

FAQ van het BIPT bestemd voor de consumenten in verband met de verplichte identificatie van de gebruikers van prepaid kaarten

Inhoudsopgave

1.	Waarop slaat de nieuwe reglementering?	3
1.1.	Wat verandert er?.....	3
1.2.	Geldt de nieuwe reglementering ook voor de prepaid kaarten van buitenlandse operatoren die in België worden verkocht?.....	3
1.3.	Geldt de nieuwe reglementering ook voor M2M-simkaart?.....	3
1.3.1.	Wat is een M2M-simkaart?	3
1.3.2.	Moeten de afnemers van M2M-simkaarten geïdentificeerd worden?.....	3
1.3.3.	Ik gebruik een gewone voorafbetaalde simkaart, dus geen M2M-simkaart, voor een M2M-toepassing. Moet ik me voor deze simkaart identificeren?.....	3
1.3.4.	Ik heb een voorafbetaalde simkaart nodig voor een M2M-toepassing. Welk type simkaart gebruik ik best?	3
2.	In welke gevallen dient men zich te identificeren?.....	4
2.1.	Ik wens een prepaid kaart te kopen. Wat moet ik doen?	4
2.2.	Wat moet ik doen als mijn operator me opnieuw vraagt me te identificeren?.....	4
2.3.	Ik ben verhuisd of mijn identiteitskaart is veranderd. Moet ik me opnieuw identificeren?.....	4
3.	Wie moet zich identificeren?	4
3.1.	Hoe kan een rechtspersoon (vzw, vennootschap, enz.) prepaid kaarten kopen?	4
3.2.	Hoe kan ik een prepaid kaart aan een derde afstaan?	4
3.2.1.	Wat wordt bedoeld met "een kaart aan een derde afstaan"?	4
3.2.2.	Mag ik een prepaid kaart kopen voor een andere natuurlijke persoon, bijvoorbeeld voor mijn kind?.....	4
3.2.3.	Mag ik een geactiveerde prepaid kaart afstaan (bv. doorverkopen) aan andere personen?	5
3.2.4.	Mag ik een kaart kopen voor mijn personeel?.....	5
3.2.6.	Wat zijn de toepasselijke sancties?	5
3.2.7.	Wat zijn de oplossingen om een kaart voor een derde te kopen?.....	5
3.3.	Hoe kan een derde gebruik maken van uw prepaid kaart zonder dat u de kaart afstaat?	5
3.3.1.	Wat wordt daarmee bedoeld?.....	5
3.3.2.	Wat kan ik doen als rechtspersoon?.....	5
3.4.	Mag tethering nog steeds?	6
4.	Hoe moet men zich identificeren?	6
4.1.	Wanneer moet men zich identificeren?.....	6
4.2.	De identificatiemethode(s) bepalen die door uw operator worden voorgesteld.....	6
4.3.	Identificatie in een verkooppunt	6
4.3.1.	Zich al of niet identificeren in een verkooppunt	6

4.3.2	Welke identiteitsdocumenten moeten in het verkooppunt worden voorgelegd?.....	7
4.3.3.	Moet ik mijn pincode intikken?	7
4.4.	Online-identificatie en elektronische ondertekening via de elektronische identiteitskaart.....	7
4.5.	Aanbieder van een identificatiedienst	7
4.6.	Betaalverrichting online.....	7
4.7.	Productuitbreiding of -migratie	8
4.8.	Verificatie door de operator van de meegedeelde identificatiegegevens	8
5.	Risico voor fraude, diefstal of verlies	8
5.1.	Van welk soort van fraude kan ik slachtoffer zijn?.....	8
5.2.	Wat te doen om fraude te voorkomen?	9
5.3.	Ik ben mijn prepaid kaart verloren of die is gestolen. Wat moet ik doen?	9
6.	Waar kan ik terecht voor meer informatie?	9
6.1.	Aan wie kan ik me richten?.....	9
6.2.	Wat zijn de referenties van de toepasselijke wetgeving?	9

1. Waarop slaat de nieuwe reglementering?

1.1. Wat verandert er?

De nieuwe reglementering, vastgelegd in het [koninklijk besluit van 27 november 2016](#) betreffende de identificatie van voorafbetaalde kaarten, voert de verplichting in dat de gebruikers van prepaid kaarten geïdentificeerd moeten worden. Identificatie is o.a. mogelijk met uw elektronische identiteitskaart of een online betalingstransactie. Het gaat hier om een van de antiterreurmaatregelen die de regering heeft vastgesteld.

