wurde, außer im Falle eines Missbrauchs, Verlustes oder Diebstahls.

Artikel 9 − Kontrollpflicht des Benutzers

Der Benutzer ist verantwortlich für die Kontrolle des Inhalts der durch ihn über das Informationssystem versandten Meldungen und für die betreffende Betreuung anlässlich von Meldungen, die durch die Anbieter des Informationssystems an den Benutzer gesandt werden und die sich auf den/die durch den Benutzer versandte(n) Meldung(en) beziehen.

Der/die materielle(n) Fehler in einer vom Benutzer versandten Meldung, in einer Empfangsmeldung, die sich darauf bezieht oder in jeder anderen Meldung oder jedem anderen Dokument, die bzw. das sich auf den Benutzer bezieht und die bzw. das über das Informationssystem zugänglich ist, wird bzw. werden auf Verlangen des Benutzers über ein dazu vorgesehenes Berichtigungsverfahren korrigiert.

Artikel 10 − Geistige Eigentumsrechte

Der Benutzer erkennt an und akzeptiert, dass das Informationssystem, die Dienstleistungen und die Software, die im Zusammenhang mit dem Informationssystem und den Dienstleistungen entwickelt wurde, durch geistige Eigentumsrechte geschützt werden (Urheberrecht, Markenrecht, Patentrecht etc.), von denen die Anbieter des Informationssystems (oder seine Lizenzerteiler) der/die Inhaber sind.

Der Benutzer erhält ein nichtexklusives Recht, das Informationssystem zu den in der Benutzerordnung beschriebenen Zwecken zu benutzen. Vorbehaltlich der ausdrücklichen Genehmigung ist es dem Benutzer nicht gestattet, das Informationssystem wie auch immer ganz oder teilweise zu kopieren (wie auch immer oder auf welchem Träger auch immer), zu ändern, zu übersetzen, zu verkaufen, zu vermieten, auszuleihen, der Öffentlichkeit mitzuteilen bzw. abgeleitete Werke der oben genannten Elemente zu erzeugen.

ANLAGE 1 − Anwendungen über das Internetportal der sozialen Sicherheit

Anwendung	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App oder SMS) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
Berechnung der Einkommensgarantieunterstützung	Für diese Anwendungen ist kein digitaler Schlüssel erforderlich		
Berechnung der Berufseingliederungszeit			
Beschäftigungsmaßnahmen			
Simulation des Sozialbeitrags Selbständige			
Berechnen Sie selbst Ihr Kindergeld			
Checkinatwork	Ja	Ja	Ja
Kontrollkarte Vollarbeitslosigkeit (eC3)			
Kontrollkarte Vollarbeitslosigkeit (eC32)			
Betriebsschließungsfonds			
Laufbahnunterbrechung und Zeitkredit			
Mein Urlaubskonto (Abfrage)			
Horeca@work − 50 days			
Interim@work			
e-Box Bürger	Nein	Nein	Ja
Pensionsantrag			
MyPension			
Zusatzrente			
MyCareer			
Kontrollkarte Vollarbeitslosigkeit − eC32			
Meine Arbeitslosenakte			
Handiweb			
Beschäftigungsmaßnahmen			
Mein Urlaubskonto (Änderung)			
MyHandicap			
CEDRIC			
Student@work			

ANLAGE 2 − Anwendungen über das Internetportal des föderalen Dienstes

<table>
<tr><td rowspan="2">Anwendung</td><td>UID/PWD

+ zukünftige</td><td>Token mit UID/PWD

+ zukünftige</td><td>eID
ITSME
X.509 Zert.
TOTP (App)
+ zukünftige</td></tr>
<tr><td>Ausreichende Zuverlässigkeit JA/NEIN</td><td>Ausreichende Zuverlässigkeit JA/NEIN</td><td>Ausreichende Zuverlässigkeit JA/NEIN</td></tr>
<tr><td>2003 − Wahlen</td><td colspan="3" rowspan="5">Für diese Anwendungen ist kein digitaler Schlüssel erforderlich</td></tr>
<tr><td>2004 − Wahlen</td></tr>
<tr><td>2007 − Ergebnisse föderale Wahlen</td></tr>
<tr><td>Gemeinsamer Katalog</td></tr>
<tr><td>Bezahlung mit Dienstleistungsschecks</td></tr>
<tr><td>Pauschale Reduzierung der Energietarife (Energierabatt)</td><td>Ja</td><td>Ja</td><td>Ja</td></tr>
<tr><td>Police-on-Web</td><td rowspan="3">Nein</td><td rowspan="3">Ja</td><td rowspan="3">Ja</td></tr>
<tr><td>my.belgium.be</td></tr>
<tr><td>Tax-on-Web-Dienst</td></tr>
</table>

ANLAGE 3 − Anwendungen über das Internetportal eHealth

Anwendung	UID/PWD + zukünftige	Token mit UID/PWD + zukünftige	eID ITSME X.509 Zert. TOTP (App) + zukünftige
	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN	Ausreichende Zuverlässigkeit JA/NEIN
eTCT – Feedback an die Krankenhäuser über die von ihnen erbrachte Pflegeleistung und deren Kosten	Für diese Anwendungen ist kein digitaler Schlüssel erforderlich		
Authentische Quelle Implantierbare Medizinische Hilfsmittel			
Healthdata.be Data Reporting			
CEBAM Digital library for Health	Ja	Ja	Ja
Plattform ‚Welzijn & Gezondheid'			
E-Schalter ‚Zorg & Gezondheid'	Nein	Ja	Ja
Akkreditierung	Nein	Nein	Ja
Meine Gesundheit			
Web Application Metahub			
eHealthConsent			
Moduldatenbank Jugendhilfe Flandern			
Zentrales Rückverfolgungsregister			
Einzigartiges Portal			