De nieuwe reglementering regelt dus de identificatie van eindgebruikers van prepaid kaarten maar niet het gebruik daarvan (in gsm, tablet, computer, alarm, gasketel, auto, grasmachine, liften, enzovoort).

1.2. Geldt de nieuwe reglementering ook voor de prepaid kaarten van buitenlandse operatoren die in België worden verkocht?

Ja.

1.3. Geldt de nieuwe reglementering ook voor M2M-simkaart?

1.3.1. Wat is een M2M-simkaart?

Dit is een simkaart die enkel gebruikt kan worden voor M2M ("machine-to-machine")-toepassingen. U kunt in de regel met dit type simkaart niet telefoneren, vooral omdat de simkaart verankert zit in het toestel. Denk bijvoorbeeld aan een M2M-simkaart in jouw auto of gasketel.

Voor M2M-toepassingen kan u echter ook gewone simkaarten gebruiken. In dat geval is er echter geen sprake van een M2M-simkaart, aangezien u de simkaart in dat geval zeker ook in een gewoon telefoontoestel kan gebruiken.

1.3.2. Moeten de afnemers van M2M-simkaarten geïdentificeerd worden?

Ja, maar niet volgens de methodes van het nieuwe koninklijk besluit. De operator is vrij om te bepalen hoe hij de afnemer van de M2M-simkaart identificeert (idem als voor abonnementen).

1.3.3. Ik gebruik een gewone voorafbetaalde simkaart, dus geen M2M-simkaart, voor een M2M-toepassing. Moet ik me voor deze simkaart identificeren?

Ja, conform een van de methodes van het nieuwe koninklijk besluit (zie 1.1).

1.3.4. Ik heb een voorafbetaalde simkaart nodig voor een M2M-toepassing. Welk type simkaart gebruik ik best?

U gebruikt in dit geval best een M2M-simkaart.

2. In welke gevallen dient men zich te identificeren?

2.1. Ik wens een prepaid kaart te kopen. Wat moet ik doen?

Uw operator zal uw prepaid kaart pas mogen activeren (d.w.z. bruikbaar maken) nadat hij uw identiteit heeft vastgesteld.

Hij zal de kaart niet mogen activeren als hij een anomalie of een fout in verband met uw identiteit vaststelt.

2.2. Wat moet ik doen als mijn operator me opnieuw vraagt me te identificeren?

De reglementering schrijft voor dat u zich moet identificeren telkens wanneer de operator u dat vraagt. Het is mogelijk dat uw operator u vraagt om zich opnieuw te identificeren, bijvoorbeeld omdat hij een anomalie met uw identificatie heeft vastgesteld.

2.3. Ik ben verhuisd of mijn identiteitskaart is veranderd. Moet ik me opnieuw identificeren?

Nee, dat is niet nodig.

3. Wie moet zich identificeren?

3.1. Hoe kan een rechtspersoon (vzw, vennootschap, enz.) prepaid kaarten kopen?

Wanneer één of meer prepaid kaarten worden aangekocht voor rekening van een rechtspersoon (vzw, vennootschap, enz.) is het de natuurlijke persoon (één van de vertegenwoordigers) die de activering van de kaart aanvraagt, die zich zal moeten identificeren. Doorgaans is dat de manager van de prepaid kaarten ("fleet manager") van de rechtspersoon. Daarnaast mag de operator ook (maar moet niet) de rechtspersoon identificeren.

3.2. Hoe kan ik een prepaid kaart aan een derde afstaan?

3.2.1. Wat wordt bedoeld met "een kaart aan een derde afstaan"?

U staat een prepaid kaart aan een derde af als de eigendom over de kaart aan een derde wordt overgedragen, bijvoorbeeld door een kaart voor rekening van een derde te kopen, een kaart als cadeau aan een derde te geven of een kaart aan een derde door te verkopen.

De nieuwe reglementering beperkt de mogelijkheid om een prepaid kaart aan een derde af te staan.

3.2.2. Mag ik een prepaid kaart kopen voor een andere natuurlijke persoon, bijvoorbeeld voor mijn kind?

Ja, u kunt een geactiveerde kaart kopen voor iemand van uw familie (uw ouders, grootouders, kinderen, kleinkinderen, broers of zussen), voor uw echtgeno(o)t(e), voor iemand met wie u wettelijk samenwoont of voor iemand van wie u de voogd bent.

Het draagt echter steeds de voorkeur weg dat de persoon die de prepaid kaart daadwerkelijk gebruikt, zichzelf ook identificeert. De reglementering bepaalt immers dat de geïdentificeerde persoon wordt geacht de kaart zelf te gebruiken. Dit zal de persoon die de kaart daadwerkelijk gebruikt ook een betere

hulp bieden bij oproepen naar de nooddiensten (bij oproepen naar de medische spoeddienst, de brandweerdiensten, de politiediensten of de civiele bescherming wordt de naam en voornaam van de beller aan deze diensten meegedeeld).

3.2.3. Mag ik een geactiveerde prepaid kaart afstaan (bv. doorverkopen) aan andere personen?

Nee, tenzij die andere persoon zich vooraf heeft geïdentificeerd bij de operator.

3.2.4. Mag ik een kaart kopen voor mijn personeel?

Ja, als rechtspersoon mag u geactiveerde prepaid kaarten geven aan natuurlijke personen die prestaties verrichten voor u (werknemers, consultants, onderaannemers).

De rechtspersoon zal evenwel een bijgewerkte lijst moeten bewaren waarmee de link kan worden gelegd tussen de aangekochte prepaid kaarten en de natuurlijke personen die een kaart hebben ontvangen. Deze lijst moet constant worden bijgewerkt, wat betekent dat deze moet worden aangepast wanneer een prepaid kaart die aan een persoon is toegewezen, nadien aan iemand anders wordt toegewezen. Die lijst moet ten minste de naam, voornaam en geboortedatum bevatten van de persoon aan wie de kaart is toegewezen. Deze lijst moet aan de operator worden bezorgd op het moment van de activering van de prepaid kaart en op diens eenvoudig verzoek.

3.2.5. Mag ik een geactiveerde prepaid kaart geven aan mijn klanten?

Nee, tenzij uw klant zich vooraf heeft geïdentificeerd bij de operator.

3.2.6. Wat zijn de toepasselijke sancties?

Bij niet-naleving van de reglementering kunt u worden beboet. Verder zult u worden geacht de prepaid kaart zelf te gebruiken en zal de politie zich tot u richten in geval van een onderzoek.

3.2.7. Wat zijn de oplossingen om een kaart voor een derde te kopen?

Om de regelgeving na te leven zijn de volgende oplossingen beschikbaar:

- Vraag aan de derde aan wie u de kaart zou willen afstaan om zelf de prepaid kaart te kopen;
- Geef aan de derde een kaart die niet geactiveerd is. Die derde zal zich echter moeten identificeren voordat die er gebruik van kan maken;
- Zie sectie 3.3.

3.3. Hoe kan een derde gebruik maken van uw prepaid kaart zonder dat u de kaart afstaat?

3.3.1. Wat wordt daarmee bedoeld?

U blijft eigenaar van de prepaid kaart maar u staat een derde toe om tijdelijk gebruik te maken van uw voorafbetaalde kaart.

Zo'n praktijk is niet zonder risico vanwege de wettelijke vermoedens dat de geïdentificeerde persoon, in dit geval u, de kaart zelf gebruikt. In geval van misbruik van één van uw simkaarten, zal de politie zich dus tot u richten.

3.3.2. Wat kan ik doen als rechtspersoon?

Een rechtspersoon zou prepaid kaarten willen kopen voor haar klanten. Denk bijvoorbeeld aan een leverancier van M2M ("machine-to-machine") applicatie die prepaid kaarten koopt voor zijn klanten (prepaid kaarten in een auto, gasketel, koelkast, enzovoort).

Als u wil dat uw klant uw simkaart kan gebruiken (zonder de kaart af te staan), dient iemand van uw rechtspersoon zich te identificeren bij de operator. Analoog met de voorafbetaalde kaarten die een rechtspersoon aan haar werknemers uitdeelt, wordt van u verwacht dat u een actuele lijst bijhoudt van welke simkaart zich in welk toestel bij welke klant of gebruiker bevindt. De finale verantwoordelijkheid voor het gebruik van de kaarten blijft immers bij u. In geval van misbruik van één van uw kaarten, zal de politie zich dus tot u richten.

3.4. Mag tethering nog steeds?

De reglementering is niet tegen de praktijk van tethering (i.e. het delen van de internetverbinding van het mobiele eindtoestel met andere apparatuur) aan de hand van een prepaid kaart die toegang biedt tot het internet¹.

Let echter wel op dat de politie zich in geval van een overtreding eerst zal richten tot de geïdentificeerde persoon, m.a.w. tot u.

4. Hoe moet men zich identificeren?

4.1. Wanneer moet men zich identificeren?

U kunt zich identificeren op het ogenblik van de aankoop van de prepaid kaart (bijvoorbeeld in een verkooppunt) of later (bijvoorbeeld indien u de prepaid kaart koopt in een verkooppunt dat niet in staat is om u te identificeren). U identificeert zich dan later via de website van de operator.

4.2. De identificatiemethode(s) bepalen die door uw operator worden voorgesteld.

Elke operator die prepaid kaarten verkoopt moet zijn klanten minstens een van de methodes aanbieden die door de reglementering worden beoogd en hieronder worden voorgesteld.

Uw operator zal u inlichten over de identificatiemethode(s) die hij aanbiedt.

4.3. Identificatie in een verkooppunt

4.3.1. Zich al of niet identificeren in een verkooppunt

Na identificatie in het verkooppunt (al dan niet van de operator) waar u de prepaid kaart koopt, zult u kunnen vertrekken met een kaart die geactiveerd is of die snel geactiveerd zal worden (afhankelijk van de tijd die de operator nodig heeft om de betrouwbaarheid te bevestigen van de gegevens die u aan het verkooppunt hebt bezorgd).

U kunt altijd verkiezen om u niet te identificeren in een verkooppunt. Maar in dat geval zal de prepaid kaart u niet verkocht worden of zal ze niet geactiveerd zijn en zult u zelf voor de identificatie moeten zorgen via een identificatiemethode op afstand (bijvoorbeeld online) om de kaart te activeren.

¹ De "tethering"-technologie maakt het mogelijk om een internetverbinding te delen vanaf een mobiel eindtoestel (doorgaans een gsm) met een ander toestel zoals een laptop of een tablet. De interconnectie van het mobiele eindtoestel met de andere apparatuur kan tot stand worden gebracht door een draadverbinding zoals een USB-kabel of via een draadloze verbinding zoals Bluetooth of wifi, waardoor het eindtoestel kan worden gelijkgesteld aan een wifihotspot.

4.3.2 Welke identiteitsdocumenten moeten in het verkooppunt worden voorgelegd?

U identificeert zich in het verkooppunt door een geldig identificatiedocument voor te leggen. Onder andere volgende documenten worden beschouwd als geldige identificatiedocumenten:

- [Belgische elektronische identiteitskaart](#)
- Identiteitskaart van een andere lidstaat van de Europese Unie
- [Internationaal paspoort](#)
- [Elektronische vreemdelingenkaart](#)
- Een officieel document dat, tijdelijk, een van de hierboven vermelde documenten dat verloren of gestolen is, vervangt

U moet altijd het origineel van het identiteitsdocument voorleggen (geen kopie) en dat document moet leesbaar en rechtsgeldig zijn. Indien dit niet het geval is, moet de operator het document weigeren.

U moet weten dat de reglementering bepaalt dat het verkooppunt een kopie mag maken van uw identificatiedocumenten, maar dat het geen identificatiegegevens of -documenten mag bewaren, die dus worden doorgestuurd naar het centrale computersysteem van de operator.

4.3.3. Moet ik mijn pincode intikken?

Bij elektronische aflezing van de Belgische identiteitskaart kan het verkooppunt u vragen om de pincode van die identiteitskaart in te tikken. Als u dat wordt gevraagd maar u dat niet wilt doen, kan het verkooppunt weigeren om u de prepaid kaart te verkopen of enkel een niet-geactiveerde prepaid kaart te verkopen.

4.4. Online-identificatie en elektronische ondertekening via de elektronische identiteitskaart

U kunt zich identificeren door de verbinding te maken met een internetapplicatie van de operator of door een document van de operator elektronisch te ondertekenen. Deze methode vergt het gebruik van de elektronische identiteitskaart en de invoering van een pincode.

4.5. Aanbieder van een identificatiedienst

Uw operator kan u ook identificeren op basis van een account die reeds bestond of die aangemaakt moet worden bij een aanbieder van een identificatiedienst waarvoor uw identiteit al nagegaan is. Met andere woorden: u identificeert zich bij een aanbieder van een identificatiedienst, doorgaans online, en deze aanbieder zal uw operator uw identificatiegegevens bezorgen. Alvorens zijn identificatiediensten te kunnen aanbieden, moet de aanbieder van identificatiediensten een gelijkaardige toepassing hebben ontwikkeld die de toegang tot een digitale toepassing van de overheidsdiensten mogelijk maakt en deze gelijkaardige toepassing moet zijn goedgekeurd door de Federale Overheidsdienst voor Informatie- en Communicatietechnologie.

4.6. Betaalverrichting online

U kunt zich identificeren door online een prepaid kaart te kopen of te herladen en door met een debet- of kredietkaart te betalen, op voorwaarde dat de aanbieder van betaaldiensten is onderworpen aan de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme. In dat geval eist de reglementering dat er een nieuwe identificatie plaatsvindt binnen 18 maanden na de betaalverrichting in verband met de prepaid kaart.

4.7. Productuitbreiding of -migratie

Indien u reeds bij de operator ingetekend hebt op een product waarvoor u al geïdentificeerd bent (u heeft bijvoorbeeld een abonnement) en u bovendien een prepaid kaart wenst te kopen of wenst over te schakelen van een postpaid formule naar een prepaid formule, zou uw operator in principe in staat moeten zijn om voor de prepaid kaart uw identificatiegegevens die werden vergaard in het kader van de postpaid formule te recupereren.

Uw operator moet zich er echter op de ene of de andere manier van vergewissen dat de persoon die werd geïdentificeerd in het kader van de postpaid formule wel degelijk dezelfde persoon is die de activering van de prepaid kaart vraagt (bijvoorbeeld door u te vragen een identiteitsstuk voor te leggen).

De methode voor verlenging of migratie van een product werkt niet indien de operator in het kader van een postpaid formule enkel een rechtspersoon heeft geïdentificeerd (uw VZW, uw maatschappij, enz.) en deze rechtspersoon prepaid kaarten wenst te kopen. In dat geval zal de operator de natuurlijke persoon moeten identificeren die binnen de rechtspersoon de activering van de prepaid kaarten zal vragen.

4.8. Verificatie door de operator van de meegedeelde identificatiegegevens

Bij bepaalde operatoren kunt u zich identificeren door uw identificatiegegevens mee te delen (ten minste uw naam, voornaam, geboortedatum en -plaats, alsook uw woonplaats) via de communicatiekanalen die deze heeft ingesteld (bijvoorbeeld via een onlineformulier). Na verificatie van die gegevens zal de operator u uw simkaart toesturen en activeren.

5. Risico voor fraude, diefstal of verlies

5.1. Van welk soort van fraude kan ik slachtoffer zijn?

Er moet bijzonder worden opgelet voor een derde die zou kunnen proberen zich voor te doen als uw operator, uw identificatiegegevens en -documenten te vragen en u nadeel te berokkenen (deze gegevens en documenten misbruiken, oproep met toeslag, enz.).

Dit zijn enkele voorbeelden van vragen die onwettig (kunnen) zijn:

- men vraagt u een code mee te delen (bijvoorbeeld de pincode van uw identiteitskaart) of een wachtwoord;
- u wordt telefonisch gecontacteerd en de beller vraagt u om hem uw persoonsgegevens mee te delen;
- u wordt gecontacteerd via de telefoon of per sms, en het nummer is verborgen of buitenlands;
- u wordt gecontacteerd (via de telefoon, per sms, op uw voicemail, via e-mail, enz.) en u wordt uitgenodigd om terug te bellen of een sms te versturen naar een buitenlands betaalnummer of nummer met toeslag;
- er wordt u gevraagd zich te identificeren volgens een identificatiemethode die niet gemeld is door uw operator;
- u wordt uitgenodigd om verbinding te maken met een onbeveiligde website ("http://" in plaats van "https://") of waarvan de domeinnaam niet onder een officiële site van uw operator valt.

5.2. Wat te doen om fraude te voorkomen?

Blijf waakzaam en verzendt nooit uw persoonsgegevens als u niet zeker bent dat uw gesprekspartner wel degelijk uw operator is of een persoon die voor diens rekening optreedt, zoals een verkooppunt. In geval van twijfel neemt u direct contact op met uw operator via een van de informatiekkanalen waarover u beschikt: zijn website, zijn telefonische permanentie of zijn officiële verkooppunten.

Wees voorzichtig wanneer u uw pincode en wachtwoord worden gevraagd. Vergewis u ervan dat de persoon/de tool die deze gegevens vraagt daadwerkelijk verbonden is aan de operator en dat deze vraag enkel wordt gesteld voor de identificatie van de klant.

5.3. Ik ben mijn prepaid kaart verloren of die is gestolen. Wat moet ik doen?

U moet uw operator zo snel mogelijk inlichten (binnen de 24 uur) van de diefstal of het verlies van deze prepaid kaart. De operator zal uw kaart dan onbruikbaar maken.

6. Waar kan ik terecht voor meer informatie?

6.1. Aan wie kan ik me richten?

Gelieve u voor alle bijkomende vragen te richten tot de operator die de elektronisch-communicatiedienst via prepaid kaart aanbiedt.

6.2. Wat zijn de referenties van de toepasselijke wetgeving?

De nieuwe reglementering bestaat uit twee regelgevende teksten, namelijk:

- de wet van 1/09/2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst; en
- het koninklijk besluit van 27/11/2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart.